Dr. Sreenivasappa Bhupasandra,

Ashendra Kumar Saxena

NETWORKS AND CYBER SECURITY

ALEXIS PRESS

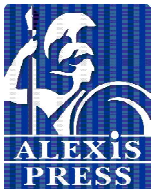
JERSEY CITY, USA

NETWORKS AND CYBER SECURITY

NETWORKS AND CYBER SECURITY

Dr. Sreenivasappa Bhupasandra

Ashendra Kumar Saxena



ALEXIS PRESS

Published by: Alexis Press, LLC, Jersey City, USA
www.alexispress.us

First Published 2022

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication Data

Includes bibliographical references and index.

Networks and Cyber Security by *Dr. Sreenivasappa Bhupasandra, Ashendra Kumar Saxena*

ISBN 978-1-64532-442-3

CONTENTS

CHAPTER 1

ANALYSIS OF DDOS ATTACK AND COUNTERMEASURES

Dr. Sreenivasappa Bhupasandra, Associate Professor,
Department of Electronics & Communication (Communication System Engineering),
Presidency University, Bangalore, India.
Email Id: - sreenivasappabv@presidencyuniversity.in

ABSTRACT:

This study provides a brief overview of DDoS attack methods and countermeasures in an SDN context. We begin by providing an overview of SDN and its benefits over conventional networks. Together with DDoS attacks, several SDN vulnerabilities are also being addressed. Next, we discuss various advantages SDN has over this significant DDoS assault. Furthermore, covered are several categories of DDoS assaults that have an impact on the SDN environment. Finally, we outline future research topics that will be essential shortly to counteract such assaults.Lastly, we look at several detailed, recently tried techniques that reduce the impact of DDoS assaults on many systems. We examine numerous methods and the shortcomings that render them ineffective against DDoS assaults. As data reveal that DDoS attacks have been occurring more often recently, we have concentrated on DDoS security issues in this article.

KEYWORDS:

DDoS Attack,Controller,CyberAttacks, SDN.

INTRODUCTION

The development of the digital society, where practically every gadget is connected and accessible from anywhere, has been facilitated by the Internet of today. Although being widely used, existing networks including data centres, workplace networks, and cloud networks are becoming bigger and more complicated. The difficult demands of today's companies, which call for increased computing resources, planning, availability, and scalability, are being met by advanced computing standards. The processing capabilities of such sophisticated systems cannot be met by current network technology. The open source communities suggested the "software-defined network (SDN)" as a new networking design philosophy in order to create networks that can satisfy these expanding expectations. SDN is a paradigm for networking that makes networks programmable[1], [2].The fundamental result of considerable research efforts made in the last several decades to transform the Internet into a more open and programmable architecture is SDN.

Modern network components have hardware capacity limitations[3]. This limits the domain's potential to scale. SDN, on the other hand, operates solely on server hardware, therefore it is the opposite idea. Device reconfiguration in response to traffic load cannot be done automatically. To deploy an application, we must manually change each networking device. But SDN puts programmes in the controller, which will evenly divide the resources to let this programme run. SDN increases flexibility, streamlines administration, and accelerates installation. Moreover, it offers the following qualities:

1. Multi-tenancy: Resource management and considerably more precise gain control
2. Service quality (QoS) enabling apps to dynamically adjust quality of service (QoS) requirements for things like voice-over-IP (VOIP) or video conferencing applications to prioritise user needs
3. Security: Resource allocation and access control based on user identification

In this chapter, we examine the security issues of SDN from a comprehensive perspective. We first go into great depth on the state-of-the-art programmable network (SDN), then we go through its architecture, and then we show the security issues that must be resolved in order to fix the design's flaws. Our main research hypothesis is unique in that we first look at the many SDN properties that may be used to counter DDoS assaults on traditional networks. Finally, we go through several SDN planes and modules that might be impacted by DDoS assaults. Outline of software-defined networking: Physically dispersed yet functionally centralised, a software-defined network is one that is centrally managed by controller software. Conventional networks' expanding sizes have made them more confusing and complex. In light of this, these networks are unable to handle and meet networking needs including dynamic scaling, centralised administration, networking cost, on-the-fly adjustments, managing network traffic, and server virtualization traffic in data centres. These conventional switches and routers also have three levels that are interconnected and reliant on one another. Each layer's ability to evolve and innovate is hampered by this linkage. Because to this interdependence, networking changes including device configuration, traffic and bandwidth restrictions, and network statistics monitoring must be made manually and separately on each device. As a result, changing a lot of networking equipment becomes a laborious operation.

The whole functionality for managing the network traffic is shifted to the controller, which is located in the control plane, and the data plane networking equipment, such as switches, become mere packet forwarding devices. As a result, the complexity of the network is abstracted by the controller, making switches less costly since they no longer need to do route calculation and can instead concentrate just on traffic forwarding. The controller can interact with the switches linked to it since it is aware of how the network is built.A controller may direct switches to deliver packets by using the southbound interface of the OpenFlow protocol. Each switch in a traditional network contains unique software to carry out a specific function. The centralised controller may operate specialised networking switches thanks to this protocol. The two entities can interact using this particular protocol, but communications within the data plane are sent using other protocols (i.e. TCP, IP).

Switch flow tables, sometimes called forwarding tables, are used by the controller to directly write orders to manage OpenFlow-capable switches. In order to determine the appropriate forwarding operations, networking devices also make use of data contained in protocol headers (TCP ports and IP address). Moreover, OpenFlow switches are also compatible with current networking protocols. The OpenFlow protocol was first created for university networks. Vendors eventually developed a genuine interest in it and began making investments. Together with the protocol, they started to notice its usage in data centres; as a result of the protocol vendors' growing popularity, networking devices with hardware support for this protocol started to be produced. This results in the development of Open vSwitch, often known as OVS. The Apache 2.0 licence governs Open vSwitch.Several common switch functionalities are supported by the switch, including VLAN tagging, the 802.1D spanning tree protocol, port mirroring, flow export using sflow and netflow, tunnelling using GRE, VXLAN, and IPSEC, and QoS management.

DISCUSSION

Background of SDN: In 2009, the phrase "software-defined networking" was first used. The development of SDN took place in three stages: active networking, control plane and data plane separation, and OpenFlow API. Active networking aimed to force network switches to conduct unique calculations on packets. The expenses of computation are decreased through active networks. A network-wide perspective was made simpler and more flexible with the separation of the control and data planes since the control logic is not dependent on hardware. The ForCES protocol, developed by the Internet Engineering Task Force (IETF) working group, was the first example of plane separation. In essence, the standard established a number of control components to regulate forwarding elements. Switches were intended to be controlled by a protocol interface, to put it another way. Both strategies, however, need new gear to be deployed and standards to be established [4]–[6].

It could be simpler to handle a larger variety of applications if the hardware is customised. The first initiative to clearly define a new architecture for commercial networks was Ethane. The primary goal of the Ethane project was to use a centralised controller to handle network security and policy. Based on the access control rules set out on the domain controller, the controller will determine the flow tables that must be deployed in switches. Custom switches that handle the Ethane protocol are needed, however. The "software-defined networking" network of today was established because to ethane. Operating on current protocols without changing existing hardware is a key idea of SDN. Basically, the plan was to make use of the gear that was already in place and control it via a common protocol. The OpenFlow protocol, which installs forwarding instructions (entries) to regulate the network's forwarding behaviour, connects with the switch's flow tables. Because switches already had flow tables, all that was needed to allow a different software controller to interact with them was to push the switch suppliers to expose the interface. A branch of the United Nations that oversees telecommunications, spearheaded the standardisation of SDN in its study group (SG) 13.

The primary research group responsible for creating the SDN framework is SG 13. A different research group 11 began creating SDN signals and protocols. With SG 13 and SG 11, ITU's ITU-D (Development) and ITU-R (Radio Communication) are cooperating. The ITU-T study group is assigned a subject by the World Telecommunication Standardization Assembly (WTS-A), which then develops recommendations for certain themes. Study Group 5 for energy efficiency and energy savings, Study Group 15 for a generic information model, Study Group 16 for the delivery of virtual content, and Study Group 17 for security services of SDN are other study groups of the ITU-T and their connected areas. The Alliance for Telecommunication Industry Solutions (ATIS), the China Communication Standard Association (CCSA), the Broadband Forum (BBF), the Internet Research Task Force (IRTF), the Internet Engineering Task Force (IETF), the Open Networking Foundation (ONF), the Third Generation Partnership Project (3GPP), the European Telecommunication Standards Institute (ETIS), Open Cloud Connect, the Telecommunication Technology Association (TTA), and IEEE P19 are additional SDOs working to standardise SDN. OpenStack, OpenDaylight, Open Network Operating System (ONOS), ONF Atrium, and Open Platform for Network Function Virtualization are a few examples of open source software projects (OPNFV).

Bottom-Up SDN Architecture Model

An SDN reference model has been suggested by ONF. This paradigm divides the control plane, data plane, and application plane in contrast to conventional networks. The "power of abstraction" is made possible by SDN by isolating the control plane from the data plane. The

whole functionality for managing the network traffic is placed into the control plane, turning data plane devices like switches into mere packet forwarders. Therefore, a network's control plane, or brain, regulates the behaviour of the network. As they just manage traffic forwarding and do not perform route calculation, switches become less costly. The controller can interact with the corresponding networking components that are attached to the network since it is aware of its structure. As a result, the controller obscures the network's complexity. The OpenFlow protocol is used to facilitate communication between the controller, which is a part of the control plane, and the data plane switches. A common application programming interface (API) is OpenFlow.

Data Plane

Forwarding devices including routers, switches, wireless access points, and virtual switches are included in the data plane. All of these components are known as switches or OpenFlow switches in SDN jargon. The packet forwarding rule is represented by a flow table in switches. The traffic is sent via switches to the specified destination in accordance with the logic of the control plane. The switches and other data plane devices will degrade to becoming basic packet forwarding devices that just handle traffic.

Southbound Interface

Southbound protocols provide effective data plane control. The most popular and widely used southbound protocol is OpenFlow. There are several companies who manufacture their own OpenFlow-compatible switches, including HP, NetGear, and IBM. The standardisation of OpenFlow is the responsibility of the open networking foundation. A flow table is used by the OpenFlow protocol to quickly manage network traffic. There are a number of additional protocols besides OpenFlow, like ForCES and OpFlex, but as more groups attempt to standardise OpenFlow, it has taken over as the accepted protocol.

Control Plane

The controller, who stands in for the network's central nervous system, is a part of the control plane. The controller decides how to route packets and programmes those judgements into the switches. SDN stands for spatial distributed network.Nonetheless, the centrally logical controller. The tasks of network administrators to setup and maintain the network are made easier by logical centralization. The controller offers security measures, device administration, and alerts. As a result, the controller may connect with the appropriate networking components. It is challenging to operate a large network with a single controller because a physically centralised controller might result in a single point of failure. In contrast, a distributed controller can handle any demand for a network, no matter how big or tiny.

Eastbound and Westbound

Physically dispersed controllers interact through the east-westbound interface. A second east-westbound interconnection is used by two complementary entities (e.g. SDN controller is communicating with VPN network). While a single controller can only manage a limited network, if one fails, the other controller may be notified to take over the traffic management. The authors of Onix and Hyperflow have recommended these tactics.Northbound interface serves as a middleman between the control plane and the application plane.

The purpose of the northbound interface is to conceal the network's underlying workings so that it may be programmed and queried for services. As SDN can be built for diverse applications using a single API to satisfy these requirements, it aids network operators in controlling the network appropriately. Thus, it is possible for several protocols to exist. To govern the network, current controllers provide their own APIs, such as rest API and ad hoc API.

Application Plane

In an SDN architecture, the application or administration plane is the uppermost plane. Applications created by software engineers to administer the network are referred to as application plane. Fault tracking and configuration management are features of the application plane.

Complex network operations including routing route calculation, network behaviour monitoring, and network access control are generated by an SDN controller in the control plane. In the application plane, high-level methods are established for how the bottom layer (the data plane) will handle packets. Users of the SDN may easily create and distribute new flow handling and network control algorithms. The control plane becomes significantly more adaptable and intelligent as a result. Much like developing an application comparable to writing an app for Android OS or iOS, we may impose protocols and additional control functionalities. An industry standard for coordinating communication between the control plane and data plane is the OpenFlow protocol. The switch must establish a TCP connection with the controller before the message flow between the controller and switches can begin [7], [8].

When a packet is received, the switch processes it as shown in Figure 15.4. An OpenFlow-enabled switch analyses the flow table for the highest priority match when a new packet enters the switch. The switch sends the packet to the specified destination if it discovers a matching flow rule entry. Otherwise, SDN's advantages over conventional networks: The separation of the control plane from the data plane is the fundamental concept of SDN design. SDN improves network programmability by separating the control plane from the data plane. This feature makes it easier to configure SDN devices and improves traffic management. Also, this feature offers the benefit of innovation in network architecture and management.

Problems with Security in Software-Defined Networks

SDN Security Problem:

In recent years, SDN security has grown to become the most well-known subject. SDN has two significant security difficulties. One is leveraging SDN technology to address traditional network security concerns. Another is protecting SDN and reinforcing infrastructure that is SDN-enabled. In light of the latter, SDN itself is vulnerable to seven significant attack vectors.Below is a list of the threat vectors:

1. A fake or faked traffic flow; B attacks on OpenFlow switches; C attacks on controllers; D attacks on the control plane; E attacks on the control plane; F attacks on administrative stations; G attacks on the lack of dependable sources for network recovery

2. The most devastating assault on the whole network among the well-known vulnerabilities is the distributed denial of service (DDoS) attack on controllers.

SDN Vulnerabilities

SDN gives networking power and flexibility. Moreover, it offers centralized control and lowers the cost of implementation. Other than DDoS assaults, this centralized control is now open to additional threats. The illustration of these vulnerabilities on several planes is shown in Figure 15.5. These assault scenarios' specifics are provided below:

Network manipulation: The basic idea behind SDN is the centralization of the controller. The attacker may programme the network and control the resources after the controller has been taken over.

Data leakage: Among the instructions that may be used to handle the packets are drop, forward, and forward to controller. By examining how packets are handled by the switch, the attacker may find out how long it takes to process each packet. The attacker may create identical sorts of packets that would be diverted to the controller in order to cause a denial of service if they learn about the packets that are being delivered to the controller. The authors of described how data leaking may be used to execute a DDoS assault. Another difficulty with SDN is securing the storing of credentials for various logical networks. Data leakage may occur if logical network credentials are not segregated from one another.

DDoS attack: By separating aircraft and using various protocols to connect with them, congestion is made vulnerable. Because to these limitations, the southbound interface, northbound interface, switch hardware, and controller may all be the target of a denial of service attack.

Compromised application: SDN enables network management by external applications. The networking resources may be manipulated and depleted by writing malicious programmes. Also, developers who write confusing code expose software applications to flaws that an attacker may use to carry out an attack.

Man-in-the-middle attack: The attacker changes the communication between the communicating entities, leading them to assume they are speaking to one another. If there is no security between the communicating protocols, this attack occurs. The usage of TLS for secure communication between the controller and data plane switches is represented by the OpenFlow switch description. Man-in-the-middle attacks result from OpenFlow manufacturers' failure to embrace TLS. The author of researched this attack and provided a workable solution. The authors of have covered a variety of security options for this vicious assault.

Data modification: As already explained, the controller configures the networking hardware. The whole system might be explicitly controlled by the attacker if the controller is compromised. At this location, the attacker may alter or introduce fictitious flow rules into the switch, allowing packets to be misdirected to various locations.

SDN internal storage modification: The management plane apps may access the underlying system with certain permissions. In other words, the controller makes some of its resources available to applications from outside the system. Hence, the programmes have access to and control over the internal database, which may then be utilised for offensive purposes.

Establishing trust: Since SDN applications and controllers have centralised system architectures, they must force the trust mechanism. While there are trust mechanisms for network devices, there are none for apps.

Authorization, authentication, and accountability: Authorization-related attacks may result in unauthorised assaults on the controller. Due to the variety of applications, authentication is a significant problem in SDN. For the permission and authentication of apps, there is no convincing method. Considering the use of network resources, accountability of the third party is another major problem.

Resource exhaustion: When malicious apps use up all of the system resources, the performance of other applications is severely hampered. As a result, malicious apps have the potential to use CPU and memory while simultaneously carrying out system commands to fire the controller.

Northbound API architecture: SDN apps may use this API's horrendous design to manipulate the actions of other applications. By manipulating the northbound API, for instance, an application may evict a running application session.

Northbound API standardisation: The SDN architecture lacks a northbound API standard. Hence, owing to the possibility of assault by knowledgeable opponents, working in an open independent development environment is difficult and dangerous.

Attack using packet in controller manipulation: When arriving packets do not match flow table entries in the flow table, the switch sends a packet in message to the controller. Even though the OpenFlow protocol is TLS enabled, the control plane of SDN architecture currently lacks an intrinsic security method that may prevent the manipulation of Packet In messages. Authorized switches have the ability to send forged Packet In signals to corrupt the controller status.

Manipulating the system variable: To revoke the controller's status, the attacker must alter the system variable's value. For instance, changing the system time might disconnect the controller from its connected switches.

The controller audits and authenticates apps: The controller is controlled by third-party applications. As a result, the security of the control plane is assessed using a scale based on controller capabilities. For instance, adequate audits and authentication of the apps aid in tracking the amount of resources they use.

Scalability of the controller: The controller is the key component of the SDN architecture. It is in charge of all network-wide decision-making. The bandwidth is unable to scale, which leads to major problems including saturation assaults, latency limitations, and single points of failure.

TCP-level attack: In the most recent version of the OpenFlow protocol, the definition of transport-level security is optional. As a result, TCP-level assaults may target the southbound interface.

Switch flow entry restriction: TCAM makes up the SDN switch flow table (ternary content addressable memory). Since that TCAM is expensive, the flow table's size is maintained to a minimum. The switch is left in an unexpected state as a result of the saturation assault that targets this restricted capability.

Compromised SDN switch: The attacker may take advantage of a compromised SDN switch to overflow the targeted switch with fictitious flow entries, which will then transfer the packet to an erroneous location. The attacker then examines the packets that the switch is forwarding.

Real flow recognition: The controller responds to the switch's Packet In message by taking action. The controller may make choices that deliver the packets to fictitious destinations if the attacker compromises the Packet In message.

Eavesdropping: Both passive and active eavesdropping methods may target the interface between the control plane and data plane. Snooping the control messages that are presently flowing will allow the attacker to get knowledge about the network topologies.

DDoS Attacks on Traditional Networks: DoS attacks include a rogue person sending a server a large number of fictitious requests. The server waits before cutting the connection because it cannot locate the attacker's return address. As a result, the server continuously cutting off the connections from bogus requests. This results in a denial of service attack that affects genuine users. Popular websites and servers are the main targets of DoS attacks, which make them inaccessible to obedient users. DoS attacks may sometimes target users as well. The victim's time, money, and resources are wasted as a result of these assaults. This assault is referred to be a distributed denial of service (DDoS) attack when it originates from several hosts (collectively referred to as BOTS) that are controlled by an evil user. The writers of [20, 33] have covered the defences against these assaults. Figure 15.6 demonstrates how the attacker amplifies their DDoS assault using bots. DDoS attacks provide the attacker several benefits, including:

Since the attacking computers are randomly scattered, it is impossible to pinpoint the attacker's location. The attacker may also use many systems to silently assault the victim.

The next paragraphs address several DDoS attack methods that might impact the victim or server [20, 33]:

Email bombing: In this assault, the attacker floods the victim's inbox with many spam emails.

Ping of Death: When an attacker delivers a bigger packet than the target's machine can process, the victim dies. To determine if a distant computer is communicating or not, use the ping command. The server's communication bandwidth is reduced as a result.

Smurf Attack: In this attack, ICMP packets that have been spoofing are used to change the victim's IP address. To communicate the network status information, ICMP packets are transmitted. The network bandwidth is used by the many responses that are sent back to the victim's PC.

Buffer Overflow Attack: In this kind of attack, the buffer, which contains a temporary storage region, receives a significant quantity of data. Such big data corrupts the data that is currently being shown in that buffer since it exceeds the buffer's capacity and goes into another buffer.

Syn Flood: The most common DDoS assault. The connection between the client and server is established when the client transmits TCP Syn packets to the server. The server replies to a Syn packet after receiving it and waits for client-side acknowledgment, but none is ever received. This keeps the server waiting when busy.

UDP Flood: This attack resembles a Syn flood attack quite closely. In this attack, the client bombards the server with many UDP packets. Syn flood uses up bandwidth far more slowly than UDP flood. Since the attacker is using a botnet, which is a collection of several computers, it is difficult to reply to each one individually.

HTTP GET Flood: In this kind of attack, the attacker floods the server with HTTP GET request messages. The attacker never responds, so the server responds to these requests and waits for an acknowledgment.

NTP Reflection Amplification Attack: In this kind of network time protocol (NTP) assault, the attacker overwhelms the victim with traffic from an actual NTP server. The attacker asks many NTP servers for the network time using faked IP. These servers address the victim directly in their answer. The victim can experience response overload because of the higher packet size coming from the servers.

DNS Reflection Amplification Attack: The attacker spoofs the client's IP address and contacts the servers through the domain name system (DNS). DNS is a system for resolving IP addresses that returns a specific IP address to the client after matching an IP address with a domain name. The attacker manipulates the DNS such that the requesting client receives the most DNS responses possible.

Zero-Day Attack: The attacker takes advantage of a software flaw that the creators were unaware of. Users of software are therefore at danger while the fix is being created.

ICMP Flood: The Internet layer protocol known as Internet control message protocol (ICMP) is used by networking devices to communicate. ICMP is the protocol used by the network diagnostic tools ping and trace route. Pinging a network device verifies that the sender and receiver are connected using ICMP request and reply messages. The attacker spoofs the victim's IP address, and To the networking devices, an unusually large number of ICMP echo-request packets are delivered. These networking devices respond by sending the target an ICMP echo-reply message. All of the mails are spoofing and addressed to the victim from the target IP address. This further results in the bandwidth and resource usage of the victim.

Useful SDN Features for Countering DDoS Attacks

SDN, in contrast to conventional networks, has certain powerful traits, and these traits provide a number of benefits for thwarting DDoS attacks.

Control plane and data plane separation: On a conventional network, the researchers are unable to conduct large-scale tests. Also, it is impossible to test and demonstrate the functionality of the newly created algorithms on the conventional network. The bottom two planes are divided by SDN, making it simpler to perform comprehensive defence trials. The main benefit of SDN is its strong configuration capability, which enables testing in actual settings.

By a seamless transition from the testing phase to the functioning phase, the novel ideas may be implemented gradually.

Global network view: The controller can see the whole network and analyses traffic to look for any security concerns. Using the data gathered by the asking end hosts, the centralization of the SDN controller aids in dynamically isolating the compromised hosts and manifesting benign hosts.

Network programmability: The SDN controller may be configured to write applications that govern the behaviour of the network. The network may be programmed, and by manipulating incoming traffic, we can stop hostile flows or hosts from causing network disruption. Moreover, clever scripts that may reroute traffic to intrusion detection systems can be built for controllers (IDS).

Using computer-based traffic analysis: Software-based traffic analysis promotes innovation since it may be carried out using a variety of software tools, algorithms, and databases. The difficulty of the transition to conduct traffic parsing is decreased by using software tools for traffic analysis.

Dynamic network update policy: A DDoS assault may be immediately countered by updating flow rules dynamically [36]. Innovative traffic engineering based on traffic analysis

A blocking rule may spread across the network. In a conventional network, only the target computers actually apply the rule for blocking the traffic. SDN allows for the dynamic updating of rules that may be installed in switches to prevent traffic from hostile hosts or bots. For updating policies in a conventional network, each switch must be manually set; however, with SDN, switch tables are dynamically updated all at once. This method makes it easier to manage all of the switch flow tables.

DDoS Attacks in the SDN: According to the prior section, an attacker may take advantage of flaws in these modules on each tier by manipulating how each module of the architecture processes the packet. We go through how the attacker may leverage these modules to conduct a DDoS assault in the SDN architecture in the subsections that follow. Several SDN modules that were abused during a DDoS attack.

Buffer Saturation:A memory known as ternary content addressable memory is kept by the switch (TCAM). The switch saves a portion of the packet into buffer memory and transmits the header as Packet In message when a flow rule is absent from the flow table. The switch transmits the complete packet as a Packet In message when the buffer memory is full. Several packets from the attacker may be sent that include entries that don't match.

Control-Data Plane Channel Congestion: When a packet is transmitted to the controller for processing, the SDN switch keeps a portion of it in the buffer. Nevertheless, the buffer also has a finite amount of space, thus the SDN switch only stores a portion of the packet there. As soon as the buffer is filled, the switch delivers the complete packet as a Packet In message to the controller for processing. Channel constriction is high when the full packet is sent to the controller utilising the single bandwidth. As a result, genuine users encounter a significant slowdown in getting their requests fulfilled.

Controller Saturation: Ultimately, when the controller receives a flood of requests, the controller becomes busy with the phoney requests, and as a result, the controller's throughput and processing capacity are reached. The whole SDN infrastructure is degraded by infecting the controller. An attacker simply has to generate a large number of anomalous packets in order for this to occur.

We conducted a thorough analysis of the software-defined networking (SDN) idea. A detailed explanation of the SDN architecture and how each layer operates is given. We also spoke about the history of SDN and its advantages over conventional networks. To defend the SDN architecture, numerous methods that are deployed at various modules are discussed along with their drawbacks. These solutions' numerous possible security challenges that we can run across while implementing them in a large-scale context are also examined. Lastly, we discussed future research issues that must be resolved in order to increase the influence of SDN.

The novel concept of a "programmable network" is introduced by software-defined networking (SDN), which facilitates flexibility and simplicity while accelerating installation. The separation of the control plane from the data plane is the fundamental tenet of the SDN architecture. The functionality for managing network traffic is shifted into the controller, which is located in the control plane, while the data plane devices, such switches, become simple packet forwarding devices. SDN increases flexibility, accelerates adoption, and makes administration easier. The distributed denial of service (DDoS) assault, one of the most common types of attacks, targets SDN because of its capabilities.

CONCLUSION

With the introduction of "programmable networks" via software-defined networking, network administration becomes more flexible and straightforward. The main concept behind this simplicity is the separation of the control plane from the data plane and the transfer of the application writing logic to the application plane. We examined the security issues of SDN in this chapter from a wide perspective, but we focused on defending against distributed denial of service attacks. This decision was made in light of current data and the sharp rise in DDoS attack events in recent years.The goal of identifying and analysing potential security flaws in the SDN architecture. Based on recent data and a rise in DDoS attack frequency, we concentrated exclusively on DDoS assaults. We are given guidance to overcome the weaknesses that still need to be addressed for the progress of SDN by presenting the research difficulties of this study.

REFERENCES

[1] B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, *Handbook of computer networks and cyber security: Principles and paradigms*. 2019. doi: 10.1007/978-3-030-22277-2.

[2] M. Ďulík and M. Ďulík, "Cyber security challenges in future military battlefield information networks," *Adv. Mil. Technol.*, 2019, doi: 10.3849/aimt.01248.

[3] P. V. Krishna, G. Sasikumar, and M. S. Obaidat, *Social Network Forensics, Cyber Security, and Machine Learning*. 2019.

[4] D. Tang and X. Kuang, "Distributed Denial of Service Attacks and Defense Mechanisms," in *IOP Conference Series: Materials Science and Engineering*, 2019. doi: 10.1088/1757-899X/612/5/052046.

[5] Akash Mittal, A. K. Shrivastava, and Manish Manoria, "A Review of DDOS Attack and its Countermeasures in TCP Based Networks," *Int. J. Comput. Sci. Eng. Surv.*, 2011, doi: 10.5121/ijcses.2011.2413.

[6] R. F. Fouladi, O. Ermiş, and E. Anarim, "A DDoS attack detection and defense scheme using time-series analysis for SDN," *J. Inf. Secur. Appl.*, 2020, doi: 10.1016/j.jisa.2020.102587.

[7] M. Conti, C. Lal, R. Mohammadi, and U. Rawat, "Lightweight solutions to counter DDoS attacks in software defined networking," *Wirel. Networks*, 2019, doi: 10.1007/s11276-019-01991-y.

[8] M. Faisal, S. Abbas, H. U. Rahman, M. Z. Khan, and A. U. Rahman, "An Analysis of DDoS Attacks on the Instant Messengers," *Secur. Commun. Networks*, 2019, doi: 10.1155/2019/1751285.

CHAPTER 2

ANALYSIS OF DISTRIBUTED SYSTEM AND SECURITY MONITORING

Dr. Shilpa Mehta, Professor,
Department of Electronics & Communication (Communication System Engineering),
Presidency University, Bangalore, India.
Email Id: - shilpamehta@presidencyuniversity.in

ABSTRACT:

With today's information technology, distributed systems play an important role for both governmental and nonprofit organisations. Distributed systems that may adjust how they behave in response to environmental changes are known as adaptive distributed systems (ADS). For instance, a distributed system needs regular monitoring to dynamically balance the load using a centralized technique to detect changes in distributed systems and all actions throughout the full network of systems, a monitoring system or tool is utilized. The effectiveness of the network as a whole may be enhanced via network monitoring. Yet, if an intrusive party gathers data from dispersed systems, they could damage the monitoring system. Adaptive distributed systems have included the many safe and unsecure monitoring strategies. Nowadays, the majority of distributed systems employ monitoring tools to keep an eye on the different networking system metrics.

KEYWORDS:

DistributedSystems, MonitoringTool, Management, Information Technology.

INTRODUCTION

With the aid of the many monitoring instruments available, the monitoring may be conducted. For network-wide monitoring, several monitoring technologies are essential. In this chapter, security mechanism monitoring has been completed using the available monitoring tool, and different distributed system parameters are investigated. This chapter's primary goal is to examine the monitoring systems already in use, such as the Wireshark monitoring tool, and to create a solution to protect the communication channel to the Wireshark monitoring tool with enhanced security features. Hence, the Wireshark monitoring tool is taken into consideration here, and its benefits and drawbacks are thoroughly covered [1]–[3].

Monitoring Techniques

Monitoring systems are a kind of system that are generally used to maintain track of other systems in a network. The term "network monitoring" refers to the application of a system that continually monitors the networked computer and, in the event of slowness or failure, notifies the network administrator. The following elements are often included in a monitoring system: a monitoring module, an event identifier, monitoring hardware, event detection, and event processing. Monitoring is specifically carried out in two activities, namely the detection of events that are pertinent to the execution of the programme and the saving or recording of the gathered data. By using a network monitoring programme, the failed nodes have been monitored. To retrieve the most recent system status, a Simple Network Management Protocol (SNMP) agent connects to a monitor of another network.

The two kinds of monitoring systems are internal monitoring systems and external monitoring systems. If an internal monitoring system is used.

Each client has a monitoring system integration. The same system's programme executions are monitored by each client's monitoring system, which logs the information here. The central monitoring system receives the recorded data. In contrast, an external monitoring system observes the target system while being located outside the current network. In this case, the dispersed system generally contains the target system. Security administrators may maintain tabs on the attacker using the monitoring system. Hence, the assessment approach enables tracking of the present attacker location and forecasting of the attacker's (her) progress across the network.

The run-time environment for the security execution control module in the Software Defined Security Architecture (SDSA) monitoring system contains the security engine for supporting dynamic system monitoring as well as a number of (sub) modules for supporting security status monitoring, security task executions, and software developer managements on top of the security engine. The security status monitoring module is in charge of keeping an eye on and managing the operating state of different security programmes, including the status of processes, memory stacks, file systems, and resource scheduling.

Tools for Monitoring

The central processing unit (CPU) usage, bandwidth availability and utilisation, latency, CPU responsiveness, and fault detection are all monitored by the network monitoring tool. The network monitoring tool can more readily assess the performance of distributed systems thanks to these observed metrics. A typical network monitoring tool consists of both software and hardware components. It keeps a close eye on network activity and, when necessary, issues an alarm.

It is very difficult to determine how much capacity is needed in an energy producing facility to achieve the desired output. There is an opportunity for capacity reviews and procedures for measuring capacity, but they should be used in conjunction with modern machines that have several functions. Using several sensors is one method of measuring capacity. During monitoring, this approach has been utilised to quantify changes in power input. It establishes the degree of manufacturing power input decrease. An energy consumption reduction system has been identified and validated using a monitoring tool [4]–[6].

Why Network Monitoring Tools Are Used

The network administrators utilise monitoring tools for a variety of tasks, such as to find defects in switches and routers.

1. To manage the resources and services offered by the internet.
2. To keep an eye on how various hosts in the network are doing.
3. To monitor the client-server computer system's inherent operations.
4. To oversee and keep track of how broadcast systems are running in order to achieve scalability.
5. To keep track of bandwidth utilisation and scattered network activity. To keep track of how users of the dispersed network are exchanging messages.

DISCUSSION

Characteristics of Tools for Network Monitoring: The network monitoring tool serves as the organization's eyes and ears in troubleshooting. These programmes keep track of server or system crashes, running applications, bandwidth use, CPU usage, and memory usage. The following features of the monitoring tool have been added: automated finding, device inventorying, alerts, and a web-based user interface. Both IPv4 and IPv6 traffic on a typical network should be able to be diagnosed by the monitoring tool. The majority of monitoring solutions rely on sensors to gather data for analysis. Some monitoring solutions use agents to gather data, but their usage compromises the system's overall performance. Hence, a monitoring instrument without agents may be seen as being just somewhat effective. Another crucial characteristic of the monitoring tool is its capacity to keep track of all network-based services and apps. They provide network managers the ability to examine performance problems originating from either the network or the application. Network administrators may monitor application response times, server request processing times, and network response times using this feature of a monitoring tool. The many aspects of the monitoring tools are shown in the list below.

1. Auto discovery: Manually putting in each healthy device is really onerous for system administrators. The majority of monitoring programmes automatically discover systems. It makes it easier for system administrators to browse the IT infrastructure inventory.
2. Network traffic status: Monitoring tools may be used to track network bandwidth consumption in addition to CPU, memory, and disc utilisation. It enables network managers to learn more about the bandwidth use of the ISP.
3. Log monitoring: Monitoring software controls the operating systems' activity logs. It carries out configuration operations and checks the activity log's file size. The system administrator may manage the complete network infrastructure with the aid of this capability.
4. Alert management: In addition to basic network monitoring activities, the monitoring tool also delivers alarm signals. For instance, if a firewall system misses more packets than usual, or if a server's CPU reaches 95% usage. In each of these scenarios, the tool should send a network administrator an alarm message.
5. Customized Web dashboard: The monitoring tool must allow users to choose what should appear on the dashboard. Determining the appropriate staff allocation for monitoring tasks is helpful.
6. Security monitoring: A secure monitoring instrument should be used. Consider probable attacks on the network layer, application layer, and data link layer a problem with this tool. Instead of monitoring all characteristics, the network administrators must pick what needs to be observed.

To evaluate the performance overhead while monitoring, a monitoring tool has been built.This chapter's major goal is to look at the monitoring tools that are now available in order to determine how monitoring activities in a dispersed network affect those activities. The findings show that there is a significant danger of information leakage to unauthorised users when the monitoring tool gathers security-critical data.

The availability of a secure communication route is the second issue may be put into practise by keeping an eye on the private data using the Rivest, Shamir, and Adelman (RSA) method. This chapter provides examples of the authors' application of their research findings and experimental findings connected to the creation of a framework for security procedures in the context of adaptive distributed systems.

The Operation of Network Monitoring: On basic networks, the ping tool is adequate for identifying connectivity problems. Microsoft network monitoring offers network packet analysis, mostly to address network problems. Open-source network monitoring software often offers accurate data based on measurements, but these call for extra tools like automated alarm signals. The cost of the open-source monitoring tools is low. These monitoring technologies, however, are not very effective.Real-time traffic data is captured using the Wireshark monitoring tool. During each time window of 10 msec, one packet is captured. The 1-hour time slot has thus been used to hold a very high number of packets. The Wireshark monitoring tool records the elapsed time, capture number, capturing protocol, packet size, source IP address, and destination IP addresses for each such capture for future reference.

The authors of provided a method for reducing security lapses during monitoring service. The SELinux OS has offered enough security protection against undesirable monitoring results. The security policy was implemented in accordance with the OS's updated configuration.Fundamentally, there are two methods for capturing packets in networks. The first is macro capturing, which deals with the capture and processing of enormous amounts of data. Micro Capturing is a different kind that just deals with particular information that has been stated by a user. The Micro-Capturing technique is used in this instance in the Wireshark monitoring tool. This programme allows for the recording and analysis of real-time network data.

Distributed System Monitoring Framework

A monitoring framework for distributed information management systems is presented in an original method by Chen et al. Web services and message queue methods are used by this monitoring system to gather log data. The information gathered is utilised to keep track of corporate operations. This tool is used to evaluate the performance cost associated with monitoring. Evaluations were done both with and without monitoring while users were under different loads. The results of the experiment demonstrate that the monitoring method has little effect on the system's performance. Nevertheless, since it only employs one message queue, the monitoring architecture is a kind of passive monitoring. Two unconnected events that happen concurrently cannot be seen by this instrument. While it is possible to use many queues, monitoring overhead is a possibility.

A system for aggregating events of certain profiles of social network users was suggested by Fonseca et al. Moreover, it routinely gathers data based on profiles and behaviours associated to them. The framework aids in calculating the typical events for certain profiles and contrasts the gathered values with the most recent profile data acquired. These numbers will make it easier to spot changes in profile activity. Also, these discrepancies point to unauthorized account or profile use. The framework also informs users when friendships between users are cancelled. Also, it notices unusual activity such as when a person adds or removes several other users.

The authors offered a framework that included two parts. The core component, one of the components, determines the user profile interactions. The web interface component is another part that manages user profile metrics via interaction and visualization. The start component is in charge of gathering activity data from numerous social networks. The statistics component examines the data when the start component has finished gathering it and produces a report. The alert module analyses the alarm signals for pertinent suspicious behaviours based on the report produced by the statistics module. The suggested approach, however, does not gather user-wanted information from social networks. Instead, the framework gathers more data than is required, which lowers the system's performance.

A novel framework for remote monitoring was presented by Antighetto and Adler. By preventing unauthorized users from accessing the monitoring components, it primarily helps security considerations. In very crowded dispersed networks, such as transitory and low bandwidth networks, the structure also facilitates cooperation. By using unique sensor data, this remote monitoring fends against spontaneous and passive assaults.A framework for describing plans of monitoring parameters has been created in. The framework first describes how to specify plans and carry them out in both friendly and hostile contexts. It then creates a model for carrying out security policies.

In their discussion of the two primary issues with adaptive distributed systems, Aredo and Yildirim Early system monitoring to gather data required for adaption may result in security problems. The monitoring node often collects information on users, their activities, and message specifics outside the destination system. When a monitoring system is taken over by an attacker, there is a serious security concern. Third, restricting monitoring may make it more difficult for the system to maintain the security mechanism and react to changing environmental conditions. Aredo and Yildirim’s discussion of adaptation does not address how to do so with the least negative effect on the security system. The authors also don't go into detail regarding the types of data that can be watched or how to monitor them without compromising the effectiveness of the distributed monitoring architecture.

The monitoring of adaptive distributed systems and security metrics for the adaptive distributed systems using security metric functions were introduced by Aredo and Yildirim. Monitoring, change detection, and reconfiguration in response to environmental changes are some of the fundamental processes of ADS.

A monitoring component is used to gather data on parameters, which are then analysed to look for changes in the target distributed system's environment. A hacker may get control of a monitoring system and utilise the data inappropriately.There are two possible situations for monitoring the target systems: one involves monitoring an internal system module, and the other involves monitoring an external system module. Because of the reasons listed below, writers here took the possibility of monitoring outside the system into consideration. One of the reasons is that it is challenging to directly operate the whole distributed system from a centralized server if monitoring is a component of the system. It need extra historical monitoring techniques.

Although the system for external monitoring depends on a single thread of control, the issue also arises when trying to directly monitor the whole system from a single surveillance site, which necessitates the synthesis of locally recorded activity in order to provide global observations. Second, while monitoring is a component of the system, there is no single hub for decision-making. As a result, a distributed system's decision-making process might also be distributed. The third reason is that because of the interdependencies between the many programmed in a distributed system, any change in one program's operations might change how the distributed system as a whole behaves. An attacker could be able to access unsecured

communication channels and obstruct user operations while gathering sensitive data.Monitoring the network has the consequence of being intrusive because incursions enter the system when resources are shared with the monitoring system. The actions could change arbitrarily as a result of intrusive. Intrusive monitoring issues include decreased system performance, inaccurate results, execution delays, and the masking or instigation of deadlock situations. By finding occurrences in the monitoring systems, the intrusiveness may be assessed. There are three types of monitoring systems: software monitors, hardware monitors, and hybrid monitors.Here, the packet capture algorithm has also been covered. Results from the implementation have been used to examine the effects of monitoring situations. Finally, using the RSA technique, a safe method of implementing monitoring systems has been explored [7]–[10].

CONCLUSION

The security concerns for the current monitoring technology are thoroughly explored. In this regard, the chapter discusses the many security-related network situations seen when using the Wireshark monitoring programme. The appropriate usage of the Wireshark monitoring tool aids in the detection of potential security concerns, such as newly emerging hacker threats, business data theft, and virus-related threats. It is addressed how to establish secure communication channels to reduce the aforementioned concerns.There have been two discussions on the security mechanism framework. In the first, current monitoring security measures will be examined; in the second, a secure communication route will be put in place.The procedure was first seen using the Wireshark monitoring tool. In this respect, a chat application has been created to allow users to send and receive messages. A thorough explanation of the algorithmic monitoring process has been provided.

REFERENCES

[1] G. Yadav and K. Paul, “Architecture and security of SCADA systems: A review,” *International Journal of Critical Infrastructure Protection*. 2021. doi: 10.1016/j.ijcip.2021.100433.

[2] M. Lou, X. Dong, Z. Cao, and J. Shen, “SESCF: A Secure and Efficient Supply Chain Framework via Blockchain-Based Smart Contracts,” *Secur. Commun. Networks*, 2021, doi: 10.1155/2021/8884478.

[3] A. Shahid, T. A. N. Nguyen, and M. T. Kechadi, “Big data warehouse for healthcare-sensitive data applications,” *Sensors*, 2021, doi: 10.3390/s21072353.

[4] T. Georgi, Y. Radoslav, and Z. Nataly, “Some security issues with the industrial internet of things and comparison to SCADA systems,” *SPIIRAS Proc.*, 2020, doi: 10.15622/SP.2020.19.2.5.

[5] B. Hong, H. Wang, and Z. Cao, “An Effective Fault-Tolerant Intrusion Detection System under Distributed Environment,” *Wirel. Commun. Mob. Comput.*, 2021, doi: 10.1155/2021/2716881.

[6] M. A. Poltavtseva, “Heterogeneous Data Aggregation and Normalization in Information Security Monitoring and Intrusion Detection Systems of Large-scale Industrial CPS,” *Proc. Inst. Syst. Program. RAS*, 2020, doi: 10.15514/ispras-2020-32(5)-10.

[7] M. Babakmehr, M. G. Simões, M. B. Wakin, and F. Harirchi, "Compressive Sensing-Based Topology Identification for Smart Grids," *IEEE Trans. Ind. Informatics*, 2016, doi: 10.1109/TII.2016.2520396.

[8] T. Georgi, Y. Radoslav, and Z. Nataly, "Some security issues with the industrial internet of things and comparison to SCADA systems | ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ И СРАВНЕНИЕ С СИСТЕМАМИ SCADA," *SPIIRAS Proc.*, 2020.

[9] Y. L. J. Huang and J. Wang, "Environmental Safety Monitoring System Based on Microservice Architecture and Machine Learning," *South Florida J. Dev.*, 2021, doi: 10.46932/sfjdv2n2-133.

[10] S. Katyara *et al.*, "Wireless Networks for Voltage Stability Analysis and Anti-islanding Protection of Smart Grid System," *Wirel. Pers. Commun.*, 2021, doi: 10.1007/s11277-020-07432-w.

CHAPTER 3

AN ANALYSIS OFDIFFERENT CYBERATTACKS IN REAL-TIME

Mr. Tirumala Vasu Galithoti, Assistant Professor,
Department of Electronics & Communication Engineering, Presidency University, Bangalore, India.
Email Id: - tirumala.vasu@presidencyuniversity.in

ABSTRACT:

Computer-based simulation techniques are crucial in helping and comprehend how humans behave in complicated cyber circumstances while acting as attackers (those who conduct cyberattacks) or defenders (those who defend computer networks from cyberattacks). In this article, we present the HackIt simulation program, which can be used to create dynamic cyberattack scenarios. When deception was present, it was simple to take advantage of honeypots during deception rounds. The attackers' intent was to steal credit card data from networked PCs in both scenarios.In recent years, danger hunters and purple teams throughout the globe have turned to the principles of deception as a hidden weapon. A target and a deceiver may communicate during a deception in an effort to persuade the target to believe the false version of the truth. Existing technologies, like as firewalls with blacklists, intrusion prevention systems, and URL filtering, may be used to commit deception. The use of honeypots for deception has been suggested by many academics. Servers known as honeypots imitate genuine servers but are false.

KEYWORDS:

Cyberattacks,Cybersecurity, Deception, Honeypots, Strategies.

INTRODUCTION

Government, business, finance, and e-commerce are all targets of alarmingly frequent cyberattacks. The cybercriminals infiltrate the network and obtain access to the data by using sophisticated cyberattacks, such as SQL injection, phishing, Trojans, ransomwares, rootkits, and malware. Finding ways to improve network security is urgently needed given the increased danger of cyberattacks on vital cyber enterprises. Nowadays, there are several cyber security mechanisms available to combat different assaults, but very few of these defences can stop zero-day cyberattacks, which aim to exploit known vulnerabilities that have not yet been fixed. Deception is a kind of persuasion in which defenders purposefully lead hackers astray, and it could provide a potential real-time defence against cyberattacks. By placing the effort, money, and cognitive costs of cyberattacks back on the attacker, deception technology may aid in the reduction of cyberattacks. This chapter's goal is to look at the possibility that deception techniques might lessen cyberattacks [1].

A variety of techniques for utilising deception in cyber security have been suggested by prior research. The deception tool kit (DTK), honeynets, honeytokens, thug, TrapX, and smokescreen are a few of these tools. One of the first tools to use deception techniques for cyber defence was the DTK. DTK processes inbound malicious requests that are typically denied by the network using TCP wrappers. In addition, researchers have suggested honeynets, which are a collection of real-time applications' honeypots. To find harmful Web-based activities that attempt to exploit client application vulnerabilities, client-side honeypots have been suggested.

Moreover, noncooperative dynamic decep-tion games have been suggested by some academics as a means of analysing cyberattack choices made by hackers via experimental and mathematical modelling. For instance, Aggarwal et al. used a noncooperative deception game to evaluate the significance of the quantity and timing of deception in a cyberattack scenario (DG). There were two stages to the DG: probe and assault. During probe, participants may investigate webservers, some of which were honeypots, while acting as hackers. Hackers may launch a genuine assault on one of the webservers after probing the network. Findings showed that applying significant amounts of deception at late times was effective in lowering cyberattacks.

The development of tools for deception and an understanding of human characteristics in abstract contexts were the main goals of earlier study. The conclusions reached in laboratory studies conducted in the past may not accurately reflect how computers are targeted by hackers in the real world since they were based on abstraction of options and results. The main goal of this project is to create a cybersecurity tool that will aid in our understanding of the psychological aspects that influence hacker choices in tricky cyberspace scenarios including deceit. To achieve the aforementioned goal, we created the HackIt tool, which allows us to simulate complicated cyber-situations and demonstrate the program's capabilities using various deceptive cyberattack scenarios [2].

We model two situations in which deceit occurs either early or late using the HackIt tool. In some cases, the hacker's objective is to get credit card data from the network. Two web servers make up the network, one of which is a genuine web server and the other is a phoney honeypot web server. This chapter tests whether deception timed early or late is more successful in luring hackers into honeypots. We do this by using the HackIt game. In addition, we contrast our findings with those made public by Aggarwal et al.

Tool HackIt: Typically, there are two stages to website hacking: scanning for weaknesses and targeting computer workstations (attacking). With the aid of two phasesthe probe phase and the assault phasethe cybersecurity tool HackIt enables researchers to model actual cyberattack scenarios. Although the assault phase entails breaking into several computers, stealing data, or compromising computer systems, the probe phase includes checking the network's webservers for weaknesses. For instance, the HackIt programme enables the creation of networks of various sizes, the use of deception to set up various webservers as honeypots, and the creation of an infinite number of bogus services, ports, operating systems, and files on honeypots. The network commands nmap, use exploit, ls, and scp may all be executed using the HackIt tool. A network tool called Nmap displays the operating system, services, and open ports on the given website.

The list of vulnerabilities on the associated webservers is provided by the nmap software. The use exploit command assists hackers in accessing a website by taking advantage of system flaws. The ls command then displays a list of all the files presently present in the machine's file system. Files are sent to the distant system using the scp command. With the nmap command, webservers on the network are scanned during the probing phase. Hackers may use the nmap programme to get details about the open ports, services, and security holes present in the network. The assault phase also includes information theft and vulnerability exploitation. A hacker may use the use exploit command to visit any website and exploit it. Using the scp command, the hacker could then steal data from computer systems. The experiment using the HackIt tool to test the impact of timing deception using honeypots on mitigating cyberattacks is described in the next section.

DISCUSSION

A simulation tool that may be very useful to cybersecurity researchers looking to understand how hackers and analysts make decisions in actual cybersecurity situations. While using the HackIt tool, hackers might utilise genuine instructions to probe networks, attack vulnerabilities, and transmit data in more realistic job settings. As a result, the creation of the HackIt tool may provide us a platform to transition from purely theoretical to practical and sophisticated decision-making tasks. We demonstrated a real-world study case utilising HackIt to assess how timing of deception affects hackers' choices. Findings showed that honeypots were more effective at catching hackers when deception was used later rather than earlier. We think the HackIt tool would be useful in developing further cybersecurity scenarios incorporating varying deception tactics, dynamic network sizes, and dynamic network topologies [3].

Used the HackIt programme to simulate an information-theft situation in which a hacker attempted to steal a credit-card file from a typical webserver system. HackIt was used by researchers to replicate a deception approach that changed over time. When deception occurred later as opposed to earlier, we discovered that the percentage of honeypot assaults was greater. In a similar vein, we discovered that when deception occurred late compared to early, the percentage of regular assault activities was lower. These results from the HackIt tool are consistent with those from. This discovery is most likely due to the hacker's lack of knowledge of the existence of deceit in the first rounds. According to IBLT, decision-making is influenced by the recentness and frequency of experiences. No memories were stored that indicated the existence of honeypots in the early deception phase. As a result, the hackers targeted normal webservers more often. Hackers began depending on input in subsequent rounds because of the trust they had established in earlier rounds. As a result, they attack honeypots more often than conventional webservers.

Also, findings from the HackIt tool point to the benefit of analysts using deception at the end of a series of cyberattacks on a computer network. As a result, first attacks without deception will probably lead hackers to trust in the data supplied by the network. Additionally, analysts will probably benefit from late deception in their efforts to catch hackers.Presently, we have just looked at the time of deception as a factor regarding deception utilizing the HackIt programmed. We also want to look at the number of honeypots that will be necessary for a network to effectively catch hackers in various methods. We also want to examine the efficacy of deception technologies against other cyberattack types (such SQL injection, denial of service (DoS), and zero-day assaults) and against hacker probing operations using various cost models.

Today's military and marine technology is advancing quickly in a variety of ways, such as high-distance tracking radar, the fusion of disparate systems to shorten operating times, and joint operations with air and sea. Search and rescue (SAR), hydrography, and ocean bottom mapping are examples of expensive, unpredictable, and risky tasks that are now carried out quickly, efficiently, and with the least amount of human participation. On the other side, entrusting people with very dangerous (and sometimes fatal) mission’s poses ethical questions given the evident value placed on human life.

However, these procedures are very expensive, mostly because of the energy and fuel consumption of the relevant equipment and platforms. While planning such operations, the cost-efficiency aspect must be carefully taken into account, particularly when time and money are also required to repair damaged air, surface, or subsurface vehicles. The employment of autonomous and unmanned vehicles, which are self-managing, economical, and successful in completing a number of very unsafe and resource-demanding jobs, is a

crucial answer to this problem. Unmanned vehicle systems and platforms below, above, and in the air have thus become a top focus for both military and non-military enterprises [4], [5].

Unmanned underwater vehicles have grown in popularity during the last ten years. In partnership with academic institutions, the North Atlantic Treaty Organization (NATO) has created specific fields for specialized study on this subject. Drones and remotely operated vehicles (ROVs), also known as unmanned or autonomous underwater vehicles (UUVs/AUVs), have been developed for many years. They vary in a number of ways, with the human aspect being the most important. UUVs/AUVs behave entirely independently the majority of the time, displaying some kind of intelligence by determining their own course without relying only on people. In contrast, ROVs need a distant human operator, which has led to a number of use constraints. Typically, ROVs and UUVs/AUVs both function in an underwater wireless sensor network (UWSN). This kind of network enables the wireless bidirectional transfer of data between users, such as underwater vehicles, as well as the monitoring of the aquatic environment.

Nowadays, UUVs/AUVs are regarded as a potent scientific and military "weapon" that, when working in swarm formations, accomplishes amazing feats. Several UUVs that can cooperate, communicate, and act as a group are referred to as swarms of UUVs. The leader of the UUVs should be the one who makes the majority of the decisions. There could also be a number of smaller groups with leaders. Every unit in the swarm should be able to assume leadership in cases when the leader is unable to do so (for whatever cause, such as damaged circuits), as well as having the authority to do so. The use of UUVs in swarms is a potent platform that offers significant advantages for a successful operation (military, scientific, or other), even in risky and hazardous circumstances, putting aside any ethical concerns of a human (such as a military commander or chief scientist), particularly when the leader achieves full autonomy in decision-making.

In order to successfully accomplish interoperability in a swarm of UUVs and guarantee all the aforementioned criteria, semantic knowledge and ontologies are essential answers. UUVs/AUVs may effectively assist any mission or activity, whether it be for military, navy SAR, or civilian purposes. completed the precise mapping of the seabed at a depth of 3000 m in the powerful currents of the Atlantic, and it also successfully identified various debris and wrecks. Moreover, AUVs helped a significant investigation into an aeroplane disaster (Air France Flight 447), using side-scan sonar to find fragments of the aircraft and its "black box". Ultimately, US Navy Knifefish can locate and categorise mines in significant depths in an environment with significant levels of clutter. NATO is increasingly incorporating UUVs into its fleet in an effort to address several difficulties.

Interoperability is a crucial, unresolved topic in this area of study. The majority of NATO's platforms and systems, as well as those created by research organisations, adhere to their own standards and procedures for command, communication, and control, making cross-platform interoperability essential. Also, the security of underwater networks is a major concern when using the water as a medium for data transfer between UUVs. More precisely, coupled with data sender/receiver authentication, cybersecurity assessment and security upgrades should be a constant concern. The amount of sensor data collected and transmitted in a communication network is at least substantial in the age of big data and the Internet of Things (IoT). The four Vsvolume, variety, velocity, and veracityare additional properties of the data transmitted in this environment. Given that big data exchange between various heterogeneous underwater/surface/air systems/platforms should be carried out in real-time, this process is regarded as extremely dangerous when carried out in a medium of transmission with an extremely low bitrate (i.e., in the water), where a number of physical phenomena can affect

the quality of transmission. The main issue with latency in secure communications is the time it takes to review warnings from cyber-incidents and then take action against them. Also, because to the amount of information exchanged, repetition of the same data is another deterrent problem that is experienced. By "sieving" these data, the underwater network may be decongested and the speed at which information is transferred can be increased.

In order to reach the scene of an aircraft crash safely and promptly, a swarm of UUVs must cooperate in an underwater sensor network (UWSN), exchange information and data in real-time, and use adaptive path-planning. The resilience of the network architecture is compromised when they are carrying out their assigned responsibilities due to an unusual communication latency between them and with the underwater nodes, which prevents them from getting information from the commander. automatic evaluation of the incident's problems a warning for very high packet volumes that overwhelm the network, signaling an impending DoS (denial of service) assault as a result, an automatic process of different countermeasures techniques and protocolssuch as honeypots, encryption algorithms, security regulations, etc.is started. Such a scenario must be simulated for commanders in order to improve training and anticipation, develop a simulation tool that is always available for consulting and training, validate and update security protocols, and learn to anticipate such urgent situations quickly and effectively by testing alternative topologies, among other things, minimizing handling costs and casualties.

In order to provide a unique simulation tool-supported strategy to assist commanders of military/search-and-rescue operations in successfully making crucial and life-saving choices, this research aims to analyse relevant works, outstanding problems, and obstacles. In order to attain and create safe transmission of data/information, this article especially seeks to provide SAR and battle commanders with an effective UUV swarm simulation environment that will emphasis interoperability and cybersecurity challenges. Based on this objective, this paper makes two contributions: (a) a review of existing techniques and tools for semantic modelling and simulation for cybersecurity and interoperability on the IoUT; and (b) a discussion of unresolved problems and challenges in the development of a new simulation strategy to support commanders of military and search-and-rescue operations in making crucial and life-saving decisions.

UUVs are autonomous mechatronic devices that potentially increase human participation in underwater tasks such as ocean ranching, underwater search and rescue, and marine engineering building. They are strong assets that can operate independently in underwater missions and operations. They are capable of situational awareness, autonomous decision-making, and trajectory planning. They also collaborate with other surface, air, and aquatic vehicles and platforms. You may think of a UUV as a kind of knowledge-based autonomous agent. It also has the ability to govern itself, including the capacity for self-configuration, self-healing, self-optimization, and self-protection. Recently, a fascinating study reporting on improving UUVs' capacity for self-diagnosis and self-adaptation using a "metacontrol" framework and the use of ontological reasoning was published. The authors were driven by the absence of real-time communication in the work of UX-1 in the UNEXMIN project (a robot created to inspect flooded ancient mine sites), and they proposed a framework to improve its capacity for self-diagnosis and self-adaptation. Localization is essential for connecting these priceless resources and achieving an effective information exchange. A vehicle can locate and establish its orientation in the environment using this capacity, both underwater and on land.

Due to the ease of information exchange, the localization capability of UUVs and underwater assets is more than significant in developing robust network architectures. Nonetheless, this necessity brings about fresh difficulties to conquer. There are several localization methods that may be used with a UWSN and are categorized into two main groups, namely range-based and range-free schemes, as we have seen in previous work. The first category is based on precise measurements of distance and angle utilizing factors like Time of Arrival (ToA).

The approach depends on rigorous temporal synchronisation for the precise information transmission and receiving instances, while being highly accurate in determining the location of an item. The second one relies on simplicity and does not need range or bearing information, although it increases node localization error; this schema is appropriate for terrestrial sensor networks.

UUV technical advancement is necessary for effective operation in the maritime environment. They are used to lower operating expenses and lessen the danger to human life. As marine activities grow more complicated and dangerous, such as aiding the construction of oil and gas facilities or settling undersea cables at previously uncharted depths, there is an increasing demand for robust and intelligent UUVs. Also, in the context of military operations in an IoUT environment, a team of UUVs is taking part in SAR or mine deactivation operations for anti-submarine warfare, each with a specific duty and being linked to the others. Also, taking into account the UUVs' interoperability is important while planning an operation, particularly when they operate in a swarm configuration. A number of self-organizing autonomous agents with the goal of successfully completing diverse joint activities make up a swarm system of independent assets.

The secure and safe mobility of an undersea vehicle is a crucial concern in IoUT. The challenges that arise are enormous, especially in a swarm of UUVs where efficient collaboration amongst agents is a tough aim to achieve. These challenges include safe mobility and interoperability as well as secure communications between them. It is generally known that science often strives to mimic nature; as a result, UUV/UAV technology was created from the observation of bird flocks. Notwithstanding the numerous obstacles that stand between science and nature, substantial progress has already been made towards the creation of autonomous UUVs that operate in a swarm. A novel sort of autonomous underwater vehicle (AUV) swarm was suggested by the science department.

Without putting much focus on ruggedness, they have created an AUV with particular features and auxiliary systems like a camera for taking images, identifying fish, or spotting pollution. They used the Matlab/Simulink programme to simulate a swarm of 25 AUVs in order to analyse their mobility, connectivity, and system performance. Despite not having a "leader" truck or a central platform from which to give further directions for the operation, the outcomes were good. The Naval University of Engineering in China proposed a method for autonomous UAV path planning, demonstrating its efficacy through the use of Matlab, a dataset from GEBCO (General Bathymetric Chart of the Oceans) for coordination, a grid system, and the fusion algorithm PACO based on PSO (particle swarm optimization) and ACO (ant colony optimization).

Internet of Underwater Things:

The worldwide network may now be accessed by millions of devices thanks to technical advancements. The Internet of Things (IoT), the phrase used to represent this industrial transformation, was driven by consumers' demand to be continuously connected to their gadgets in order to carry out everyday tasks. Home automation is one way that the Internet of Things promotes a "smarter" way of life by helping with everyday duties and our welfare.

There are many everyday chores that may be made easier in the underwater (sea) "world," and several underwater vehicle equipment must cooperate in an underwater sensor network (UWSN) or underwater wireless communication network (UWCN). Some of these activities include the study of marine species, maritime security, naval military operations, and gas and oil production. The Internet of Underwater Things (IoUT) has been developed to facilitate the effective connectivity of underwater vehicles, gadgets, and sensors to the Cloud, not necessarily to make such operations simpler.

The IoUT has opened up new avenues for research and development in a brand-new environment that makes it easier to link resources "alive" both below and above the water. In order to further research, business, and underwater military or civil activities, it intends to address a number of UUV problems, including interoperability, data management, and secure communications. Establishing a fault-tolerant link between undersea and surface assets in such an ecosystem is necessary to address important needs including heterogeneity, network coverage, low latency, low power consumption or battery efficiency, and cyberattacks. To efficiently interoperate in UWCNs and UWSNs, the IoUT must combine diverse assets. The prerequisites for a UWSN are specifically longevity, accessibility, complexity, security, and environmental sustainability. In addition, a taxonomy based on particular essential qualities, such as architectural components, communication, routing protocol, security, and applications, is required. Since the dangers that must be fended off advance in sophistication, the development of a strong and safe undersea environment is an ongoing process [6], [7].

The amount of data to be transferred, as in the IoT, along with the IoUT's limited bandwidth, transmission medium (acoustic communication), and slow propagation speed cause delays in the dissemination of information. This fact enables cyber-adversaries to stay even more unnoticed and successfully complete their mission. More particular, sluggish transmission rates have an impact on how quickly an alarm is assessed and how quickly a cyberattack is responded to. The creation of data processing tools to streamline the procedure is a solution to cope with underwater communications' restricted bandwidth, latency, and environmental and ambient noise. In order to balance data traffic loading in an underwater network and reduce latency problems, such a strategy is suggested in. IDA, which supports high packet allocation together with low latency and little energy usage, is used to accomplish this. In underwater sensor networks like UWSN, multiple communication channels may be established to enable data collection and address bit-rate problems. Similarly, putting in place an information-centric paradigm makes it easier to address this issue. In order to balance latency difficulties and the sharing of superfluous information, a depth-based caching mechanism is thus suggested in, suggesting that the development of hybrid communication models is crucial to overcoming the physical phenomena of the water and advancing IoUT.

The interconnection of IoUT assets is already being significantly improved by fifth generation (5G) and the impending sixth generation (6G) connectivity networks, which enable their communication and data exchange at incredible rates (>1 Gbps) across a wide range of devices. In a related study, optical wireless communication (OWC) is suggested as a way to enhance underwater wireless communication. The study finds that OWC combined with RF technology can effectively manage large amounts of data while having high bandwidth, low latency, high protection, and low fuel consumption.

Semantic Modeling in IoUT:

Semantic modelling is the conceptualization of subject-matter expertise for the purpose of logically describing structured data (with formal semantics/metadata). Ontologies are formal vocabularies of ideas and relations that are used to integrate and describe diverse data in a meaningful way. According to the definition of an ontology given by [22], an ontology is the

formal and explicit specification of conceptualizations that are used to help programmes and people exchange knowledge by specifying items and connections among them. Ontologies are flexible tools that provide computers the ability to comprehend the meaning of concepts given in natural language. In terms of their ideas, axioms, examples, and connections, they need to be reusable. Additionally, ontologies should provide interoperability, modularity, and extension, according to the NeOn (networked ontologies) paradigm. Formal ontology uses semantic tools including query engines, knowledge management systems, and automated reasoners in conjunction with machine-readable languages like the Resource Description Framework Schema and the Web Ontology Language (RDFS/OWL). The capacity of a computer to deduce logical conclusions from a collection of acknowledged facts is known as semantic reasoning. Ontologies can make IoUT assets more interoperable.

To account for the uncertainties of underwater settings, proposes a hybrid method to context reasoning for underwater robots. An ontological, rule-based, and Multi-Entity Bayesian Network (MEBN) reasoning approach is suggested in order to increase UUV/AUV collaboration and cooperation as well as the idea of context awareness. This framework, which presents a comprehensive approach to context management and modelling of diverse contexts using ontologies for underwater robots, is presented to assist the SWARM project and SWARM ontology. By enhancing standardisation and offering a shared framework for comprehensible information transmission, information fusion and reasoning approaches promote cyber and trajectory situational awareness.

The ontology represents situational awareness (SA), which is a need for UUVs to be able to work together and travel safely. It is crucial that data can be handled successfully across many platforms and domains, and should be able to be evaluated, saved, retrieved, and disseminated fast in order to accomplish an autonomous decision-making loop for the "leader" of a swarm. The mission's flexibility and capacity to bounce back from setbacks are almost as crucial as the planning of the goal and course. The problem arises when many communication protocols are employed, and since there is a lack of standardization, interoperability is considerably more difficult to establish. To achieve semantic interoperability amongst IoUT assets, common communication protocols expressed as ontologies must be semantically modelled. It makes it possible for autonomous cars to comprehend their surroundings, incorporate new technologies by virtually instantly recognising them, understand why they are doing the way they are, and achieve the ideal autonomous decision-making loop.

Interoperability in the IoUT

Interoperability is "the capacity of two or more systems or components to share information and utilise the information provided," according to the Institute of Electrical and Electronics Engineers (IEEE). According to the capacity for system interoperation, interoperability grows in six tiers. But, in this assessment, we'll concentrate on the first three layerstechnical, syntactic, and semanticwhere network connection and simulation/implementation are made possible. Water as a channel is a key deterrent in UWSNs, since interoperability is intrinsically related to communication and facilitated via the transmission of acoustic and electromagnetic signals. The authors in present the SUNRISE model, which offers an abstraction layer for facilitating the connectivity of various control software of various undersea vehicles, in order to address the primary problem of IoUT, namely interoperability. The authors developed options for a heterogeneous network of mobile assets in response to the first attempt to define a common language, which is JANUS from NATO Science and Technology OrganizationCentre for Maritime Research and Experimentation (STO CMRE), and its limitations to initial contact and emergency message exchange. Even if a standard

physical coding system exists, encoding and decoding of signals is required; communication across underwater assets utilising various control software is not feasible. The collaboration of heterogeneous platforms is thus supported via a protocol called SSC (Software-to-Software) [8], [9].

CONCLUSION

The network's capacity was also restricted to two webservers, one of which served as a honeypot webserver and the other as a standard webserver.The efficacy of deception in networks of various sizes, we want to expand our current study on building deception in the HackIt tool. Depending on how many computers are present, a network may be categorized as small, medium, or big in size. Depending on the size of the network, honeypot efficacy may change. Any number of web servers may be set up as conventional web servers and honeypots using the HackIt programme. The expense of installing and maintaining honeypots is high, both in terms of money and labour as well as in terms of time. This chapter explores the various cybersecurity assaults on different networks in modern era.

REFERENCES

[1] P. Aggarwal, C. Gonzalez, and V. Dutt, "HackIt: A real-time simulation tool for studying real-world cyberattacks in the laboratory," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2019. doi: 10.1007/978-3-030-22277-2_39.

[2] S. Venkatraman *et al.*, "Time dependent anomaly detection system for smart environment using probabilistic timed automaton," *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02769-3.

[3] P. Mercader and J. Haddad, "Resilient multivariable perimeter control of urban road networks under cyberattacks," *Control Eng. Pract.*, 2021, doi: 10.1016/j.conengprac.2020.104718.

[4] T. Alves, R. Das, A. Werth, and T. Morris, "Virtualization of SCADA testbeds for cybersecurity research: A modular approach," *Comput. Secur.*, 2018, doi: 10.1016/j.cose.2018.05.002.

[5] V. Okhrimchuk, "GENERAL DIFFERENTIAL-GAME MODEL OF POTENTIALLY DANGEROUS PATTERN OF CYBER-ATTACK," *Cybersecurity Educ. Sci. Tech.*, 2020, doi: 10.28925/2663-4023.2020.8.113123.

[6] N. K. Kandasamy, "An Investigation on Feasibility and Security for Cyberattacks on Generator Synchronization Process," *IEEE Trans. Ind. Informatics*, 2020, doi: 10.1109/TII.2019.2957828.

[7] S. Khan *et al.*, "Cyber range for industrial control systems (CR-ICS) for simulating attack scenarios," 2021.

[8] L. P. Flowers, "Cybersecurity: Preventing Infection in a Body of Data," *J. Pet. Technol.*, 2020, doi: 10.2118/0820-0034-jpt.

[9] M. Aazam *et al.*, "Fog computing - Glimps of Upcoming Research Area (#4)," *Futur. Gener. Comput. Syst.*, 2017.

CHAPTER 4

BIOMETRIC FINGERPRINT SECURE COMMUNICATION SETUP PROTOCOL

Ms. Ginkawar Shwetha, Assistant Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - swethag@presidencyuniversity.in

ABSTRACT:

A variety of cryptographic approaches offer information security. One of these techniques that needs a shared secret key among two parties in order to function is symmetric key cryptography. The fundamental difficulty with symmetric key cryptography is the distribution of such a secret key. Efficient and reliable approaches are required to distribute the shared secret key across communication partieswith the assistance of their combined interruptible fingerprint templates and a random shuffle key supplied to them by a trustworthy authentication server. Between the connecting parties is an authentication server. Public key cryptography is used to safely communicate cancellable templates between the two users. When the communicating parties create the identical session key at their end, there is no need to communicate the secret key through an insecure channel.

KEYWORDS:

CloudComputing, Cryptography, Cryptographic Key, Session.

INTRODUCTION

Digital data must be kept someplace once it has been transferred through a communication channel. A secured data transfer and the security of this digital information become crucial. The number of Internet-connected, digitally identified gadgets is growing daily in Internet technology. The Internet of Things (IoT) has grown in importance as a result of technological advances. For a fully developed IOT ecosystem, a number of security vulnerabilities are regarded as critical challenges. Take, for instance, cryptographic procedures.Information security is provided by encryption-decryption techniques. They stop an attacker from capturing data and stealing information from a machine. The Kerckhoffs' principle states that the confidentiality of the cryptographic key determines the security of cryptography. Symmetric key cryptography and asymmetric key cryptography are two main categories for cryptographic approaches. A shared secret key is used in symmetric key cryptography for both encryption and decryption. The Data Encryption Standard (DES) and Advanced Encryption Standard are two examples of symmetric key encryption systems (AES).

In comparison to asymmetric key cryptography, symmetric key cryptography is more effective at encoding big messages. Symmetric-key cryptosystems are also quick and appropriate for real-time applications. Short message encoding is more quickly accomplished with asymmetric key cryptography. A secret key that both parties share is required for symmetric key cryptography. One of the issues with this symmetric key is the number of keys needed. If Alice wants to speak with N persons, she will need N distinct keys, for example. Hence, a total of N(N-1) keys are needed if N persons wish to connect with N individuals. Now, N(N-1)/2 keys are required if a key is to be utilised in both ways. Hence, if a million individuals need to communicate with one another, each of them has approximately a million

unique keys, and a trillion keys are needed altogether. This issue is referred to as N2 since N entities need N2 keys. Another issue is symmetric key distribution. Considering that symmetric key cryptography requires that both parties' keys be transferred and secured against unwanted access.

Every communication session uses a different shared cryptographic key to reduce the risk of message compromise. As a result, the strength of symmetric cryptography relies on how well communication parties that wish to share data securely communicate using symmetric keys. The agreed-upon shared key has the same effect on both communication parties. We need an effective method to manage and distribute secret keys in order to distribute these shared secret keys. These shared secret keys are distributed by the Key Distribution Center (KDC). Each participant creates a shared secret key with the KDC in order to limit the number of keys. Each member of KDC receives a unique secret key. The member and the KDC are the only parties who may use this key. There must be a common secret key between users A and B if they are to communicate. Using their key with the KDC, A and B's session key may be created by KDC. Before the session, A and B authenticate themselves to the centre and to one another using their shared session key.

The two parties only utilize this shared session key once. One such protocol that employs several challenge-response exchanges between participants to produce an error-free protocol is the Needham-Schroeder protocol. Similar authentication protocols like Kerberos also function as KDCs. Problems with these protocols include the lack of a solid connection between the secret key and its owner. In contrast, symmetric key cryptography methods use a public key and a private key that are mathematically connected. The architecture of this cryptosystem makes it difficult to compute the private key from the public key. This public key is disclosed to the public and is used in encryption. It is necessary to keep the private key, which is needed for decoding, a secret. A few examples of public-key cryptosystems include the RSA (Rivest, Shamir, and Adleman) algorithm, elliptic curve cryptography, and the Diffie-Hellman key exchange protocol.

There is no need for extra key management strategies with this public-key cryptosystem. As the sole shared key is the public key, which is made known to the public, a secure channel is not necessary for exchanging the secret key. Public-key cryptosystems, however, are computationally costly and unsuitable for real-world applications. An aa an a,,arteminart an an e an e a In a symmetric-key cryptosystem, the symmetric key is utilized for encryption and decryption. While several authentication-based session key exchange protocols exist, none of them are able to create a reliable connection between the user and the secret key. Biometric data-based key management strategies have been suggested as a solution to this issue in order to create a solid connection between a person's identification and the accompanying cryptographic keys. This method, known as crypto-biometric systems, integrates biometric data with cryptography to offer robust security (CBS). In order to offer robust security, crypto biometric systems integrate biometric data with encryption.

To create a cryptographic key using biometric data, either a standard hash function or user-defined methods may be employed. Using both users' biometric data and conventional encryption allows two users to communicate via messages. Combining both users' biometric data while maintaining the privacy of both users' biometric data is the most difficult challenge. Since biometric data is ingrained, it cannot be changed if it has been compromised, unlike pin numbers or passwords. The notion of a cancelable template has been floated in the literature as a potential solution to this problem while simultaneously maintaining the privacy of biometric data. The original biometric template is transformed one way to create the cancellable template. Thus, it is better to derive cryptographic keys from the user's

cancellable template rather than straight from the original biometric template. A session key-based protocol has been suggested in this chapter. A shuffle key given by an authentication server is utilised to construct a 128-bit session key using the fingerprint templates of the communicating parties.

Before sharing the user's original biometric information with the other party, the biometric data is first converted into a cancelable template. In this way, the confidentiality of biometric data is also maintained. There is no need to disclose the secret session key in order to begin communication between the two parties since the session symmetric key is produced by both sides independently [1]–[3].The network's ability to communicate information is becoming better every day. Not only is data storage crucial, but data transmission over the network is also important. Network security becomes crucial when exchanging information over a public network because data must be shielded from unwanted access. Network security refers to more than just the safety of the computers at each end of the communication chain; it also refers to the security of data transfer via any susceptible communication links. In order to get the data and alter it, an adversary might attack the communication route. Network security is thus just as important as PC security and message encryption. The three security services listed below must be accomplished while creating a secure network.

Availability It is guaranteed by this security feature that only parties with permission may use a certain communication channel.It is the most typical component of a security objective. Confidential information must be safeguarded by making sure that only the intended recipient can see the message. Information must be sent in a confidential manner, as well as stored in a confidential manner.Integrity Changes to information must only be made by authorised organisations. The recipient is assured by this security feature that the message they have received has not been altered in any way from the original.Information security is greatly aided by cryptography, which conceals data that only authorised users may access. It is used to send data across an unsecure connection in a safe and private manner while preventing data tampering and listening in. Security objectives are pursued via the use of cryptographic techniques including public key, asymmetric key, and private key, symmetric key algorithms. Nevertheless, the issue of key distribution and sharing plagues this private key or symmetric key encryption. Key management, which includes key sharing, maintaining key secrecy, and key distribution, is necessary for symmetric cryptography.

As both the encryption and decryption techniques employ the same key, key exchange is required between the communicating parties before any communication can take place. Keys with more bits are more difficult to memorise. Integration of biometrics with cryptography under the existing situation, where keys are created and distributed through an unsafe route, is one likely approach. Moreover, in biometric-based cryptography, the biometrics of the two communicating parties may be utilised to generate a cryptographic key that links the users together and satisfies their need for non-repudiation of the communication. It may be difficult to directly derive cryptographic keys from biometric features. This is so that, unlike a password or PIN number, if the biometric information is hacked in any way, it cannot be changed. Biometrics-based cryptographic keys must not be reversible so that the reverse calculation is not possible. To put it another way, hackers would not be able to determine the user's biometrics from the cryptographic key if the key were hacked in any way. This is the rationale for the current research project's use of the cancelable biometric concept for the direct production of a cryptographic key using a user's cancelable fingerprint biometric. The use of biometrics in creating session key generation and authentication protocols has been suggested in several schemes, but none of them fully exploits the capabilities of biometrics in all areas. These all-important contemporary security concerns served as the impetus for developing a session key generation technique that is impervious to security intrusions, an

improved system to safeguard user templates, and a biometric template storage scheme that uses the least amount of space possible.

DISCUSSION

Earlier works that deal with protocols that are specifically created for exchanging crypto-bio keys or protocols that provide biometric-based secure authenticated sessions. A biometric-based remote authentication mechanism using fuzzy extractors was presented by Boyen et al. The issue with this technique is that it simultaneously keeps the protected crypto-biometric template and the reference biometric template. While this reference biometric template is kept confidential, there may still be a tradeoff in terms of privacy. One-time biometric authentication protocol was proposed by Ueshige and Sakurai, however it necessitates the storage of traditional biometric templates and creates biometric authentication-based secure sessions. In this protocol, a one-time transformation that is specific to the session is created. Both the new biometric data and the saved templates are subjected to this change. Tang et al. offer an authentication mechanism based on a fuzzy extractor. This protocol uses the ElGamal public-key cryptosystem to provide security[4].

In 2009, Fan and Lin suggested a three-factor remote authentication system that makes use of smart cards, passwords, and biometrics and uses fuzzy sketches and key regeneration on smart cards to secure keys. A technique for ePassport authentication based on elliptic curve cryptography was proposed by Abid and Afifi. They safely generated the elliptic curve parameters using fingerprint biometrics. The authentication of the ePassport bearer is done using these parameters. Since it needs a reliable, continuous input from biometrics, which is nearly not conceivable, this idea is just speculative, and no experimental assessment is recorded. A plan for privacy-preserving authentication using a fingerprint-based system was developed by Barni et al.The ElGamal cryptosystem, which enables biometric comparison in an encrypted domain, is used in this technique. A homomorphic encryption-based blind authentication approach was provided by Upmanyu et al. The subject can only be authenticated by a few authentication techniques.

The cryptographic keys needed for safe transmission, however, are not producible by them. Certain protocols in permit the use of the same keys during all sessions. It is hence susceptible to replay assaults. For secure communication in the modern world, the majority of practical solutions, such as the transport layer security (TLS) protocol, propose using a session-specific symmetric key. Every session generates its own set of session keys. To communicate this key, public-key cryptography methods are used. Scheirer and Boult put up the concept of "bipartite biotokens" combining fuzzy vaults with their prior suggestion of revocable biotokens which allows for the securely sharing of keys via biometrics. The client and the server share a set of transformations in this system. Every communication session involves the application of a new transformation. The bipartite biotokens allow for the sharing of session-specific data between two parties and are session-specific.

A technique called "Secure Ad-hoc Pairing with Biometrics: Safe" was put out by Buhan et al. and may be used to create a secure connection between two parties. The fuzzy extractor approach is used to get keys from biometrics. This protocol's disadvantage is that it demands mutual confidence between the two parties and calls for a secure channel in order to exchange the biometric data. A unique secure key exchange mechanism leveraging the sender and receiver's biometrics was suggested by Barman et al.The key distribution issue in symmetric cryptography still exists in this approach, too, since the biometric-based key must be communicated over a communication channel.A model for a biometric cryptosystem that generates a symmetric key from the user's biometric was put out by Sarkar et al. Nevertheless, the resulting symmetric key does not undergo the suggested randomness

testing. The created key is also constant throughout all communication sessions. Relatively few studies have been conducted in the past to develop cancelable templates based on fingerprint biometrics for symmetric and asymmetric cryptographic keys for safe communication between two users. The suggested method first converts biometric templates into cancellable ones before combining the cancellable templates of both users. Next, using that cancelable template, cryptographic keys are constructed. By Barman et al. a method of distributing cryptographic keys based on biometrics has been developed. Chakraborty et al. have suggested utilizing Cartesian transformation methods to generate cancelable fingerprint templates. Barman et al. have put forward a number of methods for creating revocable cryptographic keys using combined cancelable sender and recipient biometric data. Moreover, symmetric cryptography using this biometric-based key enabled safe communication between participants.

Sharing of the secret key presents the biggest problem in symmetric key cryptography. Symmetric key cryptography requires the use of a single key, which must be secured against unwanted access. Every communication session uses a different shared cryptographic key in order to limit the quantity of messages that may be compromised by a key breach. As a result, the strength of symmetric cryptography relies on how well communication parties that wish to share data securely communicate using symmetric keys. These shared secret keys are distributed through a key distribution center. In the modern day, smart cards or knowledge-based authentication are employed to certify the confidentiality of key exchange protocols. Yet, there is a serious issue with this kind of approach.

There is no proven connection between a secret key and its owner. Crypto biometric systems employ a combination of biometric data and cryptography to create a connection between the user and the key and to provide excellent security. To create a cryptographic key using biometric data, either a standard hash function or user-defined methods may be employed. Combining both users' biometric data while maintaining the privacy of both users' biometric data is the most difficult challenge. Since biometric data is ingrained, it cannot be changed if it has been compromised, unlike a pin number or password. One of the likely options is a cancellable template, which is a one-way change of the initial biometric template. So, to preserve the privacy of user biometrics, it is better to derive cryptographic keys from the user's cancellable template rather than straight from the original biometric template. In this chapter, session keys are generated using the fingerprint templates of communicating parties and a shuffle key supplied by an authentication server.

Before sharing the user's original biometric information with the other party, the biometric data is first converted into a cancelable template. In this way, the confidentiality of biometric data is also maintained. The session symmetric key is generated by each party involved in communication. As a result, the session symmetric key is not required to be shared by the communication parties. The server is key in this situation. User A and User B authenticate with one another and provide each other their public key certificates before sharing their cancelable templates. One of the parties, say A, receives a random shuffle key from the server. After that, User A hands User B the random shuffle key. Only the authorized users A and B will have access to the server's key and be able to create the final session key. This server-generated random shuffle key is only good for one session. It assists both parties in establishing mutual trust with the server, guards against either of them being impersonated, and also randomises the components of the combined template. This chapter also analyses the suggested approach's security effectiveness.

Using the Suggested Protocol in a Cloud Scenario at Number Seven. Through the Internet, cloud computing offers shared services and computational resources. Internet use has

increased significantly over the last several years, driving up hardware and software costs. Sharing resources is a concept that cloud computing has developed to lower total costs. There are four different kinds of cloud computing networks. They include communal, hybrid, private, and public clouds. Several organisations that exclusively belong to one community share a community cloud. Private clouds are very secure, hold just the user's private information, and are not shared. Depending on its use, hybrid clouds may be either public or private. A public cloud is a platform where all of the computer power is housed at a business that provides cloud services. Cloud computing poses various security implications in addition to cost reduction, as will be discussed below.

Cloud Computing Abuse and Reprehensible Usage Foreign hackers take advantage of the straightforward registration processes, relatively open access requirements, and cloud services to Application Programming Interfaces that Are Insecure (API) Consumers may access cloud services using interfaces or APIs. Security must be included into the service models of cloud service providers. End users need to be informed of security risks concurrently [5], [6].Unsavory Insiders An increased hazard in the cloud computing environment is posed by malicious insiders. This is a result of customers' unclear understanding of rules and regulations. Insiders may get unauthorised access to cloud computing resources with malicious intentions.

Multi-tenancy/Shared Technology Problems Nature Security problems arise from multi-tenant architecture since the same cloud database may house data from several users.Data Blowout Composed data may comprise data that has been deleted or edited without a backup. Losing an encoding key while removing a record from a bigger context is possible. Once again, unauthorised access to sensitive data may cause significant losses for consumers.Service, Account, and Traffic Hijacking Attackers have access to crucial cloud computing service components including service availability, integrity, and secrecy. These assaults include phishing, fraud, and the use of software flaws, as examples.

The suggested approach may be used in a cloud environment without risk. In this case, the user is authenticated by a single authentication server. Users and the authentication server may both be a part of the hybrid cloud platform. When communication parties exchange biometric information, the information is highly encrypted using RSA public key encryption. Moreover, the data being transferred is cancellable using biometrics, therefore the message exchange is unaffected by cloud environment security concerns. It produced only valid for one particular session. Hence, key management and key distribution are addressed by this protocol. Due to the usage of both users' cancellable templates and the additional shuffle key from the authentication server, the produced key is random for each session. The National Institute of Standards and Technology's test methods are used to verify the randomness of the produced session key (NIST). This chapter also covers how the suggested protocol may be used to a cloud-based environment. This suggested protocol might soon be used to simply add other biometric data, such iris and facial scans[7], [8].

CONCLUSION

The main causes of cryptographic key management methods are key sharing and key management strategies. In this suggested biometric-based session key protocol, the final session key is generated using a combination of the cancellable templates of the communicating parties and a random shuffle key supplied by a reliable authentication server. The user is not required to memories or keep a cryptographic key on any device. It is not necessary for the two communicating parties to exchange the session key through insecure channels. Without the requirement to exchange the final session key, communicating parties produce the identical session key at their respective ends.A user must register with the

authentication server during the registration step. He does not need to register again if he has previously done so. If not, the authentication server generates a new ID. The transaction will become secure and the procedure will become authenticated after registering itself. The authentication server then provides a username and password for accessing the cloud when authentication with the server is complete. The user has to register in order to view the data throughout this procedure. At the same time authentication server transmits the username to cloud provider

REFERENCES:

[1] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG and fingerprint bimodal authentication," *Sustain. Cities Soc.*, 2018, doi: 10.1016/j.scs.2017.12.023.

[2] F. Abundiz-Pérez, C. Cruz-Hernández, M. A. Murillo-Escobar, R. M. López-Gutiérrez, and A. Arellano-Delgado, "A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map," *Math. Probl. Eng.*, 2016, doi: 10.1155/2016/2670494.

[3] R. M. Thanki and K. R. Borisagar, "Compressive Sensing Based Multiple Watermarking Technique for Biometric Template Protection," *Int. J. Image, Graph. Signal Process.*, 2014, doi: 10.5815/ijigsp.2015.01.07.

[4] P. V. Krishna, G. Sasikumar, and M. S. Obaidat, *Social Network Forensics, Cyber Security, and Machine Learning*. 2019.

[5] D. Das, S. Maity, B. Chatterjee, and S. Sen, "In-field Remote Fingerprint Authentication using Human Body Communication and On-Hub Analytics," *Conf. Proc. ... Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Annu. Conf.*, 2018, doi: 10.1109/EMBC.2018.8513667.

[6] M. Anuradha, A. S. Oliver, J. J. Justus, and N. Maheswari, "IOT based monitoring system to detect the ECG of soldiers using GPS and GPRS," *Biomed. Res.*, 2018, doi: 10.4066/biomedicalresearch.29-18-1126.

[7] R. Arjona, M. Á. Prada-Delgado, J. Arcenegui, and I. Baturone, "A PUF-and biometric-based lightweight hardware solution to increase security at sensor nodes," *Sensors (Switzerland)*, 2018, doi: 10.3390/s18082429.

[8] F. D. Tatar and M. Machhout, "Improvement of the Fingerprint Recognition Process," *Int. J. Bioinforma. Biosci.*, 2017, doi: 10.5121/ijbb.2017.7201.

CHAPTER 5

CLOUD COMPUTING SECURITY FRAMEWORKS FOR MOBILE DEVICES

Ms. Samreen Fiza, Assistant Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - samreenfiza@presidencyuniversity.in

ABSTRACT:

The concept of mobile cloud computing (MCC) has increased the potential of mobile computing by merging it with cloud resources. Cloud services may be used to get around mobile devices' memory, battery, and other computing resource limitations. Mobile cloud computing applications may be able to ease some of the challenges associated with resource limitations by moving work to cloud servers. Despite these advantages, mobile cloud computing is still not widely utilized because of a variety of security-related challenges, including difficulties with invoicing models, service level agreements, privacy concerns, access control issues, and interoperability. The topics of security in mobile cloud computing and the crucial elements of a security framework for MCC are the main focus of this chapter. We first outline key designs applicable to a number of mobile cloud computing applications before examining a few security frameworks given for MCC in terms of controlling privacy, security, and risks.

KEYWORDS:

MobileCloudComputing, MobileComputing, Security, Cloud Resources.

INTRODUCTION

With wireless connection becoming commonplace, mobile computing is integrating into daily life. Mobile phones are currently used more and more as a computer device because to technical advancements in mobile devices and the invention of smart phones, which have changed how they were traditionally used for voice communication. Incorporation advanced features like an internal camera, GPS, multimedia capability, etc. provided mobile devices extra functionality. The primary factor fueling the development of mobile computing is the variety of tasks that mobile devices are capable of carrying out. The processing and software overhead on mobile devices are increased by all these cutting-edge capabilities. In addition, software development for mobile devices is progressing more quickly than hardware development. Due to the physical restrictions of mobile devices, such as their restricted processing power, storage space, and battery life, users are unable to fully use these sophisticated functionalities [1]–[3].

With Internet connectivity growing more and more widespread over the last ten years, connecting to a cloud server from a mobile device is no longer a challenging task. As a result, the notion of employing cloud resources to meet the processing and storage needs of mobile devices was inspired, and the concept of mobile cloud computing was born.

Under this paradigm, storage chores, communication tasks, and computation-intensive jobs are offloaded to cloud servers rather than being completed on mobile devices themselves in order to get over the aforementioned hardware limitations of mobile devices. Just the thin client will remain on the mobile devices for user interface or result presentation. Apps like YouTube, Facebook, and other mobile applications are examples of such thin clients.

Smart phone use and mobile cloud computing are both expanding quickly. Global mobile cloud computing customers increased from 42.8 million in 2008 to over 100 million in 2014, according to industry intelligence firm ABI Research (Allied Business Intelligence, Inc.). According to a different Juniper Research research, the market for cloud-based mobile apps increased from $400 million in 2009 to $9.5 billion in 2014, a growth of roughly 88%. According to reports, more than 240 million users of mobile cloud computing (MCC) would make use of cloud services in 2015, generating 5.2 billion dollars in income. According to Gartner, worldwide mobile phone shipments would rise 1.6% in 2018, with a total of over 1.9 billion devices sold. It will increase by 5% year in 2019. It is now possible to improve applications like location-based services, information exchange, etc. thanks to the advent of mobile cloud computing.

The need for cloud computing has expanded quickly in recent years in line with the expansion of network capacity, the development of virtualization technologies, and the emergence of cloud-based business needs. By 2013, mobile devices will surpass PCs as the most popular online access devices globally. Hence, cloud computing and mobile technologies will be combined in the future Internet work environment. Data processing and storage that takes place outside of the mobile devices from where an application was launched is known as mobile cloud computing (MCC). A mobile entity also includes cloud resources, infrastructure, services, and users, making it more comprehensive than just a mobile device. Similarly, MCC is a cloud-based system where mobility affects the infrastructure, resources, services, user devices, and even people. Unlike traditional computers, MCC has given birth to a number of problems that cause people to hesitate and feel dread. Concerns about privacy, data ownership, and security are a few of these challenges. Several of these issues are particularly important for mobile devices. The main goal of this work is to provide an overview of security in MCC, however in order to completely comprehend MCC and security in MCC, it is crucial to have a thorough knowledge of Cloud Computing [4]–[6].

Using the Cloud Sharing resources and shared infrastructure has been made much easier thanks to cloud computing. Because of this, it is now feasible to provide on-demand services across the network to meet a variety of modern business demands. The final user in this kind of dynamic corporate environment is unaware of where the available physical resources and tools are located. Applications that are developed, used, and managed "in the cloud" require the virtualization of resources that are maintained and directed by facilities that are made accessible to users. An previous Cloud Security Alliance guideline had an impact on how researchers at the National Institute of Standards and Technology (NIST) in the United States described cloud computing. The Working Definition of cloud computing, which was developed in conjunction with the NIST, has generally been favorably received. Because of the consistency and agreement around a single language, we can focus on concrete examples rather than conceptual nuances. As a consequence, businesses all across the globe adopted and used this approach. Nevertheless, as the NIST is a US government agency, the widespread acceptance of this definition should not be interpreted as ignoring other viewpoints or those from other nations. The NIST definition of cloud computing included

three cloud service models, four cloud deployment types, and five fundamental characteristics.

A description of the use of mobile cloud computing for emergency services and disaster recovery can be found. While the idea of employing cloud resources has increased the usefulness of mobile computing and given it the freedom to execute any activity, the security and privacy concerns related to cloud computing are preventing its widespread acceptance. Notwithstanding the research that has been done, both in business and academia, there are still a few security gaps in mobile cloud computing. Surveys indicate that 74% of IT executives are not interested in using cloud services because of the risks and security concerns involved. Applications that need a lot of compute and storage on a mobile platform face several additional constraints, such as low processing power and storage. Since data from mobile users is processed and kept in clouds that are hosted at the service, there are significant threats to data security, including data loss, breach, and privacy.

DISSUCION

Mobile devices and cloud computing are two key technical advancements that have emerged in recent years. Mobile Cloud Computing is the result of the integration of cloud computing, mobile computing, and wireless networks to enable the provision of powerful computational resources to mobile users. Rich computing resources are readily available, which benefits both network operators and cloud service providers. All of the processing and storage capability that was previously housed by mobile devices is now moved to more potent and centralised platforms found in the cloud thanks to mobile cloud computing. By using on-demand self-service, it offers a variety of IT resources and information services through the mobile network. By fully using cloud computing, mobile users are given access to new types of services and facilities. Instead of being contained on a single local computer, resources in mobile cloud computing are dispersed among a number of virtualized distributed machines [7]–[9].

For the benefit of customers and businesses, several businesses provide a variety of mobile cloud solutions, such as the Android operating system provided by Google. Google has introduced new services like geographic search and Google maps using mobile devices and cloud computing.A platform with software and services called Live Mess was created by Microsoft, allowing users to access and share their data and apps. For the purpose of data backup and storage for apple customers, Apple created iCloud. The hardware limitations of limited calculating power and storage capacity may be overcome via mobile cloud computing, which also enables easy access to data.Recently, there has been a lot of interest in mobile cloud computing since it enables data processing and storage outside of mobile devices. It is becoming more and more popular as smart phones that function as small Computers proliferate. By transferring the processing and storage to a cloud, the mobile device's drawbacks, such as its smaller size, poor battery life, and other aspects, may be fixed. A faraway data centre, a local computer or group of computers, or even nearby mobile devices, may receive the offloading.

A framework called cloud computing allows various mobile devices to share resources, data, and software capabilities. The materials will be accessible through the cloud and available for the devices to distribute as needed. The client may utilise the cloud in a mobile cloud computing environment to backup data on mobile devices. General Purpose Mobile Cloud Computing (GPMCC) and Application Specific Mobile Cloud Computing (ASMCC) are the two main methods used to implement mobile cloud computing. Without using any programmes created especially for this purpose, GPMCC uses the internet through mobile devices to access the processing power of distant computers. To exploit the cloud computing

infrastructure, customised mobile apps are created at ASMCC. ASMCC technique is used for the deployment of the cloud service known as Mobile Service Clouds, which was first suggested in. Author: Cochin University of Science and Technology, India.According to, there are two main types of mobile cloud computing: those that utilise mobile devices as thin clients to offload computation to internet-based cloud services, and those that employ them as computational and storage nodes as part of a cloud computing infrastructure.

Despite significant advancements in processor power, memory, and operating systems, mobile devices still have several significant flaws. The data transport bottleneck in cloud computing is the main obstacle for mobile devices. As batteries are the main energy source for these gadgets, advancements in battery technology have not been able to keep up with the power demands of rising resource demands. In the foreseeable future, mobile phone customers' typical time between charges is probably going to decrease by 4.8% annually. Infrastructure scalability becomes a problem as the cloud's popularity and size increase. Growth will lead to an overly high network load and an undesirable service response time without a scaling solution.

Data caching is often used in wired and wireless networks to increase the effectiveness of data access by lowering the end-users' perceived latency or waiting times. Data that is likely to be utilised again is temporarily stored in a cache. Caching is successful in the computing field because locality of reference is seen in access patterns in typical computer applications [3]. Network latencies and bandwidth consumption may be effectively reduced by caching. Holding frequently visited data items in a mobile node's local storage may decrease network traffic, response time, and server load in a wireless mobile network. The neighbour nodes may work together to serve each other's misses in order to fully benefit from caching, thereby lowering wireless traffic [10].

The majority of mobile cloud computing apps require data interchange with cloud servers that are out of the control of mobile users. Private user information, such as a user's location or use patterns, may also be included in this information. Thus, it is crucial to safeguard sensitive user information from intruders. A prospective enemy may likewise be thought of as a cloud provider as it is also a third party. The fundamental and required elements of security in mobile cloud computing would be (1) authentication, (2) data integrity and confidentiality, and (3) privacy. The security needs in MCC may vary somewhat depending on the application.

Authentication Mobile users employ cloud resources for storage purposes in mobile cloud computing, offloading compute and communication responsibilities. There should be an authentication method between mobile users and the cloud since a large number of users will be using cloud servers. Virtualization and cloud-based image maintenance are both employed in the before described MCC architecture. With this design, further virtual image-to-virtual image authentication is necessary.Integrity and confidentiality of data Using cloud resources to store user data is one of the key uses for cloud computing. One of the main benefits of mobile cloud computing is this. Mobile devices often have a certain amount of storage. Files are offloaded to cloud servers in order to get over this restriction and make them accessible anytime, anyplace. Cloud service providers might potentially be a potential enemy since mobile users do not have control over the cloud servers. For the contents saved on cloud servers to remain secret and intact, effective encryption techniques must be in place. Moreover, users should have the ability to check the consistency of files at any moment.

Privacy Mobile users regularly connect with cloud servers to access their resources in mobile cloud computing. The mobile user's privacy must be safeguarded in this procedure from the cloud service provider as well. This is especially crucial in certain applications, such as

mobile cloud computing-based location-based services, where the user location information has to be secure from third parties.Using an implicit authentication approach allows for safe authentication. To protect users' privacy, observable user data is gathered and saved on a data aggregator after being hashed at the mobile client. This data is used by the implicit authentication engine to provide results for the implicit authentication consumer. Nevertheless, to do this, the mobile client must often employ the hash function each time user-related data is sent to the data aggregator. The mobile device may have to do more computations as a consequence. The proposal put up by Zhao et al. in of combining biometric data together with encryption or a secret key for authentication may be implementable in the future since biometric sensors can fit into mobile devices. Nevertheless, not many mobile devices currently on the market have biometric sensors to execute the suggested architecture. Moreover, there are certain drawbacks with biometric features. They are more likely to have issues like false acceptance, attacks by the closest imposters, changes in fingerprints with age, etc. The safe storage of biometric data presents additional difficulties. Moreover, since biometric science is continually evolving, a thorough investigation of the difficulties connected with employing biometric encryption is also necessary.

The plan put out in and another authentication framework by Zhou et al. are comparable. Nevertheless, this one could be more secure than since it takes into account additional factors when creating context-aware data for a specific user, such as periodic events, location information, and others. Nevertheless, with this method, changing the user's context data in the cloud may also result in communication and compute overhead for the devices. The authors explain how the most reliable way for protecting against unauthorised and illegitimate clients is biometric authentication of individuals. The authors haven't, however, actually used the log files or even replicated them using their plan. They should also revise their access regulations since gatecrashers, the cloud provider, and others may use them to track down unauthorised attempts to access data. The authentication framework suggest using a middleware layer with an interface to social media networks to manage authentication with Amazon S3 on behalf of mobile devices. Nevertheless, this plan once again has the issue of first identifying with the middleware using an ID and password. Hence, if the user uses social media to identify himself to the middleware, and if the attacker can get the user id and password via phishing or other social engineering methods, he may access both the data stored in Amazon S3 and the user's social network accounts.

Consolidated IDM (CIDM), a novel IDM architecture that mitigates potential vulnerabilities, was presented by the authors in. Nevertheless, the authors did not look into the likelihood, effects, or preventative measures of cloud provider breach brought on by, say, altered binaries, hostile insiders, or maliciously inserted malware. Moreover, the insufficient dynamic federation and agile mechanisms in present IDM systems, which are architectural concerns and need to be addressed at the design level, have not been addressed by the authors. Through cross-certification between service providers and mobile operators (MO), the suggested strategy in preserves the MOs and builds a trustworthy foundation. While PKI is necessary for mutual dependence-based communication and ID management by service providers, the authors have not assessed the context of DoS attack, which should be done regularly. More research on the PGP algorithm is also required. The security scheme proposed in previous research by Panneerselvam et al. is based on the concept of creating a tunnel using secure shell protocol and secure file transfer protocols for secure migration of Weblets from mobile to cloud and vice versa.

This security scheme is one of many presented for computation using MCC. While the plan is simple and workable, it necessitates a further effort of ongoing tunnel monitoring since attackers may exploit the tunnel to get over the firewall on either side. It is shown that the

MobiCloud framework put out by Huang et al. in improves MANET functioning. Nevertheless, the authors did not take the reliability of the cloud node into account while developing the suggested security method. Information on mobile users should be safely kept in the cloud as well. Zhang et al. proposal for an elastic mobile cloud application paradigm may be found in. Moreover, they put forward a security architecture that would feature safe Weblet installation, secure Weblet migration, authentication across Weblets, and secure Weblet authorisation. Despite the fact that the suggested approach guarantees a safe installation, it makes no mention of the security danger to Weblets after they have been installed in the cloud. Changes to DEM and CES setup are possible if an attacker can alter the Weblet's code in the cloud.

The security method suggested by Chen et al. to protect the privacy of LBS users is based on the notion of employing hashed IMSI numbers, which is one of the privacy preservation security strategies that have been described. But, if the genuine user's IMSI number is taken, the whole system collapses. Xiao et al. offered another privacy-preserving approach that was covered in this study. It is built on the idea of dynamic credentials, where the credentials are continually modified depending on user and cloud communication. Yet in this plan, a cloud that is also a third party is taken into account to be a trustworthy entity, which is a very solid premise. Wang et. al. privacy-preserving architecture for location-based services employing mobile cloud computing is another privacy-preserving plan. Nevertheless, the historical lower limit of the number of users in each grid cell is what determines how accurate the suggested technique will be. This is due to the fact that it estimates the number of users in each grid cell based on past data, which may be inaccurate at that precise moment and compromise privacy. A significant processing power difficulty as well as a two-tier network coding challenge must be overcome by improving secure pseudonym schemes to safeguard the privacy of mobile cloud data and unconditionally secure lightweight network coding pseudonym schemes.

Regarding safe storage frameworks, a secure data storage plan based on proxy re-encryption and identity-based encryption has been presented. In order to upload files to the cloud, mobile users must first undertake cryptographic procedures, which use a significant amount of energy. This approach is intended to offload the majority of security chores to the cloud. Moreover, using cloud resources for all cryptographic work may result in higher customer use fees. also put forward a security architecture based on an attribute-based data storage system and privacy-preserving CP-ABE. It has been shown that the underlying CP- ABE system has linearly growing ciphertext as the number of characteristics increases. The suggested method has the same flaw since it too uses a kind of CP-ABE.

Another idea put up by encrypted the data using common asymmetric encryption methods before storing them on cloud servers. Nevertheless, this procedure increases the computational burden on mobile devices. The security architecture put out by Itani et al. gives mobile users a mechanism to check the accuracy of data kept in the cloud. This plan is built on trusted computing and incremental cryptography. For two primary reasons, the suggested security system is undeniably energy-efficient. First off, by using incremental MAC, we can avoid computing the hash value for the whole file every time it is modified, considerably reducing computation load for the mobile client. Second, the crypto coprocessor handles the job of calculating the MAC value for the file(s), thus the mobile client just has to compare MAC values when confirming the integrity of the file(s). Nevertheless, the suggested plan merely offers a mechanism to check the consistency of the cloud-stored file. While data are sent directly to the cloud and in a cloud computing environment, the cloud service provider is also a third party and might potentially be an enemy, it does not safeguard the contents from modification or illegal access.

The authors of presented a deep learning model for cyberattack detection, however they haven't tested it on actual devices or assessed its efficacy in real time. However, they haven't compared the deep learning model's energy use and detection time to those of competing approaches. The authors of this work explain sophisticated risk management techniques to reduce losses brought on by cyberattacks, including how to choose the best security measures, deploy software and hardware, and cope with various sorts of assaults. The relationship between security and insurance providers, however, has not been investigated using bundling tactics and matching theory. They also concur that they haven't looked at how a direct loss relates to its indirect losses. The ExpSOS system with the security parameter was proposed in the work and is cost-aware in that it may provide various degrees of security at various computing costs. Thus, it is challenging to estimate the price of full procedure in advance. The authors recommended using Boolean circuits and private pseudorandom bit sequences that the servers employ to generate jumbled circuits. Even if the assessing server conspires with all but one of the cloud servers that took part in the building of the muddled circuit, this strategy protects the confidentiality of the client data. For the purpose of detecting security risks and malicious assaults, the authors of this research presented a deep-learning-based model that would include location data into the detection framework. Yet, managing streaming and quick-moving input data while using it to train a deep learning model is a major difficulty.

Since mobile cloud computing is an offspring of cloud computing, it shares many of the security problems with the latter. In designing the security frameworks, it is also important to take into account the additional MCC restriction of the restricted computational resources at the mobile device end. Hence, certain security concepts that are effective for cloud computing may not be appropriate to MCC. Frameworks that are lightweight are required for mobile cloud computing. To prevent overhead on mobile devices, every framework we examined in this chapter does CPU-intensive activities in the cloud. Hashing and other computationally intensive cryptographic operations are made to be offloaded to the cloud. This idea of offloading compute chores really becomes a trade-off between energy saved at the device side and costs paid for the cloud use since cloud services are often priced depending on usage.

Major Mobile Cloud Computing Problems

Mobile devices, networks that connect them to the cloud, and mobile apps are the essential components of a mobile cloud computing strategy. Mobile devices and wireless networks, the first two parts, provide the biggest obstacle to cloud computing. Due to this, mobile cloud computing deployment is more challenging than that of stationary clouds. The key problems with mobile cloud computing are listed in this section.

Mobile devices have certain restrictions: Mobile devices lack the processing power, display quality, storage space, and energy resources of personal computers. Despite significant advancements, smart phones still have a limited battery life.Network Latency and Bandwidth: In contrast to wired networks, which rely on a physical connection to guarantee bandwidth constancy, mobile cloud computing leverages wireless networks for data transport, making bandwidth a critical problem. Also, cloud services may be distant from where mobile consumers are, which raises network latency.

Heterogeneity

Mobile networks and mobile devices are the two main sources of heterogeneity in mobile

cloud computing. The group of users who share the network utilise a variety of mobile devices. The operating system and application software used by various devices differ, which has a significant impact on how well they work together. The many radio technologies used to reach the cloud is another field. Changes in bandwidth and network overlay will result from this.

Services Offered:

Service accessibility is a crucial concern in mobile cloud computing. There is a chance that mobile clients won't be able to connect to the cloud because of network problems, traffic congestion, and signal problems.Security and Confidentiality Cloud computing and storage offloading raises trust and security concerns. If the cloud services stop working owing to any technical problems, mobile clients might lose their data [11]–[13].

CONCLUSION

Despite the limited resources in their mobile devices, mobile cloud computing (MCC) offers users of mobile devices a wealth of resource capabilities. At the beginning of this chapter, we covered the significance of several mobile cloud computing frameworks and their inherent benefits. Secondly, we discussed the main mobile cloud computing architectures and the main security features in this environment. The security frameworks that have been suggested for mobile cloud computing were then analyzed. Using mobile cloud-based services presents substantial privacy challenges, especially when processing mobile users' data or apps and moving them from mobile devices to heterogeneous dispersed cloud servers situated in various places. After that, the topic of privacy concerns in the context of mobile cloud computing has been covered. Also, we spoke about possibilities for mobile cloud computing security in terms of both storage and compute. After presenting an overview, we contrasted several methods and compared them with potential directions for future research in the discussion section that followed. Consequently, for individuals who are interested in doing research and developing applications in this field, this chapter will be a useful summary of the security work in MCC.

REFERENCES

[1] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2917555.

[2] T. Bhatia and A. K. Verma, “Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues,” *J. Supercomput.*, 2017, doi: 10.1007/s11227-016-1945-y.

[3] D. S. Abd Elminaam, F. T. Alanezi, and K. M. Hosny, “SmCACC: Developing an efficient dynamic secure framework for mobile capabilities augmentation using cloud computing,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2929954.

[4] R. Somula and R. Sasikala, “A survey on mobile cloud computing: Mobile Computing + Cloud Computing (MCC = MC + CC),” *Scalable Comput.*, 2018, doi: 10.12694/scpe.v19i4.1411.

[5] Y. Mansouri and M. A. Babar, “A review of edge computing: Features and resource virtualization,” *J. Parallel Distrib. Comput.*, 2021, doi: 10.1016/j.jpdc.2020.12.015.

[6] A. Alreshidi, “Towards security as a service to protect the critical resources of mobile computing devices,” *Int. J. Adv. Comput. Sci. Appl.*, 2018, doi: 10.14569/IJACSA.2018.090549.

[7] A. Kumari, V. Kumar, M. Y. Abbasi, S. Kumari, P. Chaudhary, and C. M. Chen, "CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3001152.

[8] U. Shaukat, E. Ahmed, Z. Anwar, and F. Xia, "Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges," *Journal of Network and Computer Applications*. 2016. doi: 10.1016/j.jnca.2015.11.009.

[9] Z. Ning, X. Kong, F. Xia, W. Hou, and X. Wang, "Green and Sustainable Cloud of Things: Enabling Collaborative Edge Computing," *IEEE Commun. Mag.*, 2019, doi: 10.1109/MCOM.2018.1700895.

[10] K. Huang, X. Liu, S. Fu, D. Guo, and M. Xu, "A Lightweight Privacy-Preserving CNN Feature Extraction Framework for Mobile Sensing," *IEEE Trans. Dependable Secur. Comput.*, 2021, doi: 10.1109/TDSC.2019.2913362.

[11] T. A. Khoa *et al.*, "Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study," *Wirel. Commun. Mob. Comput.*, 2020, doi: 10.1155/2020/8896637.

[12] M. Abbasi, E. Mohammadi-Pasand, and M. R. Khosravi, "Intelligent workload allocation in IoT–Fog–cloud architecture towards mobile edge computing," *Comput. Commun.*, 2021, doi: 10.1016/j.comcom.2021.01.022.

[13] J. Hu, K. Wu, and W. Liang, "An IPv6-based framework for fog-assisted healthcare monitoring," *Adv. Mech. Eng.*, 2019, doi: 10.1177/1687814018819515.

CHAPTER 6

ROLE OF CLOUD PLATFORMS IN DATA MANAGEMENT

Ms. Ashwini Bhat, Assistant Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - ashwini.b@presidencyuniversity.in

ABSTRACT:

Data security and data retrieval time are two equally crucial factors that affect the quality of data placement when developing data placement methods for cloud storage systems. To provide the quality-of-service guaranteed by the network/cloud service provider, we must strike a balance between data security and retrieval speed since these two factors are often mutually exclusive. The placement strategy should be flexible enough to take into account threat characteristics in order to ensure the data integrity of data stored on network storage nodes in the event of threats or cyberattacks. In order to determine the most susceptible threat type for each node, this is accomplished by incorporating machine intelligence into the network that is exposed to assaults.

KEYWORDS:

DataPlacement, MachineLearning, Security, Data Retrieval Time.

INTRODUCTION

With the advent of data-driven applications, quick and secure storage is essential. The effectiveness with which these programmes can provide correct results is often what defines their usefulness. Financial systems based on customer data, Internet of Things (IoT) systems based on sensor data, and programmes for driverless autonomous cars in smart cities all depend on the ongoing processing of massive amounts of data. Organizations are more hesitant to accept cloud storage as a viable option for their sensitive data because of the sensitivity of the information handled by these systems and the general worries surrounding security and privacy of cloud storage solutions. On the other hand, a scalable storage system with rapid reaction time is required by the data handled by large-scale applications.

By making a trade-off between both, strategic data placement may be helpful in simultaneously solving the problems of time performance and data security. Via a data placement decision unit, the cloud service provider (CSP) may put these strategic data placements into practise so that elite clients can be guaranteed of the highest level of protection for their stored data in accordance with their service agreement. By dividing the file into smaller pieces of data and dispersing it throughout the network, data fragmentation is a common method for achieving data security. Fragmentation makes sure that no valuable information is revealed, even if the attacker manages to get a single piece of data. Data replication is one of the extensively used strategies to decrease the time it takes to retrieve data. Data retrieval time may be decreased by spreading several copies of the same data across the network since there are more possible places from which to obtain the data. Current research on cloud storage security and performance optimization focuses on these two issues separately. While there are trade-offs involved, strategically integrating data fragmentation and replication may help solve both the concerns about data security and retrieval time [1].

Data breach or data loss on a cloud storage system may be caused by cyberattacks such Trojans, Denial of Service (DoS), Distributed Denial of Service (DDoS), Packet Forging Attacks, Application Layer Attacks, and Fingerprinting Attacks. As each storage node in the cloud may host several applications, it is vulnerable to different attacks and weaknesses. Based on the apps that are hosted on the nodes and historical data about network assaults, information about the most probable danger on each node within a specific data placement solution may help to enhance the data placement solution's overall security and quality. The network's logs may be used to find information about the assault. Machine learning methods may be quite helpful in determining the danger that is the greatest for a certain node. Depending on the apps hosted on the node and the frequency of application-based assaults, machine learning algorithms may be used to categories the nodes in various danger categories. Attack graphs or attack models that focus on a certain application or vulnerability may be used to train them. Systems may be made scalable and successfully deployed to multiple cloud topologies by employing machine learning methods. These flexible and scalable data placement techniques might be helpful in resolving cloud storage security issues in applications for smart cities.

Our most recent research, which was presented in unambiguously showed that ARRT, which yields a collection of Pareto-optimal solutions, provides users with a balance between desired security and retrieval time. We further evaluate the proposed locations using machine learning methods to help with placement decisions for specific data chunks to increase security. While the suggested method must be flexible to protect the data integrity in the event of attacks, our solutions ensure the shortest retrieval time and highest degree of security. The whole plan would only be workable at that point.Data replication is used in datacenters by Boru et al. in to enhance overall quality-of-service (QoS) by lowering network latency and bandwidth utilization, with a particular emphasis on maximizing energy efficiency. Data availability, response speed, and network congestion were efficiently addressed through data replication. Data replication is used to increase performance in by combining two tactics, the one to boost QoS and the second to reduce the cost and amount of replications. The authors of describe a strategy for data replication that is especially designed for a computing cloud context. This policy increases the availability of access to the data files, which in turn increases fault tolerance overall. These solutions which concentrate on enhancing the retrieval time performance through replication do not address the data security problem emerging from extra data copies. In order to preserve QoS and increase execution speed, network use, and replication frequency in data grids, Mansouri suggested a novel replica replacement strategy in.

To ensure response speed and security, the dynamic replica management technique chooses a replica depending on variables such past replica access, replica size, number of accesses, and security features. A significant factor in our proposed SDP approach is that the solution recommended by this strategy does not give customers the option to choose a data placement solution that fulfils their time and security criteria. Hudic et al. in propose a data fragmentation approach to ensure security and confidentiality for data stored on cloud platforms by classifying the data in accordance with user requirements into different confidentiality levels to use selective encryption, making this approach comparably efficient to general data fragmentation and encryption. The work in suggests an improved data fragmentation strategy to keep data private even when there is data reliance between the pieces. By recasting and resolving the problem of minimal and closed pieces as a constraint fulfilment problem, the information leaking issue is solved. Data fragmentation is used to enable sufficient data separation to avoid complete encryption and to give further privacy for distributed storage systems in.

Nevertheless, since there is extra complexity involved in merging the data pieces, these solutions do not take data retrieval time into account. Based on their worst-case execution durations for various file types, several data fragmentation strategies for cloud servers, including basic fragmentation, predetermined pattern, random pattern, and encryption with random pattern, were compared in. As a result, we may deliberately combine data fragmentation and data replication in our suggested SDP to solve both concerns about data security and retrieval time [2]–[4].

In, a solution to the data placement issue for a globally dispersed cloud storage environment is proposed. This solution uses mixed integer linear programming to lower overall costs while ensuring that performance and latency requirements are met. In, Khalajzadeh et al. provide a graph-partitioning based a strategy for maximising social media data placement that meets the necessary latency requirements while minimising data storage costs. Nevertheless, with the suggested data location option, these methods do not solve the issue of data security. By replicating smaller partitions rather than the complete dataset across the network, the data placement method described in uses data replication to enhance the performance of an Infrastructure as a Service (IaaS) cloud system. This suggested approach increases the resilience of workload misprediction and lowers storage needs, but it ignores the security concern brought on by data replication. The authors of provide a data placement technique that minimises storage costs while still meeting the needs of scientific users, accommodating large data sets, and taking other dependencies into account.

Although offering cost-effectiveness, this integer linear programming style ignores the problem of data security. A heuristic optimization technique was published by Matt et al. in to recommend a data placement solution in a cloud-based storage system. By analysing data access patterns to find the optimal solution, this method reduces storage costs and optimises latency while fulfilling QoS limitations. Data placement strategy based on ant colony optimization is used in to solve data security for intermediate data collected in a scientific procedure. In terms of data confidentiality, data integrity, and authentication access, the algorithm finds data centres that provide the highest level of data security for intermediate data. However while formulating a plan, the issue of data retrieval time is not taken into account. The use of machine learning algorithms in various cybersecurity applications is widespread. Suggests a number of machine learning-based approaches for cybersecurity intrusion detection, including artificial neural networks (ANN), Bayesian networks, clustering, decision trees, evolutionary computation, support vector machines, hidden Markov models (HMM), etc. A thorough collection of datasets for training machine learning models for intrusion detection at various network levels has also been supplied by the authors.

An ANN is used by an intrusion detection system (IDS) described in to evaluate the data gathered by an IoT device and spot a DoS assault. Internet packet traces were utilised to train the ANN, and a simulated Internet of Things network was used to verify its performance. Using the network traffic characteristic traits that distinguish DDoS attack traffic from legitimate traffic, Saied et al. in used ANN to recognise and defend against known and new DDoS assaults. The approach was used in actual physical settings to correctly identify DDoS assaults with a restriction of DDoS attacks utilising encrypted packet headers using both outdated and contemporary pattern datasets for training the ANN. As a result, machine learning methods like ANN may be quite helpful in cybersecurity applications. Our SDP-recommended data placement refined using machine learning offers optimised time performance with enhanced data security by ensuring data integrity and data availability in case of cyberattacks, in contrast to recent data placement strategies that focus on either data security or time performance separately. The authors of underline the necessity to protect

sensitive user identification data from smart city systems for transportation, healthcare, and intelligent surveillance against data breach and privacy leaks due to unwanted access and cyberattacks.

Yet, the computational burden associated with guaranteeing data security is a significant obstacle to boosting the overall effectiveness, since applications for smart cities demand large amounts of data processing. By limiting data overcollection, Li et al. Provide a mobile-cloud system to solve user privacy leaks in smart cities. The active strategy attempts to fully alleviate the issue of data overcollection while maximising the release of user operation pressure. The effect of this framework's implementation on on-time performance, however, was not taken into account. Consequently, using data placement techniques for cloud storage systems like SDP that concentrate on both retrieval time speed and data security may be extremely beneficial even for smart city applications [5].

DISCUSSION

Threat Categories in Machine Learning for Improved Security

Each node in the specific cloud network will host a different application. Different dangers may be present in various applications. Imagine a cloud network that hosts a collection of apps indicated by A and susceptible to threat types denoted by T such that A a1, a2, a and T t1, t2, , tn , where a1, a2, , a represent the applications and t1, t2, , tn represent the threat types. Here, we make the assumption that not every node will host every application. CSPs or network administrators may secure against either individual applications or individual threats, i.e., they can adopt either software-focused strategy or threat- focused approach for security against network assaults as detailed in. Applications a1, a3, and a4 may be affected by threat type t1, making nodes hosting any of these apps exposed to threat type t1. Thus, any nodes hosting any of these apps must be secured in order to combat threat category t1.

As an illustration of a software-focused approach, application is susceptible to threat types t1, t2, and t3. Let's assume that application a2 is another one that is weak to threat types t2, t5, and t6. As a result, any one of the threat types t1, t2, t3, t5, or t6 may be used to attack a node that hosts both apps a1 and a2.We can determine the most susceptible threat type for a given node based on the apps hosted on the node and the frequency of attacks leveraging a certain threat type. The security of data placement will be improved with the help of this information.

Several characteristics or traits for each storage node must be assessed in order to determine the threat type that is most likely to affect it. The underlying threat identification system must be updated as new storage nodes are introduced to the network or when new threat kinds are discovered there. This must be done without adding extra overhead via a laborious computing process. Only a learning entity can automate this procedure in order to meet this complex demand for near real-time processing. This implies that it will occasionally, or as needed, use the pertinent danger information in its learning process. Various CSPs use various cloud topologies depending on their preferences and resource availability, hence the probable threat detection system should be deployable regardless of the topology used. Since machine learning-based implementation is network topology agnostic, it can guarantee the system's adaptability. A neural network should thus be enhanced in order to fulfil the aforementioned objectives [6]–[8].

Multilayer perceptrons will be the machine learning model utilised to identify the most susceptible threat type. The following characteristics or inputs will be used by the neural network. Software installed on the node: Every network-accessible application has a matching input. If the node hosts that application, the input value for that application will be

1, else it will be 0. Even if each programme may be vulnerable to a separate flaw, there may be a situation in which two more apps are exposed to the same danger. The node will most likely be used to exploit that specific threat type in such a situation. It is crucial to understand the programmes that are hosted on each node. For instance, if there are four separate apps hosted on the network, each node will have four inputs: A, a1, a2, a3, and a4. This corresponds to the number of applications hosted on the network. The input values or feature values of application inputs corresponding to a1 and a2 will be 1, whereas the same for a3 and a4 will be 0 for this node, assuming that this node only hosts a1 and a2.

Attack Frequency:

Determining the exact threat type to which a specific node is most exposed requires more information than just knowing the apps hosted on that node. Attackers often target the same vulnerability over time in order to exploit certain threat categories. Consequently, it is crucial to understand the attack frequency that each threat type on a certain node is exploiting. The key to utilising these frequencies as input characteristics for machine learning is that nodes hosting the same apps but with distinct attack history data may be exposed to various threat types. For each danger class, there will be one input correlating to the frequency of assaults. Attack frequency bins are made in order to equalise frequency input between 0 and 1. The feature value is increased in 0.2 increments in accordance with the number of assaults.

It should be noted that the inputs or features are chosen such that, for each detection of an attack on a node, the characteristics specific to that node must be updated. In this manner, the number of write operations per each update is minimized.Training data and the attack model: An attack model was created and put into practise to gather threat labels that matched the node feature set in order to provide the training data needed to train the neural network. We provide an attack model that perfectly replicates scenarios in which a node is vulnerable to application-based assaults, as shown in [7]. As a result, much as in a real-world situation, the system developed using this attack model will be able to protect data integrity and stop data loss brought on by application-based attacks. The following presumptions and concepts were employed while creating the attack model to provide realistic quality training data that would accurately represent real-world circumstances.

The programmes won't all run on every node. As a result, it is less probable that the whole network would be affected while providing the service to customers. The network administrator or CSP is aware of hosted apps and any possible risks to exploit them. If multiple assaults are required to exploit a particular vulnerability, we boost the attack frequency feature value correspondingly. After an attack, modify the node's attack frequency feature values and accompanying threat category label.On cloud platforms, we carried out in-depth performance assessment tests. The sizes of the data chunks for the performance assessment of the previously described ARRT technique were arbitrarily selected to range from 150 to 300 units. According to the network standard, the transmission time for a unit amount of data between two nodes was normalised.In order to maintain consistency, we show a typical output from ARRT. Each node in the graph represents a placement solution that has the number of nodes necessary to hold the file's data chunks multiplied by the replication factor. We ran a thorough discrete event simulation to show how resilient each set of placements would be against an assault in terms of the number of storage nodes that may be compromised while maintaining the data integrity.

In a network with 200 nodes, we produced a total of 7000 attack events using the approach outlined in Section 4 and our attack model. In our assessment, an attack on a node indicates that the node is unavailable for communication or storage, and as a result, the data on the attacked node is no longer retrievable. The proportion of successful assaults that are resisted

by keeping at least one copy of each chunk available for retrieval is what we refer to as the resilience factor. This robustness factor will be used as a benchmark for contrasting the placement recommendations made by ARRT and SDP. The maximum number of nodes that may be attacked in each scenario will be equal to F P since the number of nodes attacked in each circumstance corresponds to the same threat type. For this experiment, the replication factor m was set to 3 and the number of pieces to 10. The proposed collection of nodes for the data placement technique corresponds to a random distribution of data chunks and their copies. As opposed to the ARRT method's random distribution across the same set of nodes, the SDP strategy places the data chunks and their accompanying copies in accordance with the neural network's output. We now use several ranges of F values, which serve to assess the quality of the data placement, to show how the effect of machine learning technique improves the resilience of the data placement solution.The ARRT approach works pretty effectively under the same threat type and therefore for few nodes assaulted. Unfortunately, the strength of ARRT placement eventually begins to decline as the number of attacked nodes rises. On the other hand, the resilience of the SDP solution is very high and constant. It is possible to efficiently avoid deploying copies of the same data chunk on nodes with the same threat category by using the information supplied by the learning model in SDP on the threat kinds of each node. Such data placement is more likely to occur when the hosted apps are evenly dispersed over the network, reducing the number of nodes that will share the same vulnerability.

While it is not as excellent as in the preceding situation, the quality of data placements with 1/m F (m 1)/m is still acceptable for a possibly safe data placement. In our example, the worst-case situation is that up to 20 nodes might be affected by the same threat type, which could lead to data loss for ARRT placement if they are hacked. According to ARRT placement, the robustness starts to rapidly decline as the number of attacked nodes exceeds 10 because, with a large number of nodes vulnerable to the same threat type, ARRT placements tend to place all replicas of the same data chunks on similar nodes, which has an impact on the robustness of the placement solution. the robustness of the more secure data places proposed by SDP remain consistently superior than ARRT since F is still within the safety limit. Such a value of F may appear on networks with uneven application distribution, making numerous nodes vulnerable to the same threat kinds.

This is an example of inadequate and unintentional application distribution, which the CSP should prevent in order to provide dependable quality-of-service. If an attacker takes advantage of that specific vulnerability and creates a disjointed network situation, it might cause a significant disruption if several comparable apps are hosted on the majority of the network's nodes. It should be emphasised that SDP-assisted data placement outperforms ARRT placement in terms of performance (when the number of attacked nodes is less than 20 in our experiment). Nevertheless, the resilience performance of data locations indicated by both algorithms dramatically declines with an increase in the number of attacked nodes. This demonstrates why F should stay within the allowable range for the data placement to be secure and dependable. By helping the service provider improve the data placement nodes initially recommended by ARRT, our suggested SDP technique improves the robustness and quality of service provided to customers. To the best of our knowledge, this research is the first of its kind to show how a neural network affects large-scale networked storage systems while also taking data security and retrieval time into account. As an immediate extension, one might employ different learning models like SVM/rule-based approaches to further improve the performance, even though this research provides as a clear representation of what a machine learning model may offer to boost performance [9], [10].

CONCLUSION

The two most important performance indicators for any storage system are data security and retrieval time. Data security requirements must get extra attention because of the ongoing danger of cyberattacks, particularly on cloud systems. In this study, we improved a multi-objective optimization data placement approach that balances retrieval speed and data security. This is accomplished by greatly enhancing the data integrity and security of the basic ARRT algorithm with an artificial intelligence paradigm, making the whole method a workable solution. For instance, we took into account application-based attack types in our simulations and especially created a training model that allows a neural network to learn the threat aspects that would be used to categorise in accordance with the most susceptible threat kinds

REFERENCES

[1] J. Han, W. Zang, M. Yu, and R. Sandhu, "Quantify Co-Residency Risks in the Cloud through Deep Learning," *IEEE Trans. Dependable Secur. Comput.*, 2021, doi: 10.1109/TDSC.2020.3032073.

[2] W. Ding *et al.*, "DFA-VMP: An efficient and secure virtual machine placement strategy under cloud environment," *Peer-to-Peer Netw. Appl.*, 2018, doi: 10.1007/s12083-016-0502-z.

[3] C. Delimitrou and C. Kozyrakis, "Bolt: I know what you did last summer.. In the cloud," *ACM SIGPLAN Not.*, 2017, doi: 10.1145/3037697.3037703.

[4] C. Delimitrou and C. Kozyrakis, "Bolt," *ACM SIGARCH Comput. Archit. News*, 2017, doi: 10.1145/3093337.3037703.

[5] A. Ramegowda, J. Agarkhed, and S. R. Patil, "Adaptive task scheduling method in multi-tenant cloud computing," *Int. J. Inf. Technol.*, 2020, doi: 10.1007/s41870-019-00389-5.

[6] K. G. Jeffery and L. Schubert, "Initial 2016 HOLACloud Roadmap," in *Procedia Computer Science*, 2016. doi: 10.1016/j.procs.2016.08.296.

[7] P. Naschekin, "Theoretical Justification of the Method Design of Information Security Systems in Virtual Environments and Cloud Platforms," *Vopr. kiberbezopasnosti*, 2020, doi: 10.21681/2311-3456-2020-06-14-22.

[8] S. F. Astika, M. Jauhari, N. Isbatuzzin, M. Salman, and K. Ramli, "BUILDING A DYNAMIC SCALABLE PARALLEL CLOUD-BASED SNORT NIDS USING CONTAINERS AND BIG DATA," *J. Southwest Jiaotong Univ.*, 2021, doi: 10.35741/issn.0258-2724.56.5.27.

[9] R. V. Kale, B. Veeravalli, and X. Wang, "A practicable machine learning solution for security-cognizant data placement on cloud platforms," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2020. doi: 10.1007/978-3-030-22277-2_5.

[10] F. Lamberti, V. Gatteschi, C. Demartini, M. Pelissier, A. Gómez, and V. Santamaría, "Blockchains Can Work for Car Insurance," *IEEE Consum. Electron. Mag.*, 2018.

CHAPTER 7

SECURITY CHALLENGES IN COGNITIVE RADIO AD-HOC NETWORKS

Ms. Amrutha Nair, Assistant Professor,
Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - amruthavnair@presidencyuniversity.in

ABSTRACT:

An intriguing subtype of opportunistic networks is the cognitive radio network (CRN). It is rapidly expanding in popularity as a result of its unusual capacity to address the issue of spectrum shortage. It has distinct security concerns than other wireless networks, particularly opportunistic networks, for the same reason. The chapter discusses the topics of study, security implications, and different methodologies put forward in the literature to address security-related research concerns. In order to save space, the image offers a succinct overview of the subject rather than a thorough exposition.Wireless networks have seen substantial expansion and popularity as a result of the general availability of inexpensive wireless devices. As a result, both the quantity of wireless applications and the size and complexity of those applications are continuously growing, as is the need for wireless spectrum.

KEYWORDS:

Security Challenges, Cognitive Radio Network,Security, Wireless Networks.

INTRODUCTION

Contrarily, 15–85% of the allotted spectrum, according to the FCC (Federal Communications Commission), a US-based organisation responsible for spectrum management, is underutilised as a result of random and regional changes. Hence, intelligent spectrum exploitation is urgently required. A remedy for the issue has emerged: the cognitive radio network (CRN). Software-defined radio (SDR) and the dynamic spectrum allocation (DSA) approach enable wireless devices to migrate from one frequency band to another at a little cost. Spectrum is used in a flexible manner. There are four fundamental phases to putting it into practise: spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility. Primary users (PU), who own the spectrum, and secondary users (SU), who utilise it when appropriate, are the two different kinds of nodes in CRNs. Hence, in order to establish a suitably stable network, the SU node must be informed of the behavioural activity of the main user. The Cognitive Radio Ad Hoc Network (CRAHN) or Cognitive Radio Mobile Ad Hoc Network are other names for the CRN [1]–[3].

A specific kind of wireless network is the CRAHN. Hence, a number of security issues in CRAHNs are comparable to security issues in other computer networks. In contrast, the security flaws in CRAHNs are rather distinct from the increased communication complexity brought on by asynchronous sensing, optimization of cooperative sensing, localization, joint spectrum choice, reconfiguration framework, etc.The chapter discusses security concerns in the decentralised architecture in which SU nodes interact with one another haphazardly. These sorts of networks' physical specifications are described in IEEE 802.11 b/c/g/f/h and IEEE 802.16. The SU node collaborates on a number of tasks, including spectrum sensing,

spectrum sharing, spectrum mobility, and spectrum management. The coexistence of one or more wireless networks operating in several unlicensed bands is also covered by the design. The CRAHN inherits general characteristics from mobile ad hoc networks (MANET), including decentralisation, mobility of nodes, dynamic topology, wireless connectivity, etc.; however, CRAHN-specific characteristics, such as spectrum mobility and limited authorization, have distinct security implications. A CRAHN node's ability to effectively utilise a channel, for instance, may be jeopardised by frequent interference from authorised users, which might result in system failure or subpar performance, and the network may experience congestion, interference, and jamming.

Networks for Cognitive Radio Ad Hoc

The CRAHNs may be seen in two separate sections. Three categories make up the main network: licensed-I, licensed-II, and unlicensed band. The xG ad hoc network, commonly known as CRAHN is a network that uses an unutilized band of PU(s). The CRAHNs are made up of a group of independent SU nodes. The SU node is capable of cognitive processing as well as reconfiguration. Spectrum sensing and mobility are handled by the cognitive capacity, while spectrum sharing and management are handled by the spectrum reconfiguration capability. A node learns about its surroundings, discovers spectrum gaps, and records them thanks to its capacity to sense. The local channel set refers to the group of channels that are accessible at Campus (LCS). A common channel perceived by two SUs is known as a common control channel (CCC), and the total number of channels detected by all participating SUs is known as the global channel set (GCS). The SUs are competent enough to make a choice based on local observation (s). These dots

The area of local observation is shown by the circle around the SU node. The breadth of learning and decision-making based on local observations is shown by the bold circle. A reconfiguration tool is included within the SU node to adapt to the surroundings. The SU node lacks comprehensive topological information because of independent behaviour. This might lead to collisions with both PU and other SUs. As a result, in order to create a network, the SU nodes interact and work together. The SU nodes may detect spectrum gaps from one or more radio environments in a linked component (s). Similar to this, an SU from one network may link to another SU from a different network.The following fundamental operations are used by linked SU nodes in CRAHNs:

Sensing the spectrum According to spectrum sensing, devices are able to detect their radio surroundings, choose the optimal band, and change to the best available transmission mode (for example, modulation type) in the open band. To identify the PU transmission, the SU node does a sensing operation either independently or collaboratively. The channel detection time, sensing band, and channel move time are among the SU's sensing characteristics. A weaker section of the PU band or free band may be used by an SU. The research in spectrum sensing has mostly focused on interference-based, cooperative, and transmission-based detection. The main goal of using these strategies is to find PU interference. PU shouldn't be affected by the signal that SU transmits. The SU nodes must opportunistically identify spectrum gaps due to the PU's random appearance [4]–[6].

Spectrum Evaluation

The secondary user examines several network features such as capacity, bit error rate, and latency to produce highly reliable as well as spectral efficient communication. Spectrum analysis deals with the detection of the capacity of spectrum holes. Many variables, including interference, route loss, wireless connection error, link layer latency, and concealed terminal issue, have an impact on spectrum characterisation. But, the random manifestations of PU in

the networks are the most harmful. In this situation, the SU node may pool its knowledge with other linked components and locate an appropriate alternative spectrum.

Spectrum Decision

The choice of the best available spectrum hole for transmission is referred to as the spectrum decision. It may be output by a number of cooperative SU nodes or taken by a single secondary user. Spectrum characterisation, spectrum selection, and spectrum reconfiguration are all parts of the spectrum choice process. The SU node reconfigures the spectrum operating frequency with the best spectrum hole after analysing the network parameters. The desired spectrum switching may be carried out beforehand in cooperative spectrum choice on the basis of feedback data from SU neighbours.

Applications of CRAHNs

The research community has recently been interested in the cognitive radio network because it provides a variety of intriguing applications; see Fig. 10.2. CRAHN may be utilized in a variety of contexts, including the military, private, professional, and emergency situations, like other ad hoc networks. Nonetheless, the following are some important CRAHN applications:

Defense Services

The CRAHN had its first testing at an American military defence laboratory. A crucial characteristic of CRAHNs that intrinsically improves information security is spectrum mobility. Yet, in order to increase security in walkie-talkie, conflicts, terrorist attacks, sensors, and other vital applications, forced spectrum mobility has to be applied.

Commercial Use

The CRAHNs have undergone testing for commercial TV use. The CRAHN has developed into an essential component of 4G, LTE, and other cutting-edge networks that support ubiquitous computing environments. The network enables cognitive users to run programmes and interact with one another at any time and from any location effortlessly and omnipresently.

Cellular Services

The CRAHN's capacity to function on any network and over any service, despite the fact that the service and network are non-cognitive, makes it beneficial for offering mobile services. CRAHNs may be used to boost a cell's capacity for subscribers. Moreover, CRAHNs improve the quality of cellular service communication.

DISCUSSION

The capability of cognitive radio networks to scan the full spectral band for the presence or absence of main users is one of their key criteria. Spectrum sensing is the name of the procedure, which is carried out either locally by a secondary user or collectively by a group of secondary users. The appropriateness of the available spectrum bands for communication is then assessed. The best band may be chosen using factors such as signal-to-noise ratio (SNR), linkerror rate, delays, interference, and holding time. After the selection of the spectrum band, secondary transmission occurs in that band. When a secondary user or network notices a broadcast from a main user, it leaves the corresponding spectrum band and searches for another one that is open. Spectrum handoff refers to the transfer of a licenced spectrum band to a principal user. Later, we demonstrate that many of the suggested assaults on cognitive networks are brought about by the latency associated with spectrum handoff. Cognitive radio networks may be divided into two categories: dispersed and centralised. The

secondary users of the centralised network are handled by secondary base stations, which are in turn linked via a wired backbone.

Ad hoc communication between secondary users occurs in a decentralised architecture. In a decentralised architecture, spectrum sensing operations are often carried out cooperatively. Moreover, coexistence of two or more wireless networks using unlicensed bands is covered by this sort of design. The presence of IEEE 802.11 and IEEE 802.16 in the same network is an example of this sort of system. We begin by discussing some fundamental security principles in the context of cognitive networks in order to examine the security of these networks. Availability, integrity, identity, authentication, authorization, confidentiality, and non-repudiation are some of the key components of communication security that we take into account. We divide the security difficulties in cognitive networks into two categories: security assaults and intrinsic reliability problems. We focus on dependability challenges specific to cognitive radio networks, such as high susceptibility to weak main signals, uncertain primary receiver position, strict synchronisation requirements in centralised cognitive networks, absence of common control channel, etc. We next demonstrate how each of these flaws may be used by an adversary to launch attacks at different communication protocol levels. Considered are attacks at the physical, link, network, transport, and application levels [7]–[9].

The capacity of cognitive networks to scan the spectral band and locate open channels suitable for opportunistic transmission is one of their key prerequisites. The main user network and the secondary user network are physically distinct, so the secondary users do not directly get feedback from the primary users about their transmission. To find main user transmissions, secondary users must rely on their own individual or group sensing capabilities. Accurately detecting the full spectral range is a difficult undertaking since the main consumers may be dispersed across a wide geographic region. To gauge their existence, secondary users must depend on shaky main transmission signals. The majority of research on spectrum sensing approaches may be divided into three groups: interference-based detection, cooperative detection, and transmitter detection. All of these methods are primarily intended to prevent interference with primary broadcasts. The interference temperature at a place in space is the total amount of interference generated by all secondary users there. At the main receivers, the interference temperature should be below a specified threshold while a primary user transmission is occurring. The position of the main receiver is unknown to the secondary users, making it difficult to do this.

Moreover, secondary users scanning the spectrum should avoid confusing broadcasts from secondary users in other secondary networks with main transmissions when many secondary networks overlap. Spectrum Analysis and Decision 2.1.2 Due to its frequency range and the quantity of users (both main and secondary), each spectrum band has certain distinctive characteristics. The list of possible spectrum bands is determined by spectrum sensing, but the secondary users choose the band that is best suitable for their needs. Interference, route loss, wireless connection failures, link layer latency, and holding time are some of the characteristics of spectrum bands that may be used to assess their efficacy in addition to the often-used SNRparameter (expected duration that the secondary user can occupy the band). Spectrum Mobility 2.1.3 Spectrum mobility describes how quickly cognitive radio networks may transition between different spectrum accesses. Spectrum mobility becomes a crucial consideration when constructing cognitive protocols since secondary users are not guaranteed continuous spectrum access in any of the permitted bands and the availability of unoccupied spectrum bands often varies over time.

The delay experienced during spectrum handoff is one of the key elements impacting spectrum mobility. The protocols used at different tiers of the communication protocol stack are negatively impacted by this delay. The amount of time that passes between the secondary network recognising a main transmission and the secondary users departing the spectral band is another crucial aspect of spectrum mobility. Transmissions from secondary users will interfere negatively with the prime users during this time. To prevent protracted interference to the principal user, the FCC has established upper restrictions on the length of spectrum handoffs.

By protecting data during on-the-fly transmission, security aims to increase network efficacy and dependability. In general, the communication systems-based CR technology must verify the communication security criteria, including data confidentiality, privacy, integrity, and availability, as well as identity, registration, authentication, authorization, and access control. Confidentiality guarantees that the network's data is well-protected against malevolent users and that it cannot be accessed by unauthorised users. Integrity is the SU node's ability to identify any deliberate or accidental alterations to the original data that the malicious user may have made while the data is in transit. As necessary, SU nodes and people may access spectrum gaps thanks to availability. The spectrum gaps that are open to the unauthorised user for their ad hoc usage are defined by access control. The unlicensed user must compromise with its network control if the licenced user shows up. Identification guarantees that a device or SU user must be permitted to participate due to their tamper-proof identity. It is necessary to safeguard node or resource identification, including channel, data, and message, with a strong keying technique. In order to stop unauthorized users from accessing spectrum gaps, authentication is employed. The degree of authorization for each entity specifies the ability of SU nodes to regulate network access in an opportunistic way, even while PU nodes have the ability to affect network control policy. The SU node's sender or recipient might refuse to acknowledge a sent message thanks to non-repudiation. As the messages have already been received, a malicious user's disruption might lead the SU node astray and prevent them from being sent.

Security History

CRAHN's Areas of Security: A selfish or malevolent user might alter the air interface in cognitive radio networks to imitate a prime user or secondary user. During spectrum sensing, spectrum sharing, spectrum mobility, and spectrum management, it may deceive a reliable node. Based on their needs for security, the CRAHNs may be divided into the following domain:

1. The bounds of the actual network: It is a study of how physical networks, or spectrum holes containing SU devices, are configured. The wireless specifications of 802.22, 802.11 b/c/g/f/h, and IEEE 802.16 that enable the cognitive radio features must be supported and used by the accessible WANs and LANs.
2. The areas of liabilities the conventional insurance coverage cover widespread wireless network breakdowns. Nevertheless, during operating transmissions, CRAHN may experience additional malfunctions, unwelcome hazards, threats, or assaults. In order to create a policy that can guarantee successful use of cognitive radio ad hoc networks, this research highlights additional liabilities.
3. The following functional fields: The components described by systems equipped with software-defined radio (SDR) are separated and abstracted via the study of data networking and software. The goal is to prevent the maliciously coded module from interfering with the initial outcomes.

4. The importance of the apps and data It deals with using networks and wireless LANs or WANs effectively across all application domains. But, CRN's added difficulties make the conversations tiresome. In order to develop a successful usage strategy, it is necessary to further investigate the transmission-related concerns.
5. Possible geographic restrictions: The potential for network utilisation is limited by regional variance. The CRAHN may be deployed in hazardous terrain, which might have a detrimental effect on its dependability and impose additional geographic restrictions. The analysis of these variants aids in identifying possible new applications.
6. The study of performance or measurements of network availability is known as traffic and capacity needs/availability. Accounting for the constant amount of data transfer is made easier by it.
7. Continuity and recovery requirements: This is the study of the design of a system free from errors. The achievement of design goals might be challenging, but improved resource management and robust backup mechanisms are helpful.
8. The domain of business applications is the study of application domains. The reachability and scope of the network application area may be expanded by the efficient and effective use of spectrum.
9. The area of business support studies the atomicity, consistency, isolation, and durability (ACID) properties of business transactions carried out in CRAHNs.
10. Development and testing domains: These domains deal with quantifying potential test spaces (such as learning parameters and critical testing knowledge) inside the system that guarantee desired outputs with the least amount of resources. Also, optimal learning for spectrum selection and knowledge testing avoids redundant information and lowers the likelihood of a risk in the linked component.
11. Production domains: This is the study of interoperability and platform viability. In CRAHNs, the interoperability-related problems are more difficult.
12. The alarm management domain identifies distinctive events in the learning and reconfiguration processes. The integrity of the system must be preserved while in transit. Improved alarm management may lessen the danger factor in CRAHNs as well as the network and system latency.
13. Administrative and management responsibilities: Protecting user data from security flaws is the responsibility of information security managers. Information security may be ensured by a well-designed security procedure, which can also prevent catastrophic failure (s).

Aggression in CRAHNs

The CRAHNs are susceptible to a variety of assaults, particularly while they are in the sensing phase, unlike other wireless networks. Generally speaking, there are two types of assaults in CRAHN: aggressive and passive. If a genuine SU node's identifying key has been successfully encrypted by a hostile user, who then gained control of authorisation to lead other SUs astray, such behaviour is referred to as an active attack. Similar to how a rogue node may impersonate a PU without being noticed by other SUs. On the other hand, if the attacker wants to cause a network node to vary from expected behaviour, the attack is said to be passive. The passive attack should be dealt with proactively because, if it has malicious purpose, it can prevent a passive attacker from moving to an active one. While making a

sensing judgement, a passive attacker's harm may be ignorable, but an active attacker's damage may not be.

An open research question is how to develop a proactive evaluation process that prevents an attacker from changing its status from passive to active. Many problems with spectrum sensing, sharing, mobility, and management may surface from an ineffective proactive evaluation. As a result, the application requirements' goal must be well defined so that the SU may use a sensing technique that will be useful for making judgements on how to avoid interference.

Three sorts of attackers have been established in CRAHN: malevolent users, greedy users, and accidentally acting users. False observations sent by malicious users to confuse other SUs may induce band evacuation by genuine SUs or interfere with PU signals. By reporting constant occupancy by incumbent signals, the greedy users monopolise certain bands. Users that act inappropriately inadvertently may report inaccurate information regarding band availability as a result of a hardware issue or a software flaw.

Primary user emulation assaults, spectrum sense data falsification attacks (SSDFA), and beacon falsification attacks are the three attack methods that are exclusive to CRAHN (BFA). The PUEAs are localization-related attacks in which a malicious user may have misled an SU node by using misleading sensing findings, such as the signal emission from a PU node. It is an assault involving the physical layer. An unauthorised user might disrupt an ongoing conversation between two Parties via an SSDFA-type attack [7]–[9].

The actions of the attacker may also be categorised as being inappropriate, self-centered, dishonest, or malevolent. The bad user doesn't follow the guidelines established by the network authority. Selfish people just care about their own needs and don't care if other users are getting anything out of the network or not. The user who is using the network resources dishonestly withholds accurate information about them need to provide the optimal level of service (QoS). The malicious users deliberately attack the network in an effort to lower QoS and reduce network effectiveness.

The Security Methodologies

1. Spectrum-aware approach (SAA): One of the distinguishing characteristics of CRAHNs is spectrum mobility. Using functional functions including spectrum sensing, spectrum mobility, spectrum sharing, and spectrum management, the mobile SU node dynamically modifies the tuning parameter. To share state data during communication, the SU node must use a cross-layer methodological approach and take into account spectrum mobility. In order to safeguard information from potential assault, behavioural analysis of the spectrum via learning may be useful.
2. Hammer model framework (HMF): The SU node experiences network jamming, channel information change, PU and SU spoofing, and more. The effectiveness of channel usage may suffer in such a situation. Threats of this kind are connected to denial-of-service attacks. Information protection from risks connected to DoS has been accomplished using the hammer model framework.
3. The CRAHNs are a very dynamic network, hence propagation-based methodology (PBM) was used. The CR technology significantly expands the communication spectrum access potential due to its spectral fluctuations. There is enough spectrum mobility across the whole band to support conversation. Yet, as it is hard to discern PU appearance, it could negatively impact communication. The buried terminal issue could occur rather often. In order to anticipate with high accuracy, the suggested technique proposes to monitor the spectrum at runtime that maps the spectrum

in'multidimensional' space and frequency domain. The model lowers the likelihood of potential risks from nefarious users.

4. Robust security model (RSM): The SU nodes in CRAHNs work together and cooperatively to communicate with one another. Hence, in order to improve the efficacy of the network, a trustworthy and strong security protocol must be created. The protocols that are aware of the issue with Byzantine generals may be the proper strategy for achieving resilience. Such design principles may be used to increase the dependability of cognitive radio ad hoc networks and have been utilised to offer fault tolerance in distributed systems. The design strategy could also provide security defences against intruders in cognitive radio ad hoc networks.
5. Selfish attack detection techniques (COOPON): By enlisting the assistance of other reliable neighbouring SUs, the cognitive radio nodes in COOPON are able to identify assaults made by selfish SUs on multiple channel access. The participating SUs in CRAHNs share the information from the detected channels. Every receiver SU that notices a disparity in the figures in its immediate area views SU as an attacker in the network.
6. Distance analysis method (DAM): The SU node calculates the metrics of the distance and collaboratively accesses that data in the linked component. The data manager uses the distance data that has been gathered to account for trusted value. The neighbouring node is seen as malevolent in CRAHNs by the SU node if it discovers any discrepancy.
7. Strategic surveillance (SS): The strategic examination of interactions between defenders and attackers through network management is referred to as strategic surveillance. The management systematically monitors the attackers' behaviour and coerces them into making a strategic commitment.
8. The location-based defence (LocDef) mechanism is based on exchanging and comparing the estimated localization information with the PU's already-known location information. The SU node flags the node as malicious if it discovers any discrepancy in the estimated value.

CONCLUSION

The CRAHN differs considerably from conventional wireless networks, and because of its limitless potential for applications, it is developing into the technology of the future. While the chapter's purpose was to account for security concerns with CRAHNs, the example may assist novices define their research objectives for future studies on security vulnerability in order to increase the efficacy and dependability of CRAHNs. In addition, the information is meant to inspire the reader to gain understanding of network vulnerability, security needs, and repercussions as well as to come up with novel defences against different sorts of attackers that target CRAHNs. A channel may be subject to a jamming or congestion attack by a hostile user. This attack targets the connection layer. In connection with beacon authentication methods, the BFA refers to situations in which an unauthorised user produces a beacon signal and attempts to pass it off as genuine. The purpose of a malicious user's false alarm is to conflict with genuine users of the spectrum.

REFERENCES

[1] H. Khaled, I. Ahmad, D. Habibi, and Q. V. Phung, "A Secure and Energy-Aware Approach For Cognitive Radio Communications," *IEEE Open J. Commun. Soc.*, 2020, doi: 10.1109/ojcoms.2020.3009241.

[2] E. Summary, "Future Directions in Cognitive Radio Network Research NSF Workshop Report," *Network*, 2009.

[3] Y. Kim, "Fast and robust asynchronous rendezvous scheme for cognitive radio networks," *Appl. Sci.*, 2019, doi: 10.3390/app9122481.

[4] F. Badghan, R. Namdar, and N. Valizadeh, "Challenges and opportunities of transgenic agricultural products in Iran: Convergence of perspectives using Delphi technique," *Agric. Food Secur.*, 2020, doi: 10.1186/s40066-020-00259-5.

[5] Y. Kim, Y. H. Oh, and J. Kang, "Asynchronous Channel-Hopping Scheme under Jamming Attacks," *Mob. Inf. Syst.*, 2018, doi: 10.1155/2018/5032934.

[6] I. V. Onut, "3rd Workshop on Smart Surveillance System Applications," *Proc. 2012 Conf. Cent. Adv. Stud. Collab. Res.*, 2012.

[7] NSF, "Future Directions in Cognitive Radio Network Research," 2009.

[8] Y. H. Oh and D. J. Thuente, "Sequence sensing Jamming attacks against modular-based channel hopping rendezvous algorithms for cognitive ratio networks," in *IEEE International Conference on Communications*, 2013. doi: 10.1109/ICC.2013.6654849.

[9] S. Men, Y. Zhou, X. Sun, and Z. Zhou, "A cooperative spectrum sensing scheme in wireless cognitive sensor network," in *IET Conference Publications*, 2012. doi: 10.1049/cp.2011.0734.

CHAPTER 8

COORDINATED DEFENSES AGAINST DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Mr. Ashutosh Anand,Assistant Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - ashutoshanand@presidencyuniversity.in

ABSTRACT:

One of the main problems the Internet community is now facing is the distributed denial of service (DDoS) assault. By overtaxing the network and server resources, DDoS attacks try to prevent the legitimate users from accessing resources. The collaboration between the nodes fails as a result of the absence of incremental payment mechanisms. Sometimes there are no payment structures, and other times there are payment structures but the incentives aren't good enough to get the nodes to share their resources. The assault phase, detection phase, and reaction phase of a DDoS attack may all be separated. As the attacking machines work together, the defence mechanism should also work together in order for it to be effective. One of the main problems the Internet community is now facing is the distributed denial of service (DDoS) assault. These are carried out by the botnet army's slave computers, which follow orders from the master machine with the aim of using up server and network resources like bandwidth and storage so that genuine customers cannot access them.

KEYWORDS:

Defence Mechanisms, Distributed Denial of Service (DDoS) attack,Internet Community, Economic Incentive.

INTRODUCTION

The greatest known DDoS assault had a 400 Gpbs volume in 2014. The frequency of DDoS assaults has increased since that time. The efficacy of these systems and the methods for implementing them are constantly improving, which presents a significant challenge for security specialists. The study of Internet economics has recently become a quickly developing subject of research for cyber defence. This research is crucial from the perspective of information security and policy developing because of the dispersed workstations throughout the network and the diverse interests of the users. Any framework's primary goal is to maintain the security requirements of confidentiality, integrity, and availability without placing an undue burden on the deployer [1]–[3].

The "tragedy of the commons" idea is crucial in how the Internet's finite resources are distributed. Because of their personal self-interest, the users in this scenario undermine the community's overall interest in sharing the resource. A pricing plan that can accommodate the competitive advantage of several network providers that provide the same set of services at various price points is one that is sustainable. Differentiating the services provided to consumers will be made easier by a price structure, but setting the incentives is also crucial. The various QoS needs are made possible in large part by the pricing approach. Security experts now understand how important it is to take into account the "theory of mind" when creating any security mechanism since it explains how attackers and good users make decisions about whether to trick or trust the system.

Distributed denial of service attacks are the ones in which the attacker gets control of the system by exploiting its weaknesses. The attacker is able to compromise numerous computers in this way, and once they are all compromised, they band together to create an army of zombie slave machines. The attacker or the master computer then issues a command to the slave machines to start the attack by either flooding the victim's address with malicious packets or by using up all of the server and connection bandwidth. Attacks on servers' resources occur at the application layer when the attacker's goal is to deplete them, whereas attacks on connection bandwidth occur at the network and transport layers. According toa distributed denial of service attack differs from a denial of service attack in that the former requires the coordination of numerous zombie machines and Internet connections to execute the attack, whereas the latter only requires a single machine and a single connection under the attacker's control. Why not protect the system in a similar manner by establishing cooperation amongst numerous nodes that are willing to pool their resources in return for some financial incentive? When the attacker conducts the attack, it does it with the collective efforts of hundreds of thousands of computers [4]–[6].

The economic incentive component of the issue, which has been the crucial element in thwarting DDoS assaults, has traditionally been disregarded by the business and academics when addressing DDoS attacks. The foundation of the human race is incentives. The issue is that despite the existence of several distributed cooperative defence measures, DDoS assaults continue to affect the systems. This is due to the fact that no solution has been successful in getting ISPs to pool their free cache memory for collaborative defence. Due to the lack of an incremental payment system or the absence of one, they have not been often used on the Internet. Cooperation has failed as a result of this. The implementation of distributed solutions is a hard issue that is strongly associated since detection and responses are dispersed across several sites.

The method used to identify the assault may be used to categorise the DDoS attack defence methods. It is categorised as third-party detection, pattern-based detection, and anomaly-based detection. In the pattern-based attack detection method, the traffic is compared with the signatures that have been saved in the database, and if the signatures match, the DDoS assault is effectively identified. This method's fundamental flaw is that it is susceptible to zero-day assaults. As new viruses are created and attacks are periodically conducted, the system will inevitably defeat numerous new attack types if the stored database is not updated in real time. In anomaly-based attack detection approach, an ideal model is defined, after which the actual traffic is contrasted with that ideal model. The assault is recognised if the deviations exceed the predetermined permissible boundaries. This method has an advantage over pattern detection in that the system may be taught to recognise brand-new varieties of malicious communication.

DISCUSSION

The Internet Service Providers (ISPs) are experiencing a challenge of rising levels of fraudulent traffic. This malicious traffic's primary goal is to use up all available bandwidth and storage on the network. The amount of resources needed to sustain network performance is insufficient, and the quality of service (QoS) that the network offers quickly deteriorates. Misbehaving users that either consciously or accidentally execute flooding distributed denial of service attacks from their computers generate a very huge amount of malicious traffic. At the network level, congestion management methods are used to throttle traffic before it reaches its peak value. To avoid a network connection from collapsing from traffic overload, throttling refers to controlling the pace at which traffic is carried across it.

Nevertheless, this technique falls short of sustaining the necessary degree of QoS. One of the greatest risks to the Internet's security is the DDoS assault, which may produce enormous amounts of unwanted traffic. Websites are the primary targets of DDoS attacks. They interfere with the good user's access to the website or server. The first signs of the DDoS assault, which lasted for two days, date back to 1999. Since then, several DDoS detection methods and countermeasures have been created. A more sophisticated kind of DDoS assault is referred to as an amplification attack, such as a DNS amplification attack or an NTP amplification attack, in which these servers act as reflectors and intensify the onslaught. These attacks don't target the servers directly; instead, a number of servers are leveraged to produce a lot of traffic in response to modest requests that are delivered to a fake IP address that was given by the attacker. It generates unwanted traffic using the response data. As noted, there are two key features that prevent DDoS defence solutions from offering trustworthy security. The inability to separate harmful from benign communications comes first. There is no system that effectively separates the traffic while causing the fewest possible collateral damages to the valid requests. Second, it is exceedingly difficult to detect DDoS attack origins since they are dispersed over several websites [7], [8].

Each system's security failure may be attributed to two different factors. Poor motivation comes in second after bad design. While the design aspect has been well examined, the incentive portion remains naïve. Computer systems malfunction because the organisation in charge of protecting them does not experience total setbacks when they do. The theory of computation has benefited the security business in the same way that cryptography, which was developed using mathematical notions, did 25 years ago current microeconomics. Many scams in the banking sector have been caused by the issue of mismatched incentives. To maintain security requirements and reduce system failure rates, systems must be built and developed that encourage ethical user behaviour. The creative idea of using online auctions as a reputation system has inspired the academics to look into further similar possibilities.

Cooperative DDoS Defense Mechanisms Taxonomy: DDoS defence techniques may be divided into two groups: distributed and centralised. This depends on whether the detection, mitigation, and response defence mechanism stages are deployed at the same area or at other locations. The whole DDoS defence system is built up at the source, destination, or intermediary network in the centralised mechanisms. Yet, under centralised methods, the victim node may be the site of detection, the intermediary nodes might be the site of mitigation, and the attack traffic generator itself might be the site of reaction. This indicates that the whole process is dispersed over the Internet, but for the DDoS assault to be effectively thwarted, all of these participants must cooperate with one another.

The emphasis of this article is on the many cooperative defence mechanisms that are accessible, but before that, we explain why these mechanisms are necessary when centralised ones are already in place. In the action cycle is shown. Single point of failure is the major problem with centralised systems. It implies that if the one location where all of the defence system's components are placed is attacked, the whole system might crash. This issue may be resolved by the cooperative system by having numerous nodes engaged in defence at various places. As several nodes perform similar functions, we can still protect the target site even if all the nodes in one area are hacked. Second, since the Internet lacks a centralised control structure for its autonomous systems, a defence model without a centralised command structure will be advantageous.

Packaging and Pushback: Combining the pushback message and packet marking techniques, Chen and Park suggested a cooperative approach. Attack Diagnosis (AD) is a technique where the victim computer first recognises the DDoS assault and then transmits AD orders to

the network's upstream routers. This defensive strategy is reactive. It takes advantage of AD-enabled routers, which begin deterministically labelling each packet with the information about the interface it is going through. The target system then utilises this information about the associated interface to determine where the infected packets originated.

The Time To Live (TTL) field of the IP packet header is used to verify the authenticity of the AD-related directives. When there is a DDoS assault, the AD scheme is useless and is carried out on a big scale, hence AD has an expansion known as Parallel Attack Diagnosis (PAD). Whereas PAD diagnoses and stops the traffic from several routers at once, AD can only stop the traffic from a single router at a time.

Port marking and IP tracing: one more distributed DDoS mechanism based on the concept of router port marking and packet filtering. They are shown as two commonly used modules. By adding the router's interface port number to the packets, the router port marking module marks the packets probabilistically. It is a six-digit, geographically distinctive number. When the target system is bombarded with malicious packets, it uses the attached data to determine where the malicious packets came from.

After that, the upstream routers filter the malicious incoming packets using the function of the packet filtering module. Low processing and communication overheads characterise this technique. Nevertheless, it has two drawbacks. First off, because no authentication is required, attackers may falsify the marking data to keep their true location a secret. Second, even though this method successfully locates the IP, it is unable to locate the DDoS assault master who is in charge of the army of hacked or zombie devices.

Defense Based on Signature: The Coordinated Suppression of Simultaneous Attacks (COSSACK) method was suggested by Papadopoulos et al. It makes use of the watchdog software system, which was created for edge routers. It is predicated on a number of crucial premises, including the presence of attack signatures, the capacity of edge routers to filter packets based on these signatures, and continuous connection availability. In order to interrupt the flow of DDoS attacks, the watchdog software performs ingress and egress filtering on the edge routers. It also sends multicast messages to the source side. It cannot survive DDoS attack traffic produced by older networks without COSSACK deployment.

Defense Based on Capabilities: Based on the capabilities, Anderson et al. have suggested dispersed defence techniques. With these techniques, the sender must first get the receiver's consent before sending anything. These rights might be thought of as coins, short-term contracts, or authorizations. We may use the example of applying the postage stamp to the letter before mailing it to better grasp this. The sole distinction is that the sending rights are acquired directly from the recipient, whilst the postage stamp is purchased via the post office. Another example is the receiver setting the window size in advance for the data connection layer's sliding window protocol. The capability setup channel is not secure, which is this scheme's main flaw. The fact that these techniques must constantly be in use adds to the processing and memory overheads.

Defense Based on Datagrams: A datagram filtering approach was presented by Argyraki et al. as an alternative to capability-based filtering, which denies all communication by default but only identifies the traffic that is blocked as malicious. Active Internet Traffic Filtering is the term for this (AITF). The recipient may then get in touch with the disrespectful senders and request that they cease. Every ISP must enforce rules against misbehaving nodes in order to avoid losing connection to the victim system, which may serve as a key access point. So, there is a great need for the participating ISPs to work together. Since AITF protects the receiver's bandwidth at a low per-connection cost, ISPs can afford to install it. When the

handshake packets and the DDoS attack traffic are travelling via the same flooded channel, it is possible that the three-way handshake used to confirm the validity of the traffic will not be successful. Due to the fact that this technique does not depend on edge routers for real filtering, it also has a number of deployment problems. The network's centre is where the routers are located.

Defense Based on Anomalies: Another distributed defence method against network and transport layer DDoS assaults, called StopIt, was presented by Liu et al. Each receiver in this system installs a network filter to stop unwanted traffic. It utilises Liu's suggested Passport system for authentication. Its design makes use of third generation and looping telecom networks. Every autonomous system has a StopIt server that handles StopIt requests and responses. The source is equipped with a filter, and the peer nodes communicate each other about filter requests. If queries from nearby autonomous systems are permitted, the StopIt server may be assaulted using packet floods and filter requests in this way. Moreover, StopIt's extensive detection requirements make it challenging to implement.

A distributed DDoS defence technique was suggested by Walfish et al. to thwart application layer level assaults. The idea of offence as defence is used in this essay. By sending more helpful traffic to the server that is the focus of the DDoS assault, it encourages the truthful clients to speak out. As a result, the attacker's flooded network is overcrowded and less bandwidth is being collected by the good clients. The study does not clarify how the server will recognise the assault. Only session flooding assaults, not request flooding or asymmetrical attacks, are subject to the speak-up mechanism.

A Defensive and Offense Wall (DOW) plan was put out by Yu. et al. This adds an anomaly detection mechanism as an extension to the speak-up work of Walfish et al. The K-means clustering strategy is utilised as the basis for the anomaly detection technique to identify asymmetric, request flooding, and session flooding assaults. Two modelsthe detection model and the money modelhave been used to describe the workings of the mechanism. Whereas the latter's purpose is to promote an increase in session rates by genuine clients, the former's duty is to discard questionable packets. This mechanism's main flaw is that it requires too many resources to use in practise. The assault deluge may be routed to these several servers, each of which will only handle a small portion of the attack flow, reducing congestion. While this resource is currently available and will only cost the parties concerned a little amount, managing network resources is one of the most crucial problems with the Internet. The major goal of mechanisms like double auction is to encourage sustainable individual gains over the long term in addition to increasing the usefulness of free cache resources, which has always been the foundation for addressing issues in economic engineering [9].

CONCLUSION

The common problem encountered by all DDoS detection, mitigation, and response frameworks, according to study, is to increase the rate of detection while maintaining QoS for good users. The DDoS defense mechanism may be divided into three parts: detection, mitigation, and response. This applies to all of these strategies. The defenses created throughout the network include both victim-end and source-end methods, in addition to both. A very effective cooperative mechanism that ensures rigorous and reliable communication continues to be the foundation of these hybrid processes. So, it's crucial to consider any scheme's incentive and payout structures from an economic point of view. The Internet, for example, has a number of cache servers that may not be utilized to their maximum capacity. These unused cache capabilities might be employed in cooperative DDoS defense.

REFERENCES

[1] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, 2013, doi: 10.1109/SURV.2013.031413.00127.

[2] Q. Wang, W. Tai, Y. Tang, H. Zhu, M. Zhang, and D. Zhou, "Coordinated defense of distributed denial of service attacks against the multi-area load frequency control services," *Energies*, 2019, doi: 10.3390/en12132493.

[3] B. Rodrigues, T. Bocek, and B. Stiller, "Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS)," *Semant. Sch.*, 2017.

[4] K. Malialis and D. Kudenko, "Distributed response to network intrusions using multiagent reinforcement learning," *Eng. Appl. Artif. Intell.*, 2015, doi: 10.1016/j.engappai.2015.01.013.

[5] K. Munivara Prasad *et al.*, "DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey DoSandDDoSAttacksDefenseDetection andTraceback Mechanisms-A Survey DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey," *Glob. J. Comput. Sci. Technol. E Netw.*, 2014.

[6] M. Essaid, D. Y. Kim, S. H. Maeng, S. Park, and H. T. Ju, "A Collaborative DDoS Mitigation Solution Based on Ethereum Smart Contract and RNN-LSTM," in *2019 20th Asia-Pacific Network Operations and Management Symposium: Management in a Cyber-Physical World, APNOMS 2019*, 2019. doi: 10.23919/APNOMS.2019.8892947.

[7] *et al.*, "A UNIFIED APPROACH FOR DETECTION AND PREVENTION OF DDOS ATTACKS USING ENHANCED SUPPORT VECTOR MACHINES AND FILTERING MECHANISMS," *ICTACT J. Commun. Technol.*, 2013, doi: 10.21917/ijct.2013.0105.

[8] Z. Chen, Z. Chen, and A. Delis, "An inline detection and prevention framework for distributed denial of service attacks," *Comput. J.*, 2007, doi: 10.1093/comjnl/bxl042.

[9] Q. Li, W. Wei, M. Tao, and Q. Chen, "A DDOS defence scheme based on two-stage traffic flow control," *Int. J. Commun. Networks Distrib. Syst.*, 2014, doi: 10.1504/IJCNDS.2014.064638.

CHAPTER 9

DDOS ATTACK-INDUCED BOT EXPANSION IN THE E-COMMERCE NETWORK

Dr. Sampath Sivaperumal, Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.s
Email Id: - director-international.relations@presidencyuniversity.in

ABSTRACT:

Cybersecurity is the safeguarding of information systems against serious crimes including cyberwarfare, cyberterrorism, and cyberespionage while maintaining user privacy. It is sometimes referred to as computer security or IT security. The "information warfare" may affect and fully destroy a nation's or an organization's vital IT infrastructure. There are many other kinds of cybercrime, on a DDoS assault on an E-Commerce network to propagate bots over the network. DDoS assault may be used to destroy a service or as a cover for bot distribution. In this chapter, a dynamic SIS-SEIRS model is suggested to depict how DDoS attacks spread bots across the E-Commerce network. The development of Internet technology has created a number of difficulties, including the need for an appropriate cyber security mechanism to safeguard the crucial corporate data housed in e-commerce systems and for information travelling across networks. Understanding the many forms of network attacks and creating mathematical models to characterize their behaviour are crucial steps in achieving this aim. In this chapter, a mathematical model for understanding DDoS attacks while distributing bots within an e-commerce network will be developed.

KEYWORDS:

Cyber-Attack,Computer Network, DDoSAttack, E-commerce, Malware, Network Security.

INTRODUCTION

The goal of a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is to prevent a network's legitimate users from using its computer resources. In a DDoS assault, an attacker might utilise your computer to conduct a DDoS attack against a different computer in your network or against others using a variety of tools, including Trinoo, Tribal Flood Network (TFN), Stacheldraht, Shaft, MStream, etc. DoS/DDoS attacks are often launched using botnet. A set of infected computers (sometimes referred to as zombie machines) operated by hackers and executing malware from a shared command and control infrastructure are referred to as a "botnet". A bot is an automated software that performs certain tasks, often via a network. Bots have all the benefits of worms, but they often have a considerably wider range of infection vectors and frequently change their behaviour within hours of a new exploit's publishing [1]–[3].

An new nonspecific entry validation method based on proxy ring signature has been proposed by Tianhan Gao et al. for the CPS Wireless Mesh Network (CPS-WMN). The anticipated technique using SVO logic has a known safety immune that has been provided.In their study, Lianwen Wang demonstrated how the occurrence percentage of an SEIR endemic model propagated via a drop and a shift in the scope of all occupants to a general nonlinear arrangement. The author has focused on presenting the updated geometric technique based on

the third additive compound matrix in order to establish the SEIR model's global stability. Its findings are relevant to two separate incidence functions that capture the impact of the mass media . The global asymptotic stability of multi-group SIR and SEIR age-structured models has been investigated by Jinliang Wang et al. These representations enable the infectiousness and mortality rates of susceptible entities to fluctuate and rely on susceptibility, which they used to gauge the population's diversity. They recorded global dynamics and showed that the fundamental SIR and SEIR with age-dependent vulnerability's dynamical creation is unaffected by heterogeneity.

The industrial safety-critical instrumentation and control systems (I&Cs) are subject to extra information (in general and cyber, in particular) security oppressions and assaults, as Kharchenko et al. outline in their article. Their paper's objective was to illustrate the procedure and available resources for MV FPGA-based I&Cs condition-based security estimation.

A primary latent danger to critical infrastructures is benefited by cyberwar (CIs). Decision-makers who seek to develop resilient CIs must think carefully about the strategic, operational, and nonlinear dynamics defining such cyber-physical systems. Elisa Canzani and Stefan Pickl form an association with System Dynamics (SD) using a game-theoretic approach to understand the dynamics of CI processes resulting from attacker and protector strategic relationships in cyber epidemics. Their research was criticised for their prior work by a novel block structure that served as the basis for a study of the influence of unrest in networked CIs.

According to research by Kuldeep Kaur et al., data in financial organisations may be disclosed over a lengthy period of time without damage. The increasing span of the study of security is employed to lessen dangers. Long-term usage of security reduces the number of branches, as well as the costs of linked and connected properties.A Lyapunov function may serve a variety of functions, such as validating a system's stability or termination or enabling the construction of invariant groups, which can then be used to suggest safety and security. The putrefying strategy, which reduces the graph structure before spreading the disintegration process, should be improved, according to Eike Mohlmann and Oliver Theel.

Liping Feng has provided an enhanced SIRS model for studying the dynamics of worm spread in WSNs. This model helps explain how worms spread by using energy, as opposed to distributed node densities. The explicit mathematical analysis has produced a control parameter R0 1 based on this model that completely controls the global dynamics of worm proliferation. When R0 1, worms have been shown to be controlled in WSNs; otherwise, they become widely distributed. Last but not least, the author presented distributed node densities in WSNs and the threshold of worm spread about communication circles, both based on R0. The precision of theoretical research is supported by mathematical simulations.

For the first time, Jinhua Ma has looked at the convoluted interactions between harmful and benign worms in various M2M networks. Ma et al. showed that the threshold value R0 controls the overall dynamics. In different vaccination programmes, they are able to acquire the final size formula in the absence of birth, death, and the treatment impact of users. The findings show that higher node degrees are more susceptible to contamination than lower node degrees. Their article provides a solid theoretical foundation for activities that may be taken to effectively stop the widespread infection of mixed M2M networks by malevolent worms.

Canzani's analysis of the volume of material now available in epidemiology shows the range of techniques used for demonstrating dynamics. From compartmental SIR models that exclusively predict organic pathogens to the various social network models, the complexity

of modelling epidemics has increased. For example, the Kermack-McKendrick threshold condition, conventional models and novel findings have proven very effective in guiding public health policy. This assessment serves as a beginning effort to identify high dynamics of disaster situations, such as the propagation of computer viruses in the online community and of information on a company's IT infrastructure.

Meng Wang has proposed a patch for the transmission of benign worms via the mobile network. After gathering all of the mobile network's problems, the detection and repair process introduces efficient benign worms to the environment to increase the effectiveness of the repair when eruption of evil worms. In order to swiftly combat harmful worms, they initially employed the benign worm's active mode. After the malicious worms were under check, they switched to the benign worm's passive mode and further released the resources of the mobile network. As a result, they verify the security of mobile networks and also adjust the network accordingly [4]–[6].

The research by Elisa Canzani et al. provides an analysis of freely accessible IT security information for mobile devices in Germany and reports on openly available information on IT security, its accessibility, and its brilliance. They acknowledged that there aren't many consistent trends in terms of quality, substance, or timeliness.In their article, Alomari E. et al. provided a thorough analysis to show the risk of Botnet-based DDoS attacks on application layer, namely on the web server, as well as the increasing frequency of such assaults that have definitely grown in recent times. Also highlighted are botnet-based DDoS assault occurrences and the financial demise of well-known corporations and official websites. This provides a better knowledge of the issue, the available solution space, and prospective research opportunities to effectively defend against such assaults.

The challenge of simulating the realistic arrival process of bot requests on an e-commerce web server is one that Suchacka et al. present in their study. Sessions made by bots were reproduced and their important characteristics, such as the inter-arrival time of bot sessions, the quantity of HTTP requests per session, and the inter-arrival time of requests per session, were evaluated, based on actual log data for an online shop. Regression analysis was used to create a mathematical model of the characteristics of the bot traffic, which was then implemented in a bot traffic generator. These results support the occurrence of a strong tail in the distributions of bot traffic characteristics.

In their study, Xu et al. first achieved an in-depth investigation of the characteristics of online bot traffic before presenting a competent way to perceive web bot activity in a significant e-commerce marketplace. The following parts make up the authors' anticipated bot detection method in detail: The most distinctive characteristics should be extracted using (1) an Expectation- Maximization (EM)-based feature selection approach, (2) a gradient-based decision tree, (3) a threshold approximation mechanism, and (4) a mechanism to recover a reasonable percentage of non-bot traffic flow. The analysis's findings show that they vary in a number of ways, including active time, search phrases, item and shop preferences, and many more. Our findings provide fresh insights for public websites to advance web bot traffic identification for safeguarding priceless online contents.

DISCUSSION

Several mathematical models that provide a clear perspective of assaulting behaviour as well as the propagation of harmful software in networks have been established. In this chapter's portion, we'll create a model for a DDoS assault that spreads bots across an e-commerce network. DDoS attacks overload servers, network cables, and network devices like routers, paralysing Internet infrastructure as a result [7], [8].Hosts and routers make up a network,

which also comprises a core and an edge. The hosts are located at the edge, while a network of linked routers makes up the core. The intermediary between an organization's internal network and the public Internet are hosts. Servers serve as the entry point for assaults that disseminate bots across the network.

The majority of the dynamic models for infectious illnesses are based on compartment structures, which Kermack and McKendrick first presented and subsequently improved by other mathematicians. The complete e-commerce network has been split into two sub-networks: the exterior network, which is mostly made up of host computers (SIS model), and the internal network, which is made up of the remaining nodes (SEIR model), which include routers, servers, and other network-connected equipment. We have used an interactive epidemic SIS- SEIRS model, which comprises of two sub-models, to graphically simulate the DDoS assault and the propagation of malware into the network. Moreover, it is mathematically shown that if the reproduction number is bigger than 1, the suggested model is asymptotically stable at the endemic equilibrium point.

Also, it is shown visually that, when the reproduction number is smaller than 1, the model's stability results from the lack of malware in the system. The comparison of Si and Ibi reveals that when is raised by a set amount (0.01), Si's value falls and Ibi's rises, increasing the system's infectiousness. Moreover, Ibi is growing at a faster pace than Si is declining. The drawback of our suggested paradigm is that it prevents the addition of additional nodes to the internal network. Smurf DDoS, also known as a distributed denial of service assault, is a kind of network attack in which the attacker uses victims as digital props to get access to data, files, or the server itself.

Smurf DDoS attacks are a genuine threat to networks because they utilise packet flooding techniques including ping flooding, IP flooding, TCP flooding, and UDP flooding to block authenticated users from accessing networks, servers, or other systems. Smurf DDoS attackers go from attacking people to attacking institutions including banks, government buildings, and hospitals, among others.Attacker uses a variety of techniques to access the user's system with Smurf DDoS attack, which is also referred to as the attack's deployment location. Spam emails, compromised websites, downloading and opening malicious files, logging into infected computers, and installing pirated software are a few examples. Misconfigured network devices that enable packets to be distributed to all computer hosts on a certain network through the network's broadcast address rather than a single machine are the foundation of a Smurf DDoS assault. The distributed denial of service (DDoS) attack known as SmurfDDoS targets the network layer. Smurf virus that makes it possible to execute. Both smurf attacks and ping floods are carried out by delivering a massive number of ICMP Echo request packets.

Owing to flaws in the system interface, distributed denial of service (DDoS) attacks are easy to deploy and highly challenging for security specialists to prevent. DDoS assaults account for the majority of severe attacks in cloud computing. DDoS assaults cost major firms an average of $444,000 in lost revenue, and they may cost businesses six figures. Overall, during the course of the yearlong research period, approximately 1 in 5 firms were subjected to a DoS assault. DDoS attacks are among the most dangerous ones for the safety of computer networks. Also, as Internet use grows, it is important to combat DDoS assaults, which according to a research rank first among all attacks.

DDoS attacks are both effective and reasonable, which encourages more people to use this kind of attack. The cost-related barrier to a portion of DDoS attacks has mostly vanished. This means that anybody may launch an attack, whether it is a group of blackmailers, a disgruntled ex-employee, or a rival. Moreover, the individual in issue may be anyone.

Different types of DDoS attacks is one of our customers. A small company that provides training for those working in the construction industry, yet they endured years of abuse.Although DDoS assaults are less complicated than other kinds of cyber-attacks, they are nonetheless evolving and becoming more expert. There are three main types of attack categories. Volume-based assaults, which engulf an organization's transmission capacity by making use of heavy traffic. Protocol assaults, which focus on using server resources. Application attacks are said to be the most recent and authentic kind of assaults since they focus on online apps.

There are typically two ways to stop a DDoS attack

Taking use of programming flaws - Programmers may deliver twisted packages to target both well-known and obscure programming flaws in an effort to destroy the framework of the victim. Burn up computational or correspondence resources - Programmers may send enormous amounts of realistic-looking packages, using the victim's organization's memory, central processor, or transmission capacity until the predetermined. Framework is currently unable to handle any requests from actual customers.

Techniques for Counter measurement of DDOS

The network may be protected from malicious activity or attack by using detection and mitigation countermeasures for any cyber or network attack prevention. The goal is to provide preventative measures, such as updating Java, Adobe Reader, Anti-virus software, and other third-party apps to protect against Smurf DDoS attacks. If the assault is still occurring, the first step in making your network safe is to identify the attack by choosing the attributes and comparing them to a database for identifying Smurf DDoS attacks.DDoS prevention technology used to stop attacks before they start. This gives the authorised user backup services that are accessible as needed, allowing them to decrease attack attempts without limiting access to the services. While this method may be the recommended one for DDoS assaults, it may not work with all flooding attacks.

Detection System:

During an assault, a DDoS detection system is employed. This makes it possible to stop an assault before it spreads and react right away to lessen its effects. The detection system looks for any unusual patterns or behaviours in the packet. The two main categories of DDoS detection systems are signature-based detection and anomaly-based detection. Anomaly-based detection is focused on traffic that deviates from the norm, while signature-based detection primarily focuses on attacks on packets and protocols that follow a certain pattern. Nowadays, distributed denial of service (DDoS) assaults are one of the most successful attack tactics and have severely harmed the growth of e-commerce, e-services, and other e-technologies. A distributed denial of service (DDoS) assault employs several computers to perform a coordinated denial of service attack against one or more targets, according to the World Wide Web Security FAQ.

By using the resources of several unknowing accomplice computers that act as attack platforms, the perpetrator is able to dramatically increase the efficacy of the Denial of Service using client/server technology. DDoS attacks basically aim to overwhelm targets' bandwidth and other resources with excessive data flows that the target cannot handle effectively, which could result in QoS degradation or even network breakdown and result in denial of service to the target's legitimate users. This is particularly harmful to e-commerce websites because their survival is entirely dependent on remaining online and accessible to their intentional customers, and the vulnerability lies in the target's network infrastructure. Attacks of this kind are often concealed and paroxysmal, making protection more challenging. Detecting and

defending against DDoS assaults is now a popular topic in network security research. To identify and defend against DDoS assaults, certain methodologies and strategies have been advanced. These techniques may be divided into detection deployed in victim networks, detection deployed in inter-networks (often placed on Internet core routers), and detection deployed in source-end networks.

The benefits of source-end DDoS detection are as follows: Attack data flow could be jammed at the bottleneck if it is restricted before accessing the Internet. 2) Compared to detection implemented in victim networks, it is simpler to track DDoS attack origins from source-end networks. 3) As the attack flow is smaller in source-end networks, more specialised techniques might be used to identify DDoS attack flows there. 4) As opposed to a busy core router on the Internet, a source-end network's exit router might make use of more resources to identify DDoS assaults.

Each circumstance that might have an impact on security in e-commerce is a risk that has to be mitigated. Even if the effect varies depending on the kind of company, it is nonetheless unwelcome and rejected. The environment being used controls the security concerns. A security breach has an impact on customers as well as company owners. The Internet has grown to be the biggest and most popular market for all consumers, suppliers, and company owners because to its ability, openness, strength, and presence. Because to the open nature of the Internet, there are numerous invaders, viruses, worms, and Trojan horses that attempt to compromise the e-commerce industry. There are hazards associated with data system loss as well as financial risk. As DDoS assaults get more sophisticated, more businesses are now being targeted by them. The attackers never stop or have a certain season of the year when they commence their assaults.Many instances demonstrate the detrimental effects of security concerns on e-commerce. In this study, we investigate the impact of two examples on e-commerce operations of the distributed denial of service (DDOS). The DDoS results in challenges with website access, such as interruption, which has an adverse effect on both the website's users and its business [9], [10].

CONCLUSION

The DDoS assault and the introduction of bots into an e-commerce network are represented in this chapter by an interactive epidemic SIS-SEIRS model that is made up of two interactive sub-models. The suggested system is analytically shown to be unstable if the reproduction number is more than one and asymptotically stable at the malware-free equilibrium point if the reproduction number is less than one.Because of Internet of Things (IoT) systems, there have been more insecure devices recently, which has led to additional vulnerabilities being used by attackers to launch DDoS attacks. According to a recent investigation, attackers increasingly exploit tens of thousands to millions of individual routers from small offices and home offices (SOHO) to carry out sophisticated DDoS operations. The DDoS assaults surged by 240% in 2014, according to a study from Incapsula, a well-known CDN service provider, and traffic topped 100G. According to the 2014 DDoS assaults study, the average economic damage during an attack was 40,000 USD per hour, and 49% of DDoS attacks lasted between 6 and 24 hours.

REFERENCES

[1] K. Kalkan, G. Gur, and F. Alagoz, "SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment," in *Proceedings - IEEE Symposium on Computers and Communications*, 2017. doi: 10.1109/ISCC.2017.8024605.

[2] S. Y. Nam and S. Djuraev, "Defending HTTP web servers against DDoS attacks through busy period-based attack flow detection," *KSII Trans. Internet Inf. Syst.*, 2014, doi: 10.3837/tiis.2014.07.018.

[3] R. Sanjeetha, A. Prasanna, D. Pradeep Kumar, and A. Kanavalli, "Mitigation of Controller induced DDoS Attack on Primary Server in High Traffic Scenarios of Software Defined Networks," in *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, 2018. doi: 10.1109/ANTS.2018.8710066.

[4] M. Boussard, S. Papillon, P. Peloso, M. Signorini, and E. Waisbard, "STewARD:SDN and blockchain-based Trust evaluation for Automated Risk management on IoT Devices," in *INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019*, 2019. doi: 10.1109/INFCOMW.2019.8845126.

[5] J. Wang, X. L. Yang, M. Zhang, K. P. Long, and J. Xu, "HTTP-SoLDiER: An HTTP-flooding attack detection scheme with the large deviation principle," *Sci. China Inf. Sci.*, 2014, doi: 10.1007/s11432-013-5015-2.

[6] A. Amuthan and P. Harikrishna, "Mean availability parameter-based DDoS detection mechanism for cloud computing environments," in *Lecture Notes in Electrical Engineering*, 2019. doi: 10.1007/978-981-10-8663-2_12.

[7] M. Muthuprasanna and G. Manimaran, "Distributed divide-and-conquer techniques for effective DDoS attack defenses," in *Proceedings - The 28th International Conference on Distributed Computing Systems, ICDCS 2008*, 2008. doi: 10.1109/ICDCS.2008.10.

[8] S. Behal and K. Kumar, "An experimental analysis for malware detection using extrusions," in *2011 2nd International Conference on Computer and Communication Technology, ICCCT-2011*, 2011. doi: 10.1109/ICCCT.2011.6075135.

[9] "Proceedings - International Conference on Network Protocols, ICNP," *Proceedings - International Conference on Network Protocols, ICNP*. 2016.

[10] J. Tang, Y. Hao, Y. Cheng, and C. Zhou, "Detection of resource-drained attacks on SIP-based wireless VoIP networks," in *GLOBECOM - IEEE Global Telecommunications Conference*, 2010. doi: 10.1109/GLOCOM.2010.5684028.

e

CHAPTER 10

DEFENDING WBANS AGAINST SECURITY AND PRIVACY THREATS

Mr. Kiran Dhanaji Kale, Associate Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - kirandhanaji.kale@presidencyuniversity.in

ABSTRACT:

With the use of sensors and radio channels, wireless body area networks have made remote health monitoring simpler (WBANs). WBANs capture in-the-moment health information using bio-sensors that are placed on or within the human body. These sensors use wireless communication channels to gather data and then transmit it to a medical server. Readings related to human health are very important, yet wireless channels are not always safe. As a result, WBANs are uneasy about security and privacy. The most typical target of an intrusion in WBANs is a sensor node. The WBANs' medical server and communication routes are similarly vulnerable to intrusion. WBAN is hence in need of protection when transmitting sensed data to the medical monitoring system. When sending the data to the server, we must also preserve secrecy. Wearable body sensors have been popular in recent years for use in sports, fitness training, and health monitoring. To raise people's awareness of their health, businesses are releasing smart products with wearable sensors built in. WBAN assists in gathering a patient's home health readings.

KEYWORDS:

Attacks, Encryption, Privacy, SecureKey, Security.

INTRODUCTION

A lot of people use insulin pumps to check their blood sugar levels. In the event of an insulin shortage, these pumps are configured to start and alter the dose amount. Heart patients utilise implantable cardioverter defibrillators (ICDs) as pacemakers. Using the radio channels, ICDs may be remotely programmed and managed. ICDs are programmed by the government to deliver electric shocks in the event of a sluggish heartbeat. Business organisations provide several different patient remote monitoring services [1].Technology's role to raising human standards of living may also be utilised directly against a patient[2]. The interoperability of network devices raises the security risk. Research has shown that insulin pumps may be compromised and dose amounts changed. The wireless connection between a device and a remote interface may be hacked, making insulin pumps unreliable. Halperin et altests .'s on pacemakers showed that they are subject to a variety of radio-attacks. The intended radio-attacks were able to modify the ICD's settings and decode the patient's name, medical history, type, and ID. So, the user of a pacemaker immediately runs the danger of losing data integrity and privacy[3], [4].

These flaws sparked research to develop WBANs that fulfil security and privacy standards. WBAN is an example of an IoT application in the healthcare industry. Several security criteria apply at various levels of the layered IoT architecture. Several security issues that might exist at the physical, data connection, network, and transport layers in WBANs were examined by Javadi and Razzaque. They did not, however, discuss the alternatives offered to

satisfy the security and privacy criteria for WBANs. The various methods for ensuring the security and privacy of WBANs that were covered in this chapter.Risks to Security in WBANs: WBAN is vulnerable to security and privacy issues in a similar way to other wireless networks. In WBAN, privacy plays the function of maintaining the patient's medical privacy, while security guards against spoofing of the physical nodes and channels used for intra-BAN and inter-BAN communication. Although inter-BAN communication refers to communication between two or more BANs implanted on various bodies, intra-BAN communication in WBANs refers to communication between sensor nodes and the coordinator. A hacker who poses as a legitimate node might cause incorrect readings in intra-BAN transmission. For sending data to medical servers, WBANs also offer inter-BAN communication. Intruders have access to the inter-BAN communication, where they may pose as a real BAN network to facilitate relaying and get readings of other people[5], [6].

The three-tier architecture that WBAN uses is composed of a tier-1 PAN (personal area network), a tier-2 LAN, and a tier-3 WAN. In WBANs, the coordinator node, also known as the hub or base station, receives data from the nodes implanted on the human body and transmits it to the coordinator node. The intruder in WBANs attacks the sensor nodes, medical server/local server, and channels. There are two types of attacks: passive and active. In a passive attack, the attacker does not alter the data; in an active attack, the attacker does. It provides a summary of the potential attack vectors, attack types, and WBAN. These are a few methods of attacks in WBANs that are covered:

Attack by Fabrication

Only verified individuals should have access to the patient's medical information. Each individual must register in order to be granted access to a patient's medical information. It might be a medical professional, a nurse, a member of the family, or a reliable friend. Unauthorized individual has access to patient information via a fabrication attack. Authorization risk results from the fabrication assault.

Masquerade Assault

When a stranger node poses as a member of the WBAN, a masquerade attack has taken place. The impersonator may submit his cardiac rate in place of the patient's, leading the medical staff astray. The validity of the gathered medical readings is at stake due to the masquerade assault.

Eavesdropping

Eavesdropping is a covert assault that compromises confidentiality. An observer listens in on the conversation while remaining still. The patient may not always feel comfortable disclosing every medical information. For instance, the patient's AIDS report may be a private record that he would never want to share with others. The confidentiality of a patient's health condition will be violated by unauthorised access to this information via a hacked sensor node or communication route.

Modification Attack

To guarantee that the patient's diagnosis is accurate, a doctor must get proper medical information. Unfortunately, because to a lack of security, the information may be tampered with, and an intrusive party might alter medical findings. This kind of assault, also known as a modification attack, results in integrity loss.Other assaults DoS, jamming, and tunnelling assaults are further sorts of potential attacks. These assaults might make it difficult for victims to get medical care. The medical information is really significant. WBANs must be resistant to the aforementioned types of assaults. In tier-1, techniques are needed to identify

intruders who attempt to pass for real members. It is also necessary to safeguard the wireless channel used for tier-2 medical report sharing. Designing lightweight security methods is another prerequisite for achieving security and privacy in WBANs with resource limitations. Other parts go into how human body and channel features may be used in WBANs to identify intruders at tier-1, as well as how security at tier-2 is given to protect communication across the channel.

WBAN Security Without Encryption

The ability to use a variety of network features to allow secure conversations is made possible by the interoperability of the devices used in WBAN. Many encryption and decryption methods are suggested in literature. Nevertheless, they are not appropriate for WBANs with limited resources, particularly intra-WBAN communication. Using channel characteristics and network attributes has enabled security in WBANs.

Three Safe Key Exchange Techniques for Encryption-Based Cryptosystems in WBANs

Commonly used key exchange cryptographic algorithms provide safe communication between parties interacting remotely. Key management requires a lot of energy. By sharing the responsibility for key management among the network participants, cooperation has made it viable to deploy key encryption in energy-constrained intra-WBANs. One such example of group key management is explained in discussion of group-based collaboration.Asymmetric and symmetric key encryption schemes are also available. A pair of public and private keys are used for encryption and decryption, respectively, in asymmetric key encryption techniques. Only the associated private key may be used to decode a communication that has been encrypted using a public key. Communication parties utilise a single key for both packet encryption and decryption in symmetric key encryption. The difficulty with key-based encryption is safely distributing keys among the communication parties. The man-in-the-middle attack, a fairly common issue in cryptography, affects symmetric key agreements.

Public/private key pairs used in conjunction with certification offer an additional degree of protection. By certifying the public key, a certificate aids in verifying the other party. As a result, in certification-based cryptosystems, both the certificate and private key are required to decode the data. On the other hand, there are methods for public key cryptography (CL-PKC) without certificates. Instead of utilising certificates, the public key in CL-PKC is authenticated by a third trusted entity, such as the network management. The CL-PKC method eliminated the need to manage certificates. The issue of key distribution is resolved by jointly creating keys at the two endpoints. This eliminates the need for key sharing across an unsecured connection [7].

Techniques for Asymmetric Key Generation

With asymmetric encryption, public keys are publicly accessible to all parties. Asymmetric keys are very helpful in thwarting repudiation attempts since they are used to create digital signatures. When a patient repudiates after sub- mitting the health data, repudiation happens in WBANs. Similar to this, a doctor may act dishonestly and insist that a patient did not get a certain prescription. The distribution of asymmetric keys is not as difficult as that of symmetric keys. For creating public-private key pairs in asymmetric cryptosystems, the elliptical curve cryptosystem (ECC) is often employed.

Techniques for Generated Symmetric Keys

The two techniques for safely generating symmetric keys at the two endpoints are described in this section. In the first way, a physiological signal based on human activity is used to create a secure key for WBANs, while in the second method, ECC is used to create symmetric keys.

Key Generation Based on Physiological Signals

In order to provide secure communication in WBANs, Venkatasubramanian et al. devised the physiological signal-based key agreement (PSKA) key exchange mechanism. Physiological signals are particular and change throughout time. Hence, due to their dynamic nature, physiological signals may be used as a cryptography key. Only the nodes that are placed on a human body in PSKA are aware of that body's physiological signature. As a result, a node outside the body is unable to decrypt the key created using a specific human physiological signal. Moreover, the BAN user's reliance on the physiological signal assures that each subject will have a unique key.To communicate secret keys, PSKA employs the fuzzy vault system for symmetric key-based encryption. A polynomial of order v and a vector of features created by trustworthy nodes associated with the BAN are used in fuzzy vaults. The nodes are already aware of the polynomial's order and the parameters used to build the feature vector. A collection of results called output Y is produced by fuzzy vault (vault). When mapped into a polynomial function, each member of the set X consists of a pair made up of a single feature vector and its value.

The message security is increased by adding chaff values to X. Chaff values are the collection of points that were chosen at random. As a result, feature pairs and chaff values make up the output set X. The same parameters provided by the transmitter are utilised to construct feature vectors on the receiving end. Receiver only knows the order of a polynomial, not its precise value. He constructs his own vault Y by interpreting a polynomial. The received vault X is then matched with pairs created in Y. If not enough pairs are matched, the receiver modifies the polynomial's coefficients. A symmetric key is considered to be the coefficient for which there are enough pairs of Y that match the received vault X.Since nodes not in the same BAN cannot produce the same physiological signal vector and, thus, cannot produce the same set of vault, PSKA precludes man-in-the-middle attacks. Even if the feature vector is breached, an outsider still won't be able to hear the whole conversation since physiological signals fluctuate over time and alter the feature vector. Real-time security is enabled via PSKA. The odd creature finds it more challenging to identify the non-chaff pairings as a result of the more chaff points.

A Symmetric Keys-Based Certification-Based Authentication Scheme

Detecting heart attacks or sleepiness early on may assist to lower the number of traffic accidents. The incidence of traffic accidents may be reduced by using body area networks (BAN). If it is feasible to determine the driver's present state of health, BAN may provide help while driving. The electronic control unit (ECU) of the vehicle is employed as a hub and the vehicle's resources are made use of. The data is gathered and processed by the ECU, which also gives the driver feedback. An authentication and encryption module that may be used together or separately to provide secure communication was described by Wang et al.For authentication, the IEEE 802.15.6 certificate validation technique is employed. The ECU verifies the new node's certificate. The certificate is first examined and verified. The username and password are then sent to the node. Password is confirmed by following challenge-response authentication. Every time a new node (with a login and password) wants to join the network, it encounters a problem. The biometric information that the nodes acquire

may provide a problem. In response, the new node creates a 256-bit secret key using the trusted members'-only secure hash algorithm-256 (SHA-256). The hub also generates a response, which is compared to the answer obtained from the new node.

Group Collaboration

In group-based collaboration, a WBAN's sensors are all similarly designed and work together as a virtual group (VG) to complete a single task. The participants in this single application collaborate to improve the effectiveness of the network. To guard against interception attacks in WBANs, a group-based symmetric key generation approach has been suggested [24]. The coordinator node creates the key using the RSSI values of each member of its VG. In order to get the symmetric key at both ends, authors took use of the RSSI's reciprocity characteristic (sender and receiver). The new node that wants to join the current VG must have the key to interact with every member of the group since this is a symmetric key algorithm. The authors assert that giving the coordinator of the VG exclusive responsibility for symmetric key generation will result in more resource use. They recommended distributing the responsibility of key generation among all group members. The new node sends a message on the multicast address that the VG is allocated, and all of the VG's members receive it. The current members then determine the RSSI value of the signal that was received from the new member and acknowledge the probe message. The RSSI value of each group member is obtained from the acknowledged message by the new node, which is then used to build the key.

On the other side, the group members provide the coordinator node the stored RSSI value (which was taken from the probe message given by the new node). Due to the reciprocity attribute of the RSSI value, the coordinator and new node have the same set of values to construct a symmetric key. The suggested solution saved energy by preventing direct connection between a new node and VG members. The assessment setup included four MICAz motes that communicated through Zigbee and a weak antenna. According to the approach tested on the setup, it is challenging for a listener to get all of the RSSI values in order to build a key that is identical.

Cloud-Assisted WBAN Security

Huge amounts of traffic are produced by continuous patient monitoring, necessitating high storage, effective use of resources, and speedy answers. With the use of cloud computing, WBANs may now provide rapid, low-cost services. The detected data is sent to the cloud, where it is stored and pre-processed to provide the necessary services. The cloud aided WBANs (CAWBANs) architecture is shown in Figure 8.3. Wherever, at home or in the workplace, a person with sensors on his body may be found. Data from the senses is gathered and sent to the cloud through cellular network by the coordinator node linked to the human body. The cloud-stored data is accessible to both patients and doctors.Clouds are set up with powerful computers and data storage. Via the provision of additional processing power, cloud aids in improving the performance of WBANs with resource constraints. Doctors and family members now have easier access to data thanks to mobile cloud computing (MCC) . Clouds may be configured to give the network the ability to make its own decisions. A successful assault on the cloud, however, has the potential to seriously harm several people. Several security concerns about MCC and the integration of the cloud and IoT were covered by Stergiou et al. The next sentences go through several strategies required to maintain security and privacy in CAWBAN.

Authentication at the cloud server, user anonymity, and repudiation attack prevention utilising CAWBANs without the usage of certificates and encryption keys are all covered in this section. We explain a technique developed by Shen et al. that protects user anonymity by using the user ID's hash value rather than the user's real ID. They took into account three elements in their model: users, NM, and cloud server (CSr). Before offering services, CSr is expected to register with the NM, which is assumed to be the trustworthy party. Initialization, registration, and authentication are the three stages of the minimal certificate-less security protocol.Initialization: NM publishes essential parameters with the name params at this stage. The NM and users create public/private key pairs using ECC utilising parameters. Using Eq, the public key Q is produced (8.4). A private key is considered to be the order k that was used to create the public key Q. K is designated as s for the NM and sU for users in this case. Randomly selected from the cyclic group indicated in params are the private keys s and sU. The same process is used by the CSr to create his public/private key pair.

Registration

Each user registers themselves with the NM after activation. The NM is expected to get the user id IDU beforehand. The user who desires registrationtransmits to the NM the hash value of his ID and public key QU. This hash value is used by the NM to confirm that the user is present in his database. The user is given an index number and a signature after being validated. The NM additionally checks the CSr against its ID IDC that is kept. The user is then added to the CSr database when the CSr has successfully confirmed the index number of the user.

Authentication

The CSr receives a service request from a user. The service request includes the hashed public key, coded index number, and current time stamp (tC). When the CSr receives a request, he decodes the user's hashed index number and compares it to the record that was stored in his database during the registration process to verify the user's identity. The request message's integrated time stamp aids in spotting illegitimate requests. The CSr creates a session key and message authentication code for the subsequent communication after the user has been declared valid. A value T 1 generated using Eq. (8.4), where k is a random member of the cyclic group mentioned in the parameters, is included in the authentication code. It also contains the session key and hash value calculated by applying a hash function to the user's public key, QU, and the current time stamp, tC. The user decodes the session key after getting the answer to their request.

Cryptography Based on Pairing Data saved in the cloud may also be kept secure using pairing-based cryptography. In pairing-based cryptography, two additive cyclic group numbers are coupled to create a multiplicative cyclic group number. The function provided by G1 G1 G2 is a pairing-map. It is believed that the key generation centre will provide asymmetric key pairs to the patient, doctor, and cloud (KGC). They made use of asymmetric key pairs to guarantee privacy. The connected body sensors' medical information are gathered by the patient's mobile device and uploaded to the cloud. With his public key, the patient encrypts his medical information. As a result, only the patient has access to the patient's reports since the private key is required to unlock the message. Symmetric key encryption is utilised for authentication between the two parties, which might be the cloud and a patient or the cloud and a doctor. The following processes are used by both communication parties to compute the session key at their respective locations.

1. A patient (or doctor) generates a message with a current time stamp and a bilinear pairing of their private key and the cloud's public key. The message is then sent to the cloud together with the patient's identify after being encrypted using the cloud's public key (or doctor).
2. After receiving the message, cloud uses his private key to decode it and compares the time stamps on the current and received messages. The authentication of the time stamp prevents replay assaults.
3. Cloud employs bilinear pairing on the patient's (or doctor's) secret key and the public key they have obtained. The bilinear pairing value extrapolated from the received message is then compared to the pairing result.
4. Both the sender and the receiver use the same hash function on the paired value to create the session key. Now that the session key has been converted to a symmetric key, both parties may encrypt their communications.

Many assaults, including man-in-the-middle and replay attacks, are avoided by using this technique. To open the reports the patient uploaded to the cloud, however, the patient must provide the doctor his private key. A patient's private key cannot be renewed, thus once it has been compromised, it may be constantly exploited against the patient.

Healthcare Cloud Computing and Multimedia

The development of smart cities was aided by IoT and cloud computing capabilities. The IoT age has made it feasible to monitor patients intelligently in a variety of ways. Video surveillance is an effective use of multimedia to keep up with the patient's activities. Bulk data generated by video surveillance is compressed and sent across networks. The multimedia data must also be protected when crossing the channels. In the context of smart cities, Memos et a .'s suggested a secure routing strategy that makes the claim that it secures the identity, path, and position of the sensor node. With this multi-hop routing, a packet is always routed to a reliable neighbour node. A node won't forward a packet if there are no reliable nodes in the area. Due to routing decisions made at each stage, the header of the forwarded packet is altered at each hop. The safety of the packet is ensured by the recalculation of the packet header at each hop. To spoof the packet, the intrusive party must keep up with the changing header, which is challenging.

The repudiation attack may also be stopped by using a watermark created from the user's signature. Using a genetic algorithm (GA), key frames are taken from the video and divided into RGB parts. A video's size may be decreased by choosing important frames. The watermark is then randomly put into each component as a signature. As a result, a watermarked video is produced and uploaded to a public cloud. By encrypting the watermark signatures with a key, the integrity of the video material is preserved. As the watermark is encrypted, an intrusive party cannot easily replicate it.

Avoiding Unreliable Authorized Users

The methods that have been explored so far aim to restrict access to the data. Yet, it is possible that the attacker, who would be the unreliable authorised user, is the only one within the network. Many methods exist for managing trust, including trust-based data access and trust-based routing system. All feasible pathways for trust-based routing are rated in accordance with the trust value of the nodes that make up the path. Similar to this, trust-based evaluation only permits access to private data after determining the trust value. Reward and punishment feedbacks are employed in trust management mechanisms. For instance,

Boukerche and Ren evaluated the nodes' level of trust using the incentive and punishment technique. Nodes that work together to transmit data safely get rewards. Conversely, naughty nodes face consequences for their misbehaviour. Node may also be removed from the network if the degree of confidence declines. A technique to offer security at a medical database was created by Kaur and Sood (20). Three factorsthe number of bad acts performed by a node in the past, feedback from immediate neighbours, and third-party inputare used to award a trust score to each authorised party. The first component is the count of bad actions committed by a node in the past [8].

Six Open Problems

There are still problems after a number of methods have been suggested to accomplish security and privacy in WBANs.

1. Flexibility: With WBANs, authorisation may keep on changing according to the necessity and thus need to be adaptable. For instance, a nurse who has permission from a certain WBAN may change her position. Now when a new nurse needed to access this WBAN, the old procedures did not allow for this flexibility.
2. Responding to a crisis: In order to protect patient privacy, the majority of techniques provide patients access control over their data. Nonetheless, in an emergency, a patient cannot give family members or any new physicians access to his BAN. For
3. For instance, the method used by Chen et al only permits the patient to decrypt his report. Such cases need the use of backups for unexpected events.
4. Interference: To improve throughput and maximise energy use, WBANs offer inter-WBAN communication. But, security and privacy are hampered by data passing via other networks. Communication between WBANs is severely hampered by signal interference. The literature has not yet addressed the security and privacy issues related to interference.
5. Single point of failure: The processing and storage capacity of WBANs have increased thanks to cloud technologies. Yet, the cloud may be used as a single point of failure in CAWBANs. The security systems in place are not resistant to this failure.
6. Trust problems Current techniques concentrate on finding network intruders. The instances when the offender is present inside the network are yet unstudied. Each technique counts on the coordinator to be a reliable party; nonetheless, this assumption is still problematic.
7. Energy considerations: WBAN implanted nodes cannot be recharged. It is highly challenging for nanoscale devices to store enough energy inside of them to lengthen the network's lifespan. The strain on these devices is increased by a sensor-level cryptosystem. Because of this, there is always need for more energy-efficient, lightweight security and privacy-preserving techniques that aid in enhancing WBAN services.

CONCLUSION

The introduction of next-generation medical services aims to improve lifestyle and health-related factors. As compared to routine doctor appointments, medical treatments delivered at home are able to save time. WBAN delivers immediate diagnosis and manages emergency circumstances. As a patient's medical readings are sensitive information, WBANs must take data security and privacy seriously. This chapter covered numerous attack methods that may be used against WBANs' three-tier design. Commercial health gadgets are not equipped to

fend against security and privacy intrusions, according to the discussion of these products. We described how resource-constrained WBANs may have security via the establishment of lightweighted security mechanisms. The utilisation of human body traits and channels to create connection fingerprints and safe communication is then briefly discussed. The cloud-based CAWBANs expanded the attack surface while simultaneously enhancing the usefulness of WBANs. We spoke about the usage of certificateless and certification-based cryptographic techniques to protect cloud communication in WBANs. The chapter includes a brief explanation of how to protect medical photos and videos while they are being transferred over a network. We provided a list of current open problems in WBANs for future development to provide widely accessible secure wireless health services.

REFERENCES

[1] B. Narwal and A. K. Mohapatra, "SAMAKA: Secure and Anonymous Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks," *Arab. J. Sci. Eng.*, 2021, doi: 10.1007/s13369-021-05707-3.

[2] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, and H. Karimipour, "Cyber intrusion detection by combined feature selection algorithm," *J. Inf. Secur. Appl.*, 2019, doi: 10.1016/j.jisa.2018.11.007.

[3] F. Skopik and S. Filip, "A blueprint and proof-of-concept for a national cyber security sensor network," *Int. J. Cyber Situational Aware.*, 2019, doi: 10.22619/ijcsa.2019.100129.

[4] R. Devakunchari, Sourabh, and P. Malik, "A study of cyber security using machine learning techniques," *Int. J. Innov. Technol. Explor. Eng.*, 2019.

[5] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," *Appl. Sci.*, vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.

[6] A. Iqbal, M. Guo, L. J. Gunn, M. A. Babar, and D. Abbott, "Game theoretical modelling of network/cyber security [Review paper].," *arXiv: Computer Science and Game Theory*. 2019.

[7] S. Han, S. Zhao, Q. Li, C. H. Ju, and W. Zhou, "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation with Fault Tolerance," *IEEE Trans. Inf. Forensics Secur.*, 2016, doi: 10.1109/TIFS.2015.2472369.

[8] J. John, M. S. Varkey, and M. Selvi, "Security attacks in s-wbans on iot based healthcare applications," *Int. J. Innov. Technol. Explor. Eng.*, 2019, doi: 10.35940/ijitee.A4242.119119.

CHAPTER 11

FOG COMPUTING ENVIRONMENT: DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Dr. Sreenivasappa Bhupasandra, Associate Professor,
Department of Electronics & Communication (Communication System Engineering),
Presidency University, Bangalore, India.
Email Id: - sreenivasappabv@presidencyuniversity.in

ABSTRACT:

The processing and storing of data or information is one of the most significant functions carried out by cloud computing. The idea of fog computing has been suggested as a solution to the cloud's overload caused by the ongoing advancement of technology. Fog computing extends the benefits of cloud computing to the edge of the network while also overcoming its drawbacks. Despite the rising popularity of fog services, ensuring data security and privacy remains a difficult task. In terms of security considerations, distributed denial of service (DDoS) attacks are a well-known danger and the major ideas of fog computing, DDoS assaults, and several DDoS mitigation approaches.Organizations may utilise cloud computing as a service to consume computer resources like an application, storage, or virtual machine (VM). Similar to this, we utilise power at home rather than constructing and maintaining substantial infrastructure.

KEYWORDS:

CloudComputing, FogComputing, DoS, DDoSattack

INTRODUCTION

Users of cloud computing may focus only on growing their main businesses without having to worry about anything else. It offers access to the reconfigurable system on a global scale. The system comprises of higher-level services and a pool of resources that are shared. As a result, managerial activities are reduced to a minimum. In addition to usefulness, it also imports coherence and the economies of scale. It mostly uses the Internet to provide hosted services.In a metaphorical sense, it represents a collection of networked components that may share resources but are not individually addressed or handled by users. That can be as hazy as a cloud. It has suggested a "pay-as-you-go" approach that would allow users to purchase resources in accordance with their demand. A frequent illustration of this is Amazon EC2 (Elastic Compute Cloud). About 1996, cloud computing first became popular.

Computerized Fog

This section is divided into many subsections that together discuss fog computing. A basic overview of fog computing is provided and its history is discussed. The properties and uses of fog computing are described and the security concerns and difficulties with fog computing are discussed respectively.

Overview of Fog Computing

Fog computing is a concept where applications focus on devices at the network's edge and data is processed there rather than moving practically all of the workload to the cloud. In the IoT network paradigm, Cisco Systems referred to it as a "new concept" for reliable wireless

data transport to scattered devices (Internet of Things). Peer-to-peer communication between the devices in this setup allows for effective data exchange and storage while making judgements locally.Both IBM and Cisco Systems, who like the term "edge computing," have open-ended initiatives that push the state of the art in computing to the network's edge devices. The earth is covered with fog computing devices, which have very dependable computing power and data processing, such as routers and sensors.

Fog computing is being focused on in order to process data locally at smart devices rather than transferring it to the cloud. An method called fog computing addresses the growing IoT (Internet of Things) of connected devices. Fog computing replaces the cloud's ability to create channels for storage and use at the cloud layer. It serves just to maintain all transactions with the required resources at the network's edge.Fog computing is used since it does not deliver all of the information to the appropriate cloud channels. It only compiles the data from certain access points. This distributed technology may help to save costs overall and increase productivity. Massive data and services are placed extremely near to the cloud system due to the way the system is structured [1]–[3].

All of the smart gadgets are engaging with cloud devices via fog devices. Each smart gadget has a connection to a fog device, which is connected to a cloud device, and so on, creating a working communication. The main goal of fog computing is to increase productivity while reducing the amount of data that must be sent to the cloud for processing, analysis, and storage. To encourage the use of fog computing in industries and fields of study, one must take into account both its benefits and constraints. Table 20.1 lists the benefits and limitations of fog computing.Three levels make up the hierarchical structure of fog computing, the cloud layer, the fog layer, and the end-user layer. These levels are all very important to the hierarchical design of fog computing and are further detailed below:At one extreme, the centre of the cloud layer: It offers various application services, such as smart transportation, a smart home, a smart factory, etc., together with storage devices and high performance servers. It is already a well-known location for data storage. It can also do in-depth analysis to help computation.

Modeling Security Threats in Fog Computing

Many security vulnerabilities may occur at various frameworks by using various technologies and observing the severity of the attacker's assault. The network framework, service framework, virtualization framework, and end-user devices are defined as the security threat model.

Network Architecture

Fog computing, as mentioned in the part above, links edge devices that use various networks for communication. the the an a be the a the a the a the a The a The re be the The the. the Certain communication framework weaknesses are attackable. The following are the dangers that have emerged:

Man-in-the-middle (MiTM) Assault

In this kind of attack, the attacker launches an attack after it seizes control of a network segment, as described in. attacks like traffic injections or eavesdropping.

Lack of Service Availability

This is often referred to as a distributed denial of service (DDoS) attack or a denial of service (DoS) assault. All communication networks are under risk. Because to its restricted breadth, this strike cannot totally harm. Because of its architecture and established protocols, the network's proximal devices will be disturbed by the core framework.

Crooked Gateway

In this case, the attacker compromises the gateways due to certain end-user devices' open design. It yields the same outcome as MiTM.

Data Centers at the Edge

Certain management services and virtualization servers are anchored in the edge data centres. For an attacker taking into account different APIs to access points, it is advantageous to target the data centres at the edge. The following would pose a major security threat:

Physically Bruised

The limitations are not secured against physical harm or shielded from it, as in the case of small enterprises employing a cluster of fog nodes. The attacker must be close to the target devices in order to carry out this assault; otherwise, it will be unable to destroy the targets. As a result, the attack's scope is restricted to a narrow region since there may be several witnesses, which means it will only physically damage that area.

Privacy Drained

In this case, an insider attacker or an adversary with benign intentions may monitor the information flow, violating privacy. While this assault has a small area of influence, if the knowledge is spread wider, its consequences might be severe.

Acceleration Advantage

This attack gives the external intruder access to numerous controls over end device services (there may present an internal intruder as well). Hence, handled with limited security, which either results in incorrect configuration of the framework or lack of adequate maintenance.

Service Exploitation

The attacker may abuse the services after the invader has access to control over services. Access acquired either via accelerated advantages or by taking use of internal information or perks.

Crooked Data Centre

Under the aforementioned scenario, the attacker has a number of advantages, including total command over the services that will be attacked next. Also, it facilitates information transfer to other data centres and takes use of any interfaces with other external systems.

Basic Architecture

The primary cloud and mobile core management system that make up the core architecture make it impossible to totally trust any interactions with cloud providers. This might be due to cybercrimes or other factors encroachment by government. A thorough taxonomical analysis of clouds is provided.

Privacy Drained

In order to access services or resources, terminal devices communicate information or data with the other levels, which drains privacy.

Service Exploitation

Dispersed Fog's design means that not all of the network is affected by an attack, but certain portions are still weak points that might provide false positive findings.

Twisted Framework

Although this assault on certain network limitations is unlikely, it might nonetheless have a significant effect. Some fault tolerance and security mechanisms must be implemented if the attack is successful in shutting down the whole network.

Virtualized Framework

Be a little more a little bit more a little bit more a little bit more a little bit more a little bit more a little bit more an a and a

Lack of Service

An attacker may attempt to prevent access to resources by abusing them excessively. Most edge data centres lack many of the resources seen in conventional cloud architectures.

Resource Exploitation

Instead of assaulting endpoints, the attacker targets network-wide local and distant restrictions.

Privacy Drained

Because the framework is opaque, it's possible that several APIs are implemented. It could allow access to details about its logical and physical network, including node status. These APIs must be protected by some kind of security system; otherwise, they risk being attacked and losing confidential data.

Acceleration Benefit

Infected virtual machines (VMs) increase the risk of attack. Some advantages of acceleration occur when the infected VM manages network restrictions or when it fails to provide isolation, changing the behaviour of the other VMs. This is possible because to the VM network's ability to roam around.

Manipulated VM

When injected VMs are in control of the network, they may launch a variety of assaults. Information may be extracted and changed, and security can be breached by introducing malware or logic bombs into the network.

Devices for End-Users

As they are an active participant, they have a significant role in the network. They eat up the services but could include some end-user nodes that are compromised, leaving the whole system open to attack.

False Positive Outcome

If the system is penetrated at this level, there is no assurance that the data or information being sent over the network is accurate, which results in a false positive outcome (true result due to incorrect information). The information transmission may be the result of internal sensor network aberration.

Service Exploitation

In this scenario, devices deliver services to the network under the control of a hacked virtual machine (VM), which functions as a distributed system. They are exposed because data may be changed.

DDoS Attacks in A Foggy Environment

The DDoS assault is briefly described in this section. Maintaining the security and accessibility of data in the network is difficult despite the rising demand for cloud services. The DDoS assault significantly impacted the network's overall performance.

Taxonomy

Technology improvements enhance the likelihood of more serious dangers, notably DDoS assaults. The attacker takes control of the systems by barrage the target with malicious requests. The system's services will then run out as a result provide examples of such effects, such as service unavailability [4]–[6].

DISCUSSION

Uses and Features of Fog Computing

It is necessary to thoroughly research fog computing. It may be done by outlining its features and uses, which is what the sub-sections do.

Fog Computing Characteristics

The qualities listed below are necessary for building a fog layer. Location Awareness, Close Proximity to End Users, and Minimal Latency There is a hint of conventional methods for dealing with fog. At the network's edge, they provide services to the terminal nodes. Moreover, they enable edge-based or low-latency applications like video streaming, gaming, etc.. Proof of fog computing's lower latency than cloud computing is also discussed in.

Geographical and Decentralized Distribution

In contrast to centralised cloud computing, fog computing requires geographically dispersed fog nodes. When streaming high-quality data, they take part in a few active roles, exceeding 20 The 499 which is required for moving vehicles: A Complete Study of Distributed Denial of Service Access points and proxies situated at railways and roadways enable the real-time applications. Fog computing, for instance, may provide extensive services based on the interaction and connectivity of vehicles with one another and with access points.

Heterogeneity

Between cloud data centres and end devices, a platform called fog is thought to be highly virtualized. At the edge of the network, they provide storage, computation, and processing network services—the three components that make up both fog and the cloud. Fog nodes are heterogeneous because they are virtualized platforms that may be employed as computational or virtual network nodes. High-speed lines to data centres are not the sole sources of heterogeneity; WLAN, Wi-Fi, and other wireless technologies also provide wireless access to end users [7], [8].

Federation and Interoperability

Data streaming is an example of a service that fog can provide. Fog nodes must provide cooperative and federated services across domains since these services need the collaboration of many providers.

Conserve Bandwidth and Use Less Energy

Cloud computing calls for the transmission of raw face photos to the cloud in the face recognition and resolution technique. Certain management strategies for mobile nodes' short-range communication and optimum energy use successfully reduce energy usage.

Fog computing is referred to as greener computing by Sarkar and Misra. In, a model of energy consumption based on time and flow was proposed.

Mobility Assistance

Fog must be able to connect with mobile devices directly in order to function properly. This will make it easier to implement mobility-related approaches like the LISP protocol (LISP-MN). The LISP protocol needs a distributed directory system that decouples location identification from host identity. Mobile fog nodes may be used on trains and moving vehicles, as well as at coffee shops, airports, and other static locations.

Data Security and Complete Security

When required, fog analyses sensitive data on site rather than transferring it to a faraway data centre. Fog node protection is handled by Cisco security and cybersecurity solutions in the same way that it is handled for other IT assets. Fog may secure data by isolating it and encrypting it, and it can also reduce dangers that may develop during system upgrades. Real-Time Applications. In addition to providing terminals with rich features that assist satisfy application needs, the Internet's data transfer is minimized. In the actual world, these applications are often time-sensitive. It uses real-time interactions as opposed to batch processing. They said in that the usage of fog computing decreased the reaction time for face recognition and resolution field.

Smart Grid applications for Fog Computing:

Energy load balancing applications may be used on equipment at the network's edge, such as micro grids and smart metres . Based on energy demand, needs, availability, and cheap cost, several sources of energy, including wind and solar, are employed. the w. the w. the w. the w. the w. the w. the w. the w. the by the the the by the the the The actuators of the control instructions are also given access to the processed data. Fog provides support for semi-fixed storage at the top layer and volatile storage at the lowest layer. With the use of business information analysis, the cloud issues global insurance.Cyber Physical Systems (CPS) and Internet of Things (IoT) The Internet of Things (IoT) is a network that connects physical things to a specific network. Fog computing is utilised in embedded systems in this context because the computers and software are integrated into the gadgets for purposes other than computation.

Security Issues with Cloud Computing

Authentication and Identification

Maintaining end user authenticity is a crucial challenge with the increasing number of devices. Every end user's security credentials must be effectively handled and updated on a regular basis, along with the security software.The current situation does not have any reliable identification mechanisms, yet fog computing does operate. Since end users do not need to be able to access the authentication server, there is less overhead for fog. Moreover, they provide edge data centres' authentication. In order to enable mutual authentication between fog nodes and fog users, Huang et al. devised an authentication system at the user level.

Access Control Systems

Here, the rights granted to a certain user are shown in the access control list (ACL). Unauthenticated users must not be allowed access at all since doing so would lead to information fabrication and breach. According to writers in, attribute-based encryption is used to establish access control policies and rules based on attributes (ABE). Several policy-

driven management modules that assist the orchestration layer of fog are included in the policy management architecture in.

Strained Resource Devices

Particularly for the devices with a longer lifespan, the end user devices must include a security mechanism. If their hardware or software is hacked, 506 B. Paharia and K. Bhushan cannot fix it since there is no way to change or modify it. For instance, if any hardware is compromised for vehicle makers and customers who purchased a car, it cannot be fixed after it was sold.

Virtualization

It is one of the most popular study subjects and aids in the definition of different security procedures. That also explains why security measures were extended to the fog. Virtual Trusted Platform Module (vTPM), which secures the storage and offers certain cryptographic operations, is one instance where it may be utilised at the edge.Privacy Sensitive data breaches are more likely to occur if security is compromised. If data is compromised, protection is very necessary since it would seriously affect the system's performance and could even cause it to shut down. Several security protocols, like as those in [8] for anonymous authorisation, provide communication between edge data centres and other system components.

Trust

It is challenging to maintain both a reliable environment and a scalable network in distributed fog computing if there are many nodes.Consider two specific scenarios, first, when cyber-physical systems are compromised, as was the case in the Iranian attack known as Stuxnet, normal messages are exchanged in the forehand to the administrator but a nuclear reactor spins abnormally in the background. Second, many devices that are compromised because they lack any security mechanism may produce false positive results.

Requirements and Network Security

There are several communication technologies, and each one has its own security policies and procedures. So, once communication has been established, each user's credentials are made available to the other users. Every end user's security credentials must be effectively handled and updated on a regular basis using security software. Moreover, rules should be established to preserve network security. They have cryptographic features, as mentioned in, which aided in creating session keys by utilising their qualities as credentials.

Distributed Denial of Service (DDoS)

They presented an architecture in that makes advantage of 5G networks at mobile end users to allocate intrusion detection jobs to the centralised cloud computing services. Fog computing may also be used as a means of solving different procedures and infrastructure for cloud-related issues. For federated cloud computing, which may be expanded to include fog computing, certain early warning systems, such as honeypots, can be installed.

Fog Forensics

Fog forensics may be defined as the use of digital forensics in a fog environment. In, cloud forensics is discussed. Digital forensics may be thought of as a programme that recognises, gathers, and keeps data organised in a certain way. Fog contains a considerable number of sensor nodes, which is why it is regarded as difficult. For instance, maintaining a log for data makes it challenging to analyse and gather data from several nodes.

Modeling Security Threats in Fog Computing

Many security vulnerabilities may occur at various frameworks by using various technologies and observing the severity of the attacker's assault. The network framework, service framework, virtualization framework, and end-user devices are defined as the security threat model.

Network Architecture

Fog computing, as mentioned in the part above, links edge devices that use various networks for communication. The following are the dangers that have emerged.

1. Man-in-the-middle (MiTM) assault—In this kind of attack, the attacker launches an attack after it seizes control of a network segment, as described in. attacks like traffic injections or eavesdropping.
2. Lack of service availability—This is often referred to as a distributed denial of service (DDoS) attack or a denial of service (DoS) assault. All communication networks are under risk. The 508 B. Paharia and K. Bhushan core framework cannot be entirely affected by this attack because to its restricted scope, but it will be disturbed by it because of the way it was designed and the protocols it uses.
3. Crooked gateway – In this case, the attacker compromises the gateways due to certain end-user devices' open design. It yields the same outcome as MiTM [9], [10].

CONCLUSION

For DoS attack, a single connection or a single computer is adequate to exhaust the target, while in DDoS, combination of several machines is necessary. In this case, the attacker has taken control of and infected many machines, which are then used to simultaneously assault the victim. The term "botnets" refers to these hacked systems. With all the bots acting as its slaves, the attacker serves as their master.This chapter examines the security issues with fog computing systems. It examines several architectural designs and provides a security model for each. The chapter also discusses how the CIA model might have an effect on Fog platforms. The advancement of security features in Fog systems is happening quickly, and some recent articles don't go into enough detail to allow for a comprehensive assessment. The chapter ends with a summary of the primary dangers to the two technologies, as well as references to various works in the literature that covered these dangers and the associated attacks.

REFERENCES

[1] J. H. Corrêa, P. M. Ciarelli, M. R. N. Ribeiro, and R. S. Villaça, “ML-Based DDoS Detection and Identification Using Native Cloud Telemetry Macroscopic Monitoring,” *J. Netw. Syst. Manag.*, 2021, doi: 10.1007/s10922-020-09578-1.

[2] A. K. Rangisetti, R. Dwivedi, and P. Singh, “Denial of ARP spoofing in SDN and NFV enabled cloud-fog-edge platforms,” *Cluster Comput.*, 2021, doi: 10.1007/s10586-021-03328-x.

[3] W. L. Costa, A. L. C. Portela, and R. L. Gomes, “Features-Aware DDoS Detection in Heterogeneous Smart Environments based on Fog and Cloud Computing,” *Int. J. Commun. Networks Inf. Secur.*, 2021, doi: 10.54039/IJCNIS.V13I3.5080.

[4] S. R. Zahra and M. A. Chishti, “Fuzzy logic and Fog based Secure Architecture for Internet of Things (FLFSIoT),” *J. Ambient Intell. Humaniz. Comput.*, 2020, doi: 10.1007/s12652-020-02128-2.

[5] Deepali and K. Bhushan, "DDoS attack mitigation and resource provisioning in cloud using fog computing," in *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017*, 2018. doi: 10.1109/SmartTechCon.2017.8358387.

[6] B. Dhiyanesh, S. Sakthivel, R. Radha, and S. Senthil Kumar, "Threshold based DDoS mitigation with fog layer in cloud environment," *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02369-1.

[7] R. R. Gorrepati and S. R. Guntur, "DroneMap: An IoT Network Security in Internet of Drones," in *Studies in Systems, Decision and Control*, 2021. doi: 10.1007/978-3-030-63339-4_10.

[8] M. De Donno, J. M. Donaire Felipe, and N. Dragoni, "Antibiotic 2.0: A fog-based anti-malware for internet of things," in *Proceedings - 4th IEEE European Symposium on Security and Privacy Workshops, EUROS and PW 2019*, 2019. doi: 10.1109/EuroSPW.2019.00008.

[9] S. Bishnoi, S. Mohanty, and B. Sahoo, "A Deep Learning-Based Methodology in Fog Environment for DDOS Attack Detection," in *Proceedings - 5th International Conference on Computing Methodologies and Communication, ICCMC 2021*, 2021. doi: 10.1109/ICCMC51019.2021.9418363.

[10] B. B. Gupta and S. A. Harish, "A risk transfer based DDoS mitigation framework for cloud environment," in *Communications in Computer and Information Science*, 2019. doi: 10.1007/978-981-15-1384-8_10.

CHAPTER 12

INFORMATION SYSTEM MODELS FOR CYBERSECURITY RISK ANALYSIS

Dr. Shilpa Mehta, Professor,
Department of Electronics & Communication (Communication System Engineering),
Presidency University, Bangalore, India.
Email Id: - shilpamehta@presidencyuniversity.in

ABSTRACT:

In fact, as more individuals, companies, and governments rely on information technology, the need of security risk assessment is becoming more and more important. A lack of reliable information security risk assessment, which is regarded as an ongoing process of identifying, resolving, and preventing security issues by providing information systems with the appropriate levels of security, has also contributed to a decline in the security of these systems in recent years. These costs were used to investigate the danger space and identify the source of the risk in that area. Information security threats affect businesses, governments, and people in general. These dangers have the potential to result in considerable harm, including the compromise of sensitive data's confidentiality, loss of integrity, or inaccessibility. In reality, companies might suffer a sizable loss as a result of a financial (or economic) security vulnerability.

KEYWORDS:

CloudComputing, Economic, Requirements, Security, Threats.

INTRODUCTION

Significant expenses associated with information system security breaches have been identified in recent research as well. For instance, according to the 2015 Global State of Information Security Study, a major theft of customer data was also recorded in South Korea, where 105 million payment card accounts were made vulnerable by a security breach in 2015. The report also contrasted the costs of security events in big and small firms. In fact, it said that finding compromises was the exception rather than the rule for tiny firms. That is to say, 5% fewer occurrences were discovered this year (in 2014) compared to 2009 by businesses with less than $100 million in sales. Yet, between 2009 and 2014, the number of occurrences at bigger businesses increased dramatically. In reality, between 2009 and 2014, the number of incidents discovered by medium-sized and big firms (those with sales between $100 million and $1 billion) increased by 64%[1], [2].

Managers must discover techniques to track down and comprehend the origins of security concerns in order to reduce their negative effects. In this chapter, we offer two economic security risk models that quantify security risks to information systems in order to support their efficient defence.In order to effectively analyse risks breaches, the chapter discusses quantitative cybersecurity models based on our threats categorization models described in our prior work. In reality, information system danger categories aid system managers in designing less vulnerable information systems for their firms, putting information security measures into place, and defending their assets against these threats. The first model evaluates security risk and enables managers to specify the proper countermeasures to minimise them by identifying the source of space incursion (which may be internal or

external). The second model is based on our concept for categorising threats, which enables evaluating the effect of a danger class rather of a single threat as threats change over time. Also, we demonstrate how to leverage the Cloud Computing (CC) technology with our quantitative security analysis approach[3], [4].

The structure of this chapter is as follows: The context of our chapter is presented in the first part. The inspiration for our effort is presented in the second part. A description of the cloud computing environment is provided in the third part. The fourth part offers the internal mean failure cost model (MFCint) and exterior mean failure cost model, two economic cybersecurity models built on a threat source criteria (MFCext). Moreover, we provide a fresh approach for testing our security risk models, and we utilise a Cloud Computing application to demonstrate how to use them. The model for mean failure cost extension (MFCE) is introduced in the fifth part. Moreover, we verify the MFCE model and provide an example of how this model might be used in practise.

Quantitative Cybersecurity Risk Assessment Models as a Second Motive

Managers need to analyse or estimate the system's cybersecurity breaches and accurately define them in order to make effective security choices. Many metrics are available in the literature to help determine how effectively a system satisfies its security goals, and. Literature has described a number of risk assessment methods for economic security. For instance, we may point to the mean failure cost (MFC) model, which measures the security of the information systems we'll discuss in this section.

Concurrent Work

While there may be a number of restrictions that prevent current models from accurately estimating security breaches caused by security threats and vulnerabilities, this drives researchers to create additional models. In this study, we are primarily interested in qualitative and quantitative methodologies for security risk analysis or risk assessment.The definition of the effects of security risk occurrence in a quantitative form is made possible by quantitative approach, and. In reality, they provide an accurate estimate by estimating the expenses in numerical figures. The MFC model calculates the cost per system stakeholder due to security breaches, while the mean time to failure (MTTF) model quantifies the system failure rate. The outcomes of the study using the current methodology, however, are inaccurate and even unclear. In actuality, the range and precision of a stated measuring scale must be taken into consideration. They thus fail to disclose specific costs and outcomes. On the other hand, qualitative descriptions must be added to the analysis findings to make them more accurate and thorough.

For instance, in, the authors suggest the SAEM technique, a cost-benefit analysis procedure for comparing "danger indexes" to analyse security design options. For the purpose of organising information about risks, protections, and assets, the authors of suggest a security ontology. Using its own framework, this study develops categorization for each of these categories and develops a technique for quantitative risk analysis. The required mechanisms and countermeasures must be developed throughout the risk analysis phase since the work does not employ well-known standards or recommendations as an input for its assessment model. A method for risk assessment based on the calculation of risk levels on ISO/IEC 27005:2008 was also offered in the ENISA report. If both the chance of the incident and its effect are high, there would be a significant security risk. The supplied evaluation is semi-quantitative since it provides value ranges for both event likelihood and impact but does not take into account both of those factors' combined effect.

A model that assesses information assets, their vulnerabilities, and the threats to those assets was proposed by Bojanc and Jerman in. The values of the risk parameters serve as the foundation for choosing the best risk management strategy and for assessing the different security solutions that lower security risks. In, Singh and Joshi suggested a methodology for risk assessment for the university computer environment that lowers the likelihood of a security compromise. The three-phase activities supported by the model include a first phase that evaluates threats and vulnerabilities to pinpoint weak points in the educational environment, a second phase that focuses on the highest risk and develops actionable remediation plans, and a third phase of risk assessment that acknowledges the need for compliance with vulnerability management regulations in order to strengthen the security position of the university.In order to characterise a random risk environment, Yang et al. propose in a measurement and evaluation model of cloud computing based on Markov chains. The model substantially decreased the current subjective aspects in the assessment process and created a useful and trustworthy way for risk management choices by measuring risk using information entropy. Lastly, Cayirci and de Oliveira offer a quantitative security risk assessment approach based on the performance history of cloud service providers in. By relying on reputable third parties to gather soft and hard trust data pieces, the strategy allays provider and customer worries while enabling ongoing cloud risk monitoring.

Cloud Computing Settings

Information and communication technology (ICT) development led to cloud computing. In actuality, it is built on a number of technologies, including web 2.0, distributed systems, service flows, and workflows, as well as virtualization. The growth of cloud computing in 2006 was sparked by two significant occurrences. The first was the unveiling of a new business model, "Cloud Computing," by Google CEO Eric Schmidt.A technology called cloud computing makes it possible for anybody, anywhere to use resources for data and computation that are hosted remotely. In the same year, Amazon.com unveiled Elastic Cloud Computing (EC2), one of the most significant Cloud Computing services to date.According to the National Institute of Standards and Technology, cloud computing is "a model that provides easy, on-demand network access to a shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with little management effort or service provider interaction.Astronomy, weather forecasting, and finance applications are just a few of the key modern applications that heavily rely on cloud computing.

Architecture of Cloud Computing

The framework of a cloud computing system, which comprises middleware, software components, cloud resources, and services, is known as the cloud computing architecture, which also refers to the interactions between these components. It consists mostly of a front end and a back end that are connected to one another over the Internet. The front end of a computer user's or client's operation includes the client's machine and the application needed to access the Cloud Computing system. The "cloud" portion of the system, which consists of the many physical and virtual computers, servers, software, and data storage systems, is the system's back end. The suggested architecture for cloud computing is summarised in Figure 3, and several tiers of services are available from cloud computing providers:

1. Infrastructure as a Service (IaaS): This layer offers the fundamental computer infrastructure, including servers, processing power, storage, and networks, enabling users to install and execute any kind of software, such as operating systems and applications.
2. Platform as a Service (PaaS): is a layer that offers a platform on which applications may be developed or released.
3. Software as a Service (SaaS): This layer provides programmes to thousands of consumers through a web browser without the need for installation on their systems.

Security Concerns with Cloud Computing

In the last several years, cloud computing has shown a tremendous promise for offering consumers more flexible, on-demand services that are also more affordable. Although advancing towards the idea of on-demand services, resource pooling, and transferring everything to a distributive environment, security is the main barrier to this new imagined vision of computing capabilities. Users' data is really kept in data centres outside of the cloud where the hazards outweigh the benefits. Customers' data is really kept in the cloud on a number of servers owned by third parties; as a result, neither the user nor anyone else is aware of where the data is saved. We specifically cite the loss of security and the loss of control. In fact, by entrusting crucial data to a service provider (externalisation of service), a user (whether a person or an organisation) runs the danger of jeopardising the data's accessibility, confidentiality, and integrity. When a subscriber's data is unavailable when required (for instance, as a result of a denial of service attack or just a loss), availability and integrity may be impacted. Integrity may also be impacted if a subscriber's data is accidentally damaged or deleted by someone acting maliciously [5], [6].

Security issues in the cloud environment are the subject of several studies. For instance, a Forbes article released in 2015 predicted a 42% growth in cloud-based security expenditure. Another study found that the cost of IT security has climbed to 79.1% by 2015, representing an annual increase of more than 10%. Security was identified as a top problem by 74.6% of commercial clients in 2011, according to International Data Corporation (IDC) data. In addition, virtualization, which is a foundational technology for cloud computing, poses significant security risks that can be divided into three categories, including virtual machine modification, denial of service, monitoring virtual machines from the host (MVM), and communications between virtual machines and host (CBVH), among others.

We suggest categorising CC security concerns into nine sub-categories in this section, some of which are business services and virtualization security concerns.Continuity, management interface hazards, privacy concerns, data breaches, data location issues, accountability issues, multi-tenancy challenges, and regulatory and governance difficulties.Virtualization Security Concerns Several virtualization elements, including hypervisors and virtual machines, are the foundation of cloud computing architecture. Several operating systems may run simultaneously on a system thanks to the controller known as a hypervisor or virtual machine management (VMM). It is challenging to maintain operating system security since numerous operating systems may be running on a same hardware platform, making it impossible to monitor all of these systems. In this scenario, the guest operating system has the potential to execute malicious code on the machine system and put the system to a halt or wrest complete control and prevent access to other guest operating systems, and since malicious insiders are particularly dangerous attackers, they provide a chance for a foe to steal sensitive information or seize total control of the Cloud services with little to no risk of being discovered.

DISCUSSION

Continuity of Business Services DDoS assaults are another issue with availability that may occur in CC environments. By rendering their services unavailable, attackers employ sizable botnets (or "zombies") to cut into SaaS companies' income. The loss of internet connection (which might happen due to certain conditions like natural catastrophes) is also a significant risk to the continuation of services in the cloud computing environment since cloud companies rely on having access to the internet for their information. Moreover, there are worries that the confiscation of a data hosting server by law enforcement authorities may lead to the unwarranted suspension or termination of unrelated services whose data are kept on the same physical equipment. As a result, organisations whose data and information were housed on the confiscated hardware had an unexpected consequence of business continuity issues.

Interfaces For Management Risks Customers employ a variety of software interfaces exposed by cloud computing providers to administer and engage with cloud services (like provisioning, management, orchestration, and monitoring). The customer management interfaces of public Cloud providers may be accessed through the Internet and mediate access to bigger collections of resources; as a result, they represent an elevated risk, particularly when paired with vulnerabilities in web browsers and remote access. Thus, a particularly pertinent vulnerability for Cloud systems is unauthorised access to the administration interface. Since they provide authentication, access control, encryption, and activity monitoring, which directly rely on the security and availability of generic Cloud services, these interfaces must be created to defend against both unintentional and malicious efforts.

Breaches in data Data about customers may be stored in many ways thanks to cloud computing. In actuality, the fact that data in Cloud systems is transported over clusters, virtual computers, databases, or third-party storage facilities raises the possibility of information leakage and data corruption. In fact, data centre operations might result in information leaks, such as when a customer's data gets mixed up with that of another.Also, since they are more flexible and cost-effective than purchasing a server, the majority of cloud service providers attempt to rent one from another provider. Due to this, there is a significant chance that nefarious insiders may steal client data from the external server

Governance and Conformity

As a result of the significant problem that security in Cloud Computing systems provides, cloud vendors must offer some guarantee in service level agreements (SLA) to persuade the client on security-related concerns. The SLA attempts to help the client comprehend the security rules being used by illuminating various security levels. Customers may specify their expectations for security for these kinds of systems in the SLA. Providers are required to offer a detailed set of rules governing the system and related services, as well as details on how compliance with these rules is carried out, and Yet the SLA could not guarantee that the cloud provider will provide these services, which might lead to a number of security lapses (for instance, failing to satisfy privacy and confidentiality requirements) for a variety of reasons. Indeed, according to Cloud providers cannot vouch for their own compliance with the relevant regulations and forbid external audits by Cloud customers or security certifications.

A more major issue is that there is no mechanism to define the rules for how private information is shared, handled, and stored across cloud service providers. In reality, bad data management procedures often cause information to leak. For instance, data security during natural catastrophes is a need for cloud service providers. In fact, there are some legal difficulties associated with cloud security as well, as cloud service providers must adhere to a

number of rules, some of which differ from country to country and may result in data duplication over numerous locations.

Access Issue

Data Location As client data is stored in the data centres of cloud providers, which may be found anywhere in the globe, and is thus not under the customer's control, cloud computing environments suffer from a lack of transparency In reality, it's possible for programmes to share the user space, which might result in data duplication and make it difficult to map users and their rights. Moreover, this calls on the user to keep track of several accounts and passwords, which often results in forgetting them. In fact, users of the Cloud need to consider who is managing (getting access to) their data (when they release the information into the Cloud for processing) and what sorts of restrictions are given to these personnel and.

Data breaches are a serious issue for businesses. For instance, because to the sensitivity of their information, many companies, including financial institutions, healthcare providers, and governmental organisations, are legally compelled to secure their data from compromise. These firms are often obliged to operate and maintain their own datacenters with strict physical and logical protection measures in place to guarantee the security of their data. Due to the inherent danger of data breach from systems outside of their control, some companies simply cannot use cloud computing in a general way.

Concerns Regarding Privacy

There are various factors that might cause privacy issues in cloud computing systems. First, data kept by cloud computing customers, particularly personal information, is more vulnerable to hacking than data saved on users' computers. Customers' data are really kept in service providers' data centres, therefore it is uncertain if the latter will secure the customers' data, particularly their personal data. In order to secure the customer's personal information, the supplier must ensure who has access to the data and who is maintaining the server, since the majority of servers are external. Moreover, the danger of illegal access to and disclosure of customers' private information is increased in shared infrastructure Also, the variety of privacy laws from nation to nation causes issues for enterprises with privacy. In actuality, data in cloud systems are kept everywhere, so users cannot infer if you are breaking privacy laws in the nations where you do business and . In order for different Cloud providers to use the right technological controls to secure the data, there is a need for techniques to explicitly label the data with security and privacy rules that would move with sensitive data from one provider to another. In this situation, data are vulnerable to several attacks like as sniffing, spoofing, man-in-the-middle, side channel, and replay attacks, therefore the CP may not always ensure that information will be kept private or kept from being disclosed.

Failing in Isolation (Multi-Tenancy Problem)

The basic features of cloud computing environments are multi-tenancy and shared resources (computing power, storage, network, memory, routing, etc.). Due to a vulnerability in the hypervisor, there is a danger of failure of the deferent mechanisms between the various tenants of the shared infrastructure. In actuality, the infrastructure as a service (IaaS) Cloud layer depends on architectural designs in which real resources are shared by several virtual computers, and consequently numerous consumers. In reality, resource sharing implies that harmful operations (such as spamming, port scanning, etc.) carried out by one tenant may influence and gain access to another tenant host.

Accountability Issues

Accountability involves monitoring behaviours connected to security-related tasks and obligations. It seeks to provide tracking information on user activity and system status, which may also be utilised for system performance analysis or intrusion detection reasons. Security is the main issue while adopting cloud computing, thus in this chapter, we provide security metrics to quantify cybersecurity risk and enable managers to choose the best defences. To determine the source of danger space, the MFCint and the MFCext are based on the threat source dimension. The MFCE, which is based on the HTC model, gives system stakeholders the ability to quantify the risks they assume for the security of their assets[7], [8].

CONCLUSION

Information systems face a serious security issue, and enterprises must calculate the consequences of security breaches. A number of interconnected internal and external variables may lead to security problems. Moreover, a security flaw could spread can increase via the causal chains of risk variables in various ways, creating various system security concerns. We provide three threat classification-based algorithms to predict threat risks. In addition, we recommend a cost range to categorise the security quantification for information system to determine if the system is secure or not. These security analysis models provide businesses the ability to estimate the money they would lose as a result of risks and breaches, and a case study verifies this. In order to provide more precise security loss estimates, we want to design an extensible quantitative security risk assessment model that takes into account several threat aspects.

REFERENCES

[1] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security Against Communication Network Attacks of Cyber-Physical Systems," *J. Control. Autom. Electr. Syst.*, 2019, doi: 10.1007/s40313-018-0420-9.

[2] D. Ding and J. Cao, "Overview of network security of cyber-physical systems," *Inf. Control*, 2019, doi: 10.13976/j.cnki.xk.2019.9160.

[3] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks," *IEEE Trans. Smart Grid*, 2019, doi: 10.1109/TSG.2018.2819663.

[4] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu, "A survey on state estimation techniques and challenges in smart distribution systems," *IEEE Transactions on Smart Grid*. 2019. doi: 10.1109/TSG.2018.2870600.

[5] H. Wang, N. Lau, and R. M. Gerdes, "Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures Through Work Domain Analysis," *Hum. Factors*, 2018, doi: 10.1177/0018720818769250.

[6] X. Li, C. Zhou, Y. C. Tian, N. Xiong, and Y. Qin, "Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems," *IEEE Trans. Ind. Informatics*, 2018, doi: 10.1109/TII.2017.2740571.

[7] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, 2019, doi: 10.1007/s11192-019-03222-9.

[8] B. Piontek, "The theoretical basis of strategic security management for shaping the structural order and sustainability processes," *Polish J. Manag. Stud.*, 2019, doi: 10.17512/pjms.2019.20.1.30.

CHAPTER 13

INTERNET OF THINGS (IOT) SECURITY USING PHYSICAL UNCLONABLE FUNCTION

Mr. Tirumala Vasu Galithoti, Assistant Professor,
Department of Electronics & Communication Engineering, Presidency University, Bangalore, India.
Email Id: - tirumala.vasu@presidencyuniversity.in

ABSTRACT:

While sending sensitive application data over packet switched and circuit switched data connection, security mechanisms are crucial. Modern research has developed a limited Internet of Things (IoT) architecture to offer communication between items without human involvement. IoT therefore emerges as a viable option to provide end-to-end connection despite limited network resources. An integrated circuit uses a digital logic architecture called Physical Unclonable Function (PUF) (IC). It is easy to use, lightweight, and unclonable. PUF-based security methods may be an effective solution to provide security for IoT networks with limited resources. Internet of Things (IoT) is now developing as one of the important and promising areas of 5G communications. Millions of devices might interface thanks to 5G technology, making IoT an essential component of many applications such as smart grids, intelligent transportation systems, smart cities, and many more. Every IoT application claims to give an improved experience level in routine chores. For instance, having control over the resources available would encourage a healthy economy and sustainable growth. This is the actual driving force behind the creation of smart cities.

KEYWORDS:

Internet of Things (IoT), Security, Unclonable Function, Limited Network Resources.

INTRODUCTION

Every device in an interconnected network of IoT must be directly or indirectly linked to its utility gateway (IoT gateway or LLN gateway) in order for the IoT to be successfully implemented. In order to capture application data and send it to its network centre for further processing, these limited devices must be outfitted with smart sensors (or actuators). Both centralised and dispersed networks are suggested as different forms of IoT networks. Moreover, deterministic networks as well as packet switching based on random access are being suggested for use inside IoT networks. In order to enable control/data streams for time-sensitive applications, certain IoT applications (such as Industrial and Medical Machine to Machine Communication) need end-to-end dedicated spectrum channels. Securing the data is essential for these apps to ensure the security of the end user. In order to ensure the safety of the end users, it is crucial to provide security for end-to-end communication in the Internet of Things. The widespread usage of mobile devices consistently eases activities for people and makes them easier.

One of the most significant technologies, like RFID, is created to support a variety of human jobs. RFID technology may be used to identify and verify people, animals, and products, as well as to stop the cloning and counterfeiting of items, medicines, and currency. Nonetheless, the widespread use of digital and computer devices has increased security dangers and introduced fresh security difficulties and threats. Due to these devices' considerable energy,

implementation, physical manipulation, and side channel attack constraints, these security risks and problems are getting more complex and need to be solved. Public key cryptography is one of the extant cryptography algorithms that is effective at stopping various security threats but has a difficult implementation. Researchers have developed a variety of simple encryption techniques, but they all start from the premise that the secret keys kept in non-volatile memory are well-guarded. This sensitive information, however, is readily breached or cracked by physical system assault. As a result, the cryptographic primitive known as Physical Unclonable Functions (PUF) is made to handle the aforementioned problem and effectively stop forging, cloning, and prediction. PUF offers an affordable option for applications that need high levels of security and may overcome the issues with current solutions [1]–[3].

PUF is a one-way function that is simple to assess using physical systems but challenging to anticipate because of the nature of its output, which is completely random. PUF is an integrated circuit (IC) that provides a response to a specific challenge. It is a logical circuit. When the same challenge is presented to multiple chips, the results are unexpected and diverse. Moreover, PUF provides the capacity to create unique IDs for each chip and may generate an infinite number of secret keys for one chip. An IC's fabrication process leaves special characteristics left in these circuits. PUF takes use of this uncontrolled randomness as its challenge because of certain inescapable and unpredictable changes in the process at the molecular level of each chip, and response mapping (values are all binary strings) relies on these variations. As a result, PUF equips each chip with a special challenge-response mechanism. For instance, the security of the resource-constrained Internet of Things (IoT) devices' authentication process is one of the primary problems due to the prohibitively expensive and more powerful traditional robust cryptographic methods, which are thought to be effective against certain assaults. Due to their constrained space and low computing power, these devices cannot be fitted with these strong encryptions and security procedures. In light of the aforementioned issues, these devices' tiny size and low computing power render them susceptible to attacks that aim to duplicate the authentication mechanism for the hacked IoT nodes. PUF is a good contender because of its appealing qualities, such as its lightweight nature, simplicity of design for authentication procedures, and lower processing cost in comparison to the demands of current cryptographic algorithms. Moreover, PUF offers us qualities like unpredictability, unclonability, and cheap cost computing. PUF is a strong contender for resource-constrained IoT devices because to these capabilities, and it works wonders to address the problems with secure communication in IoTs. For device identification and authentication, PUFs have been suggested in, and authors developed PUF in IC to be utilised as anti-counterfeiting. Moreover, it has been used for key-less secure communication, secure cryptographic secret storage, and other purposes. Moreover, it is important to keep in mind that, as mentioned in, the conventional assault cannot be executed if an ideal PUF is used in its stead.

Security Concerns in IoT:

It explore several security bootstrapping techniques, and this part discusses the main security problems that might result from a failed security bootstrapping.Before discussing all security concerns, it is important to realise that the word security refers to a wide variety of ideas. In this article, we focus on two major, more general elements of security in the Internet of Things: network security and physical security. The key security threats to an IoT network are authentication, access control, confidentiality, integrity, and availability.Before to sharing any protected information, communication nodes must first be verified via an authentication procedure. Even the routing path's information is crucial in this situation. IoT authentication

has to be very automated and secure. Access control is comparable to making sure the communication node is secure. Confidentiality refers to the safeguarding of sensitive information that is sent among parties over an open channel, such as a wireless medium. Integrity verifies that the data is unaltered and precisely as it was transmitted from one party to the other, i.e., that no alteration was made to the data while it was in transit. Information must be accessible to be used when needed.After investigating these dangers, we discovered that in the majority of IoT situations, whether the network consists of mobile handheld devices, a large number of static nodes, or a mix of both, it is eventually linked to the public network. In light of these issues, network security difficulties for IoT devices should be the main focus.

Physical Protection

IoT networks are centralised with several distant nodes, as is well known. The majority of these nodes are scattered across other networks, such as ad hoc and sensor networks, and get relatively little attention from humans. In this kind of situation, the attackers may take control of the device that is dispersed across a vast region and harvest security data, keys, etc. Attackers have the option of reprogramming the node or using its physical components or manufacturer information for personal gain. Attacks are more severe when a common network key is utilised than when a distinct key used. Network connectivity may also be disrupted by DoS and DDoS attacks, which are particularly difficult to identify.

Network Security

Failure of Authentication

This attack targets the network's route information and data security; it takes place at the network layer. When one of the connecting nodes is hacked, an attack of this sort occurs. The finest authentication practises are used to avoid this attack so that no unauthorised nodes may join the network.

Assault by a Man in the Middle (MitM)

By intercepting data being transferred between communication nodes, MitM attacks are conducted. This may be achieved by looking at the traffic, which gives the attacker access to network information. By encrypting the data used for routing, such attacks may be prevented. For low power and lossy networks, Advanced Encryption Standard (AES)- 128 in Counter with CBC-MAC (CCM) mode must be used [10]. The cypher block chaining message authentication code mechanism and counter mode encryption are combined in CCM. If the routing information is left unencrypted at the data connection and network layer, MitM may also be carried out by monitoring network traffic flow to effectively map traffic flow patterns. Multi-path routing can be used to reduce these, but it consumes more power and is not the best option for IoT networks with limited resources.

Data Integrity Attacks

Unauthorized change of a message or of stored data is referred to as data integrity. Access control for messages may be used to lessen the impact of this attack

Spoofing

Identity theft is another term for spoofing, which indicates that a communication node is not the one it is purporting to be. This kind of attack occurs when a hacker acquires physical or network-based access to a communication node. They are known as Sybil assaults if the attacker is able to construct numerous fake identities. Using these attacks, the attacker may

transmit bogus routing information and access secure data, disrupting the regular routine procedure. Using the proper authentication method at the network layer helps reduce the impact of these attacks.

Attacks using Routing Information Replay

These assaults take place when a message broadcast across a network is recorded and repeatedly played to the network to disrupt operations. To lessen this assault, the IETF developed routing over low power and lossy networks (RPL). Older or repetitive messages are disregarded by communication parties in RPL.

Attacks using Byzantine Routing Information

In these types of assaults, a communicating node that still has a working identity and set of security credentials is taken over by the attacker. These assaults are very difficult to identify; even authentication methods were unable to stop them.

Attacks on Availability

Attacks on availability or selective forwarding attempt to alter routing pathways and obstruct node-to-node communication. The attacker may be able to transmit certain messages and cause confusion inside the network. A black hole attack occurs when Node A sends packets (msg1 msg2 msg3) but the attacking node discards every packet it gets. By sending the packets via end-to-end or hop-by-hop multipath routing protocols, these sorts of assaults may be lessened. Since the multipath technique uses more energy, it is not suggested that it be utilised in lossy, low power networks.

Applicability of PUF

By reviewing the survey on secure bootstrapping for IoT , specifically Managed, P2P or Ad-hoc, Opportunistic or Leap-of-Faith, and Hybrid, as well as all security issues in IoT including both physical security issues and network security issues, we came to the conclusion that the lack of physical security leads to other attacks, and if an attacker has the physical access, then it is much easier to crack down attack on network layer; therefore, tamp The view is broken into two parts: first going with security bootstrapping techniques and then security in IoT, in order to grasp these facts in simpler terms and going all at once. A discussion would then provide some simpler and practical PUF use examples.

In Starting Out

To validate various nodes before communicating in the context of managed security bootstrapping approaches, centralised server-based authentication is employed. Instead than using complicated methods and programmes, a PUF may be utilized to verify nodes with the server. In contrast to P2P or Ad-hoc methods where node authentication is performed by using key exchanging programmes, a PUF-based mechanism to verify node-to-node authenticity would result in easier and safe authentication with less power consumption. This is because the basic idea of verifying nodes with servers using PUF rather than pre-shared key will result in less demand for power and authentication could be performed without executing more complex algorithms. In opportunistic or leap-of-faith procedures, the network is not presumed to be hacked when a node is verified. Even with the aforementioned supposition, it is easier and more cost-effective to use the PUF technique for authentication, which is intrinsically difficult to defeat (the authentication schema).

Securing More IoT Features

IoT security concerns may be divided into two categories: network-related problems and physical problems. Since we previously discussed that PUF output is random in nature and depends on physical factors, using PUF in IoT devices can eliminate all physical security issues. Additionally, even if an attacker gains physical access to a device or node, it is impossible to reverse engineer PUF, demonstrating its dependability for IoT physical security. Regarding concerns with network security, we must first realise that the majority of assaults are made possible by fraudulent authentication, which is the start of other attacks. PUF-based mechanisms are helpful for reducing network threats.

Using PUF may reduce the likelihood of authentication failure since it provides flawless authentication to only valid devices and prevents fraudulent authentication. Confidentiality attacks won't ever occur if PUF-based authentication is in place since only authorised nodes will ever communicate with one another. All other network assaults (apart from MitM and data integrity) begin with compromised nodes, which may happen either via physical attack or through the use of false authentication to enter a given network. They can all be eliminated using a single solution, a solution based on PUF. The current approaches, CBC-MAC, are superior in terms of security for MitM and data integrity across networks since the data is encrypted using simpler encryption schemas and is thus suitable for devices with less resources.

As the Internet of Things (IoT) enters our daily lives and next industrial systems (Industry 4.0) [, security is one of the biggest concerns now facing it. IoT devices must overcome a number of difficult obstacles, including low energy consumption, a shortage of processing capabilities, and the need to protect devices from cyberattacks. However, the cryptographic techniques that may be used on these devices are limited by energy footprint issues as well as a lack of processing capacity. Traditional security measures like an asymmetric handshake, which calls for hashes and asymmetric cryptography, are more difficult to implement as a result. Early assaults, such as permitting remote updates on an open Telnet port, demonstrate how often companies are ignorant of how simple it is to attack their devices. IoT devices must often be affordable, which makes it more difficult to install security features for them.

The security triangle in IoT has three sides: authentication, authorisation, and privacy. The first defence against a cyberattack is authentication. The use of Physical Unclonable Functions (PUFs) has been suggested as a simple, affordable, and widespread approach. PUFs are particularly intriguing for resource-constrained IoT devices because, crucially for IoT developers, they promise to offer absolutely secure authentication without requiring any cryptographic assets on the device. Newer research suggests that PUFs may not be able to deliver on all of their early promises, and that additional work will be required to implement fully safe systems using them.

We provide an overview of the current state of the art of PUFs for IoT systems, with a focus on authentication, in this study. Our key contribution is a critical assessment of the initial promise of existing PUF designs and PUF-based protocols, which is to accomplish security without cryptographic assets and with little resource overhead. We examine the special security needs for the IoT sector and the ways PUFs might meet them. We concentrate on methods that have a solid track record and are well-known for both their benefits and drawbacks. If we believe another strategy might be significant for the IoT in the future, we briefly highlight it. By incorporating a particular PUF circuit into IoT devices, such as a stand-alone ASIC or a system on chip, a PUF may be made possible. The alternative is to include a PUF circuit inside a piece of hardware that can be changed, such as a Field

Programmable Gate Array (FPGA). With the second method, IoT developers have greater control over the PUF architecture being utilised and can better adapt the system to meet the demands of their individual applications. As a result, we focus primarily on PUFs implemented on FPGAs in this study and only briefly touch upon PUFs implemented as PUFs.

Initial Definitions for PUF

Every chip has a unique fingerprint that is created during manufacture, much as individuals do. By incorporating a certain circuit design, known as a PUF circuit, inside the chip, this inherent property may be extracted (see Figure 1). PUF circuits produce a series of bits (so-called answers) after receiving a sequence of bits (so-called challenges). No two chips provide the same results in a given challenge. A challenge response pair is made up of a challenge and its associated answer (CRP).

Different results are produced by two identical physical unclonable functions (PUFs) circuits on two distinct chips.Several CMOS technologies are used to construct PUF circuits, most notably on memory chips, as application-specific integrated circuits (ASICs), or on field-programmable gate arrays (FPGAs). PUF circuits come in two varieties: weak and powerful PUFs. The number of CRPs increases exponentially for powerful PUFs as the PUF circuit size increases. It will rise linearly for weak PUFs.PUFs are often used for secure communication and authentication. PUF-based authentication is a good match for IoT devices' resource requirements since it doesn't need traditional cryptographic assets. The enrollment phase and the authentication phase are the two stages of PUF authentication protocols. The first PUF-based authentication mechanism that has been suggested operates as follows: The chip that houses the PUF circuit is directly attached to the server during enrollment (see Figure 2a). The PUF circuit responds to challenges sent by the server by sending back the replies. The server keeps a table with all CRPs in it. The chip will then be attached to the IoT device. If the server needs to authenticate the device during the authentication phase (see Figure 2b), the server sends an arbitrary PUF challenge to the device. The apparatus calculates response bits and returns them after measuring PUF. The device is verified as legitimate if the measured response matches the response that is recorded in the server database. Extracting a key from the PUF answer to start an encrypted conversation is another common PUF use [4], [5].

Risks from PUFs on IoT Devices

This section examines potential dangers to IoT devices that rely on PUFs for authentication. IoT equipment could be set up in exposed locations. They are thus subject to a range of dangers, including direct physical assaults (such as pounding), communication disruption, and manipulation of the actual operating circumstances of the device. There are also more conventional attacks like attempting to read secret keys from memory and communication assaults.The key new danger to a PUF-based security system is for an attacker to be able to deliver the right answer to a specific challenge. This may be accomplished, for instance, by building a physical copy of the PUF or by using a modelling attack to anticipate CRPs. We go into further depth on each of these strategies later. We take into account two different attacker models. In the first, the attacker has the ability to eavesdrop on device communication. In the second, the gadget is physically accessible to an enemy.

Man-in-the-Middle Attack

An adversary may overhear the communication channel between a server and a device in this kind of attack, intercept, and store CRPs that are being sent. After that, CRPs may be

exploited directly to carry out replay attacks or indirectly by feeding them into a machine learning algorithm and creating a model of the PUF that can anticipate further CRPs.As devices often link dynamically to previously unidentified devices in the IoT, man in the middle attacks may be carried out with comparably little effort. An adversary may install a cheap computer, such as a Raspberry Pi, next to the device being attacked and let it to connect to the same (potentially encrypted) wireless network. As a result, there is a fair amount of chance that such an assault will occur, hence appropriate defensive strategies must be used.

Side Channel Attack

The attacker in this kind of assault has direct physical access to the target device. Two orthogonal axes may be used to categorise side channel attacks on PUF. We can differentiate between invasive, semi-invasive, and non-invasive assaults on the first axis. Attacks might be active or passive on the second axis.

Invasive, Semi-Invasive, And Non-Invasive Procedures

By destroying the chips and having direct access to the internal components, invasive assaults may be carried out. PUFs were formerly thought to be impervious to such assaults because they would weaken a PUF's structure and make it useless. There is no secret key that is saved on the chip and that the attacker may get. PUFs are in reality susceptible to intrusive assaults, according to publications, which include making a complete physical clone of a PUF. Invasive assaults are much more expensive and difficult. The IoT device being attacked often has to be moved into a specialised lab with pricey lab equipment. Because to this, IoT devices are less appealing targets for this kind of assault, particularly when such devices are situated in public areas and cannot be transported to a lab.

An attacker needs access to the chip surface for semi-invasive assaults, although the passivation layer of the semiconductor is unaffected. Semi-invasive PUF assaults have been described using electromagnetic probing and photonic emission. Semi-invasive assaults utilise less complex methods than invasive attacks, although they still need specialised lab equipment.Non-invasive attacks aim to get sensitive data by taking advantage of data (such as power use or delay time) without having direct access to internal components. The tools required for these assaults are somewhat portable and affordable, and they may even be put close to the IoT devices being targeted. Machine learning methods are used by non-invasive assaults as an analytical tool and can accurately recreate CRPs

Active and Passive

Active assaults actively alter the system, such as by changing the operating temperature or the supply voltage Vcc, to carry out attacks on the PUF. In contrast, passive assaults target a PUF by passively observing data, such as the PUF's temperature or energy use. Both attack techniques have been shown to be relevant to attacking PUFs and need direct physical access to the target device.

Defense Policy

We described attacks on PUF-based IoT devices in the preceding section. A fresh assault is suggested daily. We now go through potential countermeasures for the various types of assaults. Attacks using side channels come first. Attacks using side channels that are intrusive or semi-invasive need direct access to the PUF. If the enemy is able to get the device to a lab, (s)he may use cutting-edge equipment to assault the system. The threat level can be reduced with adequate physical protection mechanisms for IoT devices (such as epoxy adhesive or

glueing the PCB) and anomaly detection (such as by identifying unusual device mobility using cheap gyroscope sensors), but complete protection against invasive and semi-invasive side channel attacks cannot be guaranteed. Nevertheless, keep in mind that these assaults are often costly, and cost effectiveness might be seen as a hurdle for inexpensive IoT devices. On the other hand, non-invasive assaults may be effective outside of a lab and without harming the device's physical security using very inexpensive equipment.

In order to build a machine learning-based model of the PUF, passive non-invasive assaults pose a number of challenges to the PUF and keep track of external elements like power usage. To do this, thousands or perhaps hundreds of thousands of challenges are required. To combat this, the PUF may be designed such that it either only takes very particular challenges, making it exceedingly difficult to get enough of them, or so that it only accepts a tiny number of challenges each second, greatly delaying the attack.

Moreover, active non-invasive assaults take use of PUFs' potential for changing behaviour depending on the operating environment. By changing these parameters, they may, for instance, decrease the number of viable CRPs and facilitate modelling assaults. Making the PUF more resistant to outside influences would effectively put active attacks in the same category as passive attacks while still providing resistance against the modelling assault itself. Avoiding the reuse of CRPs is a well-known defence against replay assaults for man in the middle attacks. There are two possibilities First, CRPs may be encrypted to maintain their secrecy. This is particularly useful when there are few CRPs available, such as for weak PUFs, but it uses additional processing resources, negating our initial motivation for using PUFs in the IoT. As an alternative, we may choose a (strong) PUF design with a sufficient number of CRPs to ensure that none are ever reused. Using extra computing capabilities on the chip is a tried-and-true method of increasing the number of CRPs. This method may not work well since IoT devices have limited processing resources. The number of CRPs may now be increased without expanding the PUF circuit size on the chip thanks to a method using a spatial reconfigurable PUF. Keep in mind that for further security, we may combine powerful PUFs with CRPs that encrypt data. However this will result in more overhead once again [6], [7].

In more sophisticated man-in-the-middle assaults, an adversary once again use machine learning to carry out a modelling attack and anticipate CRPs, but this time the adversary feeds previously intercepted CRPs into the machine learning algorithm. Likewise, effective assaults need thousands of CRPs. Enhancing the PUF architecture's resilience by adding more non-linearity to the design was one strategy for fending off these assaults. Regrettably, this tactic finally came up empty. Another strategy was to defend against modelling assaults using machine learning by using cryptographic techniques. While it was more successful, this method ignored the PUF design, leaving the region vulnerable to side channel assaults.

We contend that both side channel attacks and man in the middle attacks must be addressed concurrently in order to provide a safe PUF-based IoT system. As was previously said, physical defence should be employed to thwart intrusive and less intrusive side channel assaults. The most significant non-invasive side channel attack for IoT devices also involves changing environmental conditions, such as raising the PUF error rate to lower the amount of usable CRPs. Making the PUF architecture resistant to such environmental changes would increase robustness, and the design of the PUF being utilised will reduce the possibility of non-intrusive side channel assaults. Consequently, adopting a suitable PUF architecture is vital. Lastly, in order to implement an integrated strategy to defend against man-in-the-middle attacks, the PUF must be coupled with an appropriate authentication mechanism.PUF-based IoT devices are developed by VERAYO, a well-known US business that works with

reputable clients including the US Department of Defense. Also, the Dutch business "Intrinsic ID" has reputable contracts with government and military organisations and works in the area of producing PUF-based IoT devices[8].

CONCLUSION

This focused on PUF's uses in the Internet of Things and gave readers a better understanding of this amazing technology, which is thought to be useful in any setting with limited resources, but notably in the IoT. Every device has at least one integrated circuit, which has intrinsic unique qualities that may further support the appropriateness of PUF-based security methods in resource-constrained networks, including IoT. This profitable and simple-to-implement solution may revolutionise how quickly IoT networks can be secured. In order to more explicitly design unique security methods based on PUF for IoT ecosystems, more research in this area is required.For software licence authentication, almost all security service providers provide hardware-based security solutions. Due to its cheap price, incapability to be duplicated, and security, this device incorporates PUF. Another example relates to the Government of India, where PUF-based RFID tags are utilised for the Fast-Tag automated toll collecting service's authentication mechanism.

REFERENCES

[1] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, “Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2926578.

[2] W. Liu *et al.*, “XOR-based low-cost reconfigurable PUFs for IoT security,” *ACM Trans. Embed. Comput. Syst.*, 2019, doi: 10.1145/3274666.

[3] A. Braeken, “PUF based authentication protocol for IoT,” *Symmetry (Basel).*, 2018, doi: 10.3390/sym10080352.

[4] J. Lee, S. Choi, D. Kim, Y. Choi, and W. Sun, “A novel hardware security architecture for IoT Device: PD-CRP (PUF database and challenge-response pair) bloom filter on memristor-based PUF,” *Appl. Sci.*, 2020, doi: 10.3390/APP10196692.

[5] F. Chen *et al.*, “Unclonable fluorescence behaviors of perovskite quantum dots/chaotic metasurfaces hybrid nanostructures for versatile security primitive,” *Chem. Eng. J.*, 2021, doi: 10.1016/j.cej.2020.128350.

[6] F. Farha, H. Ning, H. Liu, L. T. Yang, and L. Chen, “Physical unclonable functions based secret keys scheme for securing big data infrastructure communication,” *Inf. Sci. (Ny).*, 2019, doi: 10.1016/j.ins.2019.06.066.

[7] W. Feng, Y. Qin, S. Zhao, and D. Feng, “AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS,” *Comput. Networks*, 2018, doi: 10.1016/j.comnet.2018.01.039.

[8] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” *IEEE Access*, vol. 7, no. c, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

CHAPTER 14

MALWARE CLASSIFICATION USING FEATURE SELECTION AND MACHINE LEARNING

Ms. Ginkawar Shwetha, Assistant Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - swethag@presidencyuniversity.in

ABSTRACT:

Malware is a programme that does harmful acts and steals information. To be more precise, it is software created intentionally to disrupt a computer's operating system without the owner's knowledge or agreement. Malware is now widely recognised as one of the largest hazards. This chapter examined feature choice and machine learning-based malware categorization. The idea that different aspects of PE files may correlate with one another less than class files, whether clean or unclean, was used to identify these attributes. Such functions are implemented as machine learning algorithms to assist in the categorization of malware, and as a consequence, such classification is correctly applied in antivirus systems to aid in improving the rate of detection.Malware is a programme that conducts malicious actions and steals information, which helps to specifically identify it as software that is designed specifically to break into the system of a computer without the owner's consent.

KEYWORDS:

Classification, FeatureSelection, Malware, MachineLearning.

INTRODUCTION

In the world of the rapidly expanding Internet usage, malware has become known as one of the biggest threats. Moreover, any danger to computers in general is referred to by this phrase. Moreover, it may be categorized as standalone malware or file infestations. We may also group malware according to the function it performs, such as worms, adware, spyware, or Trojans [1]–[3].Moreover, the level of expertise needed to create malware has reduced. This is because anybody may become an attacker with ease, regardless of their level of experience, thanks to the malicious tools that are now readily accessible on the Internet, automatic detection software, and the ability to buy malware inexpensively. Researchers have found that script kids are increasingly using automated assaults.Hence, one of the most crucial things that businesses and consumers should do is defend the computer system since even a tiny assault may inflict significant informational and financial harm. One should employ machine-based approaches and processes since the present ones don't provide adequate security. In order to determine the best approach and its characteristics to create an algorithm that is flawless and can separate and identify the many malware varieties, this study examines the benefits and drawbacks of machine learning-based detection for malware.

The accuracy is evaluated depending on whether the file is malicious or not, and if it is malicious, the malware family to which it belongs is then determined. Using Cuckoo Sandbox scoring, the findings will be examined in order to determine the best procedure for developing a module that is comparable. It should be noted that there won't be any further discussion on implementing this module.Malware is a computer security problem that is utilised to evade the standard detection strategies, which depend on signature matching,

according to Mohammed et al. Machine approaches are utilised to distinguish others from those who have similar virus variations and patterns. The KNN algorithm uses a variety of selection techniques to categorise malware based on the analysis of n-grams, and a comparative study of these techniques leads to the use of "principal component analysis (PCA)" feature selection in addition to "support vector machines (SVM)" classification to provide the best classification with the fewest features. The dataset utilised in this research contains 1156 malicious files in addition to 984 benign files in various file formats; the achieved accuracy in this article is 93%.

According to Gavrilut et al, the authors recommended using a framework of Perceptron Training Subroutine algorithms to differentiate malware from clean files in order to reduce the likelihood of false positives. As the authors used three datasets: a training dataset, a test dataset, and a "scale-up" dataset.It can be inferred from subsequent successful testing on medium-sized datasets that the scaling mechanism provided by this framework was extremely helpful in enabling the user to work on bigger datasets of a similar sort.

Using the Cuckoo Sandbox, Chumachenko conducted research to determine the ideal feature extraction, representation, and classification that would result in adequate accuracy. They were evaluated using "Naive Bayes and Random Forest, k-nearest-neighbors in addition to decision trees, and not to mention the support vector machines". The collection included 1156 malware files from 9 distinct families, totaling 984 unique forms. The findings gave us recommendations for using the random forest approach for multi-class classification as it offered the highest level of accuracy. It should be noted that even if the preceding approach was effective, support vector machines should be used instead [4], [5].A three-part learning malware system was proposed by Liu et al. and was studied using machines. One is the data processing and virus detection. The other is making decisions. The first addresses Opcode n-grams, grayscale photos, and importing functions in addition to extracting malware traits. The latter has a tendency to incorporate capabilities to categorise and detect files that seem to contain malware. The dataset used in this study included "20000 malware occurrences" that Anubis, Kingsoft, and ESET NOD32 had amassed. Finally, the detection phase would use the "shared nearest neighbour (SNN) algorithm" to recognise the new malware family, leading to a classification rate of 98.9% accuracy and a malware identification rate of 86.7% for this system.

Raman views malware as a threat to computers since it takes time for signals to emerge that may be utilised to recognise a particular infection to arise on a computer. This technique uses a dataset that contains 16,000 clean programmes and 100,000 malware pieces. As a consequence, the author utilises a data mining approach to extract seven elements from the Microsoft PE's formatting. These features are then passed to a machine learning algorithm, which uses them to identify the malware. The accuracy of this classification was 92%.Vinod et al.'s extraction of n-gram features revealed that the files, which ranged in size from two to five, had two selection algorithms. The principal component analysis (PCA) and minimal redundancy-maximum relevance are the two methods. Six classifiers, including the random forest technique, AdaBoostM1, Instance-Based Learner (IBK), Sequential Minimal Optimization (SMO), and Naive Bayes, were used and implemented. The datasets used for each included 6000 samples. A high accuracy of 94.1%, which can be acquired from the 2-g size comprising both preceding samples, was achieved by the majority of them being portable executable (PE), while the rest were only bingeing samples. Nevertheless, one drawback was that it was a little challenging to extract the code of n-grams since some couldn't be clearly distinguished.

Ismail et al. extracted that n-gram from packet payloads to locate malware at the infrastructure level of a network, and they subsequently suggested that a similar pattern is employed to detect malware based merely on the assumption that the new virus will contain certain characteristics of the old one. The dataset includes 27,491 training flows, 2507 test flows, and 3470 test flows in addition. The methodology utilised was the Kernel approach algorithm. After using a Naive Bayes classifier to incorporate the domain knowledge he had learned from the SNORT signatures, they discovered that their experiment had only used a small portion of the 90,000 features it contained. As a result, they were able to cut the processing time from 53 hours to just 3 by simply optimising the number of those features.

Another researcher, Moskovitch et al., was able to extract other n-gram sizes using binary codes, including not only two, three, and four, but even six. Three particular selection techniques were also updated. A dataset including 7000 harmful files and 22,000 binge sets was used to calculate the Fisher Score (FS), Document Frequency (DF), and Gain Ratio (GR). These classifiers included Naive Bayes (NB), SVM, Artificial Neural Networks (ANN), and Decision Trees (DT). Given that the Fisher Score had a substantially higher degree of accuracy than the other classifiersa stunning 95%the findings showed that it was ultimately the best selecting technique.

Moskovitch et al. also reported a high level of accuracy of 95% when the size of the gramme was five being used along with the other classifiers when identical sizes of the n-gram were extracted from two codes using only two methods of selection, those being the GR and FS, and by four machine classifiers being the DT, the NN, and the SVM in addition to the NB and a dataset which contained 30,000 files precisely.When it came to the selection feature step, where they utilised three classifiers, Reddy and Pujari applied the previous document frequency and were able to extract different sizes of the n-gram, namely the two, three, and four. The SVM is one, the IBK is another, and the decision tree using Dempster-Shafer theory is the last one. It should be noted that the dataset included 2500 samples of viruses and 2500 samples of start codes, and the accuracy of the findings was 95%.

Using three classifiers and the sequential floating forward selection (SFFS) techniques, Liangboonprakong and Sornil retrieved the sequential pattern characteristics of the n-gram, two, three, four, and one. A dataset of "9448 instances by 682,936 feature vectors" is utilised in this study. The SVM classifier delivered a result of 96.64% accuracy when it came to the 4G employing the multilayer perceptron, C4.5, and SVM classifiers.N-gram features from dynamic and static characteristics were used by Lin et al.. The authors also suggested a genetic approach and used over 790,000 n-grams to categorise malware. They used feature reduction and selection, and with 10 features and 100 features, respectively, they were able to achieve accuracy levels of 90% and 96%. The dataset for this study included 389 benign samples in addition to 3899 malware samples. In order to read from the behaviour of dynamic and static from the files, feature reduction and selection had been done on the determined number of n-grams; it is not strictly related with the number of features.

The RIPPER method of detections was created by Gavrilu et al. and is based on rule induction techniques. The dataset used had 4266 files, of which 3265 were malicious and the remaining 1001 were benign applications. They did, however, accomplish a 69.90-96.18% accuracy. It is important to note that these algorithms have a significant number of false positives, with the top accurate algorithm having 84 false positives. The algorithm that was most effective had a rate of 93.01% for both high accuracy and a small number of false positives.

Two algorithms were utilised in Singhal and Raul's analysis of the detection approach, one of which was the "random forest mixed with information gain" algorithm, which offers a better representation of features. The dataset assembled contained files with 5000 executables, and the 12-feature extraction was simpler to provide an accuracy of 97% while keeping a very low proportion of false positives up to 0.03.A method of extraction that would be based on the API in addition to the DLLs and the PE and use different SVM techniques was proposed by Baldangombo et al. 1000 benign apps and 4500 malware files made up the dataset for this study. In order to give a high degree of accuracy utilising the first approach with a 99% using the PE header and a combination of the header with the API function, they are also employing J48 decision trees and Naive Bayes. And finally, the API only offered 99.1%.

In order to train the classifiers, Alazab et al technique entailed gathering big datasets that comprised "29580 binary executables." They used a variety of data mining algorithms, including KNN, SMO, and NB, to get high-performance outcomes. One data mining algorithm's benefits for properly detecting zero-day malware may be effectively studied and assessed. The data collected revealed a high degree of accuracy of 98.5%.Data mining was used by Siddiqui et al. to identify Trojans , and the author extracted n-grams from the Trojans' bodies. When the main component analysis and random forest techniques are added to the latter and the SVM while classifying, the rise in detection reaches 94%. The dataset had around 5000 PE files, of which 3000 were Trojans and the others were absolutely clean.

In order to find new executables, Schultz et al.created a framework for data mining using a dataset that contained 1000 malicious files and 1000 clean ones. Three algorithms were used by the author. The final one was a learner based on inductive rules to later be deported into an algorithm of signature-based nature yielding 97.76% success rate. One was a multi-classifier, the other was a probabilistic predictor, and the last one was a learner based on inductive rules.

The "PE-Miner" system by Shafiq et al. allowed the author to extract a number of features in order to immediately identify malware. This was accomplished by utilising the SVM algorithm to evaluate the aggregate values of the PE header files and coming to 189 unique characteristics. Using datasets from Malfease and VX Heavens, they additionally improved the method and achieved 99% detection rates with fewer than 0.5% of false positives.Ultimately, utilising automated malware that was exclusively dependent on the informational structure of that particular virus, researcher Kong et al. Created a structure. In addition to the decision tree and KNN techniques, the dataset used 526,179 malware samples. The authors arrived to the conclusion that there were similarities between the two malware programmes after extracting the characteristics utilising the cell graphs of each one. All of this is done by utilising distance metric learning to cluster and sort them based on family while keeping the various ones at a distance; they then put them together using an ensemble to categorise the virus and include it in the family to which it belongs (Table 36.2 summarise of malware detection methods).

However, numerous researchers have used feature selection in the field of network security, including who used and evaluated feature selection as a method for intrusion detection, who combined feature selection with neural networks to find P2P bots, and who used information gain as a feature selection approach with evolving clustering to find malware.

DISCUSSION

Among all the classifiers tested, the J48 had the most relevant classification algorithm data. The following are some of the characteristics that convey important information about the different components of the PE file: The outcomes of using numberofsections, virtualsize, resourcesize, exportsize,imageversion, and debug Size as input in the machine learning

classifiers will be assessed and contrasted with the projects carried out in the past [6]–[8].To enable other researchers to explore them, the Ridor, PART, J48 Graft, and J48 categorization criteria were built as a Python script. The script would be an example of a malware classifier because comparing the classifiers produced the following findings in relation to the number of characteristics used for the classification. Malware analysis and detection have recently taken centre stage. This is due to malware becoming a problem in more computer systems and networks held by businessesand people, as well as the ease with which malicious software may be produced and released. Analyzing typical security threats reveals that despite the methods most businesses use to stop them, the rate at which Internet crimes are growing outpaces them. Cybercriminals launch new assaults every year that have the potential to do greater damage than in years before.

It is certain that in recent years, hundreds of millions of new malware samples, including computer viruses and other dangerous software, have been produced. This suggests that every day, approximately a million new dangers are presented. Due to this, several researchers have worked very hard to analyse malware. One popular definition of malware is provided by, which defined it as any kind of software system code alteration intended to harm or impair a system's performance. Malware is a phrase that broadly refers to all varieties of spyware, viruses, and trojans, among other dangerous and malicious software, according to. Every software with a malicious goal is classified as malware by.

Malware is often designed to jeopardise the availability, confidentiality, or integrity of data or information in a computer system or network. As it is clear that better hypotheses may be generated by understanding what the malware does,'s explanation of some of the categories in which most malware fall is provided below. backdoor, botnet, downloader, malware that sends spam, scareware, rootkit, malware that steals information, worms, and trojan horses.It's interesting to note that computer networks, particularly the internet, are becoming more and more crucial to the efficient operation of many enterprises, making their security a need. We defined malware in the sentences before. Nonetheless, identifying this virus is necessary for protecting our computer networks. Static analysis (observing the malware without executing it) and dynamic analysis (observing the malware while running it) are two fundamental methods for malware analysis and detection. Static analysis approaches for malware detection have been suggested by a number of malware experts. These methods could, however, be troublesome.

Examined the drawbacks of static analysis for identifying malware and made the case that malware may readily elude pattern matching detection by by altering the code structure. According to, the variety and quantity of malicious software versions seriously reduce the efficacy of traditional signature-based detection. Introduced a malware detection technique that aids in overcoming the drawback brought on by using instruction semantics to identify dangerous software traits.According to their experimental review, their malware detection algorithm can identify different types of malwares with just a little amount of run-time overhead. Moreover, their semantics-aware malware detection system is resistant to widely used hacker obfuscation tactics. Further research on malware identification may be found in the references. They use datasets for training that include a lot of the common characteristics of harmful code. They emphasized the fact that we may train our machine learning classifiers to be able to identify unknown dangerous software, for example, by employing Byte n-gram format.

Proposed a scalable clustering method for identifying and classifying malware samples with similar behaviour. Their system's goal was to group several virus instances together based on how they behaved. Their system made an effort to identify a segmentation of a certain malicious software package to make sure that subsets share some characteristics. Detailed some of the machine learning procedures necessary for malware identification, such as first extracting common characteristics from all binary files in the test and training datasets there will be a variety of malware and clean file pairings in the training set. computer learning. The required parameters are then tuned by applying algorithms to the previously stated. Lastly, an analysis of the different malware detection procedures on the training dataset is performed. Put out an approach for using machine learning methods to detect fraudulent office documents. The XML-based office documents under investigation have a high rate of harmful content detection equivalent to the leading antivirus engines.In order to explore the impact of feature selection, the proposed work uses machine learning to identify malware. The greatest outcomes in this study came from supervised machine learning combined with feature selection. The phrase "learning with a teacher" refers to supervised learning. We use an algorithm to learn the function that maps the inputs to the outputs in this sort of learning, which includes both input and output variables.

Labeled examples are given in this form of learning. The specific goal of this article is to analyse the effect of feature selection in malware analysis using machine learning, which is important and, to the best of our knowledge, has not been addressed in this manner in other literature, for which the current research is crucial [9], [10]. Without human involvement, malware may propagate swiftly over networks. Using building kits that are accessible online, malware authors may create newer iterations of malware. Various malware versions have comparable fundamental capabilities that they gained from their progenitors, but their source codes either include an additional functionality (extension) or some non-functional modifications. Since malware authors constantly update newer malware versions utilizing various obfuscation strategies to escape current detection methods, malware detection is still an active research subject. Based on better misuse (signature-based) or anomaly (non-signature-based) detection methods, new detection strategies must be created to avoid the emergence of new malware kinds.

The high false alarm rate of anomaly detection techniques is an issue. Traditional misuse or signature-based detection, on the other hand, focuses on the identification of specific fingerprints for each virus. This method is unable to find new malware types. The size of signature databases is growing as a result of the daily increase in the quantity of these signatures. As a result, it now takes longer to process packets to match them for signatures. Hence, machine learning has lately been suggested as a way to identify malware in order to get around this problem. In general, machine learning approaches concentrate on identifying relationships in observed data and mining these relationships. It has been shown that machine learning is capable of spotting new malware strains. The growing false alarm rate caused by ineffective feature selection methods, weak and redundant features, and unsuitable algorithms for creating classifiers is a drawback of machine learning approaches. N-gram characteristics have been effectively exploited by Lima et al., Zhang, and Ismail to identify unknown malware. The selection of characteristics among the explosion of features that occurs as n-gram size rises is a major problem with n-gram analysis. Simple statistical filtering procedures are ineffective because to the complicated interactions between the characteristics.

The learning machine training procedure is not simple when dealing with enormous datasets. Many studies have used various feature selection and classification approaches to find malware In order to determine the optimal feature selection and classifier combination when

n-gram features are utilised in host-based malware detection, six feature selection strategies and four machine learning classifiers are analysed in this study. The remainder of the essay is structured as follows. The relevant efforts are covered in Part 2, along with an overview of the methods that are often combined with n-gram characteristics to identify malware. The suggested n-gram analysis approach is further explained in Section 3. The accuracy of four classifiers and the experimental findings are covered in Section 4 along with a study of many characteristics using various feature selection techniques. The paper's results are presented in Section 5 along with a discussion of more research that needs to be done. 2.0 OTHER WORK In order to find harmful programmes, intrusion detection systems (IDS) use a variety of approaches. The suggested n-gram approach, which employs supervised learning methods, is one of these methodologies. N-gram characteristics were retrieved from file opcodes by Vinod et al... They used two feature selection techniques, Principal Component Analysis (PCA) and Minimal Redundancy-Maximum Relevance, to extract n-grams of varied sizes, 2, 3, 4, and 5. Random Forest (RF), Instance Based Learner (IBK), AdaBoostM1, J48, Sequential Minimal Optimization (SMO), and Naive Bayes were six of the classifiers they learned. The dataset utilised included 2828 benign samples and 4805 portable executable (PE) files for malware. The findings shown that a 2-gram size with PCA and Random Forest may provide a greater accuracy of 94.1%. This work's weakness was in extracting the opcode n-grams straight from the files since certain executables couldn't be adequately disassembled.

Ismail et al.'s method of detecting fresh malware at the network infrastructure level included extracting n-gram attributes from packet payloads. Based on the idea that new malware versions include part of the codes from the older malware, they suggested a pattern similarity detection technique. They used a Naive Bayes classifier with the domain information they learned through SNORT signatures. They were able to demonstrate via their experimental work that a tiny features search area with just 90,000 features could be exploited by using the Information Gain feature selection approach. The test dataset comprised 3470 flows collected in 2010, 2507 training flows obtained in 2010, and 27491 training flows and 17301 tested flows obtained in 2011. The optimization of the amount of features led to a reduction in processing time for the model development from 53 hours to 3 hours. Their research had the drawback of using the Naive Bayes classifier, which performs less accurately than other classifiers After feature selection, the researchers used IG to choose just the most useful features; they did not utilise some characteristics that were really malware features since IG only selected features that often occurred in the dataset [11], [12].

CONCLUSION

A presentation of seven essential characteristics was given to help distinguish between applications that are malware-free and those that are not. The idea that different aspects of PE files may correlate with one another less than class files, whether clean or unclean, was used to identify these attributes. Such functions are implemented as machine learning algorithms to assist in the categorization of malware, and as a consequence, such classification is correctly applied in antivirus systems to aid in improving the rate of detection.The necessity for intelligent techniques to malware detection is thus essential due to the shortcomings of the static ways of malware detection and analysis. Machine learning, which may be thought of as the acquisition of structural descriptions from instances, is one of these clever ways. The descriptions that have been discovered may be utilized for understanding, explanation, and prediction. The work of, who suggested a way of discovering previously undiscovered viruses by categorizing them together, is at the forefront of this study. Their research demonstrates that the majority of machine learning models use classification methods to detect dangerous software.

REFERENCES:

[1] V. Syrris and D. Geneiatakis, "On machine learning effectiveness for malware detection in Android OS using static analysis data," *J. Inf. Secur. Appl.*, 2021, doi: 10.1016/j.jisa.2021.102794.

[2] D. Ö. Şahin, O. E. Kural, S. Akleylek, and E. Kılıç, "A novel permission-based Android malware detection system using feature selection based on linear regression," *Neural Comput. Appl.*, 2021, doi: 10.1007/s00521-021-05875-1.

[3] R. Taheri, R. Javidan, M. Shojafar, Z. Pooranian, A. Miri, and M. Conti, "On defending against label flipping attacks on malware detection systems," *Neural Comput. Appl.*, 2020, doi: 10.1007/s00521-020-04831-9.

[4] N. Zhang, Y. an Tan, C. Yang, and Y. Li, "Deep learning feature exploration for Android malware detection," *Appl. Soft Comput.*, 2021, doi: 10.1016/j.asoc.2020.107069.

[5] D. Ö. Şahin, O. E. Kural, S. Akleylek, and E. Kılıç, "A novel Android malware detection system: adaption of filter-based feature selection methods," *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-021-03376-6.

[6] H. Abubaker, A. Ali, S. M. Shamsuddin, and S. Hassan, "Exploring permissions in android applications using ensemble-based extra tree feature selection," *Indones. J. Electr. Eng. Comput. Sci.*, 2020, doi: 10.11591/ijeecs.v19.i1.pp543-552.

[7] L. Shiqi, T. Shengwei, Y. Long, Y. Jiong, and S. Hua, "Android malicious code classification using deep belief network," *KSII Trans. Internet Inf. Syst.*, 2018, doi: 10.3837/tiis.2018.01.022.

[8] Z. Katzir and Y. Elovici, "Quantifying the resilience of machine learning classifiers used for cyber security," *Expert Syst. Appl.*, 2018, doi: 10.1016/j.eswa.2017.09.053.

[9] B. M. Khammas, A. Monemi, J. S. Bassi, I. Ismail, S. M. Nor, and M. N. Marsono, "Feature selection and machine learning classification for malware detection," *J. Teknol.*, 2015, doi: 10.11113/jt.v77.3558.

[10] L. F. Martín Liras, A. R. de Soto, and M. A. Prada, "Feature analysis for data-driven APT-related malware discrimination," *Comput. Secur.*, 2021, doi: 10.1016/j.cose.2021.102202.

[11] A. Maryam, U. Ahmed, M. Aleem, J. C. W. Lin, M. A. Islam, and M. A. Iqbal, "Chybridroid: A machine learning-based hybrid technique for securing the edge computing," *Secur. Commun. Networks*, 2020, doi: 10.1155/2020/8861639.

[12] S. Li, Q. Zhang, X. Wu, W. Han, and Z. Tian, "Attribution Classification Method of APT Malware in IoT Using Machine Learning Techniques," *Secur. Commun. Networks*, 2021, doi: 10.1155/2021/9396141.

CHAPTER 15

SECURITY ANALYSIS OF SOFTWARE-DEFINED NETWORKS (SDN)

Ms. Samreen Fiza, Assistant Professor,
Department of Electronics & Communication Engineering,
Presidency University, Bangalore, India.
Email Id: - samreenfiza@presidencyuniversity.in

ABSTRACT:

By separating the network functionality from the underlying forwarding devices, software-defined networks (SDN) fundamentally alter the network architecture. This architectural modification revitalizes the network layer, enabling centralized network management and technical competence. SDN divides security problems into the control and data planes from a security standpoint, and this architectural recommendation presents both intriguing prospects and difficult obstacles. Conventional IP network devices use integrated circuits and chips that are made specifically for each application and are intended to achieve high throughputs. Network administrators must configure each device separately using low-level vendor-specific instructions in this "hardware-centric" network topology. As a result, network setup in heterogeneous networks is time-consuming, and autonomous reconfiguration and response are almost unattainable. Moreover, combining the data and control planes limits flexibility, stifles creativity, and delays the development of networking infrastructure.

KEYWORDS:

Data Plane, SDN Security, Software-Defined Network (SDN), Security.

INTRODUCTION

Recent studies have actually demonstrated that traditional networks will ultimately be unable to keep up with the rising demand and ongoing growth in the number of devices and applications brought about by advancements in cloud computing, the Internet of Things (IoT), and cyber-physical systems A new network architecture called the software-defined network (SDN) separates the control plane from the data plane in networking devices. The "brain" of the network is now located on a dedicated central controller thanks to this architectural recomposition, which allows for centralised administration and a comprehensive view of the network. The "dummy" devices that make up the data plane forward packets in accordance with rules that are remotely established. These rules may be programmed by the application operating on top of the controller and activated in response to information retrieved at the packet level [1]–[3].

The "separation-of-concerns" concept a basic security engineering need that is absent from the current Internet architecture, is followed by the layered design of SDN. As a result, SDN theoretically provides a robust foundation for enhancing network security, and significant efforts have already been undertaken to take use of SDN's capabilities to improve security for both network providers and consumers. The literature on SDN security is divided into three categories: studies aimed at securing the software-defined network platform itself; solutions aimed at enhancing current network security services (such as firewalls); and suggestions for developing new security services. In this research, we choose the first approach and concentrate on the security risks related to the SDNs' data plane.

Networks that are software-defined (SDN): The administration plane, the control plane, and the data plane are the three functional planes that traditionally make up computer networks. Briefly stated, network rules are created at the management plane, sent to the control plane for enforcement, and carried out at the data plane. Hence, the terms "data plane" and "control plane" refer to the network devices that forward packets, "control plane" refers to the protocols used to build up forwarding tables, and "management plane" refers to the group of software services used to set up control capabilities (e.g., SNMP, NETCONF, etc.). The control and data planes are created and integrated into the same device by the device manufacturer in "hardware-centric" traditional IP networks. The final product has improved network speed and resilience quite a little. Nevertheless, this architecture is difficult to set up, debug, and administer. It also adopts innovations slowly and is particularly resistant to change.

The loose connection between the control and data plane is the major specific characteristic of the emerging software-defined network (SDN). In order to create different independent working layers for policy creation, enforcement, and execution, SDN shifts network component integration from vertical to horizontal.Principal Elements and the Architecture: Software-defined The capacity to manage, alter, and control network behaviour dynamically via open interfaces is made possible by network frameworks, which enable networks to be programmed. By retaining a live, centralised view of every component of the data route throughout the whole network, it provides centralised management of data plane forwarding devices regardless of the technology used to link the devices. Via its sophisticated orchestration and provisioning system, SDN makes long-anticipated capabilities like on-demand resource allocation, self-service provisioning, and totally virtualized networking possible. The high-level standard SDN architecture supported by the Open Networking Foundation (ONF). The data plane, control plane, and application plane are the three fundamental layers that make up the architecture. The components that are always present in an SDN deployment are the southbound API, SDN controller (or network operating system), northbound API, and network applications. Each layer has its own unique functions. We use a bottom-up approach to provide a brief overview of each of these components in the sections that follow. While developing solutions to protect the data plane of SDNs, an understanding of these components' fundamental features is important.

the data plane: Networking devices like switches and routers with a focus on packet forwarding make up the data plane. These, in contrast to conventional networks, are only straightforward forwarding components with no inbuilt intelligence to make independent choices. The controller and these devices interact via common OpenFlow interfaces, ensuring interoperability and compatibility in device setup and communication.The forwarding table of an enabled forwarding device is divided into three sections: rule matching, actions to be taken when packets match, and counters for matching packet statistics. Switch Port, Source MAC, Destination MAC, Ethernet Type, VLAN ID, Source IP, Destination IP, TCP Source Port, and TCP Destination Port are among the rule matching parameters. It is possible to specify a flow rule as a concatenation of these fields. The most frequent operations are: (1) sending the packet to the outgoing port(s); (2) encapsulating and sending to the controller; (3) dropping; (4) enqueuing; and (5) changing the field. Installing a default rule instructing the switch to transmit the packet to the controller for a decision is the most frequent scenario.

The majority of the research conducted in the first several years following the introduction of SDN was in these two directions. Yet recently, the focus has turned to creating cutting-edge security services that were previously impractical to execute. For instance, securing Internet-of-Things (IoT) devices, smart grids, and cloud computing employing network capabilities Further, we'll go over additional instances of SDN-enabled security services.The fourth

avenue is research aimed at securing the SDN platform itself, which is essential and directly affects the adoption of SDN. Several strategies have been put up to protect SDNs at different levels in this very hot research field. The goal of proposals like is to create secure controllers (for a categorization). Securing the northbound interface of an SDN is the focus of another area of study. For instance, present a permission mechanism that makes sure that only the trusted programmes may access controller operations. A crucial necessity is also to secure an SDN's southbound. The authors of provide a summary of the OpenFlow protocol's vulnerabilities. As a result, solutions like those take into account various OpenFlow features that present security issues and provide fixes. The authors of present a thorough analysis of the SDN attack research that have already been done and assess how these assaults affect the solutions that have been published for SDN protection [4]–[6].

In general, the adoption rate of a technology heavily influences the attention on its security, since many vulnerabilities are only identified with larger deployment. SDN has already been embraced by significant industry companies like Google and HP [68], which has accelerated research in this field even further. A number of thorough studies that summarise the current initiatives in this field have been published including.Finally, we further categorise the literature on SDN security. Every research falling under one of the first three categories of the previously described four research lines is categorised as SDN-based security services. We divide research aimed at securing SDN into three sections, including research aimed at safeguarding (1) SDN's five key components, (2) its fundamental principles, and (3) implementations. The centralised administration and programmability that are the basic components of SDN have already given rise to a number of suggestions to secure their protection. The deployment of SDN comprises safeguarding the various controller platforms, OpenFlow-enabled devices, OpenFlow protocol design and implementations, and software forwarding devices like Open vSwitch. Decomposing the literature in accordance with the SDN components that proposals seek to achieve is an alternate method. In Sections 6 and 7, we, respectively, examine strategies put forward to protect the data plane and control plane of SDNs.

Security of the Data Plane

Attackers have found network forwarding devices to be a particularly alluring target. In reality, cunning opponents, including intelligence agencies, have long sought to install backdoors in forwarding devices because to the vast quantity of information that may be disclosed via hacked ones. For instance, Edward Snowden exposed the NSA's significant expenditures in core network infrastructure, which allowed for widespread monitoring. Most recently, WikiLeaks' "Vault 7: CIA Hacking Tools" disclosures revealed that the CIA has actively exploited a flaw in 318 distinct Cisco routers to conduct surveillance operations around the globe. Moreover, WikiLeaks has shown that the NSA has been tinkering with forwarding devices in its upgrade laboratories before they are out on the market. Yet, skilled opponents are not the only ones who may assault forwarding devices. Attackers are able to exploit forwarding devices thanks to software and hardware vulnerabilities of the devices and insecure implementations of network protocols. For instance, as described in a beginner hacker could easily execute arbitrary code on routers using specially designed packets that targeted the device's particular purpose.

In order to conduct attacks against the network operator and its users, a hacked forwarding device may be used to drop or slow down, clone or divert, inject or fabricate network data. Examples include the exploitation of hacked routers for data gathering, exfiltration (such as Operation Aurora, manipulation and modification (such as inserting HTML code on websites), and cover tunnelling, according to the papers made public as part of the "Vault 7"

leaks. In addition to bypassing firewalls and intrusion prevention systems, a hacked routing system may also be used to violate the isolation requirements in multi-tenant data centers , breach VPNs. SDNs are far more at danger from a hacked forwarding device than conventional networks are. In fact, as mentioned in, an attacker in possession of a forwarding device has the ability to completely shut down an SDN. SDN simultaneously increases the difficulties in fortifying networks against tainted forwarding devices. For instance, innovative attacks on the data plane of SDNs, as those described in were not feasible in conventional networks. An OpenFlow-capable forwarding device's data flow diagram is shown in a condensed form in Figure 14.10. For such a device, it is expected that there are four primary processes: (1) Data Path, which is in charge of performing forwarding tasks, (2) OpenFlow Module, which is CPU-based software and is in charge of orchestrating interactions between Data Path, (3) Flow Table, and (4) Secure Channel. The flow table includes counters, actions to be taken on flows, and flow rules for matching L2-4 headers.

However communication with the controller must be mediated through the secure channel. The authors of detail how they were able to identify this process's vulnerability to information leakage, Denial of Service, and tampering attacks by employing the STRIDE mnemonic and carefully examining each component. When an attacker tries to jam too many flow rules onto the table, it is referred to as denial of service against the flow table. In an information disclosure attack, the attackers look for variations in controller response times and gather details about the network state, such as active flow rules. We define a tampering attack as one in which the attacker has complete control over the packet forwarding process and can put up any flow rule on the table. So, using this revised definition in comparison to, we assume that a tampering assault poses the greatest hazard.The following, in our opinion, are the primary challenges to protecting the SDN data plane:

1. Incompatibility with currently available solutions: The protection measures used by conventional networks for traditional networks do longer function in SDNs due to the loss of intelligence from the forwarding devices. In reality, we would need to completely rebuild the OpenFlow protocol in order to include conventional protections into SDNs.
2. Unverified dependency of the control plane on the data plane: For their understanding of the network, SDN controllers rely on Packet In messages. These mails are not checked or validated, nevertheless. Even with TLS authentication enabled, a malicious forwarding device may deliver faked or spoofed communications to alter the controller perspective of the network. A hacked forwarding device may conduct a Denial of Service (DoS) attack by flooding the controller with requests thanks to the same vulnerability.
3. Switches in software: End host servers support programmable soft switches like Open vSwitches. Soft switches provide a greater attack surface than physical switches, making them more vulnerable to assaults.
4. Stateful SDN forwarding devices: Stateful SDN switches were previously covered.

In general, the performance benefits of transferring some intelligence and authority to the data plane include a shorter latency response to network events and greater fault tolerance via the continuation of essential network functions under failed controllers. Moreover, data plane intelligence is needed for well-standardized protocols including encryption, MAC learning, and codec control message (CCM) exchanges. Nevertheless, under SDNs, these suggestions bring back a few of the weaknesses of conventional networks.A sizable body of research focuses on safeguarding a data plane against malicious flow rules created by hacked apps. In

order to do this, tools like FortNox allow a NOS to instantly check for flow rule inconsistencies and to approve applications before providing them access to amend the flow rules. As an alternative, configuration debugging tools like FlowChecker and VeriFlow are used to spot errors and flawed flow rules. The authors in implement a timeout proxy on the data plane as an extension to normalise the NOS delay in order to avoid side-channel attacks. The timeout proxy responds with default forwarding instructions if the controller doesn't reply within a certain amount of time. Several additional data plane debugging tools are offered to check if flow rules at forwarding devices are consistent with the controller's perspective or to keep track of whether packet forwarding behaviours are in line with control plane policies Unfortunately, since all of the aforementioned methods rely on reliable forwarding devices, they are ineffective in the event that such devices are hacked. In reality, it is well recognised that the adversarial model used in current SDN data plane security solutions is flawed. Their adoption and effect are directly impacted by this constraint. For example, the methods suggested in presuppose that all or most of the forwarding devices are reliable. Path verification tools contain cryptographic information so that the controller may check if the actual route travelled by packets matches what the controller expects in an adversarial environment Nevertheless, these techniques add a lot of bandwidth cost and additional header space.

Also, these solutions raise the cost of implementation since they need for the change of forwarding devices. There are four categories of relevant literature for packet forwarding anomaly detection: cryptographic techniques, flow statistics, packet probing, and acknowledgment-based procedures. Packets are signed using cryptographic techniques like and forwarding devices check to see whether the packets have been routed appropriately. The application of these methods is hindered by two key drawbacks: (1) Cryptographic operations entail substantial processing cost, and (2) IP packet formatting must be changed. Analyzing traffic data at forwarding device ports is a powerful substitute for cryptographic solutions (e.g., Unfortunately, flow statistic approaches are unable to recognise packet modification assaults because they largely depend on precise temporal synchronisation across forwarding devices, which is challenging in large-scale networks. To find forwarding abnormalities, packet probing algorithms like sample and analyse probing packets. The majority of these solutions cause considerable communication overhead since they are primarily concerned with anomaly detection at the first and final hops of a network. Packet dropping is detected by acknowledgment-based systems like via routine interaction between nearby forwarding devices. Given that each forwarding device in this scenario must retain the whole forwarding route of flows and regularly collect acknowledgement packets, there is also a significant cost in computation and storage [7], [8].

SPHINX is one of the well-known early efforts to protect the SDN data layer. SPHINX, a platform to identify attacks on network topology and data plane forwarding, was proposed in 2015. One of the few methods for securing the data plane of an SDN that does not presume the reliability of the forwarding devices is SPHINX. Via (1) abstracting network processes using incremental flow graphs and (2) pre-defined security rules given by its administrator, it identifies and mitigates threats originating from malicious forwarding devices. It also uses a similarity index metric to check for flow consistency throughout a flow channel; in order for a switch to be considered "good," the metric must be comparable. Which is a picture imported from the author's published work, displays the SPHINX architecture.In order to (a) enable incremental validation of all network updates and constraints, thereby verifying network properties in real-time, and (b) detect both known and potentially unknown security threats to network topology and data plane forwarding without compromising performance, SPHINX uses the novel abstraction of flow graphs, which closely approximate the actual

network operations. In order to understand novel network behaviour, it examines particular OpenFlow control messages. It also analyses metadata for both topological and forwarding state, and it generates flow graphs for each traffic flow seen in the network. It regularly refreshes and checks these flow graphs for allowable changes, and if it notices abnormal activity, it raises alarms. SPHINX uses proprietary algorithms to analyse network updates progressively in order to decide in real-time whether to accept updates triggering anomalous behaviour or not. Moreover, it gives administrators access to a lightweight policy engine that allows them to set expressive controls over network resources and find security breaches.

The first intrusion prevention system (IPS) for SDNs' data plane based on SPHINX. The greatest enemy that may exist at the SDN data plane and not anticipated in previous work, the authors assume a resourceful adversary who may have fully control over one or all of the forwarding devices in comparison to existing solutions. The attacker is specifically believed to be capable of randomly or selectively discarding, replaying, misrouting, delaying, and even producing packets (which includes both packet alteration and creation). Obviously, the adversary has the capacity to target network hosts, other forwarding devices, or the control plane thanks to the aforementioned capabilities. WedgeTail is a controller-independent IPS that is intended to "hunt" for forwarding devices that are not processing packets as anticipated, according to the developers of On the network, WedgeTail views packets as "random walkers" and examines packet motion as geometric space trajectory. It is possible to automatically locate malicious forwarding devices and pinpoint the precise harmful behaviour by examining the predicted and actual paths of packets (e.g., packet drop, fabrication). Administrator-defined rules may be used to train the WedgeTail's reaction to threats. A tailored immediate isolation policy may, for instance, direct the possibly malicious device to reset all the flow rules while also periodically reevaluating the device by repeating the packet(s) that first raised suspicion.

WedgeTail starts by giving forwarding for inspection priority in order to improve scanning efficiency and raise the likelihood of discovering harmful devices sooner. In order to classify forwarding devices into scanning groups of varied priority based on the cumulative frequency of occurrence in packet pathways crossing the network, it uses unsupervised trajectory sampling WedgeTail maintains a virtual clone of the network and intercepts the pertinent OpenFlow messages sent back and forth between the control and data plane in order to recover the predicted trajectories. The integrated header space analysis (HSA) component of this virtual replica processes it to determine the anticipated packet paths. Yet, the actual packet paths are calculated by monitoring a unique hash of the packet header. As an alternative, WedgeTail looks up packet history to find the packet trajectory if NetSight is installed.

Recently, other alternatives have also been put up, such FOCES FOCES uses a set of linear equations to represent the appropriate forwarding behaviours. In contrast to current verification tools, FOCES does not need special criteria to discover forwarding abnormalities that affect the whole network rather than just specific flows. Moreover, the authors of suggest DYNAPFV, which makes use of dynamic packet sampling to check the accuracy of packets on networks and dynamic flow statistics to check how packets are forwarded, in order to identify attacks that violate packet integrity.

Security for Control Planes

The control plane in conventional networks is spread over millions of lines of code and is described in hundreds of RFCs. In order to make networks simpler and more affordable than conventional networks, the control plane is removed from network forwarding devices and implemented as an external controller in SDNs. The SDN controller, however, is an entity

that does not exist in conventional networks, thus extra care must be taken to ensure its security. In reality, several of the same issues that make it difficult to safeguard the SDN data plane, such as the incompatibility of current solutions and the control plane's unproven dependence on the data plane (see Section 6), also apply when examining the security of the SDN control plane. Attackers may remotely distinguish between an SDN and a conventional network by examining the flow response time, according to a solution put out by the authors of Security via obscurity3, which relies on the assumption that an attacker cannot tell an SDN from from a regular network, is thus not appropriate in this situation.

Attacks against the control plane of a software-defined network may be divided into manipulation, availability, and software hacks, as was covered. We divide down these assaults into more specialised threat vectors in this section because we believe they provide the biggest obstacles to protecting the NOS. The top six threats to the network control plane.We go through each of these danger vectors in the paragraphs that follow.

Attacks against NOS software: An attacker may alter the functioning of the device by taking advantage of software flaws in the network operating system, which is hosted on a common server. An attacker may, under rare circumstances, seize control of the NOS. The attacker is deemed to have complete control of the network in this scenario, which is the most adversarial setting possible for an SDN. To the best of our knowledge, a NOS operating on a commodity server is believed to be protected by traditional security measures (such antivirus), and the bulk of available solutions work to identify a NOS that has been successfully hacked by an attacker. Gwardar was recently suggested by Shaghaghi et al. with the aim of safeguarding networks against a hacked NOS. Gwardar is really the first intrusion prevention system (IPS) created to safeguard an SDN against hacked SDN controllers. The suggested method expands on features provided in the author's prior WedgeTail trajectory-based IPS for SDNs' data plane In order to construct standard models for packet trajectories passing via network forwarding devices, Gwardar collects the packet trajectories from the data plane. By intercepting the OpenFlow communications that are sent back and forth between the control and data planes, Gwardar also keeps a virtual copy of the network alive. The aforementioned normal models are validated using this virtual replica. When derivations are found, Gwardar initially uses the attack detection algorithms of Venaticus to undertake a trajectory-based examination of the forwarding devices. To find potential malicious forwarding devices, it does this by comparing the suspicious packet paths with the predicted ones calculated across the virtual copy it keeps. It then examines the control plane whether the anomaly conforms to the rules provided by the control plane. For this, Gwardar presents flow rules with a high priority to the controller, matching the typical set of trajectories, and assesses whether the controller (a) appropriately submits the flow rules to the data plane and (b) updates the global network view accessible to applications following these modifications. When any of the aforementioned requirements are not true, Gwardar identifies a compromised NOS. The administrator of Gwardar has the power to programme the creature's response to danger. But, by default, it applies the legitimate flow rules to delete the malicious trajectories and obtains rules from the most current virtual replica copy it keeps. Gwardar may even be set up to take over the network in dire circumstances until the NOS has been restored.

DoS assaults: Much of the complexity in SDNs is pushed upon the controller due to the separation of the control and data planes. A bottleneck may develop if the controller gets a lot of flow decision requests (Packet In messages). Since these messages lack authentication, an attacker may take advantage of holes in the OpenFlow protocol or transmit a lot of them in order to overwhelm the controller with traffic. As mentioned in an attacker may also continuously broadcast IP packets with unpredictable headers to render a NOS unresponsive.

As adding more controllers has the potential to cause a cascading failure of those controllers, it is ineffective against DoS attacks on its own

DoS attacks may often be mitigated by efficient and dynamic response techniques, which fundamentally function by keeping an eye on unusual traffic patterns and scrutinising the flow patterns and data recorded by forwarding devices. Self-organization maps (SOM) are used by the authors in to identify Distributed Denial of Service (DDoS) flooding attacks and categorise network traffic into attack- and non-attack-related flows by uncovering hidden relationships between flows entering the network. The performance of the controller may be negatively impacted by their suggested solution, which necessitates continuous gathering and monitoring for necessary characteristics. Thus, propose to streamline this procedure by selecting network traffic for such evaluations. An even more straightforward strategy is suggested by the authors in in which the controller adds a flow rule to delete packets as soon as a certain traffic threshold is reached. An alternative OpenFlow-based approach to find and neutralise botnets is COFFEE Several approaches have been presented in the literature and are examined in including McNettle DISCO, and HyperFlow which try to boost the processing power of NOS using distributed designs. While a DoS attack may be very damaging to a network controller, it cannot, at least not immediately and by itself, provide the attacker complete, unlimited access to the network.

Attacks that use spoofing: The NOS has to understand the mapping between hosts and switch ports in order to setup the forwarding devices to offer connection across hosts. For this, the controller may tell the forwarding hardware to send itself any ARP requests and unknown packets. The hosts that connect to the various forwarding device ports may then be determined using the Packet In messages obtained for such packets. The controller sends a Packet Out message instructing the forwarding device to flood the packets to unidentified target hosts. The controller discovers the position of hosts as a result of receiving the answer from the destination. Since this learning process depends on the data supplied by forwarding devices and hosts, it is susceptible to spoofing attacks (e.g., MAC, IP, VLAN tag, etc.). Moreover, by creating a large number of packets with arbitrary MAC and IP addresses, which results in a large number of host profiles and controller interactions, an attacker may exploit this vulnerability and perform a DoS against the controller.

The authors in establish a particular element called address resolution mapping (ARM) in the controller to monitor MAC addresses of allowed hosts in order to avoid ARP spoofing attacks. ARP answers that haven't been validated by ARM are discarded after the controller speaks with this component. OpenFlow must also be configured to allow SSL encryption, which is not done by default, in order to avoid ARP spoofing. Moreover, as covered in packet-level information may be used to defend against ARP spoofing attacks. A forwarding device may designate its ports as user-to-network interface (UNI) and network-to-network interface (NNI) to prevent VLAN spoofing and, as a result, remove VLAN tags from packets received from UNIs The authors of suggest an OpenFlow virtual source address validation edge (VAVE) integrated in the controller to validate the address of packets when there is no matching entry in the flow table of the forwarding device in order to avoid IP spoofing. This work was expanded by Feng et al. in which each forwarding device has a collective understanding of address assignment and routing (i.e., adding some limited intelligence to the forwarding devices). Software-defined filtering architecture (SEFA), which expands the VAVE-based strategy to IP spoofing, is introduced by the authors in In this situation, the network forwarding devices are able to gather and create flow rules as well as add filtering rules depending on spoofing instances.

Protocol for Link Layer Discovery

Assaults: An SDN controller must initially discover the network topology using a control protocol like OpenFlow Discovery Protocol (OFDP) during a boot-up procedure in order to establish the flow tables on forwarding devices. The output port is configured to all forwarding devices when the NOS delivers an LLDP packet as a component of a Packet Out message. The LLDP message is sent to all neighbours and forwarded on all ports by each forwarding device in the network. A Packet In message, which also contains the port number that received the LLDP packet, is sent by each controller that receives an LLDP packet to the controller. The controller learns the network architecture in this manner by finding the connections between the forwarding devices. Clearly, this procedure is susceptible to spoofing attacks, in which a perpetrator may trick the controller's network topology by sending counterfeit LLDP packets A forwarding device may designate its ports as NNIs and UNIs and reject LLDP packets that are received from UNIs in order to prevent LLDP spoofing attempts LLDP message integrity and authenticity implementation may help lessen LLDP spoofing threats.

Attacks on inter-NOS communication: Several NOSs may be established for redundancy or each accountable to oversee a portion of the forwarding devices in order to manage a big network effectively and reduce the risks of a single point of failure (SPOF)5. When an active controller fails in the first scenario, forwarding devices create an uplink with the next available controller. For this, a distributed election protocol that elects a slave replica as the master controller in the event that the current master fails may be utilised. Moreover, controller states must be constant across all controllers. An inter-NOS communication channelalso known as an eastbound and westbound interface in the literatureis necessary for these communications. Several methods may be used by an attacker to intercept inter-NOS transmissions. For instance, the attacker may use spoofing techniques to influence how controllers are elected (e.g., a non-NOS involvement in the election protocol). Alternately, a tainted controller might choose manually the shortest permitted time to succeed the current master. An attacker might take use of protocol flaws like BGP in the scenario of governance being divided among forwarding devices.

When the ports that the SDN controller communicates to are known, the fake election messages that other UNIs send may be dropped. Otherwise, message origin authentication and integrity must be established for the election protocol and state replication in order to prevent an outsider from taking part in or meddling with the voting process (e.g., using mutually authenticated TLS among the controllers). Similar to other distributed protocols, the communication between the controllers needs extra security measures such information corroboration, message authentication, and integrity to prevent attacks from a rogue controller taking part in the election. In general, protecting against spoofing, LLDP, and inter-NOS communication attacksall of which are introduced in SDN distributed architectureis not unique to SDNs and is a common problem in distributed network systems. So, stopping these attacks is mostly a question of implementation, where each controller developer must put the finest operational security procedures in place to do so.

Network application attacks: The installation of procedures to authenticate and authorise them while utilising controller resources via proper isolation, audit, and tracking is one of the two key issues in safeguarding a NOS from malicious apps. For instance, although an intrusion detection system needs the ability to examine the packet headers, the access authorizations needed for a network load balancer are mostly linked to network statistics.The basic floodlight controller is advanced by the security-enhanced Floodlight controller (SE-Floodlight) with the addition of a secure programmable northbound API that expressly

upholds the privilege separation concept. Moreover, a run-time OpenFlow application verification module is included for ensuring the consistency of class modules that produce flow rules. Moreover, it compares the authoritative roles of rule producers to give authorization roles to OpenFlow apps in order to resolve rule disputes.

Using secure flow rule mediation, SE-Floodlight may also limit the Packetout messages generated by various applications. A collection of permissions (read, notification, write, and system permissions) and isolation techniques are used to impose permission constraints in PermOF proposal for fine-grained permission systems for applications. An application must subscribe to the set of permissions specified by Operation Checkpoint It also provides a module in charge of carrying out permission checks prior to approving application instructions. This paper identified three types of issues that are crucial for the identification and mitigation of harmful activity: rule conflict detection and rectification, application identification, and priority enforcement. FRESCO which comprises of an application layer and a security enforcement kernel, is another option. The former performs the following four primary tasks: (a) translation of scripts into modules; (b) database administration; (c) event management; and (d) instance execution. To prevent rule conflicts, FRESCO also has a security enforcement kernel. The NOS is protected against malicious programmes using a number of additional methods, which are reviewed in

Security Services Based on SDN

Exciting opportunities for network security enhancement arise from the capacity to inspect network status in real-time and programmatically regulate network behaviour. For instance, a threat mitigation application may dynamically reprogram the forwarding devices at the network's perimeter to discard the relevant traffic whenever a DoS assault is detected in the network. Similar to this, if malware is found in a network segment, the network may direct forwarding devices to limit traffic flows to that segment while more analysis is being done. Security as a service is a feature of other solutions that make use of SDN's capabilities. As an example, one privacy-enhancing service is the anonymization of a user's identity by disguising their IPs at the network level. Instead, by rerouting related traffic, sensitive data may be safely offloaded inside the company's network. These security features may be selectively activated for certain traffic flows, enabling an elastic pricing mechanism for value-added services. Creating SDN-based security services is a current subject of study, and a growing number of solutions are appearing, as was noted in Section 5. The extant literature is divided into seven categories, and each category is followed by an example.

Intrusion Prevention Systems: SDN enables the centralised collection of intelligence from various network segments, which when combined with the network's reprogrammability provides an improved platform for designing and developing intrusion detection and prevention systems that are more effective and efficient.Here, we examine some of the most notable initiatives in this field, which served as inspiration for the dissertation's suggested answers.For the purpose of detecting and mitigating anomalies, the authors of mix sFlow with OpenFlow. Their suggested solution consists of three main modules that interact with one another continuously: (a) the collector, which gathers flow statistics using OpenFlow and sFlow's capabilities; (b) anomaly detection, which is in charge of analysing the statistics and anomalies; and (c) anomaly mitigation, which inserts flow rules to counteract the threats that have been identified. A learning intrusion detection system (L-IDS) is presented by Skowyra et al. that makes use of the SDN architecture to identify and respond to network threats in embedded mobile devices. L-IDS incorporates traffic analysis and anomaly detection into forwarding devices in addition to embedding IDS functionality within the network controller.

A solution to safeguard data centre networks with OpenFlow support is called NetFuse In order to obtain active network flows and resource use, NetFuse monitors OpenFlow control messages. The overflow flows are then determined by evaluating them using a flow aggregation technique. Upon the discovery of such a flow, NetFuse dynamically controls the flow in accordance with rate-limits. OrchSec, which employs several distinct controller instances, sFlow for packet-level monitoring, and the creation of controller application software, is proposed by the authors in (instead of embedding them into it). Cognition is another another intriguing unique solution. Cognition makes use of SDN features, such as network-wide views and data for forwarding devices, to identify environmental, network configuration, and traffic variations from the norm and foresee possible security risks. NICE, an intrusion detection framework for virtual network systems, is suggested by the authors in NICE uses the features of the OpenFlow protocol to track and examine network traffic. When a vulnerability is found, the suspect virtual machine (VM) is isolated and examined in accordance with pre-established guidelines. Such a dynamic and adaptable IDS is barely practical on traditional networks, much like the aforementioned alternatives. Snort is integrated into an OpenFlow-enabled SDN via SnortFlow. The NOSs receive the actions that the SnortFlow server creates after evaluating the data collected from the Snort agents (if more than one, the matching NOS is chosen depending on the network segment, where actions should be performed). In order to make intrusion detection systems more effective and compatible with other home network applications like QoS, Mehdi et al. make use of SDN capabilities to move intrusion detection systems from the network core to home networks.

Security Middleboxes: SDN makes it possible to reroute a portion of network traffic via network middleboxes, which are commonly used to provide security services. As compared to conventional networks, where this choosing routing was not available, this is a significant gain. According to the authors of a centralised controller installs and migrates functions onto middleboxes using the Slick architecture. The network security software instructs the Slick NOS to deploy features for routing certain traffic in this case. The NOS is then in charge of deciding where the middleboxes' functions should be placed and creating the appropriate pathways for network traffic. As it doesn't interfere with the SDN capabilities or middlebox features, the SIMPLE policy enforcement layer provided in is more useful than the one in To identify the processing status of tunnelling packets between forwarding devices, SIMPLE uses tag-based packet categorization. It should be noted that tag-based systems process information faster than hash-based processes for packet categorization. Each node in the network has a certain security clearance, and the flow rules are set up such that communication is only routed via the receiver with a security level that is higher than the sender. This is how Liu et alpropose to combat hidden channels. Flow is sent via a middlebox for further automated verification if the threshold is lower. With conventional networks, it would not have been possible to implement this dynamic and adaptable design. In order to improve network middleboxes, other systems with a similar architecture have also been developed and are examined in.

Privacy-enhancing Services: Since the controller can dynamically coordinate the installation of custom flow rules across the network forwarding devices, SDN makes it easier to establish anonymization services. So, online and through the forwarding devices themselves, anonymization is carried out. For instance, to eliminate IP-based tracking on the Internet, the authors of suggest AnonyFlow as an anonymization service. Here, the ISP utilises unique IDs to track user traffic exiting its domain and allocates temporary IP addresses to consumers. Jafarian et al. propose OpenFlow Random Host Mutation (OF-RHM), which transparently and randomly modifies the IP addresses of network hosts. Each host is given a temporary, random virtual IP address by the controller, and only authorised parties are allowed direct

access to a host using its actual IP address. More recently, use SDN capabilities to improve the deployment of Decoy Routing. In this scenario, the NOS manages the Decoy Routers and is in charge of observing the network traffic to "identify covert signalling by clients who seek Decoy Routing services, decryption and appropriate traffic redirection, identifying maliciously behaving switches, load balancing, and automatic failover".

Safeguarding Cloud Services: SDN offers interesting chances to study better security in cloud systems The authors of propose an Automatic Malware Quarantine (AMQ) supported by SDN, in which network hazards are automatically segregated to reduce related risks by use of SDN applications designed for this purpose. There are two primary parts to their suggested remedy. First, the real-time malware detection provided by the Bot Hunter Network Service Module. The second is the Threat Responder Network Service Module, which is in charge of removing threats from the network and placing them in quarantine. As a result, enhances reaction time and eliminates the need for manual settings and difficulties as compared to AMQ in conventional networks. Another suggestion to increase cloud system security by using SDN capabilities is CloudWatcher. By offering a straightforward policy scripting language for employing these services, CloudWatcher regulates network traffic and assures that their examination by security devices. The network is dynamically controlled using SDN capabilities, and routing flow rules are established to make sure that flows travel through the designated security services. Software-defined clouds (SDC), which make it simple to reconfigure and adjust physical resources in a cloud architecture, have recently been suggested. SDC is thought to possibly enhance the security of cloud services in addition to the many operational benefits and efficacy it offers.

1. Secure Data Offloading: SDN enables network packet routing in accordance with application requirements. This is anticipated to significantly affect computation offloading. Enterprise Centering Offloading System (ECOS) is a proposed enterprise solution by Gember et al. that enables mobile applications to offload data in line with user-defined privacy, performance, and energy limitations. The corporate resource pool's idle resources are processed by the ECOS-enabled NOS. User-private, enterprise-private, and no-private data classifications have an impact on the NOS's choice of policy. Using ECOS, latency may be increased by up to 94%, energy can be conserved by roughly 47%, and execution state can be reduced by up to 98% for mobile apps. The use of networking capabilities made possible by SDN to handle application-layer issues in a dynamic and flexible manner is shown brilliantly by ECOS.

2. IoT Security: The two key issues with IoT device security are heterogeneity and scalability In the last several years, researchers' focus has turned to a new area: using SDN capabilities to handle these security concerns. After a brief overview of a few instances, we direct the reader who may be interested to for surveys. An identity-based authentication strategy for IoT devices utilising SDN is suggested by the authors in In essence, the SDN controller has a certificate authority built in that is in charge of managing all security settings and certifying devices and gateways through a security protocol. Nobakht et al.'s proposal for an IoT-IDM host-based intrusion detection and mitigation system makes use of SDN's centralised network view and reprogrammability. On top of the NOS, IoT-IDM is deployed, and upon detection of assaults, it gives network forwarding devices instructions to avoid attacking target IoT devices. In the authors suggest Black SDN for IoT as a method to prevent traffic analysis and data collecting by encrypting both the content and header of each packet. Bull et al.'s proposal uses distributed SDN gateways, which keep an eye on traffic going to and coming from IoT-based devices, to mitigate DDoS assaults. In the S-based IoT architecture proposed by Fauzac et al. each node in the ad hoc network is considered as a hybrid of an SDN-capable forwarding device and a legacy host. The security controllers are in charge of keeping an eye

on network activity and enforcing security regulations. The flexible routing offered by SDN, which is activated by the controller upon detection of assaults on one network connection, is how the authors in intend to increase the resilience of IoT communications.

3. Additional: SDN capabilities have shown promise in several fields. These, however, are still developing fields that are scattered among many literary fields. An SDN-driven authentication, authorization, and accounting system, for instance, is presented in to enhance the security of medium-sized

Security of the SDN Data Plane: Problems, Solutions, and Future Directions

Business networks. A different approach is taken by the authors in who employ SDN capabilities to create an architecture that allows residential internet customisation and might be used to protect home equipment. Vehicular ad hoc network is another area that expands on SDN capabilities (VANET). To this purpose, a number of ideas have surfaced attempting to use SDN to solve the primary issues in VANETs, such as uneven flow traffic among multi-path topologies. These approaches often rely on a centralised Road Side Unit Controller (RSUC) that can interface with data plane components and provide instructions to cars and RSUs about the forwarding rules. The operational advantages of an SDN- enabled VANET include reduced service latency, enhanced user experience, and effective use of network resources via collision reduction Moreover, it strengthens a VANET's resilience by enhancing the mitigation of security flaws like Sink Holes and DDoS assaults [9], [10].

Shaghaghi et al. have proposed a network-based insider attack resilience architecture to identify and deter insiders in businesses by using the SDN capabilities. Network Context Attribute is a brand-new collection of attributes introduced by Gargoyle for context analysis (NCA). The capabilities of the user's device, its level of security, the type of network connection it is using, the network's status, its recent and past interactions with other devices, and any suspicious online activity are all included in NCAs, which are extracted from the device-generated network traffic. For instance, Gargoyle identifies devices with hacking tools (such as port scans and vulnerability scanners), outdated software, strange activity (such as unexpected locations, device interactions, etc.), and suspicious browsing patterns, such as visiting sites that have been banned. Gargoyle uses the capabilities of SDNs to passively analyse network traffic and gather contextual data.

As a result, Gargoyle may operate independently of the user's device-integrated sensors and be easily and cheaply transported to other enterprises implementing SDN. Gargoyle evaluates the risk related to an access request using NCAs and user behaviour modelling (both current and historical). Gargoyle must make sure that the data plane forwarding devices are secure since it is a network-based solution that relies on them for context extraction and access enforcement. To do this, it incorporates reports from WedgeTail when assessing a context's credibility. Moreover, Gargoyle incorporates PEPS and supports host- and network-level access controls that may be set. In reality, Gargoyle's SDN App (GSDN) supports a defense-in-depth security paradigm and improves policy enforcement. For instance, it may be necessary to prevent a suspect device from using the organization's network while additional inquiries are being made. Lastly, Gargoyle's mobile app (GAPP) may limit a set of functions for a data requestor based on assessed trustworthiness of a context by implementing Function-based Access Control (FBAC). In order to increase efficiency and security, SDN has also been used in other fields, such as critical infrastructures, smart grids, and wireless local area networks (e.g., for a survey).

New Research Initiatives

While there has been an "SDN-boom" in recent years, this technology is still in its early stages and will only become more secure and dependable as it is adopted and deployed more widely. Particularly, SDN systems may be susceptible since protocols like OpenFlow and the various NOS platforms are constantly updated. In conclusion, our analysis of current safeguards for SDNs' control and data planes reveals that: - The bulk of current SDN data plane solutions presume that forwarding devices are trustworthy and are not built to operate in hostile environments. Contrarily, solutions assuming otherwise have the following main drawbacks: significant network processing overhead (e.g., cryptographic solutions), detect threats in accordance with pre-established rules, are unable to differentiate between specific malicious actions (e.g., packet drop, misroute, etc.), and have limited ability to effectively respond to threats. Lately, some of these restrictions have been partly solved by solutions like Wedgetail

The difficulties in securing this layer are made worse by recent ideas for data plane enhancements, such as stateful data planes. Briefly put, stateful data plane ideas recommend the addition of switch-level programming abstractions in order to provide localized stateful flow processing, which would give the devices some amount of intelligence. Stateful SDN data planes do, however, provide three additional forms of vulnerabilities as compared to regular SDN data planes:

1. Unbounded Flow State Memory Allocation: Each forwarding device has to have memory space to keep track of the state changes brought on by the incoming flows if data planes are to be programmable. Each forwarding device needs a lot of memory, therefore an attacker might use that to their advantage and use up all of the device's memory.
2. Absence of Authentication Mechanisms in the Data Plane: If stateful data planes were to have independent control features, this would need the employment of probing messages between forwarding devices or information travelling between switches and "piggyback" within ordinary traffic packets Safeguarding inter-forwarding device communications is a crucial topic that has so far mostly gone unaddressed in the literature. In reality, a hacker may trick a trustworthy device into sending a bogus event or packet into the network. Moreover, if the connections are not secure, an attacker might manipulate the particular flow statuses and the data sent between the forwarding devices. An attacker may create fictitious events that would cause a connection failure and impair network performance.
3. Absence of a Central State Management: State inconsistency is a problem that affects interconnected stateful data planes as well as all distributed systems. The lack of a central organisation to oversee the synchronisation of states within the forwarding devices makes this situation more worrying, nevertheless.

In particular, an attacker has the potential to induce state transitions, driving the network into an inconsistent state, since state transition is triggered when packets are received.On the other side, several of the attacks that were conceivable in conventional SDNs are reduced by the architectural modifications brought about by stateful data planes:Stateful data planes lessen the amount of communication between the control and data planes that is necessary. Enforcement Attacks: We described enforcement attacks. By increasing its scalability, this increases SDN's resistance against availability threats.

Attacks during implementation:

Stateful SDNs are built to combat the following vulnerabilities: (1) flow information leakage and (2) exhaustible TCAM utilised for flow tables In reality, the forwarding devices may be configured to manage incoming traffic without interacting with the controller using stateful data planes. In light of this, stateful data plane deployments significantly reduce the relevance of the flow information leakage problem.All in all, new approaches are needed to secure and safeguard SDNs that include stateful forwarding devices due to the increased number of vulnerabilities they create.The bulk of currently suggested solutions to secure the NOS are built to defend it against certain threats (such DoS Attacks), which often come from the application and data plane. In reality, there aren't many ways to defend a network against a malevolent NO. Moreover, we are not aware of any other solution outside Gwardar that is intended to identify a NOS that has been effectively infiltrated and defend a network against it.The attack surface against forwarding devices has grown over the previous several years, as highlighted throughout this work [11], [12].

CONCLUSION

We were able to identify the main threat vectors that an attacker would have access to while attacking a software-defined network by analyzing the architecture of SDN and the security of this new technology. In respect to the main components of SDN, we have created a taxonomy of different attacks. Next, we described the main issues that make SDN's data and control plane security more complicated and examined the existing solutions in the literature. The literature has recently begun to pay greater attention to SDN-based security services; therefore, we also provided a categorization of them. Finally, we provided a number of suggestions for fresh paths of research in this field. Today's routing protocols and network diagnostic tools, however, continue to operate on the assumption that the underlying hardware is reliable. Hence, networks need ways to automatically identify malicious forwarding devices and defend the network against them, regardless of the reason for the attack and regardless of the underlying hardware and software. Yet, anticipating threats is a useful addition to detection and reaction. To the best of our knowledge, there aren't any solutions in the literature that are intended to foresee assaults on SDNs before they happen

REFERENCES

[1] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, “Software-Defined Network (SDN) data plane security: Issues, solutions, and future directions,” in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2019. doi: 10.1007/978-3-030-22277-2_14.

[2] T. Alharbi, “Deployment of blockchain technology in software defined networks: A survey,” *IEEE Access*. 2020. doi: 10.1109/ACCESS.2020.2964751.

[3] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, “Security in Software Defined Networks: A Survey,” *IEEE Communications Surveys and Tutorials*. 2015. doi: 10.1109/COMST.2015.2474118.

[4] S. Kim, S. Yoon, J. Narantuya, and H. Lim, “Secure Collecting, Optimizing, and Deploying of Firewall Rules in Software-Defined Networks,” *IEEE Access*, 2020, doi: 10.1109/aCCESS.2020.2967503.

[5] Y. Zhao, Y. Li, X. Zhang, G. Geng, W. Zhang, and Y. Sun, “A Survey of Networking Applications Applying the Software Defined Networking Concept Based on Machine Learning,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2928564.

[6] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Futur. Gener. Comput. Syst.*, 2021, doi: 10.1016/j.future.2021.03.011.

[7] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y. W. Chong, and Y. K. Sanjalawe, "Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller-A Review," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3013998.

[8] T. A. Assegie and P. S. Nair, "A review on software defined network security risks and challenges," *Telkomnika (Telecommunication Comput. Electron. Control.*, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13119.

[9] R. Sultana, J. Grover, and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges," *Vehicular Communications*. 2021. doi: 10.1016/j.vehcom.2020.100284.

[10] G. Hessam, G. Saba, and M. Iyad Alkhayat, "A new approach for detecting violation of data plane integrity in Software Defined Networks," *J. Comput. Secur.*, 2021, doi: 10.3233/JCS-200094.

[11] S. Ahmad and A. H. Mir, "Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers," *J. Netw. Syst. Manag.*, 2021, doi: 10.1007/s10922-020-09575-4.

[12] M. P. Singh and A. Bhandari, "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Computer Communications*. 2020. doi: 10.1016/j.comcom.2020.02.085.

CHAPTER 16

AN ANALYSIS OF PRIVACY ISSUES IN ELECTRONIC HEALTH RECORDS

Ashendra Kumar Saxena, Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India,
Email Id: - ashendrasaxena@gmail.com

ABSTRACT:

The ability to gather, store, manage, and distribute medical data on a broad scale has been made feasible by recent innovations in the health industry. Electronic health record software is largely required for managing and sharing health information, but reusing electronic health records in a distributed setting or allowing third parties access also requires adherence to international privacy standards and legislation. The primary problem while working with real-time datasets in the health industry is privacy protection. Algorithms for privacy preservation must guarantee the security of sensitive data pertaining to patient diagnostics and illnesses. Data perturbation, anonymization, and modification in accordance with system requirements are the focus of privacy-preserving data mining (PPDM). One of the greatest PPDM strategies, data perturbation mostly works with numerical quantities and focuses on privacy implementation. The idea of privacy is not well defined since it depends on many cultural factors. The conventional method of keeping medical records has altered due to the rapid growth of information communication and technology.

KEYWORDS:

ElectronicHealthRecord(EHR),PrivacyStandards, Security, Data Perturbation.

INTRODUCTION

ICTs (information, communication, and technology) have been incorporated with other diverse fields throughout the last 20 years. The healthcare industry was not exempt from the dramatic growth of ICT, as it was with other sectors in emerging and underdeveloped nations. Social and professional work technology have a significant influence on many of our everyday duties. The eHealth domain requires security for patient-related sensitive data, including heart failure status, cardiac rhythms, blood pressure, and oxygen-related issues [1]–[3].The main driving force from the discussion above is that both a person and an organisation are deeply concerned and have given it a higher priority level. Researchers are aware of the need for privacy protection, data accessibility, and the storage of data in database systems in order to create effective mechanisms. Electronic health records must provide information security, greater access rights to the owner of the information, data privacy, and safe database administration. Various users of the system will be concerned about the leakage of personal information and wish to protect electronic health records. By releasing the bare minimum of data in the electronic health domain, the proposed chapter offers the means to safeguard the privacy of patient electronic health records. Future machine learning (ML) algorithms for electronic health records will be assessed and used with consideration for sensitivity, data privacy, task-based access restriction, and minimum data storage.

The right to privacy is described as "the assertion by a person, group, or institution to control the manner, mode, and degree in which information about them is disclosed to others." Around 9.6 billion devices are now linked to the Internet, and there are 1.3 billion mobile broadband connections. These linked gadgets produce and exchange around five times as much data in diverse locations every two days, as shown. The resulting massive data generation and sharing is known as the "data revolution," and the big data digital world exposes various vulnerabilities when individuals converse online, do online banking transactions, or use email or instant messaging. Electronic health records (EHR) on eHealth are accessible to hackers.

EHR Privacy Protection

Present SituationInternet and may abuse user information for personal gain. Today's accelerated technological progress has an impact on healthcare organisations as well. ICT (information and communication technology) was widely employed in hospitals and therapeutic settings. In order to adopt eHealth infrastructure in the health sector and enable online health advice and true health information, many countries around the world have public-private partnership (PPP) policies. However, there is a chance that patients' sensitive information will leak in this type of distributed environment. Via the Internet and Intranet, health information technology (HIT) services promote service demand much as in other economic sectors and significantly lower service costs for many stakeholders and users. With eHealth, doctors, pathologists, and medical clinics may access patient electronic records whenever and wherever they are needed. Patient health records may be dispersed around several hospitals and clinics in order to improve the diagnosis and treatment of a certain ailment or test, but this dispersed information runs the risk of being compromised and posing problems for the patient's data privacy.

The eHealth domain includes many patient record types that have been in-depth analysis by academics working in related fields. In the eHealth industry, privacy and efficient data storage have emerged as the two biggest issues. A basic right to privacy has been stated. The Indian Supreme Court has ruled that everyone's right to privacy is now a basic one. Demographic and sensitive information is stored in electronic health records and shared with many parties. Electronic health records must meet fundamental criteria such as consistency, completeness, accuracy, data protection, and security. EHRs have entered the group of most private data, such as patient personal information. Utilizing a patient-centric approach and fine-grained data access control methods, has developed a protected personal health record. Nevertheless, sending data via the Internet exposes users' personal information and places a significant burden on the system's processing power. A unique paradigm for creating a secure connection has been presented, and it uses holomorphic encryption [4]–[6].

The required degrees of privacy provided by the electronic health record, as defined in the literature, should be carefully handled. Within the eHealth area, several medical facilities and associated employees are dispersed. Researchers have proposed a number of strategies to improve privacy utilising a variety of encryption techniques, including hashing, the AES (advanced encryption standard), the DES (data encryption standard), and access control mechanisms.

Notwithstanding these methods, patients cannot be guaranteed anonymity when data are shared throughout medical institutions. As a result, several medical authorities that are involved in the care of the particular patient must request access to the patient's data. To reduce the privacy risk in the electronic health record, trust-based privacy techniques have been presented in the literature. Using this strategy, users' roles were segregated in order to protect data privacy. While this method overcomes the security and privacy risk issue, it

limits how other users may use the programme. More calculations are needed, which raises the relevant cost.

The use of privacy and security regulations might be based on the content and orientation. The amount of privacy seems to rise as illnesses get more complicated and need participation from several experienced doctors for diagnosis and treatment. This study leaves certain questions unanswered on how and to what degree to protect privacy levels. As shown in , study effort was done to strengthen the data mechanism in the eHealth sector. Nevertheless, only a small number of these studies used data protection both throughout the research process and during storage. A developed and demonstrated privacy method for electronic health records proved time effective and dependable. According to, eHealth records need a lot of space, while describes how wireless sensor technologies might reduce space complexity while still requiring automated process mechanisms for data administration. A greater degree of danger is there when data are exchanged or when information is leaked straight from the database during communication. Privacy and security are two distinct concepts that cannot coexist without applying security to the data, according to the authors of [7], [8].

DISCUSSION

Security and privacy are connected and even used interchangeably. Some of the several encryption methods that may be used to protect data include the RSA, DES, and Diffie-Hellman key exchange algorithms. A federal strategy has already been employed, which focuses primarily on the risks and rewards for service providers while ignoring the privacy concerns of specific customers. Several research initiatives have been handled in western nations on the basis of the federal method. The privacy of health information has been protected by a variety of PPDM algorithms in the past, although some of them just employ basic categorization and clustering before analysis on that particular region. The authors of have described the novel classification-related anonymity challenge and suggested a genetic method for real-time datasets. The anonymity algorithm is suggested in for integrating data from many stakeholders. The algorithm reported in uses a pseudonymous mechanism to offer a model for medical research and applies the horizontal partitioning technique of data distribution. This approach may be merged with privacy algorithms for data security while exposing data from one party to another.

Many cryptographic and noncryptographic privacy preservation techniques are used in the eHealth sector. Several of them utilise symmetric key and public key encryption as information security techniques to safeguard the eHealth data they use. On the basis of an attribute-centered approach to access control of health data by various parties and numerous accessibilities of different owners in multiuser environments, an encryption technique was developed in. In lieu of an attribute-centered method, attribute revocation is employed to govern user identity verification. Due to the bilinear computing required for data decryption, the attribute-based technique is seen as more costly. Owners of the data may develop and distribute the key offering the automatic revocation feature, but it is expensive in terms of calculations. Health record data are encrypted and decrypted by Lagrange multipliers in generation of symmetric key encryption. It had been stated in that the role-based authorization strategy is only for the authorised user to access electronic health records for a specified amount of time, however this approach limits the usefulness of data and increases complication when a person assumes many roles within a particular time frame.

During communication, the patient health record's data security is offered as smart card- and pin-based is an illustration of a biometric authentication strategy for patient health data security and privacy. As shown by Jafari et al, the cryptographic key management system is

encrypted and the same key is again decoded at the other end to ensure that only authorised users may access the relevant data. Due to permitted device connection in the electronic health records syste, triggered several serious privacy issues. According to, information and communication technology have created a scenario where patient health data are subject to fresh security and privacy issues. Confidentiality, integrity, and availability (CIA) are three essential security objectives that are also crucial to the privacy of an electronic health record. Since EHRs may be gravely endangered by hackers, viruses, and worms, CIA principles are the main criteria for privacy protection of EHRs [9]–[11].

It is guaranteed that individual data will not be reidentified by the user when it is shared and utilised by academics or other parties. Aggarwal, Philip, and Sweeney created the formal model for k-anonymity protection, which states that it only applies to shared data if each member can't be uniquely recognised before k 1 individual information is made public in the shared list. The main goal of this essay is to identify the identification assaults that occur when information is released.Software for electronic health records (EHR) stores and processes a variety of data kinds, including photos, text, numbers, and many more. The privacy and security literature has a number of publications that demonstrate how individual identify may be disclosed through quasi-identifier disclosure even when qualities directly relevant to direct identification are excluded from the list. The maintenance of the quasi-attributes for maintaining the privacy of individual data have been suggested in. SDC was used on a clinical dataset that included nonnumerical variables. Many theoretical ideas have been published in literature by scholars. Also, they used randomization and k-anonymity-based approaches on partitioned horizontal and vertical data using an open dataset. The survey in this research included many methods from the literature that were applied in various areas and privacy-preserving data mining. To keep the records, other businesses made proposals to EHR systems.

While Microsoft HealthVault, Google Health, and other openEHR software offered data protection, they did not meet the consumer privacy criteria outlined in or the laws and guidelines outlined in the constitutions of the various nations' privacy and security standards. EHR security and privacy may be breached, and viruses and worms can be used to delete sensitive data. A study and analysis of the electronic health record's current situation may be found in. Regarding security and privacy concerns, it was more important to pay care while disseminating personal information in distributed systems. Cloud computing is a GenNext technology that is now evolving because to ICT advancements. The retrieval and transmission of encrypted electronic health records are the main topics of this research. For data privacy and security, the authors of this research focused on Diffie-Hellman key exchange algorithms. In a recent research, authors demonstrated how machine learning may be utilised to apply security and privacy policies properly. ML can cover the gap between data regulation, standard, and technology. The automated NPL-based de-identification model has also been suggested and evaluated in, along with the machine learning-based data de-identification method. Data are saved throughout a distributed environment's numerous servers. Sensitive data values are protected in EHRs because linked data is maintained apart from clinical data, but these systems are not sufficiently safe enough to preserve and manage an individual's privacy. The criterion put forward in European 2020, "privacy by design," served as the foundation for the framework created by the authors.

The diverse patient data types that are stored in EHRs include sensitive patient data as well as data linked to quasi-identifiers and demographic values like DOB, name, and age. Even when the identifying data are deleted, linked data remain related. How to separate the related data after a certain time period has been shown in. It was suggested in that the new computerised approach of sanitising textual medical papers, which was previously done manually, is

expensive and time-consuming. Little sums are utilised for nonstatistical data values while large sums are employed in statistics. A new statistical framework for privacy called SPLU permits the release of data. Framework used data-randomized perturbation for the privacy of sensitive data. For the purposes of query processing and auditing technique, the SPLU essentially uses sanitised data. Maximum utility for big sum queries was enforced by the framework. The architecture incorporated a small sum querying technique for privacy protection. The availability of EHR data today may be exploited for ancillary purposes. While the clinical data may be utilised to safeguard privacy, converting the data into the EHR system that is currently in use is a rather laborious process. This methodology, which is detailed in, turns the clinical text content information into EHRs and uses privacy algorithms to de-identify sensitive data. In the past, CIA criteria that solely employ conventional database systems have been fulfilled using statistical techniques.

The results of GWAS (genome-wide association studies) are not used in this system. When a system offers the highest level of data privacy, its scalability may be evaluated. According to the authors of, privacy preservation might be offered in two stages. The data is cleaned up and privacy-preserving methods are implemented in the first step, and expert analytics perspective is used in the second phase for further filtering. WSN data processing and automated data collecting are used in ubiquitous health computing. The vulnerability of WSN-based ubiquitous health makes it increasingly important to establish data security and privacy measures to protect people's personal information. In survey article, most pertinent PPDM methodologies and issues are emphasised. Suggested framework identified user behaviours and monitored the activity appropriately from sensor actuators. ICT development has an effect on the healthcare industry as well. Healthcare sectors are confronting the issue of privacy breaches when data are shared in the distributed system, however improvements in this sector provide patients better facilities, better treatments, and lower costs. Identification of a person's identity may have an impact on their daily lives or businesses.

Anti-identity Disclosure Algorithms

In order to prevent identity revelation, privacy methods must be used in a manner that would prevent data usefulness from being compromised. The utility optimization in altered datasets, however, is not maintained by the majority of privacy-preserving approaches. Using heuristic techniques on each prime identification trait might be an efficient way to preserve identity disclosure. Algorithms are further categorised in light of this.Quasi-Identifier Transformation: For the purpose of avoiding identity revelation, quasi-identifiers are transformed using three basic methods:

1. Microaggregation
2. Generalization
3. Suppression

Using summary statistics, micro aggregation approaches substitute a set of values in a quasi-identifier (QID) (e.g., centroid or median for numerical and categorical QIDs, respectively). This method has mostly been used successfully with demo visuals, but not with diagnostic codes.On the other hand, generalization used semantic consistency to apply the QID value replacement. The terms "global" and "local recoding" refer to two generalization approaches that are used to protect privacy.

a) Global recoding entails translating the QIDs' domain into generic values. These values are groupings of values or aggregate notions (for example, British rather than English for Ethnicity) (e.g., English or Welsh for ethnicity, or 18– 30 for age). As a result, a dataset's instances of a particular value (such as English) will all be generalized to that same value (e.g., European).

b) Local recoding maps a specific record into a generic record on a group basis. For the purpose of avoiding identity exposure, like values that are maintained in American English in two separate entries may be substituted in one record.

Thus, with present approaches, data usefulness may be maintained by using the following broad strategies:

1. Calculate the information loss using an optimization metric.
2. Making the assumption that data will be utilised in certain analytical activities and working to maintain its correctness on released data.
3. Generating data in accordance with the accounting utility specifications set out by data owners exclusively.

By quantifying the information loss caused by data transformation, data usefulness may be captured.

Laws that Protect Data and Privacy

1. Canada: For the protection of its citizens, the Canadian government created the (PIPEDA) statute. The Personal Information Protection and Electronic Documents Act (PIPEDA) lays forth precise guidelines for the gathering, use, and disclosure of personal data by third parties. The PIPEDA outlines the need for regulations in the health industry, and it makes it simple for Canadians to comprehend the PIPEDA's obligations and justification for protecting personal information.

2. Morocco: The personal data protection act (09-08 act), known as PDPA in Morocco, safeguards user information and upholds data privacy while utilising sensitive and personal information. By limiting the personal disclosure of sensitive data throughout the operation, data controllers are accountable for upholding and managing the safety of people' privacy.

3. European Union: Article 8 of the European Convention on Human Rights guaranteed the "right to privacy" in one's personal and family affairs. Since the EHR may divulge medical information, the EU government established a strict privacy rule. Every year, the European Commission publishes the data protection regulation for privacy and data protection. A data protection legislation was accepted by all European nations.

4. The US: HIPAA, The Health Insurance Portability and Accountability Act (HIPAA), a legislation signed by President Obama, mandates that identifiable health information shall include the following and that no one's identity may be compromised:Almost all privacy and security laws were incorporated in HIPAA, and they were implemented in all 50 states.

i. It is required to get permission from the owner of the laws if it is essential to divulge personal information.
ii. Individual data may only be disclosed by the owner if it is necessary for further action in health-related matters.

5. India: The UID system stores personal data. To identify personal and demographic data while connecting it to medical artefacts, UID is utilised with health records. As a result, if sensitive data is poorly connected on EHR systems, identity theft is simple. Hence, all health

record systems follow the guidelines below when collecting data on patient identification and demographics. Broadly speaking, the Indian IT2012 Act

Health Informatics—Identification of Subjects of Health Care

1. The Aadhaar number must be used as a distinctive health identification that is guaranteed and required of implementers. The system must enable the user to provide at least two other identifiers in the absence of an Aadhaar number. In cases when there is no accessible identification, a temporary identifier may be established and replaced in a certain amount of time by a verified identifier. Temporary IDs may be used (according to the HSP's protocol) in cases when the patient's identification cannot be determined or retrieved, and afterwards verified identities may be introduced (while making earlier ones as inactive).

Identification of patients in EHRs: It is challenging to match a patient's record when records need to be exchanged on a distributed EHR system since the Aadhar number (UID) is not necessary for maintaining patient data in electronic health record systems. The result is that a person's identity may be utilised for peculiar reasons by various individuals in different places.

Applications for Privacy: Applications for privacy-preserving data mining (PPDM) are many. Data mining is most needed in practically every discipline, whether it is connected to research, the arts, or business. PPDM is often employed in diverse fields; this chapter presents some of them. The term "right of a person" has been used to refer to privacy, as was covered in several sections above. Privacy-protected individual data is used in practically every industry. We will talk about a variety of uses for privacy-preserving data mining techniques in this section.

PPDM applications may be categorised in a variety of ways. The primary application fields are further divided into categories including cloud computing, wireless sensor networks, and location-based services (LBS) (Location Based Services).The cloud computing model is "a model for enabling ubiquitous, on-demand network access to share pool of configurable computing resources that can be rapidly provisioned and realised with minimal management effort or service provider integration," according to the U.S. National Institute of Standards and Technology (NIST). In other words, cloud computing makes advantage of dispersed infrastructure that is available through the Internet. Every aspect of cloud architecture operates as a service. Location-based development methods are used in cloud computing. It may be a communal, private, or public cloud.

Cloud, it all relies on the needs of the business. The terms SaaS, PaaS, and IaaS, which stand for software as a service, platform as a service, and infrastructure as a service, respectively, are used to describe cloud architectures. Since our data are kept in the cloud, which allows them to be stored anywhere in the globe, and because each nation has its own privacy laws, regulations, and standards, it is essential to pay greater attention to safeguarding our data on the cloud. As data are shared or stored in distributed computing, privacy-preserving solutions are mostly needed. Techniques for query control and auditing that safeguard privacy are crucial for data security.

Data are saved in EHRs using distribution-based partitioning. Most significant two medical systems Several clinics utilise Datafly and the scrub to retain clinical data. As the majority of healthcare data is in the form of text and pictures, scrub data system is used to deidentify clinical notes and letters. Clinical papers often employ acronyms. The algorithms and people who are familiar with medical jargon both understand these acronyms. So, it is difficult to identify a person from clinical data and only 30–40% of data may be used to do so. The scrub system employs several methods when a piece of text contains an address, phone number, or

name. In the scrub system, these algorithms compete with one another. The scrub system makes use of local knowledge sources to determine outcomes by comparing their values to one another. More than 97% of the time, the scrub mechanism is successful in eliminating personally identifying information from the data.

The Datafly solutions are renowned for protecting user privacy while transferring electronic health data. Multidimensional formats are stored and created using datafly systems. Several data are stored in the multidimensional format, some of which are directly or indirectly utilised for identification. SSN is used to identify information directly, whereas age, zip code, and sex are used to identify information indirectly.The Datafly approach implies that eliminating direct identifying variables does more than just ensure that each individual's data is kept private. For the purpose of protecting the confidentiality of medical data, Datafly stem employs anonymity techniques like k-anonymity and l-diversity. A connected assault may be avoided using the k-Anonymity approach. For outlier values, the k-anonymity suppression approach is used to avoid identification. Users may customise the amount of anonymity in the Datafly system based on recipient inquiries. Anonymity levels typically range from 0 to 1, with 1 designating the highest degree of generalization and 0 indicating that the Datafly system only gives original data.

Due to the nature of monitoring, there are several applications for home security. The key issue is to install the domestic security system for preventing privacy of the person. This group includes issues with credential identification, verification, and identity theft. This system should be able to verify the identity of the individual using the credentials they provided at their house. For instance, the theft of SSN presents a significant risk. The SSN is semantically linked to other qualities in order to verify the identity of the individual and demonstrate that these records really belong to them. In order to prevent identity theft, innovative technology is deployed. Advanced intelligent identity angels are employed to scour the internet and find people who are alarmingly at danger of losing their identity.

Web cameras are a popular technology used nowadays for public monitoring. Unusual actions may be quickly and readily investigated and discovered with the use of webcams. Webcam surveillance analyses photos to determine a person's characteristics. It is an intrusive surveillance technique. By counting faces in photos and comparing the results, the webcam approach may retain sensitive information that can be utilized to spot anomalous activity. It assumes that unique actions are seen to be discovered based on the number of face features rather than a particular characteristic of a person. The majority of webcam monitoring is utilised in a certain industry. Sensitive information's privacy is lessened by this tactic.

The government needs a way to keep tabs on the actions of the terrorists and suspected activists on its list. The watch list methodology offers a method to efficiently monitor this issue. The watch list method is used to handle financial transitions in several contexts, including hospital stays, hotel stays, airline travel, and retail sales. Since transactional data are private, privacy concerns are subjective, and they even do not appear in the record list, monitoring them is a very time-consuming task. As a result, it is necessary to take strict action to protect these transactional data in order to maintain the privacy of sensitive information. Hence, watch lists may be used to identify suspected activists' transactional activity.

DNA sequencing and forensic analysis have transformed over the last three decades as biotechnology and data sciences have advanced. The number of medical record databases has increased quickly, making it challenging to adequately maintain medical data privacy. Genetic information is particularly sensitive since it uniquely identifies a person. Just deleting a unique property won't stop someone from being re-identified when data is kept in

multidimensional and dispersed systems. A common piece of software like Clean Gene has the ability to recognise a person on their own. Other demographic characteristics are not always necessary for DNA identification. On the basis of information already in the system, the clean gene determines the specific ailment that the individual has. The programme uses publicly accessible medical information and expertise about specific disorders to identify DNA entries. According to reports, this method makes it simple to identify 98% of people.

The genome technique builds a genetic profile of the person using DNA sequencing together with other characteristics like sex, age, and illness. This strategy works well when groups are small. On a genetic profile, the k-anonymity approach may be used to secure personal identity. To avoid re-identification, anonymity techniques like generalisation and suppression are quite successful. Individual data cannot be identified in (k 1) entities thanks to k-anonymity. The second strategy utilised in genome is to create fake data and introduce noise to real data. When a patient is admitted to the hospital, their information is recorded on a local or distant server, and this genetic data may be utilised in the near future for a variety of tasks, including government initiatives, insurance firms, and research. The data patterns are encoded in the portal and published in the distributed system, regardless of the patient's or doctor's actions. To reidentify a person's individuality, genetic profile data may be merged with patient released data that is in the public domain.

The global positioning system (GPS) is a modern, widely utilised technology that may be used to determine a device's precise location. LBS searches a device or a person carrying a device using location and temporal data. A person's location information may be disclosed, which is against the law and against privacy norms. Using query control and audit control approaches for protecting people's privacy, PPDM techniques like anonymity and data perturbation may be used to secure location privacy [12], [13].The popularity of EHR has dramatically risen during the last 20 years, necessitating additional security safeguards for patient data. To do this, technology should integrate privacy-preserving data mining methods with machine learning, deep learning, and artificial intelligence in its electronic health records (EHRs). The integration of the PPDM with a current application is another option for adoption, since this will enable the existing system to be secured and its stakeholder data to be preserved. Implementing personalised privacy is difficult.

It highlights the right of ownership and control over the data on one side. The many regulations and regulatory guidelines demonstrate that consumers have control over the details of their data. The full use of data for successful outcomes may be impacted, and there may be a trade-off between privacy protection and usefulness. The user being aware of the privacy dangers associated with data exposure is so damaging. Contrarily, if a user is not directly or indirectly engaged in a privacy-preserving process, sensitive data may be compromised and utilised against patients' will by a third party. Personal data control might thus lead to trade-offs between privacy and usefulness. For future study, a suitable context-based data tailored control access from the patient's side is needed. For privacy-preserving data mining, homogeneous encryption and a variety of transmission protocols are utilised, although many of them compromise usefulness and efficiency. To expand the use of technology for security and privacy preservation, more effective and efficient protocol may be developed. Nowadays, data gathering, processing, and action control are all done via the usage of ubiquitous computing.

CONCLUSION

The discipline of privacy-preserving data mining in the area of EHRs has developed adequate ways to meet privacy-preserving jobs in recent years. The adoption of EHRs is mostly tied to the future course. Every industry adheres to the principle of privacy protection, and the

electronic health record is no exception. In practical applications like EHRs, WBSN (Wireless Body Area Network), WSN (Wireless Sensor Networks), Smart Grid Security, Forensic investigation, Biomedical Information and technology, Smart Metering system, and many others, PPDM approaches have not yet been extensively implemented. Priority grounds call for the implementation of privacy protection in several domains.Several domains, such as WSN, WBAN, and Smart Grid, call for a wider range of data privacy and security. In certain contexts, context-based privacy may be achieved and used. As the statuses of its agents change, context-based privacy reacts by applying new or modifiable regulations as necessary. Making regulations for every ubiquity, however, is quite challenging.

REFERENCES

[1] R. Y. C. Ong and S. Sabapathy, "Enhancing patient privacy protection under Hong Kong's Electronic Health Record Sharing System," *Common Law World Rev.*, 2020, doi: 10.1177/1473779520914290.

[2] E. A. P. Rincón and L. G. Moreno-Sandoval, "Design of an architecture contributing to the protection and privacy of the data associated with the electronic health record," *Inf.*, 2021, doi: 10.3390/info12080313.

[3] L. C. Huang, H. C. Chu, C. Y. Lien, C. H. Hsiao, and T. Kao, "Privacy preservation and information security protection for patients' portable electronic health records," *Comput. Biol. Med.*, 2009, doi: 10.1016/j.compbiomed.2009.06.004.

[4] P. Lu and W. Zhao, "Research on the privacy protection of electronic health records," 2020. doi: 10.1117/12.2584813.

[5] S. M. Shah and R. A. Khan, "Secondary use of electronic health record: Opportunities and challenges," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3011099.

[6] W. H. Tsai *et al.*, "A technology acceptance model for deploying masks to combat the COVID-19 Pandemic in Taiwan (My Health Bank): Web-based cross-sectional survey study," *Journal of Medical Internet Research*. 2021. doi: 10.2196/27069.

[7] G. Bincoletto, "A Data Protection by Design Model for Privacy Management in Electronic Health Records," 2019. doi: 10.1007/978-3-030-21752-5_11.

[8] W. Xu, L. Wu, and Y. Yan, "Privacy-Preserving Scheme of Electronic Health Records Based on Blockchain and Homomorphic Encryption," *Jisuanji Yanjiu yu Fazhan/Computer Res. Dev.*, 2018, doi: 10.7544/issn1000-1239.2018.20180438.

[9] W. Moore and S. Frye, "Review of HIPAA, Part 1: History, protected health information, and privacy and security rules," *J. Nucl. Med. Technol.*, 2019, doi: 10.2967/JNMT.119.227819.

[10] J. Zhang, H. Liu, and L. Ni, "A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2975208.

[11] C. L. Brown, "Health-care data protection and biometric authentication policies: Comparative culture and technology acceptance in China and in the United States," *Rev. Policy Res.*, 2012, doi: 10.1111/j.1541-1338.2011.00546.x.

[12] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2937685.

[13] D. Chunyan, "Patient privacy protection in China in the age of electronic health records," *Hong Kong Law Journal*. 2013.

CHAPTER 17

SECURECLOUDDATAMANAGEMENTFRAMEWORK

Mohan Vishal Gupta, Assistant Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India,
Mail Id: - mvgsrm@indiatimes.com

ABSTRACT:

Smart meters, smart appliances, and renewable energy efficiency resources are only a few examples of the different activities and other measures that make up a smart grid of the cloud. The main challenges facing this grid are how to effectively manage numerous front-end devices, including smart metres and power assets, as well as how to handle the massive amounts of data generated by participating devices. To enable big data analysis and information management, it is intended to build a hierarchical structure of homogeneous and heterogeneous cloud centres that offers a range of computing services. Also, in order to address the serious security concerns of the suggested architecture, we provide a security-related solution based on acknowledgement identity-based encryption, signatures, and proxy re-encryption. In order to confirm that the data has been received by the end user and has not been lost in the cloud communication environment, we also introduce acknowledgments sent by the end-user to the provider.

KEYWORDS:

CloudData, SecureManagement, SmartModel, Identity-BasedEncryption.

INTRODUCTION

Traditional power grids and smart grids are compared, and it is discovered that smart grid models provide an improvement in terms of computing service dependability, substance, and efficiency Smart grids provide electrical-related grids a number of benefits, but their inclusion and accuracy are only available in smaller areas. It is advised that smart grids be implemented in bigger capacities due to a number of concerns and obstacles. The administration of obtaining, storing, and processing information is the focus of information management. Large amounts of data that are involved in the selection, deployment, and inclusion of data, monitoring of data, and analysis of data for smart cloud models must be handled and managed simultaneously. The smart cloud models' big data comes from a variety of sources. These sources might include usage activities of the users; phase-wise data used for storage and retrievals; data on energy consumption utilised by different smart location metres, administration, maintenance, and control over the data. The measurement does not directly retrieve network-related data from operational devices like servers and virtual machines, but these data are often utilised in decision-making [1]–[3].Big data measurement in terms of electricity utilities is expanding significantlybut not a, andsss,, and Real-time processing is often needed for smart grids, and any delays might have catastrophic effects on the whole system.

Encouragement for Cloud Computing

Many benefits of cloud computing exist, including cost savings, energy efficiency, scalability, flexibility, and agility. As a result, it will likely play a big role in computing in the future. The cloud is responsible for a high energy-saving platform and for addressing the

problem of large-scale information in the form of intelligent models. This is a result of two factors: (1) high scalability to handle the volume of information being processed; and (2) effective use of resources in the relevant data centres. Faster processing, effective storage, and distributed computing capabilities for managing large data are also produced by cloud environments. To process the potential of big data, there is a need to learn new data analysis techniques and ways to handle the emergence of massive unexpected data. With the aid of under managed cloud infrastructure, a service provider may give better, cheaper, and more dependable cloud services to the customers and end-users. To verify the link between operational grid and certain cloud models in the form of smart-cloud models, certain of their relevant features are examined .AckIBE is built on the Smart Cloud Framework (also known as the Smart Model) for managing big data in both homogeneous and heterogeneous cloud data centres. Three things this chapter contributes are. An identity-based encryption-based security solution is introduced for the proposed smart-model of IBE and identity-based proxy re-encryption to provide secure communication.

The introduction of smart-model: A framework based on cloud computing to perform information management of big data in the form of smart models that gives reasonable scalability as well as security.We go on to introduce acknowledgments as AckIBE and demonstrate how messages, complete with signatures and the acknowledgments, are delivered from one level to another in a hierarchical cloud system.Gathering, analysing, and storing information are the three key responsibilities that make up smart model management in general. Several methods have been presented to deal with this difficulty of information collection since smart models amass enormous amounts of data from various types of devices situated in various areas A suggestion to standardise the data formats used in smart grids is made to address the interoperability difficulty.

Because to its extensive adoption, the smart grid has a number of security flaws several approaches to acquiring the security concerns with regard to the processing of information from smart metres were suggested by the authors of .Wei et al. made the same suggestion to defend the smart model from cyber-attacks. In order to maintain the consistency of the security requirements for all parts of a smart model, Zhang et al. presented security frameworks. Rogers et al. provide an authentication method using digital signatures and timestamps. Identity-based cryptography is seen as a strong choice for secure cloud computing, as mentioned in. For effective cloud data storage, authors of developed a variety of security designs. Identity-based signature (IB-S) techniques are discussed in a methodology introduced in for the non-hierarchical cloud environment. Although the suggested work offers security based on IB-encryption/signature and IB proxy re-encryption methods to the proposed model, the work provided in develops an agreement protocol dubbed IB-key in the setting of universal grid computing [4], [5].

DISCUSSION

Identity-based signature schemes (IB-S) and identity-based encryption (IB-E) are two separate cryptographic building blocks that may be used to secure the Smart-Model. Li et al. introduced identity-based cryptography to reduce the necessity to verify whether the certificates are genuine in the standard pub- lic key situation. In the IB-E scheme, the producer of the private key (PKG) key with a trustworthy party first creates the master key (mk) secret key and an associated parameter known as params [6], [7].Digital certificates that are generated using standard public key techniques are used to disseminate the private keys. Users are given their private keys after being authenticated by the PKG with regard to their identities. Any sender with IDrec may use the Encrypt algorithm to convert an initial plain-text PT(M) into a ciphertext C. After the acquisition of ciphertext C, the receiver decrypts C

by using the decryption algorithm and the KIDrec, the private key acquired from the party PKG, as inputs.

The following is a suggested description of an identity-based signature method [8]. After the user identification IDsig is provided by the signer, the party computes the private key as KIDsig with respect to the IDsig by running the extraction method with the secret master key mk as input. The signer signs using PT(M) and then executes the sign algorithm to get a matching signature using KIDsig. Instead of using digital certificates, the IB-E and IB-S both provide user certification. The user may only decrypt using the decryption technique or generate a legitimate signature after registering his or her identity and receiving their private key. Shamir had previously suggested the IB-S signature system in saw the actual implementation of IB-E. The expansion of identity-based cryptography known as hierarchical identity-based cryptography entails the root PKG delegating the creation of private keys and identity authentication to other users who take on the roles of lower-level PKGs.

Further IB Plans

Via the process of proxy re-encryption, a proxy may alter the ciphertext that was generated using Alice's public key in a manner that allows it to be deciphered with the help of a different party's private key. the first proxy re-encryption system that is completely operational. Several proxy re-encryption techniques with various functionality have been created since the work of Ateniese et al. An e-Stream-based secure dynamic update strategy for secure cloud storage was suggested by Ramesh et al. In order to offer security for effective dynamic data storage, the authors in this study looked at a stream cypher known as ChaCha20 In the Standard Model based on Computational Diffie-Hellman Problem, Xiaming Hu et al. presented Secure and Efficient Identity-Based Proxy Signature Method.

Secure Smart

This section serves as an illustration of the system architecture, component views, and information management flow. The term "Smart-Model" refers to a framework that employs cloud computing technologies and offers scalable, adaptable, and safe transformation of data created for smart-models. Here, we've accepted the notion of building the model at three distinct hierarchical levels: top-cloud, regional-cloud, and end-user. Cloud computing centres make up the first and second levels, and end-user intelligent gadgets make up the last level. The top-level cloud is responsible for overseeing and managing the data gathered at different regional cloud centres as well as the participating devices. On the other hand, the regional cloud computing devices manage lower hierarchical level situated front-end intelligent devices with the data sent from participating devices. These devices are at a level lower than the computing entities (centres) of regional cloud (i.e., homogeneous region). Information leakage of any sort should be avoided in smart grids as it may have disastrous repercussions since smart grids are sensitive and need tight security. We also include a security measure in this system, namely IB-Encryption, Signature, and IB Proxy Re-Encryption Schemes Identity-based encryption has an advantage over conventional public key encryption since it employs identities rather than digital certificates, which are dependent on public key infrastructure.

This reduces the need for resource use while conducting computations and fixes scalability issues. Moreover, we enable acknowledgement to be provided by receivers to the senders in order to verify that data reach the intended recipient and do not get lost in the huge cloud environment. These acknowledgements are likewise sent in an encrypted manner; upon receipt, the sender decrypts the acknowledgment and retrieves the relevant data. Fig. 4.1 depicts the architecture that is being employed.

Smart-Model

These territories are managed by a cloud computing centre. Either a public cloud service or a private cloud solution is used to set up and administer the computing centre. Every regional center's fundamental role is to manage end user devices that are located in the same area (i.e., the corresponding region) and to provide basic data processing services for the involved active devices. The primary computing facility at the highest level is in charge of managing and processing the appropriate information data for the involved grids. Moreover, the centre is in charge of implementing the following cloud computing services.

Infrastructure-as-a-Service (IaaS) (IaaS)

All installed apps and services may access resources thanks to this service's on-demand delivery model. This service is responsible for managing the fundamental management functions in the suggested paradigm, such as data collection, processing, and storage.

Software-as-a-Service (SaaS) (SaaS)

This service sets up the necessary components of a smart model at the systems top. For instance, mandatory services like GPM that help clients reduce and optimize their energy use.

Platform-as-a-Service (PaaS)

(PaaS) for the creation of cloud computing services and applications, this service provides a variety of tools and library functions. It is advantageous to have platform-as-a-service that has these built-in criteria for the deployment of the apps since there are several applications that must support multiple security offers to facilitate lawful interceptions.

Data-as-a-Service (DaaS) (DaaS)

DaaS may be used to provide pertinent data for statistical purposes. The volume of data from smart grids is often tremendous. Offering these statistics services to service consumers is advantageous.

Service to Users

This service includes every service a user of electricity utilises. Examples include keeping an eye on, managing, and maximising their usage of electricity. The majority of SaaS and PaaS, which provide libraries for user services, fall under this kind of service.

Services for Control and Management

This group includes all services related to system management, including governance, monitoring, job scheduling, and security.

Services for Electricity Distribution

This group includes services connected to power distribution. Examples include distribution-related services, quality-of-service assessment, and optimization services.

Security Solutions for Smart Model

In creating the security framework in this part, we make the following assumptions. The proxy re-encryption technique used in Fig. 4.5 to demonstrate how this architecture works.

1. A generator of private PKG exists that generates private keys for each participant in the hierarchy as soon as they register. It is believed that the PKG party has the authority and capability to maintain the Smart-Model typically at various levels with trustworthy credentials.

2. To identify the current cloud at the top level and assign end-users, distinct strings are utilised as IDs. They are either used to validate the signature or to encrypt the original communication
3. Based on their identification, each participating entity is given a private key that they may use to decrypt the ciphertext that contains their secret data.
4. To the participant at its peer level, each participating entity delivers an encrypted data. The data may then be sent to the local cloud providers by the end user. Similar to this, the regional cloud's entities have the ability to communicate encrypted data to a cloud that exists at a higher level.
5. Each participant's private key, which it receives from PKG, is used to verify shared data.
6. Each level that receives data has the ability to reply to the sender with an acknowledgement[8]–[10].

CONCLUSION

Due to the requirement for a security solution in the cloud environment, two methods identity based cryptography and identity-based proxy re- encryption have been offered. As a result, the suggested security architecture is safe, scalable, and customizable. In order to verify that the data is not lost and has been effectively sent, we also used an acknowledgement method to ensure that the sender gets response from the targeted recipient. We have also included a description of the architecture that demonstrates the interactions and transmission of sensitive data, signatures, and acknowledgments between regional cloud, top cloud, and end-user entities. On the basis of the aforementioned presumptions, we build the architecture, management services, and distribution services are all included in the top cloud's hierarchy. The regional clouds are controlled by the top cloud. These local clouds provide fundamental user services and data storage. There is a hierarchy of smart (intelligent) end-user devices underneath regional clouds.

REFERENCES

[1] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Trans. Cloud Comput.*, 2015, doi: 10.1109/TCC.2014.2359460.

[2] R. Nivedha and S. Arshiya Sulthana, "A secure cloud computing based framework for big data information management of smart grid," *Int. J. Innov. Technol. Explor. Eng.*, 2019, doi: 10.35940/ijitee.F1253.0486S419.

[3] D. Ramesh and S. K. Pasupuleti, "A novel AckIBE-based secure cloud data management framework," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2019. doi: 10.1007/978-3-030-22277-2_4.

[4] S. Indra Priyadharshini and M. Vigilson Prem, "Secure e-health cloud framework for patients' EHR storage and sharing for indian government healthcare model," *Proc. Est. Acad. Sci.*, 2020, doi: 10.3176/proc.2020.3.09.

[5] A. Al Hadwer, M. Tavana, D. Gillis, and D. Rezania, "A Systematic Review of Organizational Factors Impacting Cloud-based Technology Adoption Using Technology-Organization-Environment Framework," *Internet of Things (Netherlands)*. 2021. doi: 10.1016/j.iot.2021.100407.

[6] Z. Ghaffar, S. Ahmed, K. Mahmood, S. H. Islam, M. M. Hassan, and G. Fortino, "An improved authentication scheme for remote data access and sharing over cloud storage in cyber-physical-social-systems," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2977264.

[7] M. Mahmud *et al.*, "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications," *Cognit. Comput.*, 2018, doi: 10.1007/s12559-018-9543-3.

[8] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. Abd El-Latif, "Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities," *Secur. Commun. Networks*, 2021, doi: 10.1155/2021/5597679.

[9] K. P. Joshi and A. Banerjee, "Automating privacy compliance using policy integrated blockchain," *Cryptography*, 2019, doi: 10.3390/cryptography3010007.

[10] Y. Guo, S. Wang, and J. Huang, "A blockchain-assisted framework for secure and reliable data sharing in distributed systems," *Eurasip J. Wirel. Commun. Netw.*, 2021, doi: 10.1186/s13638-021-02041-y.

CHAPTER 18

SECURITY AND PRIVACY CONCERNS IN MOBILE SYSTEMS AND DEVICES

Priyank Singhal, Associate Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.
Email Id: - priyanksinghal1@gmail.com

ABSTRACT:

There are an increasing number of mobile devices being linked to the Internet, and interconnectedness has connected billions of gadgets in the cybersphere. In order to identify security and privacy concerns, as well as the existing methods of detecting and preventing them, the chapter concentrates on the security and privacy of mobile devices and systems.There are countermeasure security measures that have been created and implemented for mobile devices like smartphones, ranging from security in different software levels to information distribution more so to the end users. According to Rawat, these are excellent practises that need to be followed at all levels, from the creation of software layers, operating systems, and downloadable programmes to how they are intended to be utilised.The significance of the Internet in everyday life was stressed by Gupta et al., and the authors contend that as Internet use grew, encipherment became more necessary. One of the main areas of focus is the security of mobile systems. This chapter explores the security and privacy concerns in mobile systems and devices.

KEYWORDS:

BigData,Mobile Cloud, Mobile Networks,Privacy, SmartphoneDevices.

INTRODUCTION

Mobile computing has made mobile security and privacy more and more important, and there are many worries about the security of personal and professional information kept on mobile devices like smartphones. According to Au and Choo, more people are using cellphones to plan and manage their job, as well as their personal lives, in addition to communicating. These corporate technologies are having a significant impact on how information systems are organised in particular, and they are becoming a source of new, all-encompassing hazards. According to Au and Choo, mobile devices gather and assemble a significant quantity of sensitive information; thus, access to these devices has to be restricted in order to safeguard both the organization's intellectual property and the privacy of its users Au and Choo restate that cellphones have replaced PCs as the most popular targets for attacks. Such attacks frequently take advantage of flaws that are built into smartphones, according to Tully and Mohanraj, which can come from communication methods like short message service (SMS), multimedia messaging service (MMS), the global system for mobile communication (GSM), Bluetooth, and Wi-Fi [1]–[3].

There are more exploits that aim to take advantage of software flaws in operating systems or browsers. Some dangerous software relies more on the common user's limited knowledge. According to Rawat, McAfee's 2008 research shows that just 2% of users had firsthand experience with mobile malware, while 12% of users had heard of other people who had been impacted by it. Yet, during the last ten years, there has been an upward trend in these

statistics.In the digital era, Tully and Mohanraj contend that user anonymity is essential since computers may be used to deduce from data or information gathered during various day-to-day transactions the habits, lifestyle, associations, and locations of people. Therefore, even deleting explicit identifiers is unlikely to provide sufficient security. The fundamental justification comes from the possibility that an individual's identify may be revealed if the leaked information is combined with information that is already accessible to the public. Location privacy is another major issue in the context of mobile devices, according to Huang and Zhou.

Ther key areas include the detection and prevention of instructions, security problems with local area networks (LANs), wireless networks, botnets, and the Internet, as well as emerging technologies like optical network security and the use of optics in cryptography. The authors concentrated on public key infrastructure (PKI) and data encryption in addition to password-based authentication mechanisms[4].Gupta and Wang examined and addressed computer and cyber security concepts, including algorithms and various perspectives, in one of their most recent works. The author advocates advance security and highlights the prevalence of machines as one of the issues of computer and cyber security given the pace of advancement and complexity of assaults. In other words, the majority of current assaults take advantage of the fact that mobile systems and other devices generally work in a similar manner. It is possible to attack a single host in the same way using millions of different devices. The authors responded by recommending diversity and the usage of network automation as a method of fending off some of the threats. Virtualization and sandboxing have surfaced as additional suggested methods for fending against ubiquity assaults. Together with these methods, the author also covered the concepts of computing resource segregation and how it contributes to system resilience against attacks.

It is important to emphasise that discussions often centre on computers and cyber security, rather than mobile platforms. With new technologies like the Internet of Things (IoT) and cloud computing, it is imperative to address and concentrate on monitoring and safeguarding such systems. For all user-centered solutions, security, privacy, and trust were examined by Akram et al. The authors explored some of the methods for spotting malware in mobile devices and thought about how the three subject areas will affect the healthcare and financial sectors. The unlimited register machine of owners (URMO) paradigm, which has the ability to analyse and define the actions of mobile devices, is discussed in this study. The authors also covered additional technologies, such as secure portable tokens (SPTs), along with a mutual authentication protocol that preserves anonymity and can be integrated into mobile operating systems. This architecture should guard against several known threats.

With the expansion, uptake, and acceptability of the Internet of things, the number of attack surfaces and access points is rapidly rising. There are an increasing number of things that are related. According to Sicari et al., the Internet of Things (IoT) must satisfy both security and privacy criteria since it depends on heterogeneous technology and heterogeneous creative services for different application sectors. More cutting-edge security solutions are still needed to meet the demands of mobile system applications and use. Based on the features of IoT systems, Sha et al.'s analysis of security and privacy difficulties found several issues. On the basis of the problems found, the research also put three distinct architectural security concepts into practise.

In spite of the efforts and claims of developing unique security methods for addressing security and privacy in IoT systems, little progress has been made in mobile systems. In spite of the contact between the devices, various suppliers really utilise distinct technologies, and the majority of them lack operational synergy. As a result, implementing and enforcing

separate security and privacy features could not be successful, particularly in the context of IoT. In light of this, the goal of this work was to undertake an organised assessment of the literature with a focus on research that deal with security and privacy in mobile systems. The recommended reporting items for systematic reviews and meta-analyses (PRISMA) checklist was employed in the study's search strategy and analysis of the search results. This article's main contribution is a thorough list of technologies and information security and privacy vulnerabilities that other researchers have highlighted.

DISCUSSION

A systematic literature review (SLR) is a methodology that includes means of locating, evaluating, and interpreting accessible material, particularly that which is connected to the study question, phenomena, and area of interest. While the systematic review in this context is a kind of secondary research, studies that precede or contribute to it are often referred to as primary sources. The following picture provides a summary of the research methodology that will be used in this chapter.The field of literature study has been selected, and the proposal also specifies the following search criteria. When the proposal is approved, the next steps will take place, including document screening and the creation of a report on the review's conclusions. It is crucial to remember that the research method places a strong emphasis on systematic literature reviews and the use of the PRISMA checklist to decide which articles to include and which to leave out [5]–[7].Systematic literature review may also be referred to as a secondary kind of study that aims to find, analyse, and assess investigations which are pertinent to the research issue. Nie and Ma emphasise the SLR's attributes. The first need is that the study must have a clear review methodology from the outset. This protocol outlines the specification of the research topic for the questions that will be addressed as well as the research methodologies that will be used For this chapter, the PRISMA technique was utilised to examine the publications acquired from the database.

Second, SLR suggests developing a research plan that is well documented. Ferrari reaffirms the need for a solid approach in order to gather the greatest number of primary studies possible with reference to the literature review that is relevant to the subject being studied. The qualifying primary sources of information or articles returned from the search should also meet other exclusion and inclusion criteria, according to the author. Throughout the SLR, the steps of planning, conducting, and reporting findings are all followed. The goal of the planning phase is determining the genuine need, which serves as the primary driving force for the implementation of the SLR. Nie and Ma underline that the preparation of the protocol that directs the SLR to minimise biases that the study may commit, in addition to identifying the target, constitutes the primary actions. The execution of a search strategy, including the chosen in accordance with the stated protocol in the planning phase, is required for the identification of the study during the conducting phase To address the study topics, data are taken from the chosen works and combined. In the end, this aids in simplifying analysis and synthesising, especially for the production of outcomes. Regarding the reporting results phase, SLR documentation is connected to it In addition to preparing the research questions' responses and disseminating the findings to people who are interested, here is where the results description is carried out. In order to assist SLR performance, the state of the art through systematic review (StArt) is used, which aids in the planning and execution stages of the SLR. Identifying and exposing concerns about security and privacy in mobile systems is the goal of the SLR.

The number of articles that were retrieved, dropped, and kept varied depending on the step, as indicated in the figure, and the analysis that followed depended on the inclusion of articles that weren't necessarily appropriate for the research at the identification stage. Nevertheless,

duplicates were eliminated at the screening stage, and titles were examined to make sure they were relevant and appropriate for the area of interest. Together with the PRISMA checklist, only full-text publications that comprised both qualitative and quantitative research were eligible for the review. Nevertheless, since various algorithms, numerical methods, and cutting-edge methodologies were provided in several papers, meta-analysis of the quantitative articles was not feasible. Meta-analysis is more appropriate and relevant when it is feasible to determine the study's features. Moreover, the capacity to recognise bias risk both within and across experts demands methodological consistency and uniformity in the reporting of data.

Literature on security and privacy focuses on certain areas of security, such as security policies, needs, authorization, and inter-organizational situations. There are several security measures in place for mobile systems, including authorization, security concepts, verification, access control, and software handling failure. Depending on the underlying system, these aspects are considered at various degrees and layers of security and privacy enforcement. Rules and core concepts differ across mobile platforms, however it's important to take into account how the main application and the mobile vendor will affect the future enforcement policy. The discrepancies between the iOS and Android operating systems are an excellent illustration of how security and privacy rules may range from one manufacturer to the next. It is sufficient to note that iOS does not allow for user development or debugging, but Android does, and that as a result, the security measures between the two operating systems are radically different In order to enforce security and privacy, different operating systems and policies must be recognised and identified. For instance, it is clear that the Android operating system and its developer feature provide several security concerns since it is easy to execute a stealth attack and install malicious code if one has access to the target device and a portable memory. With iOS-based systems, the same is not achievable, making it difficult for criminals to plan and carry out social engineering assaults on such platforms.

The majority of publications also take into account concerns with online authentication security for mobile systems, sophisticated assaults on mobile system platforms and countermeasures, and secure mobile services and apps Yet, it is essential for such approaches to discriminate between various mobile system security concerns, identify those dangers, and then propose monitoring and protection techniques.The results show that these systems are not entirely made safer and more private by the new security procedures that were originally established on mobile platforms, such as the Android permission framework. Instead, they are more likely to create exploitable security flaws. The deployment of extra security frameworks is only one of the many strategies that may be used to minimise such vulnerabilities. On the other hand, completing security analysis of two-factor authentication of mobile systems and investigating the ways more so for password-based authentication that is safe on the mobile systems are all part of the online authentication security for these systems. The new methods demand an extra authentication stage or step in addition to the standard password or login authentication credentials as a technique to verify an online login attempt or banking transaction based on a one-time password (OTP). The OTP is often created and delivered to the user or transmitted straight to the user's mobile device. Open research issues and gaps are recognized from these findings, and they are also examined in relation to potential answers.

The majority of the solutions concentrate on limiting alerts and notifications that might otherwise exploit flaws in mobile devices. As a result, it is wise to examine logs and consider all the potential points of access A holistic strategy to monitoring and preventing assaults on the domains is one of the advised methods for addressing some of these difficulties. For the purpose of recognising and avoiding actions that might otherwise be harmful, researchers

advise using suggestion for warnings in conjunction with correlation rules Since it is difficult to distinguish harmful information from a huge number of false positive information, the other suggestions concentrate on minimising false-positive information streams. For instance, a warning that helps to prevent login failure is a rule that alerts the user after two login attempts fail. Such regulations may also limit the number of password resets and login attempts made each day or each week, and it is advisable to keep track of all the Internet protocol (IP) addresses of the desktop computers and mobile devices making such login attempts for accountability reasons Also, it is common practise to include and enforce thresholds for actions that constitute threats. For simplicity of viewing and query results for tracking incoming and outgoing data transmission and communication, such information is often pooled into a single atomic variable. It is also advised that the pace of infrastructure expansion and the rates of market penetration be taken into account. It is true that certain areas face more serious cyberthreats than others. Mobile service providers would be wise to take the necessary safety measures and to be aware of this fact. For matters relating to privacy and security in mobile systems, a thorough literature study will be conducted. As a consequence, main studies had to be found using a mix of human and machine search methods, and their study objectives had to be examined. The data gathered from these research questions served as both motivation for further study and a guide for identifying research gaps. Some of the topics that will need further focus include the bias among journals or publications, the quality of the papers, and the dissemination of the articles. Nonetheless, numerous papers that address various issues of privacy and security in mobile systems were discovered based on the first evaluations of the articles acquired from the ProQuest Central database. Journal papers that placed a focus on mobile networks, systems, and cloud computing within the framework of security, privacy, and digital forensics were among them.

The findings from an analysis of research journals from 2014 to 2018 concentrated on privacy and security in mHealth due to the rise in technological automation of health services, cloud computing, databases, and big data on the cloud, security of smartphone devices, aspects of mobile applications and platforms with regard to privacy and security, and privacy and security in smartphone devices. The papers published in 2017 and after concentrated on contemporary and upcoming privacy and security challenges of mobile systems, as well as specific privacy, security, and digital forensics concerns relating to mobile networks, systems, and cloud. The majority of these publications are from journals, research papers, surveys, and textbooks, all of which are concerned with user security and privacy in relation to mobile devices, networks, and cloud. to concentrate on developing hardware and software that makes mobile systems secure and private in the future. It is essential to source and seek reliable security and privacy technologies as big data continues to increase and as many industrial applications acknowledge the significance and function of mobile systems in IoT and Industrial 4.0 in general. Mobile or e-health is a real-world use for mobile technology. One area where the use of mobile or IoT technology might be advantageous is the management and administration of pharmaceuticals. For instance, an electronic reminder system for the elderly may be useful, but it also contains personal information that might be sold to commit identity theft or be illegally used to file insurance claims. As a result, it is wise to be aware of the many regions of grey that exist in mobile device security and privacy [8]–[10].

CONCLUSION

This chapter's goal was to examine publications on mobile system security and privacy. The search's results included papers that discussed security and privacy in vehicular systems, indicating that the phrase "mobile systems" was vague. Since the search results are reasonable, the word "mobile" should be understood to include cellphones and moving smart

cars. The conversation that followed and the conclusion, based on the search results, however, were more concerned with the security and privacy of cellphones than with vehicle network systems. The use and implementation of preventative, investigative, and response strategies for maintaining security and privacy in mobile systems is crucial and should be taken into account in the future. Without a suitable central authority, it will be difficult to police security and privacy rules given the rapid growth of mobile technologies, particularly smartphone devices. Finally, it is critical to note that the majority of research articles are compelled to address IoT privacy, security, and policy issues. As a result, it is essential to concentrate on mobile systems because the number of devices going online is constantly growing, security is of the utmost importance, and vendors are required to follow suit. Both mobile suppliers and service providers must be involved for the ideal situation to exist.

REFERENCES:

[1] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2917555.

[2] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G In the internet of things era: An overview on security and privacy challenges," *Comput. Networks*, 2020, doi: 10.1016/j.comnet.2020.107345.

[3] A. Fukami, R. Stoykova, and Z. Geradts, "A new model for forensic data extraction from encrypted mobile devices," *Forensic Sci. Int. Digit. Investig.*, 2021, doi: 10.1016/j.fsidi.2021.301169.

[4] Z. Zhu, R. Jiang, Y. Jia, J. Xu, and A. Li, "Cyber security knowledge graph based cyber attack attribution framework for space-ground integration information network," in *International Conference on Communication Technology Proceedings, ICCT*, 2019. doi: 10.1109/ICCT.2018.8600108.

[5] T. Fatokun, A. Nag, and S. Sharma, "Towards a blockchain assisted patient owned system for electronic health records," *Electron.*, 2021, doi: 10.3390/electronics10050580.

[6] S. Zhang, Y. Wang, and W. Zhou, "Towards Secure 5G Networks□: A Survey," *Comput. Networks*, p. 106871, 2019, doi: 10.1016/j.comnet.2019.106871.

[7] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," *IEEE Commun. Stand. Mag.*, 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[8] X. Liu, W. Ma, and H. Cao, "MBPA: A medibchain-based privacy-preserving mutual authentication in TMIS for mobile medical cloud architecture," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2947313.

[9] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Mobile App Recommendations with Security and Privacy Awareness Categories and Subject Descriptors," *Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, 2014.

[10] N. Tariq *et al.*, "The security of big data in fog-enabled iot applications including blockchain: A survey," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19081788.

CHAPTER 19

NETWORKING USING SOFTWARE-DEFINED NETWORKS

Shambhu Bharadwaj, Associate Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.
Email Id: - shambhu.bharadwaj@gmail.com

ABSTRACT:

It is necessary to reinvent conventional networks to keep up with the network traffic flow's fast change. Devices, applications, storage, and computing have all seen significant innovation, but the network has not. A new approach to network administration and operation is called "software-defined networking" (SDN). The fundamental idea of separating the control plane from the data plane has created several opportunities for network revolution. The key component of the SDN is a central controller. Via the northbound application programming interface, information is sent to applications like firewalls, load balancers, and business logic, whereas the southbound application programming interface provides information to data pathways or data components like network switches and routers.

KEYWORDS:

SoftwareDefinedNetworking, Controller, ControlPlane, DataPlane, Firewall, LoadBalancer.

INTRODUCTION

Programmable networks are the sole options for implementing the evolutionary networking principles for today's complex networks, which are expanding quickly. The requirements of today's network are constantly changing. SDN achieves network programmability with the help of a separation between network hardware (data plane) and intelligence of the network (control plane). This separation allows for the easy creation of new applications and also makes it easier to operate and manage all of the protocols used in the network. Since the intelligence of the network (control plane) communicates via the OpenFlow protocol, it is also frequently referred to as the OpenFlow controller. All of the network components used in networking are now dumb; they no longer include intelligence and are just utilised for straightforward packet forwarding under the supervision of southbound interfaces like ForCES and OpenFlow for controller and network device communication. SDN is receiving a great deal of interest from both the business sector and the scientific community. While SDN is a relatively new concept in the realm of networking and is an emerging technology, its development rate is still extremely rapid [1]–[3].

There are still a lot of issues in the SDN industry that need to be resolved. SDN was used to turn existing innovations into new ones, making the forwarding plane programmable. It is now possible to deploy new innovations more quickly and easily, as well as new applications, thanks to the division of labour between the network hardware and software components of network devices. This also simplifies the administration of all the protocols required to operate the network.

SDN, or software-defined networking, is a future architecture. The architecture of SDN is highly strong, controllable, less expensive to operate and maintain, and adaptive, making it ideal for the present situation of networks that are changing dynamically every day. The SDN allows for programming in the network's control plane (software). With SDN, the network's utilised infrastructure is also abstracted. The OpenFlow protocol serves as the foundation for all SDN systems.Alternative networking technologies' limitations: Online shopping, content distribution IP telephony, and IP television are just a few of the unique services that the Internet has made available as it has developed. These services need various sorts of criteria for such networks. As a result, the current network is under stress. It is also highly challenging to adapt to new applications and technology.

Typically, a variety of network equipment including switches, routers, Network Address Translation (NAT), etc. are needed to make the network operate. These intermediate boxes, also known as special device traffic, are used to manipulate traffic for reasons other than straightforward packet forwarding. These devices may have a variety of intricate protocols.It becomes a difficult task for network administrators to configure each of these devices using the interfaces offered by the various suppliers. These configuration interfaces vary from vendor to vendor. These configuration interfaces may vary, even within a same manufacturer. While there are many centralised networking management solutions, the majority of these devices operate at the individual level rather than on specific centralised networking management tools. This slows innovation and makes managing and running these networks more difficult. As a result, the capital cost of running these networks also rises. The fundamental issue with conventional networks is vendor specificity and software that is packaged with the proprietary hardware and their interfaces. Suppliers create highly large and complicated source codes, which causes delays when adding new features and functionalities to these networks. Such networks are also quite costly to implement. In conventional networks, the control plane and forwarding plane were closely connected. There was a close link in conventional switches between the control plane and the forwarding plane. As a result, it was difficult to introduce new innovations and functionalities in old networks due to the close linkage between the network hardware (data plane) and intelligence (control plane). It was very difficult to configure older types of network equipment since there was no single, centralised control interface. The typical network design. These days, computer networks are very sophisticated. Even more challenging is the management of such networks. Such computer networks are built using a variety of network equipment [4]–[6].

Switches, routers, firewalls, network address translation (NAT), intrusion detection, intrusion prevention, and load balancers are some examples of these network devices. All of these network devices are operated by a complicated piece of control code, which is also often proprietary and vendor-specific. The control code, whose standardisation took years, is what makes the network protocols possible. Network administrators use interfaces offered by the many respective suppliers to configure each of these network devices independently. These configuration interfaces vary across vendors. These configuration interfaces may sometimes vary, even from the same manufacturer. While there are several centralised networking management solutions, the majority of these devices operate at the individual level rather than using a specific centralised networking management tool. Conventional network technology is a bottleneck, particularly for administrators of data centres. The task of cloud managers is very time-consuming and tiresome due to the changing nature of the requirements of many cloud users. Due to the slowdown in innovation, administration of such networks and their operation are

becoming more difficult, and the capital costs associated with managing such networks are also rising.

A New Architecture is Required: Innovation is required for conventional networks. Devices, applications, storage, and computing have all seen significant advancement, but the network has not been updated. Conventional networks are made up just of intelligence and data paths, however if the network expands quickly and more devices are added, it is necessary to update the network's organisational structure. There is a need for a network that can accommodate changing needs and is simple to maintain.SDN is a subject that needs much more study. In fact, the "software-defined networking" development that is currently being driven by commercial and, shall we say, "open-source" development heavily relies on manually configuring orchestration procedures through a number of interconnected platforms to instantiate and run services and overlay technologies that run over existing lower-level networking technology.

SDN, in its purest form, precedes what we presently see in the market, where it operates autonomously and continuously learns about its topology, resources, and surroundings. Instead of the network making its own "learned" judgements, the present SDN requires that this behaviour be preloaded within the network.Southbound and northbound interfaces are two distinct application programming interfaces (API) that make up the SDN architecture. The most well-liked southbound API for establishing a safe connection between the data plane and control plane is OpenFlow.Developing OpenFlow Protocol The packet forwarding plane and the control plane are closely connected into the same hardware in conventional devices. Nevertheless, the data plane and the control plane are kept separate in an OpenFlow switch. The OpenFlow switch's data plane component is located there, while the control plane has been transferred to a centralised location known as the SDN controller. The controller and switch communicate via the OpenFlow protocol. The OpenFlow protocol specifies a variety of messages, including transmit, send packet-out, retrieve stats, and edit forwarding table. The graphic depicts the flow that is maintained by each OpenFlow switch.

Many flow rules are included in each flow table. The matching fields, actions, and statistics that make up each flow rule determine how the flow's packets will be handled. Packets are compared to flow table rules when they arrive at the switch. If a match is discovered, the relevant switch flow table operation is carried out. If the packet's match is not discovered, the developers specify the appropriate action in the flow table and carry it out. Dropping that specific packet or delivering the network packet over a secure communication channel to the SDN controller are two possible outcomes.

Structure of OpenFlow Messages The OpenFlow requirements require that applications modify the flow table of OpenFlow switches. A pure OpenFlow switch or mixed switch, an SDN controller, and a secure connection for communication between the controller and the OpenFlow switch make up the three core components of the OpenFlow paradigm. Switches keep a flow table to deal with specific packets. A flow table rule may be found in each flow table of an OpenFlow switch. The matching fields, actions, and statistics that make up each of these flow rules determine how certain packets will be handled.The crucial component of the SDN is the controller. Through the southbound application programming interface, all information is provided to data paths or data elements like network switches and routers, and through the northbound application programming interface, information is provided to applications like firewalls, load balancers, and business logic. The SDN controller is positioned between the network components and the SDN applications in the centre of the architecture. The SDN controller will be the hub of all communication between SDN applications and network

devices. The SDN controller uses the most popular protocol, known as the Open-Flow protocol, to configure the different network devices, and as a result, for the flow of network traffic, adopts the best network route.

Scalability of controllers A centralised controller makes it considerably simpler to create new apps and change the behaviour of current ones. But, when the size of the network grows, more requests and events are sent to the controller, and at a certain point, the single SDN controller is unable to manage all of the demands. A small network may be able to use the NOX controller, a centralised controller, but a big network, such as a data centre, may not be able to. By physically dispersing the controller parts while keeping an overall view of the network, we may resolve this issue Kandoo and Hyper Flow are two examples of distributed control planes.

Response and Initiative Secondly, the reactive method specifies that the OpenFlow switch runs a searching operation whenever a new network traffic packet reaches the switch and looks for any fields that match the corresponding packet. The switch instantly passes that specific packet to the SDN controller if there is no flow match. The controller inserts a rule into the flow table. It utilises the flow table more effectively, but setting up each flow takes more time. The drawback is that the switch's usefulness is constrained if the controller-to-switch link is broken. This packet-in event is prevented by the proactive method, in which SDN controllers pre-populate network traffic rules that are introduced to an OpenFlow switch's flow table. No additional time is needed to set up a flow, and the switches are unaffected if the connection is lost.

The SDN Controller's operation

The most popular protocol, known as OpenFlow protocol, is used by the SDN controller to manipulate the network flow tables kept by the network switches. The SDN controller is linked to each OpenFlow switch through the secure connection. The controller manages the various switches, sends packets to the switches, and receives packets from the switches via this secure channel. These OpenFlow switches provide packet forwarding, and the packets are forwarded in accordance with the flow rules.

Several tools are required to do the SDN experiment. We have a variety of tools at our disposal, including emulators and simulators. A technology called Mininet is used to build and test huge networks on a single platform while working with constrained resources. Mininet is a collection of several apps that also incorporates a number of the benefits of test environments, emulators, and simulators. We may conduct an experiment using large-scale networks with hundreds of hosts and switches with the aid of this network emulator. It is more affordable and accessible, and the configuration can be altered quicklyespecially when the performance is measured against several test beds. In contrast to EstiNet, a simulator, it connects to real-world networks quickly and easily. It can faithfully replicate hundreds of OpenFlow switches, and ns-3 can replicate customizable OpenFlow switches that allow MPLS extension [7]–[9].

A comparison between software-defined applications vs conventional application: A firewall, also known as a (public network/private network/protected network) security system, is used to prevent unauthorised access from any intruder to or from the network. Both software and hardware firewalls may be used as a firewall. All data packets travelling to or from the network must first pass through this program, which monitors and examines each packet individually before dropping those that do not comply with the firewall's flow rules. Firewalls control whether a certain sort of information is accepted or rejected. This data might be found in a device, a service, or an application. A firewall's operation is seen,

A conventional firewall is positioned in between a private network and a public network. Firewalls are used to inspect all incoming and outgoing packets in order to stop assaults and illegal access. According to the conventional security paradigm, network internal users are regarded as trusted users. The firewall does not check and inspect internal traffic from internal users. A firewall does not examine these information packets. This assumption that internal users should be trusted is unfounded since insiders are also capable of carrying out attacks and stealing important data. Traditional firewalls are positioned between public and private networks. The typical firewall makes use of the provided network gear, which is highly costly and difficult to set up. Network administrators cannot add alternative features or apps to these sorts of classical firewalls because of their vendor-locked uniqueness.

In order to provide a security mechanism, firewalls use two different methods. With the first method, all traffic will be blocked unless it complies with firewall rules that have been applied. The second strategy uses a firewall that permits any traffic as long as it complies with specific restrictions. Depending on the network layer it operates at, a firewall either filters or permits all traffic. The TCP/IP network model's various levels may be supported by a firewall. The fundamental activities that firewalls utilise are listed infirewalls use these operations to protect the network from illegal access.

An SDN firewall application may be simply converted into a simple OpenFlow device to create a multiple-layer powerful firewall, overcoming the drawbacks of previously created firewalls, such as their vendor lock-in and need of specific hardware. The need for separate network gear is removed, and firewall configuration flexibility is an additional benefit. Converting an OpenFlow device into an intelligent firewall has become simple with the aid of programming. The SDN-based firewall's code is readily reconfigurable. A custom topology serves as a traffic restrictor in accordance with the flow rules, which are stored within the flow table.

When online applications grew quickly in the late 1990s, load balancing was used to distribute network traffic across identical web servers, reducing user wait times and boosting server performance. Enterprise administrators at the time used strategies like DNS-based and adaptive TTL-based methods. Commercial load balancers are often used nowadays, notably in the Arizona State University production network (ASU). Yet, there are certain situations that the load balancing capabilities of commercial systems do not work well for. Rsyslog is one such programme. Syslog packet processing and file writing are handled by this programme. Firewalls in Palo Alto provide it with input. To inform the network administrator of a problem that has already occurred or a danger to the whole campus network, this firewall creates a broad range of log messages. The volume and quantity of data that this application creates are enormous, as is to be expected. The load is distributed across numerous Rsyslog servers using the load balancing method currently in use at ASU. The issue is that the current load balancer utilises the source IP address to distribute the load, therefore it does not distribute it evenly across the servers. Moreover, since there are several Palo Alto firewalls, each of which is linked to a Rsyslog server, it is unable to transmit the load to a single Rsyslog server at a time.

SDN Is Required for Conventional Load Balancing

SDN has the ability to make network administration easier while fostering innovation and network development. The idea behind it is to separate the control and data planes. The information interchange between the two planes is described in the OpenFlow standard. An OpenFlow switch in this design has a flow table with flow entries. Fields

on which incoming packets are matched and actions to be taken upon a match make up a flow entry. If there is no match, the packet is given to a controller who determines whether to insert, remove, or amend flow entries in the flow table for future packets matching the same fields. If there is a match, the packet is forwarded to the controller, who executes a programme to handle it. Moreover, statistics are gathered on packets; the controller may utilise this data to guide decision-making. This enables us to create cutting-edge apps that meet our demands and update them as conditions change. Load balancing is one of such applications.

One possible use for OpenFlow is load balancing in business networks. The space of all possible IP addresses is represented by a binary tree, as Wang et al. describe. The ith most important bits of the IP address are located at level it of the binary tree. A prefix match on the route from the root to a particular subtree corresponds to the nodes in that subtree. A tree representation works well if each IP address contributes an equivalent amount of burden to the network because at each level, the load is split evenly between the two subtrees. This approach enables fine-grained load distribution.

Obstacles to SDN

Dynamic Period of Time Modification Issues Given that today's relatively static systems take human setups into account, the ability to modify the provisioning of contemporary converged infrastructures in minutes and have a similar effect on many devices might be a game changer. With SDN, new computing, networking, and storage tools and possibilities are immediately usable. These dynamic variations in the length of time entail significant visibility gaps compared to when you were just doing daily checks on what was new in your environment. A performance observation response with an open arthropod genus might be necessary. To ensure performance visibility, you may link directly with SDN systems in this manner, monitor the event bus for new devices, services, or modifications, and immediately amend the infrastructure observation inventory.

Providing for Rapid On-Demand Growth Platforms that monitor platforms are at danger because to the inevitable rise in demand for additional cypher, network, and storage in software-defined infrastructure. These solutions have to be prepared to include observing functionality in order to handle the infrastructure's growth. If they can't swiftly expand their capacity in response to demand, performance visibility gaps will result. In contrast to legacy architecture in the realm of SDN, we will have a number of excessively complex topologies operating on top of the actual network. As a replacement service launches, it sets up the necessary virtual infrastructure, which causes the number of monitored components to increase significantly over timeexceeding the capacity of earlier capability management. The solution is to periodically install performance monitoring of each real and virtual appliance. When more performance management capabilities are needed, performance may be improved by spinning up additional virtual appliances as needed.

Contextually Integrating Service Nowadays, having service context is expected. Performance monitoring must thus be able to hear in the context of a specific client or tenant of the network. In the end, consumers should be able to inquire not just about the status and functionality of certain hardware or network lines, but also, "How is client A's HD video service from New York to London performing?"This applies to service topology as well, which means that controllers and performance monitoring tools communicate information on the physical and logical connectivity of the physical and virtual devices that make up a service, both in real-time and in the past.SDN Application

Areas: OpenFlow switches serve as general-purpose computers up to the point at which flow entries are added to flow tables. You may turn these merchant silicon boxes into a simple hub. Flow entries are combined by an intelligent learning switch, router, and load balancer. The following are the main SDN application areas:

SDN's Role in Data Centers Virtualization is a technology that data centres are using more and more of. In addition to making server provisioning automated, it has also made it considerably simpler. But, the technologies utilised for network administration and data storage are where the challenge lies. This often results in the issue of a server bottleneck. As a result, the software-defined data centre (SDDC) will be crucial in transforming this networking infrastructure into a more secure and reliable state in order to solve all the issues. The fundamental principle behind a software-defined data centre (SDDC) is to bring each component to the same level. SDN is becoming more important in the development of SDDC.

Use of SDN in LAN and WAN Outside data centres, SDN is very important in LAN and WAN networks. With the growing use of SAAS, managing WAN has become quite challenging, but SDN is the answer and can thus resolve the issue. It tackles the crucial WAN difficulties with automated provisioning of network resources in SDN. The OpenFlow protocol and SDN have fundamentally altered LANs, allowing administration of unified wireless and wired networks, improved BYOD control, and increased security.The Function of SDN in Security SDN is used to improve network security and get access to network control. The SDN offers a number of services, including increased visibility, agility that causes an increase in unevenness when evaluating network traffic packets, network traffic monitoring, and engineering for managing network traffic.

The functioning of the SDN Controller: The network switches' network flow tables are managed by the SDN controller using the most widely used protocol, known as OpenFlow protocol. Each OpenFlow switch is connected to the SDN controller over a secure connection. Via this secure channel, the controller operates the different switches and transmits and receives packets to and from them. The packets are sent by these OpenFlow switches in accordance with the flow rules defined in their associated flow.The SDN experiment requires the use of many tools. We are equipped with a range of tools, such as emulators and simulators. Using a single platform and Mininet technology, large networks may be built and tested while operating under resource constraints. Mininet is a group of several programmes that also makes use of some of the advantages of testing grounds, emulators, and simulators. With the help of this network simulator, we could do an experiment employing massive networks with hundreds of hosts and switches. The configuration can be readily changed, it is more accessible and inexpensive, and it performs better when compared to a variety of test beds. It connects to actual networks fast and effortlessly, in contrast to EstiNet, a simulator. Many OpenFlow switches can be accurately replicated by it, including ns-3 can duplicate OpenFlow switches that may be customised and support MPLS extension.

An evaluation of software-defined vs traditional application: A firewall, sometimes referred to as a security system for a (public network/private network/protected network), is used to stop unauthorised access from outsiders to or from the network. Firewalls may be created using hardware or software. All data packets entering or leaving the network must first pass through this software, which keeps track of each packet and analyses it in detail before discarding those that don't follow the flow rules of the firewall. The acceptance or rejection of a certain kind of information is controlled by firewalls. A device, service, or application may include this data.

Traditional Firewall

Placed between a private network and a public network is a typical firewall. In order to prevent attacks and unauthorised access, firewalls analyse all incoming and outgoing packets. Network internal users are recognised as trustworthy users under the traditional security paradigm. The internal traffic from internal users is not inspected or checked by the firewall. These data packets are not examined by a firewall. As insiders are likewise capable of launching attacks and stealing crucial data, the presumption that internal users should be trusted is false. Traditionally, public and private networks are separated by firewalls. The standard firewall uses the expensive and challenging-to-install network equipment that is offered. Because to their vendor-locked uniqueness, network administrators cannot add alternative functionality or applications to these types of traditional firewalls.Firewalls use two distinct techniques to provide a security mechanism. Using the first approach, unless traffic meets with set firewall rules, it will be stopped. The second method makes use of a firewall that allows any traffic as long as it abides by certain limitations. A firewall either filters or admits all traffic based on the network layer it works at. A firewall may support all layers of the TCP/IP network paradigm. It provides a list of the basic actions that firewalls utilise to guard against unauthorised access to the network.

SDN Firewall

The shortcomings of earlier firewall designs, such as their vendor lock-in and need for particular hardware, may be overcome by simply converting an SDN firewall application into a basic OpenFlow device. There is no longer a need for extra network hardware, and flexibility in firewall design is a bonus. Programming has made it straightforward to turn an OpenFlow device into an intelligent firewall. The code of the SDN-based firewall is easily reprogrammable. According to the flow rules, which are saved in the flow table, a custom topology acts as a traffic restrictor.

Load balancing was used to divide network traffic across identical web servers in the late 1990s as online services swiftly expanded, lowering user wait times and enhancing server performance. At the time, enterprise administrators used techniques like DNS- and adaptive TTL-based solutions. Nowadays, commercial load balancers are often employed, particularly in the production network of Arizona State University (ASU). Yet, there are several circumstances when commercial systems' load balancing capabilities fall short. One such software is Rsyslog. This software handles the processing of Syslog packets and file writing. Palo Alto's firewalls provide it information. This firewall generates a wide variety of log messages to alert the network administrator of an existing issue or a threat to the whole campus network. This programme generates a tremendous amount of data, which is to be anticipated. Using the load balancing technique presently in use at ASU, the load is divided across many Rsyslog servers. The problem is that the load is not distributed fairly among the servers since the existing load balancer uses the source IP address to distribute the load. Moreover, it is difficult to send the load to a single Rsyslog server at a time due to the several Palo Alto firewalls that are connected to various Rsyslog servers.

For Traditional Load Balancing, SDN Is Necessary

SDN has the power to promote innovation and network growth while simplifying network management. Its purpose is to divide the control and data planes. The OpenFlow standard describes how information is exchanged between the two planes. In this architecture, an OpenFlow switch contains a flow table containing flow entries. A flow entry consists of fields that are used to match incoming packets and the actions that

will be executed when a match is made. If there is no match, a controller receives the packet and decides whether to add, delete, or modify flow entries in the flow table for subsequent packets matching the same fields. If a match is found, the packet is sent to the controller, who runs a programme to deal with it. Moreover, statistics are collected on packets; the controller may use this information to inform decisions. This makes it possible for us to develop state-of-the-art programmes that satisfy our needs and update them as circumstances change. One such use is load balancing.

Load balancing in corporate networks is one potential use for OpenFlow. According to Wang et aldescription. a binary tree represents the space of all possible IP addresses. The binary tree's level it contains the IP addresses ithmost crucial bits. The nodes in a subtree are identified by a prefix match on the path from the root to that subtree. If each IP address places an equal weight on the network, a tree representation works effectively because at each level, the load is distributed equally across the two subtrees. Fine-grained load distribution is made possible by this method.

Challenges to SDN

Problems with Dynamic Period of Time Modification The capacity to adjust the provisioning of modern converged infrastructures in minutes and have a comparable impact on multiple devices may be a game changer given that today's largely static systems take human settings into consideration. SDN enables instant use of new computing, networking, and storage technologies and opportunities. As opposed to when you were just doing daily checks on what was new in your environment, these dynamic fluctuations in length of time include considerable visibility gaps. It could be essential to respond to a performance observation question with an open arthropod genus. You may connect directly to SDN systems in this way to guarantee performance visibility, monitor the event bus for new components, services, or updates, and promptly update the infrastructure observation inventory.

Facilitating quick, on-demand growth Platforms that monitor other platforms are in jeopardy because to the inescapable increase in demand for more network, storage, and cypher resources in software-defined infrastructure. In order to accommodate the expansion of the infrastructure, these solutions must be equipped to integrate observation functionality. Inability to quickly increase capacity in response to demand will lead to performance visibility gaps. In the world of SDN, we will have a lot of too complicated topologies functioning on top of the actual network, in contrast to traditional design. The required virtual infrastructure is created when a replacement service debuts, which causes a gradual rise in the number of monitored components over time, beyond the capabilities of prior capability management. Installing performance monitoring software on each physical and virtual equipment on a regular basis is the answer. Performance may be enhanced by spinning up more virtual appliances as needed when more performance management features are required.

Service Contextual Integration Having service context is now taken for granted. So, it is necessary for performance monitoring to be able to hear in the context of a particular client or tenant of the network. The last question that customers should be able to ask is, "How is client A's HD video service from New York to London performing?" This should allow them to learn more than simply the status and functioning of certain hardware or network lines.This also holds true for service topology, which implies that both in real-time and in the past, controllers and performance monitoring tools exchange data about the physical and logical connection of the physical and virtual devices that make up a service

SDN Application Areas

Unless flow entries are added to flow tables, OpenFlow switches function as general-purpose computers. These merchant silicon boxes may be converted into a simple hub. An intelligent learning switch, router, and load balancer combine the inputs of the flow. The primary SDN application domains are as follows. Role of SDN in Data Centers Data centres are utilising virtualization as a technology more and more. In addition to automating the process, it has also made server provisioning more easily. Yet, the issue resides in the technology used for network management and data storage. This often leads to a server congestion problem. In order to resolve all the problems, the software-defined data centre (SDDC) will be essential in changing this networking architecture into a more secure and dependable state. A software-defined data centre (SDDCguiding)'s philosophy is to level up all of its components. SDN is growing in significance as SDDC develops.

SDN use in LAN and WAN SDN is a crucial component of LAN and WAN networks outside of data centres. Managing WAN has become quite difficult due to the increasing usage of SAAS, however SDN is the solution and can therefore fix the problem. SDN's automatic provisioning of network resources addresses the key WAN challenges. LANs have undergone a fundamental transformation thanks to the OpenFlow protocol and SDN, which also makes it possible to manage unified wireless and wired networks, enhance BYOD management, and boost security.

Security and SDN:

Their Role SDN is used to access network control and enhance network security. Increased visibility, higher agility that results in an increase in unevenness when analysing network traffic packets, network traffic monitoring, and engineering for controlling network traffic are just a few of the services provided by the SDN.

CONCLUSION

The SDN controller provides the freedom to create several new applications since it is positioned in the center of the architecture between the network components and the SDN applications. Many apps are essential to networks, however because of the problems with conventional networking stated above, these applications are also growing more costly and vendor-specific. SDN may be used to develop these apps once again in order to resolve the issue. Despite the fact that there are several SDN-based applications, in this chapter we are only able to discuss firewall and load balancing. In this chapter, we'll compare conventional applications with SDN-based apps, talk about two particular applications firewalls.

REFERENCES

[1] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, “A Survey of Securing Networks Using Software Defined Networking,” *IEEE Trans. Reliab.*, 2015, doi: 10.1109/TR.2015.2421391.

[2] S. Ejaz, Z. Iqbal, P. Azmat Shah, B. H. Bukhari, A. Ali, and F. Aadil, “Traffic Load Balancing Using Software Defined Networking (SDN) Controller as Virtualized Network Function,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2909356.

[3] M. Jacobsson and C. Orfanidis, “Using Software-defined Networking Principles for Wireless Sensor Networks,” *Proc. 11th Swedish Natl. Comput. Netw. Work. (SNCNW 2015) Karlstad, May 28-29, 2015*, 2015.

[4] Imran, Z. Ghaffar, A. Alshahrani, M. Fayaz, A. M. Alghamdi, and J. Gwak, "A topical review on machine learning, software defined networking, internet of things applications: Research limitations and challenges," *Electronics (Switzerland)*. 2021. doi: 10.3390/electronics10080880.

[5] N. Satheesh *et al.*, "Flow-based anomaly intrusion detection using machine learning model with software defined networking for OpenFlow network," *Microprocess. Microsyst.*, 2020, doi: 10.1016/j.micpro.2020.103285.

[6] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "Securing Networks Using Software Defined Networking□: A Survey," *IEEE Trans. Reliab.*, 2013.

[7] A. Muthanna *et al.*, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *J. Sens. Actuator Networks*, 2019, doi: 10.3390/jsan8010015.

[8] D. Dhakal, B. Pradhan, and S. Dhimal, "Campus Network using Software Defined Networking," *Int. J. Comput. Appl.*, 2016, doi: 10.5120/ijca2016908760.

[9] R. Umar, I. Riadi, and R. S. Kusuma, "Mitigating sodinokibi ransomware attack on cloud network using software-defined networking (SDN)," *Int. J. Saf. Secur. Eng.*, 2021, doi: 10.18280/ijsse.110304.

CHAPTER 20

WIRELESS BODY AREA NETWORKS: SECURITY AND PRIVACY

Ajay Rastogi, Assistant Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.
Email Id: -ajayrahi@gmail.com

ABSTRACT:

In order to measure physical or environmental conditions, wireless sensor networks (WSNs), which are made up of spatially distributed autonomous devices with sensors, are used. Wireless communication advancements and the availability of battery-powered, miniaturized micro electronics devices have revolutionized the trend of computation and communication activities. Due to the wide range of applications, including those in healthcare, utilities, remote monitoring, smart cities, and smart homes that not only conduct efficient monitoring but also enhance quality of life, WSNs have become one of the most intriguing fields of study. To assess important physiological characteristics, even the sensor nodes may be positioned strategically within, on top of, or around the human body. This chapter provides a full analysis of the WSN and WBAN's security and privacy concerns. Beginning with a thorough examination of the networks' features, design, performance indicators, and applications, a comparison study has also been conducted.

KEYWORDS:

Privacy, Security, WSN,WBAN.

INTRODUCTION

The age of smart computing has begun as a result of developments and technical improvements in wireless communication. Nowadays, lightweight battery-powered consumer electronics with sensing and networking capabilities are more inexpensive than supercomputers. These gadgets may be used to keep an eye on and manage a variety of phenomena, from distant occurrences to routine everyday tasks. These items, sometimes referred to as sensors, may be physically dispersed across the area that needs to be watched for activity. For instance, sensors should be strategically positioned throughout a power plant if the temperature has to be tracked. These dispersed autonomous sensors come together to create a wireless sensor network (WSN) where the nodes work together to communicate their detected data to a distant station. Consequently, people seated in faraway locations may get an alert and take appropriate action if any sensor node detects a high or low temperature value. So, physical or environmental factors such as monitoring forest fires, natural habitats, earthquakes, or even the status of bridges are measured using the sensor nodes [1]–[3].

On the other hand, the notion of wireless body area network (WBAN) is being established with the introduction of tiny bio-sensors that may either be worn as watches or bracelets or be implanted like a pacemaker. Such networks may monitor a user's comfort while taking periodic measurements of their body's vital signs. As these sensors gather their bodily vitals and report to a medical facility, the users may go about their regular business in the comfort of their own homes. Hence, WBAN may be thought of as a variation of WSN in which the network is installed within, outside, or near the human body. Despite the fact that sensing and communication are the two essential components for each of these networks, which accounts for their numerous similarities, there are also some notable variances. Most crucially, if

security and privacy problems are not carefully managed in most of these circumstances, such networks lose their usefulness.

Due to its many application domains, including healthcare, utilities, remote monitoring, smart cities, and smart homes that not only conduct efficient monitoring but also enhance quality of life WSNs have become one of the most fascinating fields of study. A WSN is a network of tiny sensor nodes placed across an area to detect, track, or monitor a physical occurrence. The sensors may be put to use in a controlled setting where monitoring or surveillance are crucial, or in an uncontrolled one where the security of sensor networks is crucial Power supply, sensing, processing, and communication subsystems are the four subsystems that make up each sensor node A sensor node may further include actuators, positioning modules, etc. The sensor nodes are sometimes referred to as "motes," and they are chips with low power and high frequency transceivers and tightly packed digital circuitry The nodes collect data, which they transmit to a base station (also known as a sink) via other nodes.

Smartphones now provide an intriguing fusion of sensing, computation, and communication capabilities. Its widespread availability and use also make it a practical tool for the creation of innovative applications. These phones may establish a Bluetooth connection with the biosensor nodes to gather bodily vitals from them and perhaps transmit the data to a distant server via the Internet. Even a smartphone's accelerometer sensor may function as a wearable body sensor to gather information about a user's postures and identify actions like falls. WSN can now monitor local apps as well as distant ones. Wireless body area networks (WBAN), a type of WSN that is becoming important for smart healthcare, were made possible by the tiny, ultra-low power biosensor nodes and the widespread availability of smartphones. WBAN offers enormous potential for usage in applications for sports, entertainment, and smart homes in addition to medical internet of things (IoT) applications. Even with the availability of the bio-sensor nodes, a patient might choose proactive medical care rather than visiting a facility for a checkup when symptoms arise. WBAN makes it possible for a person to live at home and yet be under continual medical observation. For the successful treatment of chronic illnesses and eldercare in the present, this is a practical and significant choice.

Network Architecture

WBAN has developed as a WSN application area for the human body, hence both networks' fundamental structures are relatively similar. The sensor nodes are often dispersed around the area where certain occurrences are to be reported, which also depicts the communication architecture of sensor networks. Each of these dispersed sensor nodes is equipped to gather data, route it to the sink, and provide it to the final customers. A multi-hop infrastructureless design may route data to the end user via the sink using the Internet or satellite.

The health monitoring system, which is considered as a WSN application, is built on a three-tier architecture. Tier 1 focuses on the establishment of networks between bio-sensor nodes and a network coordinator or sink (which could be a smart handheld device like a smartphone), where the sensor nodes gather health parameters and communicate; tier 2 includes wireless technologies like WLAN or GPRS so that the tier 1 sink could transmit the health data to the remote medical server at tier 3 for professional medical analysis.

Both networks use battery-powered devices, making them both limited in lifespan. The length of a life may be expressed in days, months, or even years. For instance, implanted nodes in WBAN like pacemakers need to last for at least 5 years Moreover, both networks' nodes have limited storage capacities and weak processing capabilities So, it is common practise to avoid using complicated computational approaches to deal with many challenges in both networks, such as routing reliability analysis and security Yet, these resource-constrained networks (i.e., WSN and WBAN) also have a few differences. The comparison research between WSN and WBAN. The sensors used in WSN are often multi-functional devices designed for use in

wide-area networks. In addition, the WSN nodes are susceptible to movements brought on by external factors (such wind or water), or the sensors may be drawn to or carried by mobile entities, or this may be a desirable characteristic of the system Using multiple devices to gather data at the required place, the cost-sensitive network creation provides dependability. For instance, sensor networks used in military applications rely on the widespread use of disposable and inexpensive sensor nodes such that the destruction of certain nodes by hostile activities has no impact on the overall throughput. In a wireless sensor network (WSN), the nodes are placed using a random distribution, and point-to-point communication between nodes occurs. In contrast to WSN, the nodes in WBAN are often single-purpose devices intended to be used in limited network areas (i.e., in, on, or around human body). The WBAN nodes are positioned across the human body at certain points, making the relative node motions susceptible to changes in posture. Moreover, the specific absorption rate (SAR) of the electromagnetic radiation that occurs from communication between biosensor equipment is absorbed by human tissue. If the regulation limit of SAR is exceeded, a number of health risks may occur. Nonetheless, depending on their purposes, both networks deal with sensitive material, especially when it is directly tied to human people (i.e., in case of WBAN). So, both networks need a security component to prevent technology from being misused, however the security components may differ depending on their application.

Risks to security in WSN and WBAN

Every system's ability to operate effectively must prioritise security, especially when wireless technologies are involved. Security is a term related to system safety overall. Because to the inherent security risks of wireless communications, both WSN and WBAN are vulnerable. The following are the fundamental security needs applicable to both networks (shown in Fig. 7.4).

Availability: This makes that the needed network services are accessible at the appropriate moment, even while a denial of service assault is taking place.

Data authentication: This makes sure that communication between nodes is real and prevents adversaries from posing as trustworthy nodes.

Data confidentiality: This guarantees that only the intended receiver will understand the provided communication.

Data integrity: This guarantees that the sender's message won't be changed on the route before it reaches the recipient.

Freshness of the data: This makes sure that the information is current and prevents an enemy from replaying an outdated message.

Secure localization: Sensor network applications often use node location data. This security criterion makes sure that an attacker won't learn the nodes' locations.

Flexibility: This guarantees that the network will be utilised in a variety of situations where the mission, risks, and environmental conditions may often change.

Robustness: This guarantees that the network will be resilient to different security assaults. Yet even if an assault does occur, the damage should be minimal.

Time Synchronisation: Most applications using sensor networks depend on some kind of time synchronisation. For example, a sensor node's radio may often be switched off for a while to save energy.

Self Organisation: WSNs are ad hoc networks with the ability to be flexible and adaptable. Every sensor node in a WSN is autonomous and adaptable enough to self-organize and self-heal depending on the circumstances.

Wireless communication is broadcast by nature, and unguided transmission medium adds a number of security risks to both networks. According, there are many categories used to classify the possible dangers in both networks. The objective of the adversary's attack is the first category to be determined, and risks to system security or information security are imposed in response. Data alteration, eavesdropping, and replaying are examples of attacks on information security, while denial of service and impersonations are examples of attacks on system security. Attacks known as denial of service (DoS) are ones in which the attacker tries to stop legitimate network nodes from receiving service. Impersonation attacks occur when an attacker steals a trusted node's identity information and uses it to deceive other nodes in the network. In a data modification attack, the attacker may change, remove, or replace all of the information that was overheard before sending the altered data back to the original recipient for an illicit goal. Unfortunately, owing to the open nature of the wireless medium and eavesdropping, any adversary may freely and readily overhear radio conversations between the wireless nodes in order to take data for harmful purposes.

To accomplish the same goal in a different circumstance, the attacker may even transmit a piece of accurate information (obtained by eavesdropping) to the original recipient. Replay assault is the name given to this kind of attack. Moreover, there are two additional categories of system security threats: mote class attacks and laptop class attacks. Whereas a laptop class attack uses more powerful devices like laptops to attack a WSN, a mote class attack uses a few nodes with capabilities equivalent to those of the network nodes to attack a WSN. Nevertheless, system risks might be further divided into passive attack and active attack categories depending on the severity of the damage. As opposed to their passive counterparts, active attacks are more dangerous. Passive attacks, including eavesdropping or packet exchange monitoring in a WSN by a hostile node, are examples, while active attacks entail data alteration and fake data injection. Moreover, the location of the adversary, such as internal assault and exterior attack, might be used to identify system risks. Internal attack occurs when a valid node engages in unlawful or unanticipated action.

External assault is the responsibility of a node that is not a member of the WSN. A few assaults do occur at various levels;therefore, each layer has to tackle them differently. For instance, DoS attacks in WSN may involve jamming or tampering at the physical layer, collision, exhaustion, or unfairness at the link layer, neglect and greed at the network layer, homing, misdirection, or black holes at the transport layer, and malicious flooding and desynchronization at the physical layer. Lists security breaches each layer. Physical Layer Frequency selection, carrier frequency generation, signal detection, modulation, and data encryption are all handled by the physical layer of WSN and WBAN. Vulnerabilities in this situation might take the following shape [4]–[6].Jamming (59) The radio frequencies utilised by the network nodes are disrupted by this kind of assault. The whole network or a specific area of the network might be interfered with by a jamming source.

Tampering: If the attacker gains access to the target node, it may collect sensitive information from that node, such as cryptographic keys or other data.

Data Link Layer Multiplexing of data streams, data frame detection, media access, and error correction are all responsibilities of the WSN and WBAN's data link layer. Vulnerabilities in this situation might take the following shape. Reliable point-to-point or point-to-multipoint communications are made possible by this layer. Here, there are the following possible security risks.

Collision: Collision happens when many nodes try to communicate simultaneously on the same frequency.

Unfairness: Unfairness is a kind of weak DoS attack where the attacker makes the network unfair by taking use of collision and fatigue assaults.

Exhaustion: The attacker might use repeated collision to cause resource depletion.

Data must be routed from source to destination using the network layer of both WSN and WBAN. Vulnerabilities in this situation might take the following shape.

Neglect and greed: This attack happens as a packet moves from source to destination across nodes. By splashing certain packets or by misdirecting traffic to the incorrect node, the rogue node may cause multi-hopping in the network. As a result, this assault interferes with the network activity of the nearby nodes.

Homing: In this kind of attack, a search is done in the data traffic that is already flowing to find the cluster head or key manager who has the power to shut down the whole network.

Data flow is misdirected in this attack by the attacker.

Hello flood attack: In this kind of attack, a single rogue node delivers a pointless message, which the attacker then replays to create a lot of traffic and clog the channel.

Selective forwarding: In this attack technique, the compromised node distributes data to just a few chosen nodes rather than all nodes. The attacker created this list of carefully chosen recipients in order to further his nefarious goals.

Sybil attack: In this method, the attacker duplicates a single node and presents it to the other nodes in the network as many identities.

Wormhole attack: This attack allows data packets to be redirected via tunnelling over a low-latency network.

Black hole: This attack is also known as sink holes, and it seems to be highly alluring to start the assault by constructing a covenant node (i.e., it promotes zero-cost routes to neighboring nodes with respect to the routing algorithm). As a result, the most traffic is sent towards these false nodes. Nodes next to these malevolent nodes clash as a result, causing message damage and resource competition.

Acknowledgement Flooding: During this attack, a malicious node spoofs acknowledgements in order to trick the targeted nearby nodes into believing a lie.End-to-end connections are managed by the WBAN and WSN transport layers, respectively. Here, there may be the following vulnerabilities.Flooding is a kind of attack in which an attacker continually demands new connections up until the resources needed for each connection are depleted or reach a maximum limit, in which case any more valid requests are disregarded.

Desynchronization: Desynchronization disrupts an established connection, making it possible for an attacker to hinder or even completely eliminate the end hosts' capacity to effectively transmit data. So, wasting time trying to correct mistakes that never truly were is a waste of energy.

Application Layer WSN and WBAN both have an application layer that is in charge of traffic control. Also, this layer serves as a supplier of software for various applications that convert data into understandable forms or aid in information collecting by sending queries. The following vulnerabilities may exist in this area.

Path-based Denial of Service (DoS) assault: In this sort of attack, the attacker increases the amount of traffic along the path to the base station.

Overwhelming sensors: In this attack, the attacker tries to send too many sensor stimuli to the network nodes, which makes the network send a lot of data to a base station. Hence, this assault uses up network bandwidth and depletes node energy. It only works, however, when

specific sensor readings (such motion detection or heat signatures) initiate interactions as opposed to when sensor data are delivered at regular intervals.

Attack by a deluge (reprogramming): Networks that have been installed may have nodes remotely reprogramed thanks to protocols like TinyOS's Deluge network programming system. Deluge is one of these systems that is designed to be utilised in a secure environment, like the majority of others. A hacker might hijack the reprogramming process and take over significant areas of a network if it is not secure.

Security-Related Similarities and Differences between WSN and WBAN

Applications for WSN and WBAN deal with sensitive data, hence security is essential in both networks to prevent the system from being abused by an opponent with bad intentions. In both situations, network operations are conducted through a wireless media. Hence, WSNs and WBANs are both vulnerable to shared broadcast medium security risks. Moreover, in resource-constrained networks like WSN and WBAN, the lightweight security methods with minimal computation and communication overhead are desirable to increase security. Nevertheless, as previously mentioned, there are some significant differences between these two networks, and as a result, it may not be possible to use security solutions created for WSN to WBAN applications. Compared to WBAN, WSN is a larger network that has been distributed across a larger area, making it more vulnerable to outside interference with its sensor nodes. Cluster-based security solutions cannot be used with WBAN, unlike WSN, since clustering may be an overhead for WBAN. Moreover, security solutions created for WBAN must not exceed the SAR regulatory limit. The fact that WBAN includes human beings makes security of the highest importance; otherwise, it might be abused by someone with malicious intentions and potentially pose a danger to life.

Five Privacy Concerns with WSN and WBAN:

In every system that deals with sensitive information, privacy is a critical problem that has to be addressed. Who may access the information is an issue for privacy. Issues with privacy may occur for a variety of reasons, including personal beliefs, the social and cultural context, and other broad public/private problems. As WSN and WBAN both deal with sensitive information about natural events or human health, privacy is a key factor in determining whether or not people would embrace these systems. Sending data from a patient over wireless media in the case of WBAN apps presents substantial risks to that person's privacy since health-related information is inherently private. If this information is exploited maliciously by others with ulterior motives, it may even be life-threatening for a person. When deploying WBAN apps, some of the key issues that must be resolved to ensure privacy include where the health data should be kept, who should have access to the patient's medical record, who will be in charge of keeping these data in case of an emergency, and so on. In order to avoid the exploitation of this private information, it is crucial to consider whether the data were collected with or without the person's permission since that is what the system requires.

The following must be part of the privacy measures before the WBAN apps are widely used.

All communications via wireless networks and the Internet must be encrypted in order to prevent them from revealing any useful information to anybody but the intended receivers. It is also crucial that individual users not be recognized unless absolutely necessary.Another crucial step is to educate the general people on technology, security, and privacy problems and their ramifications so that they may make informed decisions about how much it could impair their own standards of privacy.Nowadays, sensors serve as the IoT-based applications' eyes. For applications in smart cities, sensing and communications work together to tackle a variety of issues. Nevertheless, WSNs are increasingly used in populated regions, such as

citywide air quality monitoring systems, as opposed to installing sensors at isolated locations like those used to monitor forest fires. At the moment, sensors are also made to be able to collect some energy. Hence, protecting data security and integrity is becoming more difficult every day due to the closeness to the sensor deployment and the rise in interested parties. The use of intelligent noise reduction methods is also possible since modern sensors are capable of some computation.

A novel method for gathering data using citizen-carried smartphone sensors is called crowdsourcing. The use of sensing data to improve citizen quality of life includes smart homes, smart buildings, and assisted living. Yet, from the perspective of a citizen, this raises a number of significant issues, such as the sharing of personal information like user location and ambient sound. Sharing this data may give rise to serious security and user privacy problems. According to, sensing and sourcing apps may gather private sensor information about specific people that may be utilised to identify behavioural trends. For instance, GPS sensor readings can be used to predict traffic congestion levels and/or anomalies in a particular community, but they can also be used to infer personal information about an individual, such as their movement patterns, the routes they take for daily commuting, and the locations of their homes and places of employment. As a result, WSN security and privacy concerns are even more important for modern sensors that are placed in populated regions and gathering information on urban living.

Just a few current technologies can solve the considerable security and privacy issues that sensors, particularly biosensors, present when worn by humans. WBANs now include situations related to homecare, particularly eldercare and hospital settings. Body sensors do not need to route packets in homecare and hospital settings since they are in direct communication range of the sink. Nevertheless, they only sometimes demand that data be sent across a maximum of two hops. Consequently, there is little research on routing attacks like sinkhole, wormhole, and selective forwarding at the intra-BAN level of WBANs. WBANs, however, may play a crucial role in the care of catastrophe victims in the near future with the introduction of mobile networks. In crisis situations, body sensors may have to transmit their data through equipment other than their direct radio range. As a result, successful end-to-end communications at the intra-BAN level of WBANs will depend on routing protocols with robust security features. Inter-BAN interference allows hackers to perform denial of service attacks by preventing any data from reaching the sink [7]–[9].

Lack of unified policy frameworks to safeguard patient privacy is the second problem that will definitely grow more significant in the near future. As WBANs spread, more organizations will participate in the system, including pharmacies and insurance firms. As a result, more parties will have access to patient-related data, and there may be more assaults on patients' privacy that might have an impact on their social life as well. As a result, privacy threats may pose as a significant barrier to this technology's growth and development as well as its widespread acceptance. WBAN may only function as a research prototype if existing and future privacy concerns are not carefully defined. To make it impossible for anybody engaged to misuse patient data, new sets of rules should take into account all potential future parties and the privacy threads connected to them.

The phrase wireless body area network (WBAN) refers to a sensor network that is built across the human body and has potential uses in the military, sports, eldercare, and the identification of chronic illnesses. As both network applications deal with sensitive data, they must be as secure and private as possible. The security and privacy difficulties associated with WSN and WBAN, as well as the defensive mechanisms in place, should thus be thoroughly researched. This will be helpful for successful implementation and will also inspire the researcher to forge their own course for greater protection/defense.

The requirement for security and privacy in both networks is thus demonstrated in this chapter along with a quick summary of both networks' intrinsic qualities. Moreover, research has been done on possible risks to network security and privacy as well as current defenses against these problems. In order to encourage additional study in this area, the open research challenges are finally established.

New security threads will be needed for this combination. Sensing technology is expanding quickly, not only for WBANs but for many other WSN types as well. As a result, present security and privacy concerns must be appropriately updated. In the near future, further topics of concern will be brought up in this area; in this part, we have only touched on a few of them [10]–[13].

CONCLUSION

The essential conditions for security and privacy in networks is very essential. To get insight into the assaults, such as their origin, type, and goal, a classification of the possible dangers to both networks has also been established. The current measurements are then analyzed appropriately after that. To encourage the researchers to do more study in such areas, the open research challenges are afterwards defined. The advantage of cloud computing technology may be advantageous for the future generation of WSNs and, therefore, WBANs. Wide-ranging applications and business models are starting to develop when mobile cloud computing and sensors are combined. With the help of mobile cloud computing, it is now theoretically possible to install cutting-edge healthcare monitoring apps with richer multimedia contents, but more diverse convergence services and more dependable quality of service are still required.

REFERENCES

[1] M. S. Arshad Malik, M. Ahmed, T. Abdullah, N. Kousar, M. N. Shumaila, and M. Awais, “Wireless body area network security and privacy issue in E-healthcare,” *Int. J. Adv. Comput. Sci. Appl.*, 2018, doi: 10.14569/IJACSA.2018.090433.

[2] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications,” *Egyptian Informatics Journal*. 2017. doi: 10.1016/j.eij.2016.11.001.

[3] *et al.*, “WIRELESS BODY AREA NETWORKS: SECURITY AND PRIVACY ISSUES,” *Int. J. Ecosyst. Ecol. Sci.*, 2020, doi: 10.31407/ijees10.315.

[4] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” *IEEE Wirel. Commun.*, 2010, doi: 10.1109/MWC.2010.5416350.

[5] S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain, and M. Humayun, “Performance Enhancement in Wireless Body Area Networks with Secure Communication,” *Wirel. Pers. Commun.*, 2021, doi: 10.1007/s11277-020-07702-7.

[6] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, “A survey on wireless body area networks: architecture, security challenges and research opportunities,” *Computers and Security*. 2021. doi: 10.1016/j.cose.2021.102211.

[7] T. Santhi Vandana, S. Venkateshwarlu, and C. V. Ravi Teja, “Exploration of an intelligent and secure wireless body area networks for health monitoring,” *Int. J. Recent Technol. Eng.*, 2019, doi: 10.35940/ijrte.B1126.0782S319.

[8] G. X. Xu, Q. Wu, M. Daneshmand, Y. Liu, and M. M. Wang, “A data privacy protective mechanism for wireless body area networks,” *Wirel. Commun. Mob. Comput.*, 2016, doi: 10.1002/wcm.2649.

[9] A. Kumari, V. Kumar, M. Y. Abbasi, S. Kumari, P. Chaudhary, and C. M. Chen,

"CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3001152.

[10] Y. Zhen and H. Liu, "Distributed privacy protection strategy for MEC enhanced wireless body area networks," *Digit. Commun. Networks*, 2020, doi: 10.1016/j.dcan.2019.08.007.

[11] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical internet of things," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2912870.

[12] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, 2012, doi: 10.1007/s10916-010-9449-4.

[13] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Comput. Networks*, 2020, doi: 10.1016/j.comnet.2020.107333.

CHAPTER 21

EXPLORING THE WIRELESS SENSOR NETWORK NEEDS, PROTOCOLS, AND SECURITY ISSUES

Manish Joshi, Assistant Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India,
Email Id: - gothroughmanish@gmail.com

ABSTRACT:

There are several uses for wireless sensor networks (WSNs), and one of these uses is in industrial automation systems for monitoring and managing machinery. The specifications for industrial wireless systems, however, vary from those for ordinary WSNs. Integration of sensors into industrial equipment, plants, shop floors, buildings, and other crucial locations benefits industries greatly. The use of WSNs in the industrial sector reduces failure rates and raises both productivity and operational efficiency in the factories. For the wireless technology to be integrated with the industrial realm, adequate security must be offered together with guaranteed dependability. The distinguishing characteristics of WSNs in factory automation are discussed in this chapter, along with how they are used in industry. Wireless sensor networks (WSNs) have developed as a result of advancements in electronics and wireless communications throughout time. WSNs are made up of distributed autonomous devices that can sense, analyse, and communicate data, among other distinctive features. Sensor nodes (SNs), which are compact, low-cost, and smart sensors that are simple to install, facilitate the deployment of WSNs.

KEYWORDS:

Cryptography,MediumAccessControl, Routing, Reliability, Security, Wirelesssensornetworks (WSNs).

INTRODUCTION

Small sensor components that detect the observable physical conditions make up SNs, while microprocessor components guarantee that the information is intelligently calculated. Moreover, SNs include an inbuilt wireless radio to help with communication between nearby nodes [1]–[3].Because of the steadily rising demand for services, industries, manufacturers, and businesses have a serious issue with expanded and consistent product supply. Low-cost process automation is essential in businesses for providing high-quality goods, enhancing process efficiency, assuring correctness, and maintaining timeliness of systems. Industries use sensors to support real-time and control functions, but they often rely on complicated and expensive wired systems. As a result, WSNs offer a number of advantages over wired solutions for factory automation, including ease of deployment, the elimination of costly and complicated wired solution installation, flexibility in sensor placement, lower operational costs, large-scale deployment, data redundancy, packet errors, and more.

WSNs are a superior choice for dependable management and energy-efficient services for high asset protection applications due to their self-organizing and self-configuring characteristics. The atmosphere of a typical factory or manufacturing facility is distinguished by specific phenomena such as movement, reflections, machinery rotations, metallic frictions, engine and boiler vibrations, temperature and humidity variations, channel interference, the presence of obstacles, and so forth. For many cases, wired systems are unsuitable since cable

separation is required. Although improving dependability, they increase complexity and administrative burden. Thus, the most efficient, practical, and appealing option in this field is wireless technology.We concentrate on the commercial uses of WSNs in this chapter. The goal of IWSN is to employ inexpensive and low-power nodes to lower the network's operational and capital expenses (OPEX and CAPEX), respectively. IWSNs' productivity and efficiency are improved by monitoring more parameters and receiving insightful feedback. IWSN's self-organization, reliable functioning, minimal maintenance requirements, and ease of deployment are some of its key traits. Nodes, network managers, process controllers, and management console are the main components of an IWSN.

Typical nodes detect, gather, and send data to the sink, the network management. in the nodes converse with the actuators or the process controller, or occasionally even the actuators themselves. Wireless sensor actuator networks are what these networks are known as (WSAN). Using information from sensors such as pressure and temperature, these actuators may control devices like valves. Moreover, one of the most significant IWSN subclasses is the subject of this chapter. The produced data's correctness, dependability, and time-criticality are the most important considerations for IWSNs. It becomes vital to ensure the data's correctness and dependability as these networks transmit and exchange factory-specific, private, and sensitive data. In the case of industrial automation, meeting deadlines is crucial since a communication breakdown or unwelcome delay might have a disastrous effect, disrupting operations or even endangering the lives of employees. Moreover, as many pieces of equipment are operated by precisely timed data, exchanging or distributing misread data might have a similar effect.

The term "Internet of Things" (IoT) refers to a network of connected mechanical, digital, and electronic objects that may exchange data and identify themselves without the requirement for human-computer or human-human contact. This concept allows for the usage of such IoT settings to create transmission networks for data and information produced by diverse applications. IoT is a quickly developing technology that has several industrial uses. IoT affects the way people move, transform, and work in industrial applications, changing how people live their daily lives. When devices connect with one another and carry out autonomous tasks, measurement displays, and outcomes, all industrial activities become smarter. For the objective of improved collaboration and development, industrial associations are often sponsored by government academy and authority, resulting in greater services for the industry and government ally. Manufacturers, service providers, the government, vendors, telecom operators, and other parties are now a primary driving factor behind industrial alliances for the Internet of Things.

While these networks are often linked to the internet's online services as well as the backend software industry, the adoption of a broad variety of technologies integrated in a single network is becoming more important. The open nature of wireless technology raises a number of concerns, including privacy, security, and dependability. If simply the energy consideration of WSNs is not a significant issue, the typical security methods for threats and assaults that exist for wired networks may also be appropriate for WSNs. Security, privacy, and dependability are all interconnected, and improving dependability requires interaction, collaboration, and participation of reliable environmental sensors. As the adversary may interrupt, eavesdrop, or even disrupt communication, adequate security mechanisms are needed while the networks communicate and send sensitive data to guarantee that the transferred data are safeguarded and secured.

It is possible to capture, reprogram, and manipulate sensors to transmit false data readings about temperature, pressure, vibrations, and movements of machine components, with fatal results like explosions or endangered lives. Moreover, in cases of inadequate security,

sensors' energy might be exhausted by constant use in collecting and relaying misleading data, which can destroy networks. The network requires comprehensive security solutions;therefore, the methods of security be incorporated to each and every SN; otherwise, even a single vulnerable network element might act as the attack's entry point, making the whole system unusable. As a result, security is essential in every area of WSN application design.The key contribution of this chapter is discussed as follows.

i. View and present the industrial viewpoint of the WSN domain in contrast to the previously addressed articles. The chapter divides the industrial applications into several groups and provides examples of each class's use. Systems that have comparable objectives and specifications are put into one category.

ii. Go through the fundamental criteria for industrial WSNs and then point out a few less important ones. A number of industrial standards are also covered in this chapter, including WirelessHART, WIA-PA, ISA100.11a, and GINSENG.

iii. Pay close attention to the three most crucial features of IWSNs: security, dependability, and MAC. They are addressed in depth along with many parts of their design specifications that assist industrial systems.

iv. Briefly discuss the security element of IWSNs. The chapter describes the many sorts of attacks that may be conducted against an IWSN and provides a short overview of how security requirements are implemented in the industrial sector.

v. Stress the need of MAC protocols in IWSNs. The paradigm change in MAC protocol design is highlighted by a number of design considerations regarding MAC protocols. A short explanation of a few MAC protocols and how they apply to IWSNs is also provided.

It lists the distinctive characteristics of WSNs used in industrial automation, including resource limitations, dynamic topology, hostile environments, and others. These needs include interoperability, minimum cost and compactness, fault tolerance, low latency, quality of service, dynamic topology, resource restricted nature, data aggregation, and others. This section also goes into depth on the industrial uses of WSNs, such as safety systems, monitoring systems, and control systems. This section explains the wireless standards like wirelessHART, ISA100.11a, WIA-PA, and GINSENG that are particularly designed for industrial WSNs. This chapter's several reliability challenges in industrial WSNs, including managing interference, diversity, multipath, identification, synchronisation, redundancy, and other issues explores the requirement for security in IWSNs by first outlining the security goals, such as confidentiality, integrity, authentication, freshness, and availability. This section also discusses many forms of assaults, including eavesdropping, denial of service, selective forwarding, node compromise, physical, and identity threats. MAC protocols are required to manage medium access and choose the timing of communications. The application criteria must serve as the foundation for the created timetable [4]–[6].

DISCUSSION

WSN Industrial Deployments in Two Samples: Manufacturing facilities, businesses, and sectors rely heavily on information obtained via a network of sensors that are put at strategic locations across the whole field or facility. As a result, the technology is advancing since it does not need a sophisticated infrastructure to handle, sense, and collect data from inaccessible locations. Wireless communication systems are used by a wide variety of businesses, such as oil pipelines, beverage and food producers, and chemical firms, to manage nontrivial tasks like air pressure, weight load, electric current, corrosion, and temperature.This technology enables remote control, real-time data access, decision-making based on the data received, the detection of anomalous or irrational processes, the gathering

and analysis of periodic data, the generation of alarms, the calculation and tracking of machine states, equipment, and instruments, etc. To effortlessly manipulate and control systems anytime, anywhere, even the current management systems and other wireless and wired devices might be effectively integrated with sensor networks and even the internet. The easy replacement of wired sensors to provide space for vibrations and temperature measurement, motor vibration monitoring sensor because some positions make wiring very difficult, and occasionally even need cable isolation, are some key uses of WSNs.

WSNs are helpful for generally enabling condition monitoring systems, such as providing recurring data on the performance statistics of small devices. By identifying uncommon and unusual circumstances, the sensor primarily aids in the maintenance of equipment. It also creates warnings to prompt quick action in the case of any unwelcome occurrences. In situ motor analysis is also possible with WSNs. WSN benefits are also used by complex systems like large power plants for multisensor machinery diagnostics and more suitable and balanced prognostics monitoring. The use of such networks in RF identification tags, which allow technicians using mobile computers to access equipment in a highly safe manner, is also mentioned by Ramamurthy et al. in their study. In and, respectively, WSNs have been used in a variety of applications, including temperature measurement sensors for vibration-based condition monitoring and end-mill inserts for tool failure.

Moreover, these networks provide fresh opportunities like multisensory data fusion techniques for estimating tool wear while managing spindle and work piece vibration. Proposes an extremely effective method for increasing the throughput and dependability of industrial networks. The purpose of the authors' use of the frequency and temporal diversity included into the IEEE 802.15.4 industrial network is to ensuring dependability and real-time throughput. By assuming the probability of analytical modelling of transmission failure probabilities in the industrial area, Miskowicz and Koscielnik assume the dependability in data transfer. In lowering the IWSN's energy requirements, Fischione et al. assured the delivery of the needed package and reduced the likelihood of a delay. The technique is exclusively based on duty cycle, randomised routing, and medium access control along with efficient energy management. Hence, the design strategy focuses mostly on restricted optimization, with energy consumption and delay as its primary functions [7]–[9].

Needs, Uses, and Specifications for Industrial WSN

A benchmark used to distinguish between IWSN and conventional WSN is requirement needs. IWSN is a vast field that is broken down into many groups depending on services and functional needs. The cataloguing of industrial systems, WSN functionality inside these structures, a list of important industrial designing requirements, and suggested high-tech standards are all covered in this part. According to the International Society of Automation, industrial systems may be divided into five groups based on operational needs and data importance. In the section following, these five classes are further explained.

1. Safety measures. This encompasses situations when circumstances call for quick responses, i.e., in a matter of seconds or milliseconds. One example of this is fire alarm systems. Nodes are distributed uniformly across the region to be covered, including the whole area.
2. Closed-loop control mechanisms (CLRS). Here, using feedback to regulate the system is included. Installing nodes in the required topology is done in the relevant field, and the controller is regularly provided the measurements that are essential for efficient system functioning. These systems might have time constraints that are more stringent than those of safety systems. On the basis of the information obtained, the controller makes a judgement. The actuators are then informed of this conclusion so they may respond to the data. For this group of classes, a new process set has been designed.

3. Closed-loop management systems (CLSS). Similar to regulatory structures, CLSS measurements rely on specific occurrences rather than being calculated on a regular basis. Those comments are not very in-depth. An example of a system like this is a supervisory system, which gathers data and only reacts when particular patterns linked to an action are noticed.
4. Open loop control systems (OLCS), which need a human operator to operate. WSN is responsible for data collection and delivery to important databases. The operator then analyses the data and takes the necessary actions as and when they are needed.

Demand for Safe IWSNs: Many concerns with dependability and security arise as a result of the open nature of wireless media. Hence, it is possible to think about old security assaults as well as current protection techniques that have been developed for wired networks. Accuracy, security, and dependability are all interconnected; as a result, protecting information security and privacy is crucial for boosting system reliability. The surrounding sensors, which are unreliable in and of themselves, must communicate and cooperate with one other more in order to increase dependability. When there aren't enough security measures in place, it might be difficult to ensure data protection since the industrial wireless network has to be able to store and send sensitive data.

This is because an adversary could interfere with, interrupt, or eavesdrop on the wireless connection. The network may malfunction, cause a delay, stop production, stop product delivery, or worsen overall QoS in the absence of appropriate security requirements. Moreover, the sensors may be hijacked and reprogrammed by the attackers to introduce erroneous data readings like temperature, vibrations, movement, and component rotation, which can seriously harm the equipment, threaten people, and trigger explosions. Also, the attacker may drain the energy of the sensors by keeping them active for an extended length of time by sending erroneous data. Security procedures must be included into each and every node of an IWSN to increase security since an attacker might exploit even the smallest vulnerability or inefficiency in the network. Many security goals, including confidentiality, availability, nonrepudiation, integrity, data freshness, and authenticity, must be taken into account while dealing with the security in IWSNs [10], [11].

IWSN Attacks

While both wired and wireless applications may use the security targets previously listed, the wireless channel used between the devices and the sensors increases risk. Industrial settings choose their security goals that need to be met based on the function and their unique demands. A few potential wireless sensor network attacks are described in this section below.

1. Attack by eavesdropping: This kind of attack allows the attacker to voluntarily eavesdrop on network traffic in an effort to steal data. Since the attacker seems to vanish from the network, these assaults are difficult to identify. This attack's primary goal is to violate confidentiality by blocking the network, listening to or sniffing at data packages being routed, and then reading them using cryptographic tools. Instead than just remaining motionless, an eavesdropper may employ modern methods to get important information. An attacker may actively influence the communication channel by jamming, interrupting, or altering the network packets. New methods of encryption, which essentially include scrambling data before transmitting it to the recipient and constructing more secure networks, may be used to avoid eavesdropping and promote digital literacy.

2. Denial of service: This technique seeks to shut down a network or system, creating problems for the people who were expected to utilise it. These occur when intruders utilise laptops or PCs to enable signal in order to interfere with radio frequencies, which are currently used by the network to disrupt communication protocols. DoS attacks may do this by flooding the target with traffic or transmitting triggered information that causes the target to crash. Due to excessive and inappropriate message retransmission, this crash consumes battery life, precious computing resources, and processing time. Buffer overflow attacks, ICMP floods, and SYN floods are a few examples of Dos attacks.
3. Compromise of nodes: That is a significant issue in WSNs that increases inside assaults. It is a sort of attack in which the attacker uses methods to reprogram nodes when physically capturing the network and doing so would be impractical. This kind of harmful behaviour is often carried out by a hacked node and includes stealing secrets from encrypted data, reporting false data, and initiating different types of routing assaults.

In addition to the network layer vulnerabilities discussed above, WSNs are also susceptible to a different attack known as selective forwarding. This attack may be identified by the data being sent by certain malicious or reprogrammed nodes in the form of packets, making sure they are disguised. Unpredictable network behaviour is another effect of this nefarious activity. Due to its multi-hop nature, the sensor network is the major target of this assault. Due to the existence of many pathways for each message transmission, this approach has a significant downside in terms of increased node power consumption. Multiple-hop acknowledgements are used in Yn and Xiao's other distributed detection approach to raise alerts in the network. It prevents such an attack by spotting intermediary malicious nodes.

Physical assaults it alludes to physical assaults directed against the node itself. It has to do with the attacker's capacity to take control of the nodes physically. This opens the door for a wide variety of assaults, such as the theft or destruction of nodes, their dislocation, the recovery of private data like cryptographic keys, the injection of malicious code, etc. Tamper proofing the hardware is an additional sensor security method, but it is expensive and may not be particularly effective against attackers.

Identity attack: An identity attack enables a hostile network user to hijack application requests and take control of application components. Attacks of the Sybil and Spoofing varieties may be launched by adversaries using identity assaults. Malicious nodes create several false identities as part of the Sybil attack to deceive the network. Malicious nodes take on several identities and operate in the network as if they are various independent nodes. Such assaults could prevent a network from operating normally. The routing systems that employ several disjoint pathways may be defeated by the attacker due to various identities. These divergent routes make use of the attacker's fictitious identities. With activities like reputation calculation and polling, one node can only participate once, while a fraud node may participate several times and can thus win the vote. By overcoming fault-tolerant and group-based voting strategies such distributed storage, redundancy mechanisms, and multipath routing, the network performance is drastically decreased. When a lawful node assigns a job to one of the other network nodes, the adversary node conducts it independently while assuming various identities, delaying the outcome. Moreover, an identity-forging node may assist in several assaults and impair network performance. These attacking nodes have the ability to act like a black hole, dumping packets with several identities. Even after being discovered, these adversaries continually use their stolen identities to impede the network. A single rogue node might thereby bring several network dangers. Also, for an adversary to achieve recognition from other nodes for its false identities, it must keep the same identity

group for a significant period of time. Moreover, many enemies may join together to execute even more powerful assaults, such manual overlay partition or node isolation from the network.

Control of Medium Access: A group of protocols known as "medium access control" (MAC) regulates medium access and determines the basic scheduling scheme for communication between sensor nodes. The timetable should be planned in compliance with any requirements particular to the application. These techniques may be divided into the major groups listed below to solve scheduling issues. Protocols for Fixed Assignments. The available resources are equitably distributed among the numerous sensor nodes. The allocation of resources to certain nodes places a temporal limit on the validity of this subdivision, making it impossible to modify it during that period. The following groups of protocols exist based on medium access control mechanisms: TDMA, CDMA, and FDMA (Time Division Multiple Access, Code Division Multiple Access, and Frequency Division Multiple Access, respectively). Time is split across a number of sensor nodes in MAC prototypes based on TDMA, necessitating time synchronisation. Several subchannels are created from the subdivision of the frequency medium in MAC protocols based on FDMA. Spread spectrum technology is utilised in MAC protocols based on CDMA to transfer signals, and this is combined with the ability to transmit numerous signals across a single channel by using a unique encoding method. Fixed assignment methods may be divided into centralised and distributed control types. In the event of centralised control, the sink often defines the timetable. In the case of distributed control, network nodes may classify the scheduling control. Some certain chosen nodes determine the schedule for the group of nodes.

Procedures for Demand Assignment. In these, a node receives resources only when they are requested. The amount of time that will be needed for data transfer in this instance limits allocation. Upon the completion of the data transmission, the resources are released. In this situation, protocols are dependent on alterations made to the network's circumstances, and their performance is adjusted in line with the volume of traffic. Both distributed and centralised control may be the foundation of a protocol.

Protocols with random access. These protocols aim to provide distributed control, and taking use of randomization starts with the resource allocation. This category is appropriate for topological changes and heavy traffic (happening dynamically). One of the oldest and most important random-access protocols is ALOHA [72]. The nodes of Pure ALOHA access the media and transmit when the data are ready for transmission. While it follows the same principles as ALOHA, CSMA is more conservative than ALOHA since it only transmits data when it detects that the channel is open for transmission.

Hybrid Protocols Many protocols combine many types of protocols; they may utilise demand, fixed, or random-access protocols, for example. To make the most of them, TDMA and CSMA are used together. For instance, the following combinations of Z-MAC, TDMA, and CSMA are possible. To plan TDMA slots, allow contention within the available timeslots. Create a timetable with a period of no conflict.The parts following will examine the importance of TDMA (in IWSN) and its advantages over CSMA, as well as design factors important to MAC protocols that have already been covered in the section on IWSN needs. Discussion would also include MAC protocol classification. The discussion of a few of the key representative protocols that meet IWSN standards concludes [12], [13].

CONCLUSION

Wireless Sensor Network Needs, Protocols, and Security Issues: These considerations centre on thoughtfully creating secure and reliable protocols beneficial for industrial settings, factories, and production lines. The needs for many key industrial systems are examined, along with potential future developments. WSNs are used extensively in industrial

applications to eliminate human requirement in a variety of hazardous environments. The chapter investigates a number of WSN-related applications in the industrial sector. Many current standards that are applicable to industrial applications are investigated together with the assault defence strategies that they utilise to fend off threats and attacks. Numerous security and reliability challenges, including as interference, work flow, process management, and equipment movements,that are prevalent in WSNs are explored in light of the particular characteristics of various sectors. These constraints need the creation of safe and reliable protocols that are appropriate for factories and industrial operations. The procedures to cope with assaults in IWSNs are investigated together with a number of current industry standards. After a discussion of security functions in industrial standards, different motivating factors for meeting IWSN criteria, including routing, transport, and medium access control, are investigated. The chapter examines several MAC protocol types and contrasts CDMA and TDMA using a number of measures. The chapter also looks at a number of MAC protocol design issues.

REFERENCES:

[1] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches," *IEEE Internet of Things Journal*. 2021. doi: 10.1109/JIOT.2020.3031162.

[2] A. Hussain *et al.*, "Security framework for iot based real-time health applications," *Electron.*, 2021, doi: 10.3390/electronics10060719.

[3] R. Singla, N. Kaur, D. Koundal, S. A. Lashari, S. Bhatia, and M. K. I. Rahmani, "Optimized Energy Efficient Secure Routing Protocol for Wireless Body Area Network," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3105600.

[4] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "A novel security protocol for wireless sensor networks with cooperative communication," *Computers*, 2020, doi: 10.3390/computers9010004.

[5] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," *IEEE Access*. 2020. doi: 10.1109/ACCESS.2019.2962829.

[6] B. Bhushan and G. Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," *Wirel. Pers. Commun.*, 2018, doi: 10.1007/s11277-017-4962-0.

[7] A. Shahzad *et al.*, "A secure, intelligent, and smart-sensing approach for industrial system automation and transmission over unsecured wireless networks," *Sensors (Switzerland)*, 2016, doi: 10.3390/s16030322.

[8] Y. H. Chuang, N. W. Lo, C. Y. Yang, and S. W. Tang, "A lightweight continuous authentication protocol for the Internet of Things," *Sensors (Switzerland)*, 2018, doi: 10.3390/s18041104.

[9] Y. Y. Deng, C. L. Chen, W. J. Tsaur, Y. W. Tang, and J. H. Chen, "Internet of things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system," *Sensors (Switzerland)*, 2017, doi: 10.3390/s17122919.

[10] Z. Ur Rehman, S. Altaf, and S. Iqbal, "An efficient lightweight key agreement and authentication scheme for WBAN," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3026630.

[11] V. Garcia-Font, C. Garrigues, and H. Rifà-Pous, "Attack classification schema for smart city WSNs," *Sensors (Switzerland)*, 2017, doi: 10.3390/s17040771.

[12] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, 2013, doi: 10.1016/j.jnca.2012.05.010.

[13] V. Shakhov and I. Koo, "Depletion-of-battery attack: Specificity, modelling and analysis," *Sensors (Switzerland)*, 2018, doi: 10.3390/s18061849.

CHAPTER 22

USES AND SAFE DATA AGGREGATION IN FOG COMPUTING

Anu Sharma, Assistant Professor,
College of Computing Science and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India.
Email Id: - er.anusharma18@gmail.com

ABSTRACT:

A significant quantity of data is created as a result of the internet of things (IoT) and is in need of adequate storage and analytical applications. Nevertheless, since smart devices lack sufficient capacity, cloud servers are often used to assist applications by offering pay-as-you-go computing power, scalable storage, and on-demand storage. Despite the widespread use of cloud computing, only a few applications, like real-time gaming, health monitoring, and emergency response, can be implemented directly on the cloud due to their latency sensitivity. In order to improve reaction times, fog computing has become a viable addition to the cloud computing paradigm. Applications that employ fog computing architecture pre-process data close to the user. Fog and cloud can work together to manage safe aggregation, preprocessing, and big data collecting, which lowers the cost of data storage and transit. IoT applications are often backed by high-end servers, which are typically put in the cloud, as everyone wants to be able to access everything from anywhere. As smart devices only have a limited number of resources, cloud computing was created in 2000 to suit end users' needs by offering enormous storage and computational capabilities on demand through a pay-as-you-go approach. The user needs to pay just for the resources which are being utilised and only for time the resources are given to the user.

KEYWORDS:

CloudComputing, DataAggregation,FogComputing, Security

INTRODUCTION

By putting data storage and application needs in the hands of the cloud provider, the notion of cloud computing basically transfers the responsibility for IT administration to the third party service provider. In this manner, the firms get a cost-effective on-premises IT solution without having to buy or acquire hardware or software or develop infrastructure. Although though cloud computing is widely utilised today, certain applications, such real-time gaming, emergency response systems, and health monitoring, are so sensitive to latency that they may not be able to tolerate the delay that results from sending a large volume of data to the cloud and back. While data sources are geographically dispersed and low-latency is essential, the data processing at cloud nodes fails to satisfy the time-constrained requirements. However, sending all of the created data to the cloud for processing and storage is not efficient since it uses a significant amount of network bandwidth and may not be scalable. Edge computing, which places the required resources close to the end-user devices for local storage and data processing, was offered as a solution to these issues. It facilitates decision-making, reduces network congestion, and speeds up data analysis. Yet, since there are so many IoT apps competing for the same restricted resources at once, edge devices are unable to manage the situation, which leads to resource contention and longer processing times [1]–[3].

Computerized Fog:

In order to overcome the constraints of cloud computing, Cisco established a dispersed computing paradigm known as fog computing, which offers services and resources at the network's edge. In the same way that fog refers to clouds that are closer to the ground, the term "fog" in fog computing communicates the idea that cloud computing and its benefits are brought closer to the data source. In other words, fog creates an intermediary layer between end-user devices and cloud data centres to create a three-layer hierarchy.

To perform computations and store data, fog computing uses IoT data that is local to the user. By using cloud resources, keeping data and computation near to the end users at the network edge, and limiting the quantity of data transferred to the cloud for analysis, storage, and processing, the goal is to increase overall efficiency. As a result, fog computing represents a potential extension of cloud computing and offers an effective fix for the IoT's data processing issue. While efficiency is a common rationale for choosing fog computing, it may also be utilised for security and compliance needs. Fog nodes are devices that provide cloud-like services at the network edge. They have more processing power than end devices but less than cloud servers, which lowers application latency. Fog nodes are computers with different processing, storage, and networking capabilities that may be resource-rich machines like Cloudlets, IOx, etc. or resource-poor devices like routers, proxy servers, smart TVs, set-top boxes, gateways, etc.

There are several design objectives for a suitable fog computing platform, including low-latency assured applications and services, effective use of energy and resources, generality, etc. To achieve the aforementioned objectives, there are a number of obstacles to overcome, such as choosing a virtualization technology, overcoming the latency caused by resource provisioning and data aggregation, network management, security, and privacy, and enabling real-time analytics by dynamically deciding which tasks must be carried out at the fog layer and subsequently assigning the remaining tasks to the cloud in order to reduce latency and increase throughput. Many applications, including smart homes, smart cities, smart grids, smart vehicles, health data management, augmented reality, and real-time video analytics, may profit from the fog computing paradigm. Health monitoring and data management have been particularly sensitive uses of fog computing. Security and dependability are crucial since health data includes sensitive and private information. Even a little delay may have a major influence on a patient's life in emergency situations. Even in the event that Internet access is interrupted, the crucial systems must continue to function safely. The health monitoring system enables individuals to monitor their own health, communicate health information with their doctor, and promptly alert the necessary providers in an emergency [4]–[6].

Data Aggregation:

The capacity to summarise information is referred to as data aggregation. Decentralized dissemination of significant system-wide properties is made possible by the data aggregation process. Many datasets are gathered from numerous sources in numerous applications and transferred to the cloud server as a result of the amazing growth in the number of geographically distributed IoT devices. Since raw data may include worthless information, this method uses a significant amount of bandwidth. As a result, it is crucial to temporarily store data close to end devices, pre-process stored data, provide notification alerts, etc. Pre-processing might include filtering, grouping, compression, and data security. The data aggregation method entails gathering and combining data from many sources before delivering it to the base station for further processing. Aggregation allows duplicate transmissions to be stopped and aggregated data to be sent to the base station.

Due to the wireless sensor network's (WSN) limited power and transmission capabilities and the need for a long network lifespan, data aggregation is often utilised in WSNs. The method is a general methodology that may be used to increase a system's accuracy. Aggregation may be used to cut down on transmissions and error rates since more data communicated always leads to more mistakes being introduced into the system. With cloud computing, any event or data is delivered to the cloud data centre inside the core network, where it is processed in a sequence of steps before being sent back to the end user. The act of moving a lot of data to the cloud entails a heavy weight. Fog and cloud can work together to manage huge data collection, aggregation, and pre-processing while minimising data transmission and storage, among other things. For instance, local data collected in environmental monitoring systems may be combined and mined at fog nodes to offer fast input, particularly in emergency situations.

It has been noted that handling analytics on massive scales of data produced by IoT applications requires the use of data processing at the fog layer. Aggregation at the fog layer is done to make the network's overall data traffic as little as possible in order to more effectively use its resources. For effective data management, low latency data aggregation is taken into consideration. There are two methods for aggregating data: size reduction and non-size reduction. It is fundamental to convert continuous data transmission into buffered transmission based on local data pre-processing capabilities in order to use different types of data aggregation effectively. Aggregation may conserve network capacity and lessen network congestion since it significantly reduces the amount of transfers.

DISCUSSION

The Uses of Fog Computing: A broad variety of applications are available for fog computing. The following list includes some intriguing applications that profit from this new computing paradigm.

Smart Home: As the Internet of Things (IoT) expands quickly, homes are being outfitted with a variety of smart gadgets and sensors to improve the living experience. Nevertheless, certain jobs may need a substantial amount of computing and storage, and devices from various suppliers may not be compatible with one another. Fog computing may thus be used to combine such devices on a single platform and provide smart home apps the necessary capacity by using cloud services [7]–[9].

Modern Grid: It is necessary to make a big adjustment in the area of the electrical distribution network. A smart grid requires the installation of smart metres at various sites so that the status of power use may be monitored in real-time. Previously, collecting and analysing the status information was the responsibility of a centralised server called SCADA. In order to maintain the stability of the electricity grid, the server reacts to any change in demand or emergency scenario. Yet, the idea of fog computing allows for the decentralisation of SCADA, dividing the power grid into fog-based micro-grids. The fog gadget will control a microgrid and interact with higher layers and neighbouring fogs. Ultimately, SCADA will provide worldwide coverage and be in charge of the long-term archive and economic analytics.

Fog computing integration in automotive networks may be divided into two types: autonomous and infrastructure-based. Infrastructure-based fog nodes are placed along the side of the road to transmit and receive information from and to moving cars, while autonomous systems use moving vehicles to support ad hoc events.

Data Management for Health: As health data comprises important and private information, the application is very sensitive. With the introduction of fog computing, users are now able to independently monitor their health, communicate health data with the appropriate doctor or

physician in charge, and enable patients to access local copies of their health information. When a patient seeks assistance from a medical lab or doctor's office, the health data may be kept at fog nodes and the data processing can be outsourced while keeping privacy protection in mind.

Real-time video analytics with augmented reality Many smartphone, tablet, and other apps that superimpose information over a real-world view are based on augmented reality. Google Glass, Microsoft HoloLens, and other well-known devices built on it. Both high compute power and large bandwidth are required by these applications for data transfer. A processing lag of greater than 10 ms might negatively impact user experience and feedback. As a result, fog computing may help these applications by increasing throughput and decreasing processing and transmission delay.A delay of even a few seconds may have a significant influence on a patient's life, making health monitoring and data management one of the most delicate uses of fog computing.

Akrivopoulos has developed a health app that leverages the patient's smartphone as a fog gateway to transmit electrocardiogram (ECG) trace data to a doctor, check health status autonomously, and immediately alert authorities in an emergency. It is possible to further analyse historical data to find trends that might one day help with medical diagnosis. The functional prototype assessed variables such as storage and reaction time, among others. Lanka et al. examine the integration of fog computing in a cloud environment to create prisons, border security, and military applications. Security troops used to monitor the border by erecting miles of walls, etc. As technology has developed, cameras are being used to monitor the borders. Cloud services are used by WSNs to enhance information management, communicate monitored values, and boost service quality (QoS). Traditional cloud computing may not be viable in real-time settings due to its inherent constraints. WSNs with fog computing assistance may prevent border assaults by making quick decisions and acting quickly. As a result, authors suggested using fog nodes to help cloud servers. The technique may be used to overcome weaknesses and assist military authorities in making judgements in real-time. The architecture is designed to deliver high-end secure applications. Fog computing may assist in the early identification of threat or incursion to improve the situation, especially when taking into account that the military as a business maintains all data on cloud servers. If one node fails, the technology should be fault-tolerant enough to prevent the network as a whole from being destroyed [10]–[13].

Nikoloudakis et al offer a virtualized, decentralised emergency system based on fog computing for smart-enhanced living environments. Between the sensing device and the wi-fi device, the system employs location service to acquire received signal strength indicator (RSSI). The service logic module queries the profiling service to update the user's location. The profiling service keeps a database of the user's location, health, and personal data. The location-to-service-translation (LoST) service makes use of the LoST protocol to identify the closest authority in charge of emergency response. In order to swiftly alert concerned authorities and local volunteers, the system analyses users' whereabouts and identifies them when they go outside of a predetermined safety zone on a regular basis. When there are serious health issues that need ongoing monitoring, the fog layer provides alarms. The system then updates the user's outside location and notifies relevant authorities and nearby volunteers through distress messages that include the user's details. The suggested strategy improves people's quality of life, particularly the elderly and those who are dependant.

A brain computer interface (BCI) that recognises various brain states in real-world situations. With the aid of the publish/subscribe message queuing telemetry transport (MQTT) protocol and fog computing, real-time synchronous data streaming is carried out. Users may use semantic searches using connected data web to search online data streams and their archives.

With the assistance of the collaboration between fog and cloud server, the system carries out real-time categorization of users' mental states. In the meanwhile, electroencephalogram (EEG) data and characteristics collected by fog servers are used to calibrate the classification models on a regular basis on the cloud servers. In fog computing, the computation-heavy tasks are offloaded to the computers located closer to the end nodes, speeding up the associated answers. To increase the security of the system, secure communication, multi-domain user authentication, and authorization are offered. Datasets are gathered by the infrastructure with user consent.

Mei et al. Describe a method for measuring ultraviolet (UV) radiation using complementary metal-oxide semiconductor (CMOS) sensors used in smartphone cameras. The local fog servers combine the data, increasing the accuracy of the results, and reply in real-time to user requests for UV values. In order to confirm and assess the correctness and precision of the technique on both smartphones and smart watches, experiments were carried out using the lightweight, quick, and efficient Android software UV metre. The scientists suggested using cellphones to calculate UV radiation in real-time straight from camera sensor readings. The history of UV levels is used to create a precise % for a place at various periods since the general percentage of UV and solar radiations varies for different locations, seasons, and time zones on the globe. Aazam and Fernando offer an intelligent transportation system (ITS) supported by fog computing to monitor driver behaviour. Data collection, communication analysis, event detection, data storage, service building, and provisioning are all tasks carried out by the system. The information is acquired by taking into account a number of variables, including the health of the driver, the state of the vehicle, and the traffic and weather conditions. Road safety algorithms are conducted at the fog layer based on the data collected to identify any unexpected conditions. The fog layer makes quick decisions and schedules critical tasks, which results in alert or emergency alerts. Results for cloud-only and fog-assisted scenarios are presented using a discrete event system specification (DEVS) simulation setup, and the usability of the suggested architecture is validated.

Cloud servers get overcrowded when the number of devices connected to the Internet rises, which increases computational burden and network delay. The purpose of this work is to propose the idea of fog computing in order to reduce the latency imposed by carrying out important functions on the cloud. In order to establish the best possible balance between fog and cloud level operations and to maximise the benefits, a fall detection and gas-leak detection method is presented. In order to speed up real-time processing, identify undesirable occurrences, and communicate important carers information, the report showed that fog nodes are mostly employed for crucial e-Health scenarios. Moreover, combining information from several sources may stop the system from sounding false alarms, allowing the user's status to be accurately evaluated at any given moment. Fog nodes are thus utilised to accelerate real-time processing for crucial applications and cloud platforms, which preserve patient histories that may be accessed as needed. Using speech and gesture control, Ali and Ghazal implemented the real-time heart attack mobile detection service (RHAMDS) that they had developed. Fog computing is used to speed up emergency response for heart attack patients and avert potential car collisions in vehicular ad hoc networks (VANETs). Smart watches are used in the system's implementation to carry out continuous real-time monitoring of voice commands or gestures. For the model to be more accurate and reliable, data fusion may be done. Low latency and location awareness are provided by mobile edge computing (MEC) servers.

Rahmani et al. Presented an e-health gateway named UT-GATE and a medical case study, and they suggested mobility support based on fog computing so that connection could be supplied to mobile sensors. In order to notify doctors and clinicians in real-time and enable risk prediction and complication prevention, the gateway processes local data locally. The

Lempel-Ziv-Welch (LZW) compression method was used by the authors. Before conducting in-depth analysis on the cloud, sensitive medical data collected by sensors is encrypted and subjected to basic data analysis to identify critical circumstances. Medical personnel may change the therapeutic orders and recording intervals in accordance with medical factors.

Gia et al. Described a fog computing-assisted healthcare system design at smart gateways. The authors discussed an electrocardiogram (ECG) case study in which parameters including heart rate, P waves, and T waves are extracted at smart gateways using simple algorithms. Moreover, bandwidth usage, quality of service (QoS) assurance, and emergency alerting are all shown to be successful with the method. The research also demonstrates online analytics at the fog layer and real-time involvement in an emergency. The device may also identify cardiac problems.

Aggregation of Secure Data: by computing numerous global parameters of an environment in a distributed manner and then merging the findings from many devices to run an application. Decentralized network property determination is possible using a number of computing functions, including COUNT, SUM, and AVERAGE. Aggregation is necessary due to energy restrictions and for improved resource usage. Occasionally it becomes necessary to create summaries using data aggregation in order to lessen the quantity of data carried over the network. Jesus asserts that "there is no perfect generic solution to distributed computing of an aggregation function, since each approach has its own shortcomings and restrictions to be implemented in a specific setting".

Device-oriented anonymous and privacy-preserving data aggregation approach (APPA) with authentication for applications in fog computing environments was developed by Guan et al. Local management of the sensor hardware and fog nodes is done via a multi-authority method. Moreover, trustworthy certificate authorities (TCA) produce pseudonym certificates that are constantly updated according to the needs of the node in order to avoid certificate forgery. Before being sent to the fog node for aggregation, sensed data is encrypted using the pseudonym certificate for the sensor node. Moreover, pseudonym matching prevents hostile sensor nodes from sending data to the fog node. Based on factors like computing complexity and communication overhead, the effectiveness of the suggested method is assessed. The registration step, data encryption scheme, data aggregation, and decryption technique all had their computational complexity analyzed.

The approach is appropriate for end user nodes with restricted resources, according to the experimental investigation. Re-ADP, a framework for adaptive -event differential privacy-based data aggregation for real-time data produced by IoT devices in a fog computing environment, was suggested by Huo et al. The system uses a window size of time stamp to safeguard the aggregated data sequence at fog nodes. The authors spoke about using smart grouping to handle tiny statistics values in sensor data while addressing perturbation errors. The long short-term memory (LSTM) model is used to first separate the sensors based on statistical predictions in the grouping technique. Following that, the sensor device grouping is done using the k-means clustering technique. Last but not least, a Laplacian technique is used to disturb the aggregated data. In terms of mean absolute error (MAE) and quality of privacy (QoP) characteristics, the findings show that the suggested framework increased data availability and usefulness.

Using homomorphic encryption-based technology, Zhang et al. demonstrated a privacy-aware data collecting and aggregation approach for fog computing. This has been utilised to secure IoT device privacy while lowering the total communication overhead of any system. The three requirements, namely privacy protection, non-repudiation, and unforgeability, have been understood. Also, the writers guarantee that personal information won't be disclosed. The effectiveness of data integrity checking was also improved by the authors' study of a batch

verification technique. The method is safe and efficient in terms of computing and communication costs, according to the security and performance study. In order to decrease packet size, data transmission volume, and data storage, data aggregation processes are utilised in smart grids in 2018 and are seen to be fundamental requirements. For fog computing-based SGs, Okay and Ozdemir introduced a brand-new Domingo-Ferrer additive privacy-based secure data aggregation (SDA) technique (FCSG).

End-to-end secrecy is maintained while minimising communication and storage overhead. Moreover, data aggregation is carried out at the fog layer, which lowers the volume of data that has to be processed and stored on cloud servers. This results in faster reaction times and reduced computational overhead. Consumer privacy is protected by FCSG's hierarchical design and additive homomorphic encryption other people. The impact of packet size as well as cloud server storage is assessed during the security study. Data transmission and storage efficiency were significantly improved by the dynamic analysis.

The limitations of IoT-based end devices were discussed by Lyu et al. For instance, data transmission in smart metres is an energy-intensive process. The innovative smart metering aggregation system, known as PPFA, allows the intermediary fog nodes to reliably extract aggregate statistics by regularly collecting data from neighbouring smart metres. The total aggregate data are calculated by the cloud/utility provider. In order to reduce privacy leakage and decrease utility loss, the study distributes noise creation across parties using a concentrated Gaussian technique. As a result, the authors provided aggregate statistics on fog as well as cloud level with verifiable differential privacy assurances. Also used for authentication is a two-layer encryption system based on OTP and public-key cryptography.

The theoretical approach has been validated using data from real-world smart metres. Currently, it is difficult to safely aggregate sensed data from cars. A lightweight and anonymous privacy protection framework for fog computing-aided vehicle-to-infrastructure communication was presented by Chen et al (V2I). Initially, the protocol verifies its security using a random oracle model and a certificate less aggregate signing cypher (CL-A-SC) technique based on data acquired by the cars. After that, a technique for anonymous aggregation is recommended. The protocol demonstrates desired security qualities, according to the security analysis. On the other hand, a considerable decrease in processing and communication overhead was seen in the dynamic study for performance comparison. The work is more useful for the system used to monitor the state of the road surface, according to analysis.

On the basis of fog computing, the anonymous and secure aggregation system (ASAS) in public cloud computing. In the suggested approach, data is collected from terminal nodes and sent to fog nodes that are supplied by public cloud server (PCS) in order to save bandwidth. The upload of data from terminal devices to PCS is also helped by fog nodes. The associated user processes the data by performing various techniques after submitting the encrypted results. The data is delivered in an anonymous and safe manner using the homomorphic encryption approach thanks to the usage of pseudonyms in the aggregation scheme, which protects the identity of terminal devices. Lu et al. present a lightweight privacy-preserving data aggregation (LPDA) method to combine data from hybrid IoT devices using the Chinese remainder theorem. The approach uses source authentication with a one-way hash chain technique to filter out bogus data that is introduced at the network edge. The system employs homomorphic Paillier encryption, which prevents fog devices from seeing individual device data while it is being aggregated. There is a thorough security study and performance analysis.

A method for data aggregation in mobile phone sensing that protects user privacy. By separating the data from its sources, the suggested method safeguards the privacy of participants and enables the data aggregator to determine the precise distribution of data. In essence, the protocol gets a random permutation of all user input without being aware of the origin of any specific data point. The writers provided an optimized grouping solution to the protocolwhenthereare largenumbersofusersandhavedifferentsourceanonymityrequirements.Therefore,the approach allows users in each group to execute protocol together and helps inreducing the bottleneck at the aggregator. The formal system model and securitymodel presented for ASAS is instantiatedbased on linear pairings, short signaturesand Castagnos–Laguillaumie cryptosystem. An aggregation scheme to aggregatedata for MapReduce jobs in cloud is presentedby Ke et al. When all the dataisforwardfrommaptaskstoreducetasksintraditionalMapReduceframework,a huge amount of data was generated. Also, the data is many times redundant,which leads to wastage of computational resources as well as processing time.Therefore, the authors proposed architectureto perform aggregation in order tominimizedatatrafficduringshufflephase.Thetwomodules,namelyaggregatorand aggregator manager, are integrated so that the existing Hadoop architecture can beenhanced and efficient aggregation can be facilitated in a virtual cloud data centre.The aggregators are located between map and reduce jobs which perform reduce-like operation to combine key-value pairs with the same key. On the other hand,aggregator manager deals with the placement of aggregator module and bandwidthassignmentproblemsothatcommunicationcostcanbereduced.Theprototypeandsimulation-basedtestswereperformedtovalidateefficiencyoftheprotocolinreducing networktraffic.

The utility of network coding so that data aggregationcan be optimized and the number of transmitted messages can be reduced, therebyreducing the network traffic in a WSN. The authors used a strategy to deploy thenodes in a network such that the topology formed supports many-to-many networkflows (multiple sources and multiple sinks). Also, the proposed technique uses multicasting instead of flooding. In case, current sensed data is significantly different from previously transmitted data, it is transmitted to the aggregate node whichsavesalotofenergyandunnecessarytransmissionscanbeavoided.Anearoptimal solution for maximum lifetime data aggregation(MLDA)problemwasproposedby Dasgupta et al. [11]. The authors presented an efficient clustering-based heuristic for datagatheringandaggregationforlarge-scalesensornetworkstermedasheuristicGREEDYclustering-basedMLDA(CMLDA)basedonexistingMLDAalgorithm.The partitioning of sensors is done using proximity-based clustering algorithm andaggregationtreesarecreatedsuchthatminimumresidualenergyamongsensorsis maximized. A 3-level hierarchical protocol proposed by Lindsey, Raghvendraand Sivalingam (LRS) is compared with the proposed protocol. LRS protocol ischain-based in which leader is chosen in a round-robin manner in each round. Theexperimental results demonstrate that “CMLDA achieves a factor of 2.27 increaseinlifetimeoflarge–scalesensornetworks,whencomparedtotheLRSprotocolandincursasmallincreaseinthedelayexperiencedbyindividualsensors.

CONCLUSION

Past few years, there is a tremendous increase in the applications of IoT devices.Such applications generate huge amount of data that requires efficient data storageand computation ability. However, IoT devices have limited storage space andcomputational power. Moreover, cloud computing infrastructure provides hugestorage capacity and computational power, although it leads to increased latency,especially in delay-sensitive IoT applications such as

healthcare, military and e-business. To tackle such latency issues, fog computing environment has beendevelopedthatprovidescloud likefacilityneartoendusers.Inthischapter,variousapplicationsoffogcomputingenvironmentaredis cussedalongwithexistingsecuredataaggregationtechniques.AstheprocessofdatagenerationbyIoT devicesisvery frequent,dataaggregationplaysanimportantroleinefficientdeploymentoffog.

REFERENCES

[1] A. Gall, T. L. Butler, S. Lawler, and G. Garvey, "Traditional, complementary and integrative medicine use among Indigenous peoples with diabetes in Australia, Canada, New Zealand and the United States," *Aust. N. Z. J. Public Health*, 2021, doi: 10.1111/1753-6405.13120.

[2] E. Kumpel, C. MacLeod, K. Stuart, A. Cock-Esteb, R. Khush, and R. Peletz, "From data to decisions: understanding information flows within regulatory water quality monitoring programs," *npj Clean Water*, 2020, doi: 10.1038/s41545-020-00084-0.

[3] M. L. Christensen and R. L. Davis, "Identifying the 'Blip on the Radar Screen': Leveraging Big Data in Defining Drug Safety and Efficacy in Pediatric Practice," *J. Clin. Pharmacol.*, 2018, doi: 10.1002/jcph.1141.

[4] A. Divya Preetha and T. S. Pradeep Kumar, "Leveraging fog computing for a secure and smart healthcare," *Int. J. Recent Technol. Eng.*, 2019, doi: 10.35940/ijrte.B3864.078219.

[5] S. Rosenbaum, "Data governance and stewardship: Designing data stewardship entities and advancing data access," *Health Services Research*. 2010. doi: 10.1111/j.1475-6773.2010.01140.x.

[6] P. Zhang, C. Wang, C. Jiang, and Z. Han, "Deep Reinforcement Learning Assisted Federated Learning Algorithm for Data Management of IIoT," *IEEE Trans. Ind. Informatics*, 2021, doi: 10.1109/TII.2021.3064351.

[7] E. Galdeano-Gómez, J. A. Aznar-Sánchez, J. C. Pérez-Mesa, and L. Piedra-Muñoz, "Exploring Synergies Among Agricultural Sustainability Dimensions: An Empirical Study on Farming System in Almería (Southeast Spain)," *Ecol. Econ.*, 2017, doi: 10.1016/j.ecolecon.2017.05.001.

[8] D. Drescher, T. Büchner, P. Guttmann, S. Werner, G. Schneider, and J. Kneipp, "X-ray tomography shows the varying three-dimensional morphology of gold nanoaggregates in the cellular ultrastructure," *Nanoscale Adv.*, 2019, doi: 10.1039/c9na00198k.

[9] K. A. Alatinga, L. A. Allou, and E. W. Kanmiki, "Contraceptive use among migrant adolescent girl head porters in Southern Ghana: Policy implications for sexual and reproductive health education and promotion," *Child. Youth Serv. Rev.*, 2021, doi: 10.1016/j.childyouth.2020.105651.

[10] N. Quadrianto and Z. Ghahramani, "A very simple safe-Bayesian random forest," *IEEE Trans. Pattern Anal. Mach. Intell.*, 2015, doi: 10.1109/TPAMI.2014.2362751.

[11] S. Hines, T. A. Carey, T. Hirvonen, K. Martin, and M. Cibich, "Effectiveness and appropriateness of culturally adapted approaches to treating alcohol use disorders in indigenous people: A mixed methods systematic review protocol," *JBI Evidence Synthesis*. 2020. doi: 10.11124/JBISRIR-D-19-00040.

[12] M. Marks *et al.*, "Electronic Data Management for Vaccine Trials in Low Resource Settings: Upgrades, Scalability, and Impact of ODK," *Front. Public Heal.*, 2021, doi: 10.3389/fpubh.2021.665584.

[13] X. Zhang *et al.*, "Conception and Application of Virtual Load in Intelligent Panoramic Grid," *Dianwang Jishu/Power Syst. Technol.*, 2021, doi: 10.13335/j.1000-3673.pst.2020.0460.

CHAPTER 23

ROLE OF INTERNET OF THINGS TO ACCESS HUGE DATA IN THE CLOUD

Rohaila Naaz, Assistant Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.
Email Id: - rohailanaaz2@gmail.com

ABSTRACT:

The term "Cloud Computing" (CC) technology refers to a system in which data processing and storage occur outside of mobile devices. Moreover, the Internet of Things (IoT), a brand-new technology that is rapidly gaining ground, is raising concerns in the "contemporary" field of wireless telecommunication systems.

Also, by relying on wireless network technology, both CC and IoT might grow quickly and jointly. In particular, the two aforementioned technologies Cloud Computing and IoT have been contrasted in order to look at their commonalities as well as the advantages of combining them to safeguard the usage and transmission of Big Data. In conclusion, the contributions of CC and IoT technologies have been discussed, along with how CC technology enhances IoT's performance as a foundational technology for Big Data systems.

KEYWORDS:

BigData, CloudComputing,InternetofThings, Privacy, Security.

INTRODUCTION

The "Internet of things" (IoT) is a cutting-edge technology that functions in the communications industry.

IoT has been referred to as "the network of gadgets, cars, buildings, and other things that are implanted with sensors and are linked to the network, letting these objects to acquire and exchange data by numerous academics.

A surge of linked devices, locations, and the tasks they will carry out during the next years is anticipated. There are security and privacy concerns that must be addressed with regard to the data utilised in a wireless network. By using BD analytic tools and services, the issue of security and data privacy in daily life may be resolved or at least reduced.

The amount of data in both organised and unstructured forms has increased astonishingly quickly, and this phenomenon is referred to as "big data" (BD). CC serves as the standard technology on which BD often operates. Similar to this, Edge Computing is another technology that may be utilised as a basic technology (EC) [1]–[3].

IoT might be defined as a network of physical things or items that are enabled by connection, electronics, software, and other components. As a result, IoT enhances rate and service by transferring data with operators and many interconnected devices.To assist other researchers who are interested in security concerns, researchers in have proposed a strategy. In this method, the most current security research activity is analyzed in terms of IoT security, and a unique IoT framework is verified using a case study. This paper's authors have shown via their study that the development of autonomous devices poses security risks.Because of the

complex calculations, the large amount of data, and the security concerns, the requirement for "cloud" assistance has therefore become ineffective. Limited processing, energy, communication, and storage capacity are a few examples. We were prompted to design a paradigm for the integration of CC and IoT by deficiencies like these. The "base" technology of cloud computing unifies a variety of technologies and applications to maximize the performance and capacity of the current infrastructure.

Moreover, as a subset of cloud computing, mobile cloud computing (MCC) emerged and was enhanced by recent advances in the "cloud computing" industry. The latter eliminates the requirement for hardware equipment in order to give access to data and information at any time and from any location. MCC is described more explicitly as the fusion of cloud and mobile computing, making mobile devices more capable. It is also a modern strategy for businesses and organisations to provide new services. In order to enhance the functionality of both Internet of Things and video surveillance technologies, CC may be employed as a valuable basis.

Moreover, cloud computing intends to provide access to data and information at any time and from any location without limitations imposed by the need for hardware. CC might be utilised as a foundation technology for the Internet of Things and for a number of other technologies in the telecommunications industry, and it could also enhance their capabilities as a consequence of how it operates [4]–[6].Due to the services it offers, CC has moreover historically served as a foundation technology for other technologies. The Big Data is among them. BD is a word used to characterise the anticipated, rapid growth in data creation that would result from devices being connected to the Internet. Thus, these massive data sets might be referred to as "a general phrase for data sets so huge or complicated that conventional data processing applications are unsuitable".

Moreover, BD is often linked to the use of sophisticated data mining techniques or predictive analytics to derive information from the data. Occasionally, it also has anything to do with the size of the data collection. More accurate BD may lead to more confident decision-making, and better judgements may lead to higher operational efficiency, lower costs, and less risk. From this perspective, it is clear that BD is now just as vital for business and the internet. This occurs because greater data allows for more precise analysis. The question of whether or not the vast volumes of data have any worth is what the actual issue isnot that they have been collected. The following goals should be attained by anticipating that businesses would be able to get information from any source, use the relevant facts, and conduct targeted analyses of them to find solutions quickly: (1) save costs, (2) shorten production times, (3) expand product lines and improve product options, and (4) make more clever choices.

Last but not least, because we are discussing BD, IoT, and CC/MCC, several researchers have attempted to identify methods for protecting this sensitive/personal data. With how many new technologies there are, security issues are still a difficulty. As a result, has developed a security system for secure transfer of sensitive data through CC and IoT devices. In order to enable the data transported from the IoT devices to the Cloud and back, a substitute for RSA (Rivest-Shamir-Adleman) security called MEMK ("Memory Efficient Multi Key") generation mechanism has been implemented. The authors of this work also used similar method to improve memory performance.

Big Data:

Big Data refers to the idea of data that is challenging to collect, store, manage, and analyse using conventional methods and technology. Big Data in the business has expanded significantly over the last 20 years and is continuing to develop tremendously. The amount of data created globally in 2011 was 1.8ZB, and in the near future, this will double every two years.According to the 3V model from Lenay, "big data" is described as "high volume, high

speed, and a broad diversity of information items that demand efficient and creative forms of information processing for increased insight and decision making.Big data is defined as "high-intensity, high-speed, and/or high-variety of information items that need novel kinds of processing to allow increased decision making, insight finding, and processing optimization" by Gartner in 2012. Large data is defined as "high-speed, complex, and variable high-volume data that demands sophisticated technologies and processes to allow collection, storage, distribution, administration, and analysis of information" by the TechAmerica Foundation.

The 5V Predictive Model for Big Data

A real-time method is suggested for forecasting Big Data's 5V that first filters data from unreliable sources (honesty) and uses the Bloom filter to discern the diversity of data. The system then incorporates the data variability while estimating the amount and speed of each kind of data that enters the system using the Kalman filter. The Kalman filter is superior to the other filters because it can be quickly modified to provide unbiased predictions across a variety of data streams, even when the volatility is significant. It is a powerful retrospective filter that enables the dynamic prediction of future trends from incoming currents derived from noisy sensor readings. Data that does not belong to a set may be filtered using the probabilistic data structure known as the Bloom filter. It is mostly considered to be text, audio, video, and video data via data streams.

Big Data Analytics

Quick real-time analysis is needed because heterogeneous data is produced from several physical devices. We require algorithms that pre-process the data before analysis since incomplete data is an issue for real-time analysis.Big Data's ability to develop and keep up with this growth is challenging as production data continues to rise.The generation of an unheard-of volume of data is one of the Internet of Things' most significant advantages. Data holding, completion, and storage become crucial. With these demands, the Internet's energy consumptionwhich already accounts for up to 5% of all energy producedwill undoubtedly rise much more. As a consequence, centralised hardware and data centres provide both dependability and energy efficiency. For intelligent monitoring and activation, the data must be wisely kept and utilised.

DISCUSSION

Artificial intelligence algorithms that can gather or disseminate information based on the demands of the moment must be developed. For the purpose of comprehending the gathered data, new fusion algorithms must be created. Evolutionary algorithms, genetic algorithms, neural networks, and other artificial intelligence tools form the foundation of contemporary non-linear, time machine learning approaches. Features like interoperability, integration, and adaptive communications are offered by these systems. They are often appropriate for IoT applications and also offer a modular architecture for both hardware and software development. To facilitate storage and analysis, a centralized infrastructure is required. The Internet of Things is thus intermediate software level, and there are other difficulties that are covered here. Since 2012, cloud-based storage solutions have become more and more common in the years to come, according to data gathered from cloud-based analysis platforms and data visualization platforms [7]–[9].

Data analysis is the process of employing algorithms to find hidden capabilities in massive data, such as hidden patterns or undiscovered correlations, such as the extraction of helpful information and their picture. This is done in the case's phrasing, often based on inferences drawn from the experience and the identification of connections among the factors. Rajaraman asserts that there are four categories of data analysis. Detailed Analysis This

focuses on what has already occurred and shows the data in a format that is easily accessible, such as diagrams, graphs, pie charts, maps, spreadsheets, etc.

The presentation provides information about what the data suggest. The display of population census data, which categorizes the people of a nation by gender, age, education, income, etc., is a typical example.

Statistical Analysis

It makes inferences from the information at hand to forecast what is likely to occur soon. Time series analysis employing statistical techniques, neural networks, and engineering learning algorithms are the instruments utilised to gather data. Predictive analysis plays a significant role in marketing that takes client demands and preferences into account.With huge data sets, it uncovers unexpected connections between parameters. Data collection and analysis from multiple sources provide more chances for unforeseen insights and discoveries. One of the most crucial applications is to identify patterns in customer behaviour from the feedback they receive from tweets, blogs, Facebook, and emails to enable businesses to anticipate customer actions like renewing magazine subscriptions, switching mobile phone service providers, cancelling hotel reservations, and so forth.

Legal Evaluation

In other words, it informs us what has to be done to accomplish a goal. It does this by identifying, depending on the data acquired, possibilities to improve solutions to existing issues. The price of airlines based on information from travel models, such as well-known locations, significant events, holidays, etc., is one of the typical applications in order to optimise profit.Moreover, Stratosphere is presented by Alexandrov ET al.and is open-source software for parallel data processing. Moreover, Kwon et al. provide a study model that draws heavily on the theoretical underpinnings of user experience and data quality management to explain the intention to purchase huge analytical datasets.

Problems With Big Data Security

By the advancement and use of BD technology, new problems and standards in data security concerns are generated and produced. In order to manage the vast volume of data and assure efficacy, this increases the need for more research on security technology. When used on large data sets, data security technologies are sluggish.

Big Data on Cloud System Scenario

Large-scale data has taken up a significant portion of all forms of data in cloud storage as a result of social network sharing that has gone through the roof as well as video-on-demand services for movies, TV shows, and other content. Moreover, numerous versions at varying bit rates are often created to enable users with differing bandwidth needs, device resolutions, and full interactive playback in large-scale data demand. Big Data schemes, which handle massive amounts of data, have performed well in a variety of cloud storage setups. These programmes, however, handle all files as if they were one big general data set, and one irrecoverable mistake will result in the whole file being permanently lost. They don't take into account the attributes of certain data types.In order for the IoT connected to it to help the development of the smart city, the cloud computing needs provide its services with a specified set of features. The vast amount of data that certain scenarios outlined, connected to the overall activity of the city, is referred to as "Big Data" or "big scale data" in the worldwide literature.In this paper, we suggest a cloud-based BD system that may be utilised and sent across an IoT network.

Internet of Things

According to the definition given in the introductory section, the IoT may be summed up as "a network of devices that transmits, exchanges, and utilises data from the physical world to deliver services to people, organisations, and society." Moreover, IoT has several uses in the fields of health, transportation, the environment, and energy, as well as for other sorts of devices including sensors, wearables, watches, glasses, and home automation.

The Data's Benefits

Businesses assess the likelihood that streaming data may create innovative markets with the goal of spurring positive change or enhancing current offerings. The following list of fields [62] includes some instances of those at the centre of these developments:

1. IoT(a): Smart transportation solution: With this, improved transportation solutions with the goal of delivering a higher standard of life might be realised.
2. Internet of Things (IoT) (b): Smart power grids integrating more renewable energy: With this, system dependability may be attained, and it would also allow for a reduction in customer fees, resulting in cheaper electricity.
3. IoT(c): Remote patient monitoring: With this, we might create a system that allows for remote patient monitoring. By enhancing service quality, expanding the clientele serviced, and saving money, this approach might provide a better and more efficiently managed healthcare system.
4. IoT(d): Sensors in homes and airports: With this, we could make homes and airports safer by installing a lot of sensors throughout the area.
5. IoT(e): Engine monitoring sensors that identify and forecast maintenance difficulties: With this, we can better replenish inventories, detect and anticipate maintenance concerns, and even set priorities for scheduling maintenance work, repairs, and regional operations.

IoT Data

For real-time support, security, personality, and high-level performance, cyber-physical systems made up of autonomous sensors, actuators, and embedded systems are connected to the physical world, including people, in the Internet of Things (IoT). Manufacturing has a lot of promise for IoT.IoT devices that generate heterogeneous data include cyber-physical systems, smart devices, industrial instruments, sensors, actuators, and OPC Server.The following IoT technologies' data collection efforts are crucial.

1. Radio-Frequency Identification (RFID): RFID technology makes use of electromagnetic fields to transport data and to recognise objects automatically. It is made up of readers and tags. Each item has a unique RFID tag. By reading labels, the reader locates items. Due to the fact that not all objects and products have RFID tags, major enterprises have difficulty storing and managing RFID data.

2. Wireless Sensor Network (WSN): In a constrained context, a WSN is a network of dispersed autonomous nodes linked to one another by wireless sensors. The sensor node organises itself and communicates with other nodes to provide data back to the main grid. Certain nodes are capable of automating the control of actuators, which are physical objects. All of the node information for sensors and actuators that may communicate and transmit instructions is included in WSNs.

3. Cloud computing: Nowadays, only as a service, by paying only as we use them, can storage, computing power, infrastructure, platforms, and software be made available. The

three primary forms of cloud computing are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The IoT's architecture For IoT data, cloud computing is crucial. With an Internet browser or other software, they may be stored in the cloud and accessed by anyone, anywhere.

4. Industrial Internet: Often referred to as the Industrial Internet of Things (IIoT), the Industrial Internet is the Internet of Things (IoT) that is exclusive to industries. Using cutting-edge technology and software, smart machines connect the industrial environment both internally and outside to facilitate communication.

Security

One area where efforts are being made to safeguard online networks and linked devices is the security of IoT systems. The Internet of Things (IoT) refers to the growing prevalence of entities and items having unique IDs and the capacity to automatically send data across a network. Computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, as well as technologies like smart energy grids, home and building automation, vehicle-to-vehicle communication, and wearable computing devices, were the main contributors to the increased use of IoT communication.

The major problem is that since networking appliances and other things were relatively novel concepts, security has not always been taken into account in product design. An IoT device that has to be directly accessed over the Internet should be partitioned into its own network and have restricted network access in order to address security and privacy problems. In order to spot any possible aberrant traffic, the network component should be watched, and if a problem is found, steps should be taken.There are system models in the IoT technology field. Considered is a wireless network model with a pair of sources and destinations, N trustworthy relays, and J eavesdroppers (J 1). Assume the global CSE is accessible. Only the source message is assumed to be secret; the eavesdropper channel, source encoding methods, decoding models, and accommodating protocol are all admittedly made public. The topic in this study is restricted to the Decode-and-Forward (DF) and Amplify-and-Forward (AF) accommodative models (AF).

Cloud Computing Security

Computer, network, and information security all include CC security as a dynamic sub-domain. It alludes to a large number of measures, technologies, and policies that have been implemented to safeguard CC's data, applications, and related infrastructure.With the objective of storing and processing their data in external data centres, CC technology provides users and companies with a variety of capabilities via its storage solutions. Thus, by attempting to provide secure network communication. The encryption technique is crucial in 21 Secure Machine Learning Scenario from Big Data in Cloud Computing. In light of the research that has been done, symmetric key encryption is a significant encryption method. With symmetric key encryption, the data is encrypted and decrypted using the same key. The AES algorithm is most often employed in this encryption method.

Inferences

There are many opportunities made possible by CC technology, but there are also many restrictions. On an infrastructure known as the "cloud," data processing and storage take place outside of mobile devices. Also, the Internet of Things (IoT) is a brand-new technology that is expanding quickly in the telecommunications industry, particularly in the contemporary cellular telecoms sector.With the purpose of creating a better environment for the use of Big Data, the major goal of the interaction and collaboration between things and objects communicated across wireless networks is to accomplish the target assigned to them as a united entity. In addition, depending on the technology of wireless networks, both the

technologies of CC and IoT expand fast [10]–[13].

CONCLUSION

In order to secure the usage and transmission of Big Data, we specifically mix the two aforementioned technologies with the intent to investigate the familiar aspects and with the intent to uncover the advantages of their integration. In addition to a presentation of how the two encryption algorithms utilised contribute to the integration of IoT and CC as basis technologies for Big Data, the suggested algorithm model also surveys the security difficulties of the integration of IoT and CC. Future study on the fusion of those two technologies may focus on this as well as the security issues covered in this article.The most recent and trustworthy encryption method, AES (Advanced Encryption Standard), is suggested by NIST to take the place of the DES algorithm. The only scenario for attacking AES that works is a brute force assault, when the attacker attempts every possible character combination in an effort to break the encryption. The AES encryption scheme may be used on several systems and is quick and adaptable. An example of the AES encryption algorithm is shown below.

REFERENCES

[1] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2017.2757955.

[2] K. Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, and M. Guizani, "Edge Computing in the Industrial Internet of Things Environment: Software-Defined-Networks-Based Edge-Cloud Interplay," *IEEE Commun. Mag.*, 2018, doi: 10.1109/MCOM.2018.1700622.

[3] B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud computing for Internet of Things & sensing based applications," 2012. doi: 10.1109/ICSensT.2012.6461705.

[4] M. Khatu, N. Kaimal, P. Jadhav, and S. A. Rizvi, "Implementation of Internet of Things for Home Automation," *Int. J. Emerg. Eng. Res. Technol.*, 2015.

[5] W. Ben Daoud, M. S. Obaidat, A. Meddeb-Makhlouf, F. Zarai, and K. F. Hsiao, "TACRM: trust access control and resource management mechanism in fog computing," *Human-centric Comput. Inf. Sci.*, 2019, doi: 10.1186/s13673-019-0188-3.

[6] A. Taherkordi, F. Eliassen, M. McDonald, and G. Horn, "Context-driven and real-time provisioning of data-centric IoT services in the cloud," *ACM Trans. Internet Technol.*, 2018, doi: 10.1145/3151006.

[7] D. R. Bestak and D. S. Smys, "BIG DATA ANALYTICS FOR SMART CLOUD-FOG BASED APPLICATIONS," *J. Trends Comput. Sci. Smart Technol.*, 2019, doi: 10.36548/jtcsst.2019.2.001.

[8] H. B. Mahajan and A. Badarla, "Detecting http vulnerabilities in iot-based precision farming connected with cloud environment using artificial intelligence," *Int. J. Adv. Sci. Technol.*, 2020.

[9] N. Jayakumar and D. P. Joshi, "Big Data & Disruptive Computing Platforms Braced Internet of Things: Facets & Trends," in *Studies in Systems, Decision and Control*, 2020. doi: 10.1007/978-3-030-39047-1_6.

[10] N. Agrawal, "Dynamic load balancing assisted optimized access control mechanism

for Edge-Fog-Cloud network in Internet of Things environment," *Concurr. Comput. Pract. Exp.*, 2021, doi: 10.1002/cpe.6440.

[11] S. Alnefaie, S. Alshehri, and A. Cherif, "A survey on access control in IoT: Models, architectures and research opportunities," *Int. J. Secur. Networks*, 2021, doi: 10.1504/IJSN.2021.112837.

[12] M. M. Eyada, W. Saber, M. M. El Genidy, and F. Amer, "Performance Evaluation of IoT Data Management Using MongoDB Versus MySQL Databases in Different Cloud Environments," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3002164.

[13] J. L. Amarnath, P. G. Shah, H. Chandramouli, and S. Arun Kumar, "Trustworthy cloud services for IoT security: Triple integration of security, privacy and reputation," *Int. J. Eng. Adv. Technol.*, 2019, doi: 10.35940/ijeat.F9536.088619.

CHAPTER 24

WIRED LOCAL NETWORK ATTACKS AND THEIR COUNTERMEASURES

Ramesh Chandra Tripathi, Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.
Email Id: - rctripathig@gmail.com

ABSTRACT:

Networking equipment not only enables users to create strong local networks but also shields their conversations, data, and networks from unauthorized access. Yet, because internal assaults might be disastrous for users, it is crucial to pay extra attention to security inside local networks. If it is accepted that all efforts and resources should be directed on safeguarding users from outside intrusions, internal security may be neglected. Such assumption is risky because it may encourage internal network device misconfiguration, resulting in a network infrastructure with suboptimal settings. In order to improve quality of service (QoS), performance, scalability, and, of course, to bolster security for network access and communications, network devices are becoming more sophisticated. These gadgets don't only enable users to create strong local area networks (LANs), while also safeguarding their connections, data, and themselves against unauthorized intrusions.

KEYWORDS:

Wired Local Network, LANAttacks, NetworkDevices, Security, Quality of Service.

INTRODUCTION

Those in charge of communications may create sophisticated topologies to satisfy complicated needs for connections and data flows by incorporating highly controllable devices into local networks. Yet, the ability to configure extensive feature sets may result in the omission of valuable or even fundamental functionality. Moreover, having so many configuration choices might be intimidating, leading one to concentrate on selecting just a limited number of fundamental functions. For networks with little needs, a simple design could be considered sufficient, but local protection is a factor that shouldn't be overlooked. Local networks include personal computers, shared resources, and many data flows. With the extensive usage of cloud computing and the Internet of Things, for instance, these data flows may include important information. It is essential to secure all of these components from outside attackers, either with robust firewalls or encryption. But, if you just worry about exterior security, you could forget about internal network security. Protection for local networks is especially essential because they often include a variety of attack vectors that may be quickly used by attackers with access to the local infrastructure and because it is not always feasible to trust all of the internal users of a local network. Hence, disobeying LAN protection might have disastrous consequences [1], [2].

Attacks coming from local networks aim to gain access to vital resources, collect sensitive data like passwords, or even block services. In contrast to hub-connected networks or networks built on simple switches, where access may be even easier, installing network equipment like programmable switches and routers may add security layers.Network devices might thus pose a hazard in addition to having low productivity when not used. These devices are often sent from manufacturers with a set of preset configurations intended to simplify the

plugging and starting of the network infrastructure. These configurations might weaken security and compromise the network. To get over a network's protections, an attacker just has to investigate the default settings of the network devices and exploit their weaknesses.

The default settings of newly introduced network devices should be checked and tested by administrators and users before they are actually deployed. It is also essential to comprehend suitable network device settings, their capabilities, and their advantages as well as any threats that may occur inside LANs.

The goal of this chapter is to provide an overview of the most prevalent and harmful LAN attack vectors that exploit network architecture settings. The theoretical underpinnings of each assault will be discussed, and then real-world examples will explain how each attack will affect the network and how it will behave under it.Real-world difficulties and a thorough understanding of what is occurring on various components of the network architecture allow for the consolidation of knowledge via the use of practical network scenarios. The use of practical scenarios for exploring these concepts requires a complex approach because advanced network devices are not always affordable and creating a variety of real topologies takes a lot of time. This is because the resources (primarily physical network devices) can be limited when dealing with these challenges.

To solve these problems, you may be able to depend on certain software, however. Simulators and emulators for networks provide dependable tools for creating virtual network infrastructures and thoroughly investigating the communications and interactions of their components. A network emulator that provides a wide range of options for the development of virtual network infrastructures is GNS3. A variety of scenarios may be created to evaluate the impact of LAN assaults in a secure setting by constructing various topologies.The ideas behind the mitigation approaches as well as the benefits and drawbacks of using the countermeasure will be explained in order to complete each simulation's set of countermeasures for each assault.

It is crucial to remember that not every assault countermeasure is best suited for a certain infrastructure. Certain countermeasures interfere with the networks' general abilities, such as their scalability, adaptability, or performance. There isn't a universally appropriate response to every assault. Administrators need to talk about which protection best satisfies their network's needs.Local Network Security Flaws: The best way to compromise private communications is via local network assaults. Due to their simplicity and ease of configuration, LAN wired technologies like Ethernet are well-liked, but this simplicity comes at a cost; functionality and self-configuration are prioritised over security, leading to the emergence of vulnerabilities that can be exploited through attack vectors [3], [4].

DISCUSSION

Security considerations were largely ignored in the design of network protocols in favour of functionality, scalability, and efficiency. Nonetheless, the ongoing growth of communications and data flows (and their value) has facilitated the creation of attackers motivated by the desire to steal sensitive data. An intrusive party with access to a wired LAN that was improperly setup might obtain important data, block local services, and even breach legitimately connected personal PCs.The idea that all efforts and resources should be directed towards safeguarding users from outside intrusions is risky because it might encourage the development of shoddy security configurations on internal network devices and delegate all infrastructure defence to border firewalls. Thus external security is essential, but network managers must also have other concerns.Switching from hub-connected Ethernet networks to switched Ethernet networks may increase overall security by giving each host its own dedicated segment and minimising the shared segments that hubs and other devices like them caused. Switches, however, do not provide a complete defence for wired networks; if

improperly designed, they can create extra openings for vulnerabilities. In-depth setup may be overshadowed by the simplicity of network device deployment and its immediate operation [5], [6].

Advanced administrators are not the only ones who need to be knowledgeable about network security; everybody in charge of a network infrastructure, regardless of its size, should be aware of how their devices are configured with security in mind. Because of this, it's crucial to educate users as well as administrators on security ideas. To prevent the most serious security concerns, it is crucial to comprehend vulnerabilities, attack methods, and their effects.LAN attacks use a variety of techniques to corrupt communications, but they mostly exploit how network protocols perform as designed, particularly at the link layer (the second layer of the OSI model). ARP and DHCP poisoning, Man in the Middle (MITM), session hijacking, resource exhaustion, VLAN hopping, and many more attacks are straightforward, risky, and common ways to compromise Ethernet segments, according to earlier LAN security assessments.

Additional resources include Cisco certifications like CCNA (Cisco Certified Network Associate), which demonstrate many attack vectors that may be used on LANs and evaluate a variety of associate-level topics in computer networking domains including routing, switching, wireless, among others.In order to compile a list with a realistic approach of the most serious wired LAN vulnerabilities and security solutions, these resources were consulted in the selection of the most critical LAN security situations and replicated them using network emulators.

Emulators and Network Simulators

As they have been launched, network emulators and simulators provide a training option by removing the need to buy actual resources, which are likely to be expensive. The fundamental difference between simulators and emulators is how they duplicate the behaviour of the target; on the one hand, simulators model and implement this behaviour so that it is accessible in a virtual environment, while on the other On the other hand, emulators allow a host system to run the binary images of another system, causing it to behave precisely as the original would in any situation.Depending on simulation software gives flexibility in exploring various topologies. These tools accurately mimic genuine hardware, with the devices' behaviour being almost identical to that seen in real-world situations. One of the most important advantages of simulating network scenarios is that it makes it easier and more intuitive to monitor the network. Users can easily capture and inspect the transmitted packets through the various links between devices by controlling all the devices through a single tool, giving them a complete and detailed view of the infrastructure and its connections. By thoroughly understanding how data flows behave under various conditions, this feature makes debugging more obvious.

There are some drawbacks, though. It's important to remember that performance and some attractive features of the virtual infrastructure may be constrained by the machine in which the network devices are being simulated. This is true even though network simulators offer the functionalities to generate complex topologies. Nevertheless, the main disadvantage is that not all features and behaviours may be incorporated in the simulation software, which may lead to misunderstandings about the ideas represented in the simulations.Network emulators, on the other hand, provide all the advantages outlined above but rely on actual operating system (OS) images, enabling the emulation of the target hardware features on a different independent hardware platform. As the functionality of the devices is only limited by the characteristics of their OS image, these capabilities make the mimicked situations more realistic.

For simulating and mimicking network devices and creating topologies using them, there are several technologies available. But, GNS3 and Cisco Packet Tracer, a network simulator, are two technologies that stand out (a network emulator).A command-line interface level simulation programme called Cisco Packet Tracer (CPT) was created by Cisco Systems as a component of their Networking Academy. Users of CPT may create virtual network topologies and study them, as well as their data flows, using a graphical user interface. Nevertheless, they only have a few characteristics, which limits their capabilities.

Moreover, GNS3 is a network simulator that offers a setting with nearly no restrictions on the capabilities of the devices. Users need authentic Cisco Internetwork Operating System (IOS) images in order to simulate the devices. Each command or argument that the chosen Cisco IOS provides is supported by GNS3. Moreover, GNS3 supports virtualization using programmes like VMware or VirtualBox and connections to networks of hosts running various operating systems.It has already been used to train people in computer networking domains using real-world examples. Considering the esoteric and highly theoretical notions behind computer networking, it is conceivable that practical techniques are required in order to fully comprehend this topic. Network simulators and emulators provide secure settings for investigating and experiencing the operation of network protocols and the behaviour of the devices making up the infrastructure under various circumstances.

It has been shown to be useful to encourage knowledge learning about computer networking to use simulation tools like Cisco Packet Tracer or emulation tools like GNS3. Because of this, these tools may be considered helpful not only for introducing network security and vulnerability ideas but also for increasing awareness of the risks associated with local network misconfigurations and for assembling information about the security of wired LANs.

Local Network Assaults

This section includes a number of real-world situations with various objectives. These topologies allow for the detailed exploration of various attack vectors and the solutions or mitigation techniques for them.

Device Security

Every network infrastructure starts with network devices. They may be controlled and tailored to meet various needs. These devices are sent with factory default settings, which are often sufficient to launch a usable network infrastructure. Nevertheless, due to their potential to create security flaws, these default settings, which will be discussed throughout this chapter, are not advised.Network administrators must get access to the equipment and run the required commands to change the default settings of the devices to the appropriate configurations.Access to these devices has to be controlled in order to stop unauthorised users from changing the settings. Additionally, device settings should be hidden from reading; even though writing privileges were carefully protected, an attacker's access to the precise configuration of the network infrastructure opens up a world of opportunities because they can research vulnerabilities or security gaps in the current settings and then exploit them without having to change the network configuration. It is crucial to rely on stable device settings in terms of its access policy and privileges for these reasons. In the absence of this, an attacker may undermine the established network security policy.

This part provides some broad principles for hardening network equipment to prevent unauthorized access to these vital components. The following security measures provide a straightforward overview of what needs to be done to protect network devices; however, more sophisticated features like the AAA framework, monitoring, access control lists (ACLs), etc., are beyond the purview of this chapter and can be used to add additional security layers.Nevertheless, network devices provide the option of remote access, which is more

practical since it does not need a physical connection to the equipment. Regarding distant connections, there are a few things to keep in mind.

Telnet, which is often used as the default protocol for these connections, is by itself unsafe because to the absence of communication encryption. The device settings may be compromised if an attacker performed malicious activities such as sniffing network traffic. For this reason, encrypted connections through a more secure protocol, such SSH, should be used for remote connections.It is crucial to first create a pair of RSA keys before blocking non-SSH connections under VTY lines in order to use SSH as the protocol to carry out remote connections. Access control lists (ACLs) may also be created to provide more granular security along similar lines and prevent unauthorised hosts from ever attempting to join. In addition to taking the necessary steps to restrict access, network administrators should make sure that no connections to the devices are made via insecure protocols.A switch with the DAI function activated intercepts every ARP message sent over an untrusted port and checks the validity of the MAC/IP communication. The switch makes use of a DHCP snooping database to verify these correspondences. ACLs may also be used to confirm these correspondences, however DHCP snooping is advised. After the ip dhcp snooping feature has been enabled, the port where the genuine DHCP server is connected has to be marked as "trusted."

The attacker is no longer able to use ARP spoofing techniques to poison the devices' ARP tables after activating the DHCP snooping and ARP inspection features (marking all ports as untrusted to ensure frame validation before forwarding them), as the switch is rejecting any untrusted packet (i.e., any packet with a MAC/IP correspondence not stored in the DHCP snooping binding database).Flooding MAC Attacks: ARP responses may be manufactured and transmitted for free, as was previously mentioned. This creates a new attack vector aimed against layer two device overflow. These devices always have a full CAM table due to the rapid pace at which they flood the network with bogus ARP responses.

Depending on how the attack is implemented, switches may respond in one of two ways. On the one hand, genuine frames would be discarded if the switch's CAM table was full since it would be unable to map any further MAC/IP traffic. The denial-of-service attack that results from the CAM table overflow prevents authorised users from sending their messages. On the other hand, the MAC flooding assault may cause switches to engage in yet another risky activity.The attacker uses the macof utility to create fake messages with fake MAC addresses in order to overrun the switch's CAM table. A successful assault would fill this table with data until there was no more room. The switch would start operating like a hub, passing every Ethernet frame across every port and losing its segmentation capabilities as a result of the assault, as was already explained.

Virtual Local Area Networks: By creating virtual networks on top of the actual infrastructure, virtual local area networks are a helpful way of increasing the level of segmentation in a local area network (LAN). As each VLAN will function as a separate LAN logically, configuring VLANs is seen to be a solid security practise. An attacker in one VLAN, for instance, would be unable to launch an MITM assault on hosts linked to another VLAN.Trunk ports provide cost savings when it comes to the ports utilised for connecting switches. All of the specified VLANs' traffic will pass via a single port after a trunk port has been established. Switches use the IEEE 802.1Q protocol to determine which VLAN each data packet belongs to.Nevertheless, there is a hazardous Cisco default option for trunk ports that can enable an intrusion to gain a trunk port if they have access to a malicious switch, having the ability to receive all traffic from all VLANs, therefore avoiding the VLAN security layer. Switches may automatically negotiate trunk ports between two switches thanks to the dynamic trunk protocol. Network administrators may achieve this by configuring a port's functioning mode

with various settings. Based on these variables, the negotiation may transform a port into a trunk port automatically when a switch detects another switch. It contains the connection between the working mode variables stated. an attacker with access to a local switch may modify the switch's operating mode such that the distant switch port automatically switches to operating as a trunk port.

It is possible to link switches that do not support the 802.1Q protocol with switches that do using the native VLAN, which is the VLAN used for trunk ports. It is not necessary to tag the native VLAN with the appropriate VLAN identity as a result. Some switches include native VLAN settings that designate VLAN 1 as the default VLAN to which all of the switch's ports belong. As the double-tagging attack may be used, this vulnerability can be used by an attacker. The network attacks that were addressed mostly targeted wired LAN weaknesses. These assaults are regarded as one of the most efficient ways to breach communications or steal information. As was shown, there are a number of simple yet effective ways to attack LAN vulnerabilities.When network devices are not properly configured, LAN vulnerabilities may be quickly exploited. It is crucial to depend on deployable devices, but their security settings must not be disregarded in favour of immediate functioning. The part on links is the one in this chapter that covers the most security flaws and vulnerabilities. Attacks on the link layer take use of low-level weaknesses and provide attackers the chance to take advantage of this level's flaws, which serves as the foundation for more sophisticated assaults. Because of this, link layer protection is key, and it's important to understand how default configurations might jeopardize this fundamental layer of the protocol stack.

Attacks based on the ARP protocol, for instance, may contaminate devices' ARP tables and trick them into believing fictitious MAC/IP address correspondences in order to carry out MITM attacks and steal sensitive data as a result. Layer-2 devices may be made responsible for stopping these types of attacks by setting features like Dynamic ARP Inspection, relieving upper layer devices (such legal hosts) of this duty. Almost all layers are susceptible to flooding assaults. Without restricting some of the network capabilities, it is impossible to prevent these assaults, which aim to cause a denial of services (as seen in the UDP flooding countermeasures, where it is necessary to establish a traffic limit rate to avoid the DoS attack). Network performance may also be hampered by packet filtering since it requires each packet to be examined before it is processed.

The DHCP starvation and rogue approaches have been handled at the application level. At this level, there are more exposed apps, yet DHCP is a crucial network function. As they are not set with a genuine IP address, if the hosts are hacked, they may be kept down until the service is restored. As previously mentioned, an attacker might use this circumstance to launch DoS attacks or set up a phoney DHCP server to forge network data. Via the scenarios, it has been able to see that the chosen network assaults are concentrated on either rejecting communications (using various MITM attack methods, for example) or intercepting them (DoS attacks). Nowadays, information is a valuable resource for businesses, organisations, and, of course, everyday people. The rewards for a successful assault include passwords, files, personal information, etc. Because of this, hackers try to intercept conversations by forging real addresses, poisoning device network information, and other techniques [7], [8].

By properly setting the network devices, the countermeasures presented throughout this chapter assist to thwart these assaults. Security measures do, however, have a price. Not all countermeasures complied with the defined network standards. As was evident in the previous situations, some of these setups, such as creating static IP/MAC addresses correspondence, might result in a lack of flexibility in the network architecture. In light of the appropriate security level, it is vital to set these measures. Certain network infrastructures require stronger security barriers because they are less concerned with flexibility and

performance, and the opposite is also true. Before beginning to configure the devices, it is essential to comprehend the controlled network architecture and its function.

It has been feasible to have a wide and realistic understanding of the effects that these assaults may have by exposing these vulnerabilities via real-world situations. Cisco equipment were employed in the chapter's chosen scenarios. Several of these gadgets rely on certain features. The scenarios' content may, however, be easily extrapolated to other networking operating systems. The network administrators must be knowledgeable of their unique infrastructure and the factory defaults of their individual devices in order to operate appropriately. The attacks that have been outlined are only a tiny sample of the wired LAN's possible weaknesses. To maintain a network infrastructure secure, it is crucial to have a broad grasp of network vulnerabilities and to stay up to date on emerging attack vectors [9]–[11].

CONCLUSION

A number of network attacks have been shown using virtualized environments and GNS3 emulation software settings. Each network administrator must be aware of how attackers exploit the network architecture, and end users must likewise grasp this in order to avoid compromised activities. By Administrators may mimic attacks by acting as the attacker using network emulators, giving them a valuable tool to test security rules before they are implemented. The most common and harmful network assaults have been covered in this chapter, grouped according to the OSI model. The emulation environment (GNS3) has offered a secure and practical context in which to freely perform and comprehend the prior attacks and vulnerabilities, as well as to demonstrate how these attacks can be avoided or mitigated by configuring the network device settings with the appropriate parameters.

REFERENCES

[1] A. Vázquez-Ingelmo, M. Moreno-Montero, and F. J. García-Peñalvo, “Threats behind default configurations of network devices: Wired local network attacks and their countermeasures,” in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2019. doi: 10.1007/978-3-030-22277-2_6.

[2] A. Sarihi, A. Patooghy, A. Khalid, M. Hasanzadeh, M. Said, and A. H. A. Badawy, “A Survey on the Security of Wired, Wireless, and 3D Network-on-Chips,” *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3100540.

[3] Suroto, “Wlan security: Threats and countermeasures,” *Int. J. Informatics Vis.*, 2018, doi: 10.30630/joiv.2.4.133.

[4] T. M. Alghamdi, “Throughput Analysis of IEEE WLAN ‘802.11 ac’ Under WEP, WPA, and WPA2 Security Protocols,” *Talal Mohammed Alghamdi Int. J. Comput. Networks*, 2019.

[5] Y. Xu, G. Chen, J. Ford, and F. Makedon, “Detecting wormhole attacks in wireless sensor networks,” 2008. doi: 10.51452/kazatu.2020.4(107).130.

[6] Y. Liu, S. Hu, and T. Y. Ho, “Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks,” 2015. doi: 10.1109/ICCAD.2014.7001350.

[7] Y. Xu, G. Chen, J. Ford, and F. Makedon, “Detecting wormhole attacks in wireless sensor networks,” 2007. doi: 10.1007/978-0-387-75462-8_19.

[8] G. Klein, H. Rogge, F. Schneider, J. Toelle, M. Jahnke, and S. Karsch, “Response initiation in distributed intrusion response systems for tactical MANETs,” 2010. doi: 10.1109/EC2ND.2010.11.

[9] D. Nagamalai, B. C. Dhinakaran, P. Sasikala, S. H. Lee, and J. K. Lee, "Security threats and countermeasures in WLAN," 2005. doi: 10.1007/11599593_13.

[10] O. N. Odhiambo, E. Biermann, and G. Noel, "An integrated security model for WLAN," 2009. doi: 10.1109/AFRCON.2009.5308183.

[11] C. Barnes *et al.*, "Wireless Security Countermeasures," in *Hackproofing Your Wireless Network*, 2002. doi: 10.1016/b978-192899459-6/50025-3.

CHAPTER 25

AN ASSESSMENT OF UNDERWATERWIRELESSSENSORNETWORKS

Gulista Khan, Associate Professor,
College of Computing Science and Information Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.
Email Id: - gulista.khan@gmail.com

ABSTRACT:

The basic introduction to underwater wireless sensor networks (UWSNs) and the comprehensive introduction to underwater wireless sensor networks are both provided in this chapter. We outline the fundamental problems and many applications that pertain to UWSNs. The discussion of the distinctions between terrestrial WSNs and UWSNs is provided in this chapter. Afterwards, we go through the various tasks performed by sensor nodes and the deployment architecture of UWSNs. We go into detail on the variables that have an impact on both the UWSNs' communication architecture and design. As a subset of wireless sensor networks, underwater wireless sensor networks (UWSNs) are used to explore a variety of topics, including marine life, climate change, natural catastrophes, and many more. In order to detect changes, sensor nodes are placed in shallow or deep water. These nodes then relay those changes to the sink nodes. To make these applications practical, underwater equipment must be able to communicate effectively with one another.

KEYWORDS:

UWSN, Emulation,SensorNode, Security,WirelessSensorNetworks(WSNs).

INTRODUCTION

Wireless sensor networks are made up of a large number of resource-constrained sensor nodes and one or more base stations (WSNs). Only sensor networks are to blame for the transformation in several areas of business and research. Many more applications, including industrial (machine surveillance), underwater, structural monitoring, habitat monitoring of microorganisms, intelligent buildings, facility management, disaster relief operations, medical and health care, agriculture, and many more, are beginning to use sensor nodes. Sensor nodes keep track of nearby surroundings or objects and relay any changes to the base station [1]–[3].Wireless sensor networks facilitate the detection and management of urgent circumstances. These networks enable a greater variety of application areas and actively pursue the development of new ones, but this is contingent upon a number of distinctive requirements, including service type, quality of service (QoS), fault tolerance, span time, scalability, flexibility, maintainability, and security. Several techniques, including as multihop wireless connection, energy-efficient operations, auto configuration, data-centric, localization, cooperation, and in-network processing, have been developed to realise these distinctive needs.

Mobile ad hoc NETworks and wireless sensor networks are distinct from one another (MANETs). An ad hoc network, which lacks infrastructure, is created to meet a particular application demand. MANET is an ad hoc network comprising wireless communications in a multihop topology and mobile sensor nodes. WSNs are used for the kinds of applications where travelling to the deployment site would be inconvenient. The network will last as long as the sensor node does. When a node in a WSN runs out of power or malfunctions for any other reason, it is very challenging to replace the battery or recharge it in such a hostile

environment. Yet, in MANETs, a terminal's big or strong battery might provide it more energy. WSNs may work together to accomplish a variety of tasks, including computing, sensing, and communication. This network can accommodate various network densities (sparse and dense deployment of the sensor nodes). Nevertheless, MANETs are unable to manage this level of network deployment variety. WSNs may aid in managing and controlling in the critical scenario by handling the rapid changes in the observation, from inactivity to high activity, with ease. Although MANETs are used to manage situations involving a certain kind of traffic through a channel in a clearly defined way. WSNs enable the network to scale from hundreds to thousands or more nodes. Nevertheless, it is challenging in the case of MANETs. Both mobile ad hoc networks and wireless sensor networks often exhibit self-configuration. Yet, WSNs closely adhere to the self-configuration feature because of the network's appropriate connection and maintenance of the energy trade-offs. The protocols of WSNs are data-centric, but those of MANETs are not since this network does not employ redundant deployment. The movement of the sensor nodes in WSNs is what gives them their mobility in accordance with the particular needs of the application. Two scenarios exist in WSNs where the sensor node may be mobile. When the sink node is mobile in the first instance, and when a node may be utilised to detect and feel an incursion within the network and it is necessary to sound the alarm or send a message to the base station in the second. Yet, MANETs allow for the dynamic movement of sensor nodes from one location to another [4]–[6].

Wireless Sensor Networks Underwater

UWSNs have a number of difficulties, including constrained bandwidth, increased propagation time, insufficient battery life, high bit error rates, and others. Due to sensor node battery life and acoustic signal transfer, these networks are more susceptible to failure.Three different kinds of sensor nodes may be used in underwater wireless sensor networks: semi-static, mobile, and static nodes. Anchored to the pier, buoys, or ocean floor are static sensor nodes. Semi-static sensor nodes are used for short-term monitoring, such as a few hours or days. These nodes are temporarily positioned by the ship and hung with the buoys. Energy is a major constraint on the deployment of sensor nodes that are static or semi-static. Vehicles including autonomous underwater vehicles (AUVs), remotely operated vehicles (ROVs), and other underwater vehicles are connected to mobile sensor nodes. The flexibility of sensor nodes allows for maximum underwater coverage, but it creates issues with network connection and node localisation. The energy shortage is less severe on sensor nodes attached to AUVs. To track changes over a specific region, sensor nodes in underwater networks are placed.

Sensor network deployment in an underwater environment is influenced by network density, sensor node coverage, and sensor node quantity. In the case of underwater networks, deployment should be sparse, have sufficient connection range, and use fewer nodes.The design of UWSNs faces certain significant obstacles, including as constrained battery power and bandwidth, channel impairment from fading and multipath, high propagation latency, high bit error rate, and sensor susceptibility to fouling and corrosion. The following are a few drawbacks of underwater communication. More storage is required when data must be buffered for a long time (before being dropped).If the sink node does not receive any messages from other nodes or the base station, it periodically broadcasts an inquiry message. The issue of power usage is brought up by the frequent sending of inquiry messages.

UWSN Applications

Sensor node deployment is based on the applications. To adapt to changes in the marine environment, UWSNs should be self-organizing and self-configurable. These qualities aid in carrying out group surveillance duties across a certain region. These sections examine several

uses for wireless underwater sensor networks. Environment monitoring, exploration monitoring, disaster detection and prevention, underwater navigation, tactical surveillance, mine reconnaissance, and ocean sampling are among the uses of UWSNs.

i. Environment Monitoring: Pollution, currents, winds, biological changes, marine life of microorganisms, and fishes are monitored using underwater wireless sensor networks. Understanding climate change and how it affects marine and coastal life is aided by this. Also, it offers details on how human activities affect the undersea habitat. It aids in the forecasting of changes in water quality and their impact on people and aquatic life.

ii. Exploration Monitoring: Underwater wireless sensor networks may be used to monitor and identify oilfields and reservoirs. It may aid in the search for precious minerals in the ocean or sea.

iii. Disaster Detection and Prevention: Sensor nodes may offer data on tsunamis or earthquakes by estimating seismic activity. This knowledge helps in averting significant losses.

iv. Undersea navigation: Sensor nodes aid in the recognition of rocks, drowning collapse dangers, dock location, and sandbank detection in shallow water.

v. Tactical Surveillance: Wireless underwater sensor networks may be utilised for surveillance, reconnaissance, and incursion detection. It can aid in the detection of submarines, frigates, short-distance vehicles, and autonomous underwater vehicles (AUVs).

vi. Mine Reconnaissance: With the use of autonomous underwater vehicles, sensor nodes may assist in the identification of change on the seabed and mine-like items.

Ocean sampling: We can learn about the unique marine environment with the use of underwater wireless sensor networks.

UWSN Simulation Tools

In order to verify a defined mechanism, the implementation of the testbed for UWSNs requires the whole network architecture and communication channels. We will go into great depth on the simulation and emulation tools that are readily accessible in UWSNs in this section. A testbed is created using a simulator, an analytical tool, to validate the planned mechanism. In order to comprehend how the planned mechanism works, simulation and emulation are crucial, according to the unique uses of UWSNs. Emulators are also used to check and validate the planned protocol without actually deploying the network, whereas simulators are used for testing and validating software or testing in real-time scenarios.

SUNSET is a tool for UWSN analysis that combines simulation, emulation, and real-time testing. Due to the real-time scheduling feature, it is more adaptable and effective. It works with several sensor nodes and five acoustic modems. This SUNSET includes an interference model, debug module, packet conversion module, and utility module. Timing module is used to offer information about packet transmission delay. The gap between the simulation and the real outcome is reduced thanks to this simulation tool.

DESERT, which was created using the NS-Miracle framework, stands for DEsign, Simulate, Emulate, and Realize Testbeds. By supporting the application layer and transport layer via the bottom layer of the protocol stack, this tool is used to develop cross-layer protocols. It has a module that supports movement. Two application layer modules that control traffic flow are uwcbr and uwvbr. Two modules of the transport layer, uwudp and uwtcp, are in charge of

multiplexing and demultiplexing as well as providing error and flow control. On the network layer, three routing protocols are described. On the data link layer, there are six MAC protocols available. In trials, it does not, however, provide superior outcomes.

SUNRISE is built on the NS-Miracle framework and is meant to perceive, monitor, and act on UWSNs. Scalability and data analysis are made possible by it. It aids in keeping underwater sound communication secure and private. Nevertheless, the battery limitation affects underwater robot applications.

A framework for remote control in UWSNs is called Records. Multichip network connection makes it feasible to transmit distant commands. Only static UWSNs are intended for use.A simulation tool for protocol stack architecture is called AQUA-NET. For embedded systems, it functions. It makes cross-layered architecture more optimized.AQUA-3D is a capable animator that can effectively examine the trace data in UWSNs. Nodes, events, and other objects are well visualised. There is a lower likelihood that UWSNs will work with numerous simulators.

Hardware that runs several modems simultaneously is supported by SEALINX. It offers cross-layer communication in a flexible manner. It does not support network layer protocols that are customised.The open-source simulator AQUA-SIM is based on NS-2. Aqua-Sim manages the packet collision and propagation model. For UWSNs, it offers flexibility and integrity.AQUA-NET MATE is a simulator with a virtual channel modem that facilitates underwater network acoustic communication. It offers protocol stack layers and real-time functionalities.NS-2 is an open source simulation tool that aids in the modelling of many protocols and supports discrete events. It makes it possible to create, test, and validate new protocols. It has been aided by network animator (NAM) to show the mobility of the nodes and the medium's connection. Occasionally, the NS-2's findings are not as accurate as those from other simulators, such as OPNET, OMNET, and many more.AUV modelling is supported by the underwater sensor network simulator UWSIM. It effectively handles UWSNs' key difficulties, such as their constrained bandwidth, frequency, energy resources, and storage capacity.

DISCUSSION

In acoustic communication, AQUA-GLOMOSIM mimics the network and physical layer protocols. The improved version of Aqua-Glomo is called Aqua-Glomosim. The sensor nodes' mobility is supported by it.AQUA-TOOLS is a toolbox for under-water communication operations at the channel and physical layer. Protocols at the physical layer, data connection layer, network layer, and energy limitations are all handled.World Ocean Simulation System is known as WOSS. For the purposes of simulating the effects of propagation in audio communication, Bellhop ray tracing is used. It includes a comprehensive database of global environmental characteristics. It replicates the intricate process of a sparsely deployed network.The 3-d deployment of the acoustic communication network is made possible by USNet, a programme for simulating underwater sensors. This simulation programme works with threads that can handle a lot of tasks simultaneously. It mimics the sensor networks' hierarchical structure.QUAL-NET is a highly effective simulation tool that makes simulation easier by analysing, designing, and evaluating the communication structure in any kind of network. QualNet Architect (a tool for visualisation), QualNet Analyzer (a statistical tool for network performance analysis), QualNet Packet Tracer (an analyzer for packet tracing), QualNet File Editor, and QualNet Command-line Interface are its five constituent parts. It facilitates localisation of the sensor nodes and parallel processing. It features an internal model of random waypoint mobility. Due to the modelling of auditory communication's features and channel qualities, UWSNs are challenging to replicate in QualNet.

An all-inclusive protocol stack is supported by the UWSN simulator AQUA-TUNE. It doesn't need the battery to be recharged and can run a testbed for up to 70 hours.UANT, an underwater acoustic networking simulator, models the shift in the acoustic channel. It solely addresses the physical layer and the data connection layer. It operates well in acoustic conditions under the surface. TinyOS and TOSSIM were used in its design.OPNET, which stands for optimum network engineering tool, is a simulation tool that may be used in industrial applications. For both 32-bit and 64-bit systems, it enables wireless communication with scalability and customizable wireless communication with graphical user interface (GUI). It allows for the data flow to be captured and seen.SAMON uses intelligent control to emulate unmanned vehicles. It serves as a testbed for mobile network simulation in ocean sampling. It operates effectively, allowing for a close match between the results of real-time testing and simulation. Because of its high price, it cannot be utilised for educational purposes.The AUWCN is a simulation tool for underwater acoustic channels and networks that operates at the physical layer to verify established protocols. To replicate the physical channel in audio communication, Bellhop ray tracing is used. It supports the sensor node's mobility and employs a variety of effects, including the Doppler Effect, attenuation, and shadow zones.

UWSN Secure Communication

Because to its distinct features, secure communication has recently been an active area of study in UWSNs. For the support of UWSNs, a protocol stack has been designed thataids in comprehending their singularity and unique properties. The five levels of the UWSN protocol stack are the same as those found in terrestrial WSNs: the Physical layer, Data link layer, Network layer, Transport layer, and Application layer. The physical layer is in charge of frequency selection, carrier frequency production, signal detection, modulation, and data encryption. Data multiplexing, frame detection, medium access control, error detection, and network connection are all responsibilities of the data link layer. The network layer is in charge of the data-centric approach and cost-effective, energy-efficient data routing. Controlling channel congestion, ensuring reliable communication, and ensuring correct data flow are all responsibilities of the transport layer. The many applications produced on the basis of sensing tasks are handled by the application layer.

The layer of the protocol stack has been related with several management planes. These planes include quality of service (QoS) management, security management, mobility management, task management, and power management. The sensor node's functioning is managed by the power management plane to keep the node's energy level constant while ensuring the lowest possible power usage. The mobility management plane is in charge of identifying and controlling the sensor nodes' movement, which aids in maintaining data routing to the sink. The task management plane schedules the sensing jobs of the sensor nodes, and the observation is carried out by the sensor nodes with more residual energy, while the remaining nodes are focused on data routing and aggregation. Error control, performance optimization, and fault tolerance are all responsibilities of the QoS management layer. Access control, authentication, authorisation, integrity, confidentiality, and other topics are covered under security management [7]–[9].

Because to their extensive deployment and dispersed configuration, UWSNs are vulnerable to many security assaults. Attacks on network protocols and sensor nodes are both possible targets. Attacks on sensor nodes are less likely due of its limited deployment and it is extremely difficult to capture or hack numerous nodes in UWSNs. Protocol attacks may be damaging at several stages of the network architecture.

The whole communication network may be compromised by these assaults. In addition, we'll go through safe communication guidelines for UWSNs.In this part, we will quickly go through each layer of the protocol stack's operation and outline potential security flaws at each tier

Active Research Questions

UWSNs are susceptible to several security threats, including jamming, wormhole, Sybil, and others, as mentioned in Section 6. Many UWSN security measures have been presented in order to protect the network. The underwater sensor nodes' movement is not taken into account by the security system's architecture. Six criteria are used to create the protocols: technique, assaults, node mobility, energy, results, and obstacles. The energy consumption, high communication costs, and computational overheads associated with UWSNs are caused by their particular properties. The following specifications must to be taken into account while building an effective and secure communication protocol:

i. Security: In communication, security is the main priority. The attacker shouldn't alter the sent data in any way. It makes sure that only authorised users should get the sent data. The developed protocol maintains the secrecy and integrity of the data since UWSNs are a data-centric network. Two valid network entities should communicate with one another.

ii. Robustness: In the event of any assaults, the network provides appropriate connection and functionality. It should simultaneously successfully identify the intruder node or make an effort to remove it from the network.

iii. Energy Efficiency: The network's lifespan is equal to the lifespan of each sensor node. The node's battery determines how long it will last. With good communication between mobile nodes, the energy-efficient communication protocol prolongs the network's lifespan.

iv. Lightweight Protocol: Because of their limited energy, memory, storage, and transmission bandwidth, UWSNs struggle. The intended protocol shouldn't be reliant on software or hardware.

CONCLUSION

An overview of wireless sensor networks and an in-depth introduction to underwater wireless sensor networks are provided in this chapter. We spoke about the key difficulties in building UWSNs as well as the distinction between terrestrial WSNs and UWSNs. We discussed the UWSNs' deployment architectures. For UWSNs, each layer's secure communication protocols and the protocol stack have been thoroughly described. For the UWSNs, the simulation and emulation tools have been correctly specified. The major goal of this chapter is to motivate researchers to create innovative, secure, and effective communication methods for use in underwater environments. Understanding UWSNs will be made easier with the aid of this chapter.

REFERENCES

[1] S. Sweta and B. Maram, “Underwater wireless sensor networks,” *Int. J. Informatics Vis.*, 2018, doi: 10.30630/joiv.2.1.99.

[2] G. Han, J. Jiang, L. Shu, Y. Xu, and F. Wang, “Localization algorithms of underwater wireless sensor networks: A survey,” *Sensors*. 2012. doi: 10.3390/s120202026.

[3] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors (Switzerland)*. 2018. doi: 10.3390/s18113907.

[4] H. Chang, J. Feng, and C. Duan, "Reinforcement learning-based data forwarding in underwater wireless sensor networks with passive mobility," *Sensors (Switzerland)*, 2019, doi: 10.3390/s19020256.

[5] B. Ahmad, W. Jian, R. N. Enam, and A. Abbas, "Classification of DoS Attacks in Smart Underwater Wireless Sensor Network," *Wirel. Pers. Commun.*, 2021, doi: 10.1007/s11277-019-06765-5.

[6] J. Luo, Y. Chen, M. Wu, and Y. Yang, "A Survey of Routing Protocols for Underwater Wireless Sensor Networks," *IEEE Communications Surveys and Tutorials*. 2021. doi: 10.1109/COMST.2020.3048190.

[7] X. Wei, Y. Liu, S. Gao, X. Wang, and H. Yue, "An RNN-Based Delay-Guaranteed Monitoring Framework in Underwater Wireless Sensor Networks," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2899916.

[8] F. Al-Salti, N. Alzeidi, and K. Day, "Localization schemes for underwater wireless sensor networks: Survey," *Int. J. Comput. Networks Commun.*, 2020, doi: 10.5121/ijcnc.2020.12307.

[9] S. Fattah, A. Gani, I. Ahmedy, M. Y. I. Idris, and I. A. T. Hashem, "A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges," *Sensors (Switzerland)*, 2020, doi: 10.3390/s20185393.