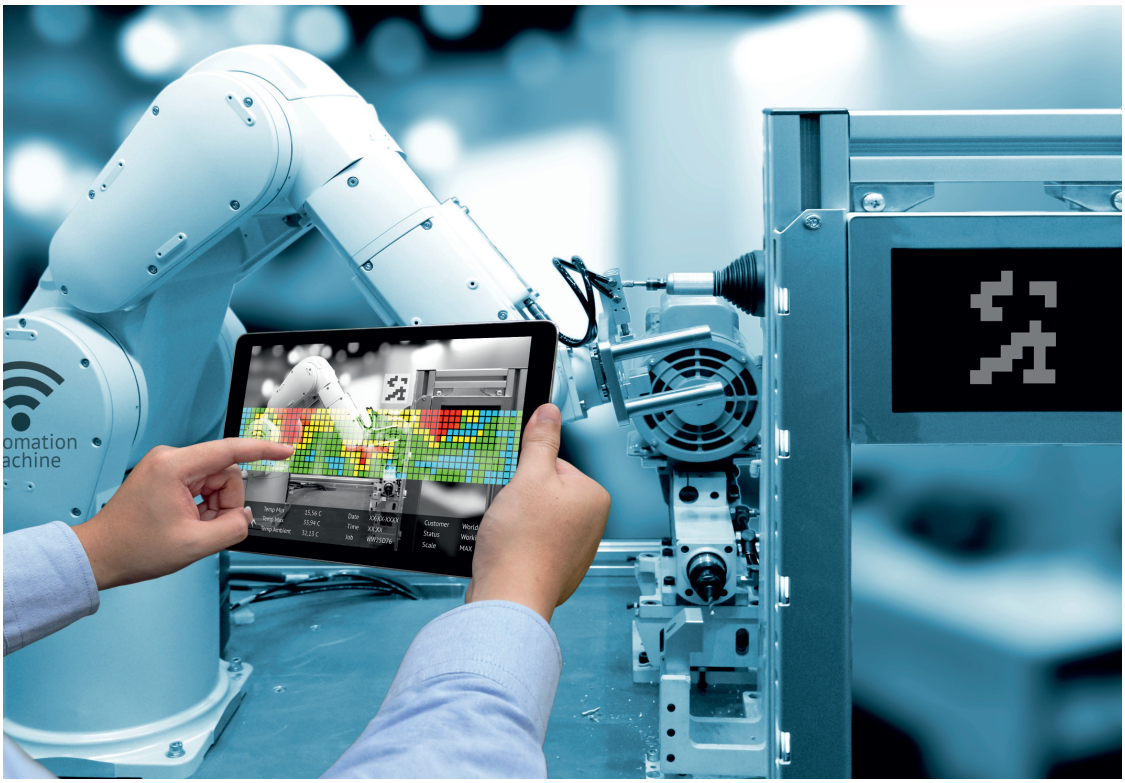
ADVANCES OF IOT

Dr. Divya Rani
Dr. Rajbhadur Singh



ALEXIS PRESS
JERSEY CITY, USA

ADVANCES OF IOT

ADVANCES OF IOT

Dr. Divya Rani

Dr. Rajbhadur Singh

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.

Advances of IoT by *Dr. Divya Rani, Dr. Rajbhadur Singh*

ISBN 978-1-64532-870-4

CONTENTS

CHAPTER 1

AN ELABORATION OF THE ARCHITECTURE OF THE INTERNET OF THINGS

Dr. Divya Rani, Associate Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- divyarani@presidencyuniversity.in

ABSTRACT

The network of physical "things" that are integrated with sensors, software, and other technologies for something like the purpose of communicating and sharing data with other devices and systems through the internet is referred to as the Internet of Things (IoT). These gadgets include anything from common domestic items to high-tech industrial gear. The Internet of Things is discussed in this paper. The integration of various technologies and communication systems is the primary enabling aspect of this promising paradigm. The most relevant technologies are those for identification and tracking, wired and wireless sensor and actuator networks, improved communication protocols, and distributed intelligence for smart things. As one can readily anticipate, any significant contribution to the growth of the Internet of Things must inevitably be the outcome of collaborative efforts made in a variety of academic disciplines, including telecommunications, information science, electronics, and social sciences. In light of the complexity of the situation, this survey is intended for individuals who want to learn more about this profession and support its development. The Internet of Things paradigm will be informed by it in the future, and the supporting technologies will be examined. What becomes clear is that the scientific community still faces challenging problems. The most important ones are covered in depth.

KEYWORDS: Devices, IoT, Internet,Sensor Nodes, Smart Homes, Wireless Networks.

INTRODUCTION

The notion of the Internet as the "Internet of Computers" as a worldwide network with services delivered as the "world wide web" constructed on top of the original platform could be realized in the early 1990s thanks to the development of new technology and new creativity. As Web 2.0 has evolved, the idea of an "Internet of computers" has given way to an "Internet of people," in which billions of people are linked through various social media platforms. With the combination of Micro Electro Mechanical Devices (MEMs) and wireless communication technologies, the limitations of the Internet are expanding each day. Devices are also growing smaller compared to the original PC while having higher processing and storage possibilities. Mobile phones, notebooks, tablets, and other electronic devices all make use of these technologies. The sensing, calculating, and connecting capabilities of these devices may be increased when they are outfitted with sensors in addition to actuators via the network connection [1].

The "Internet of Everything" is defined by Cisco as bringing together people, processes, data, and everything to transform information into action and increase the relevance and importance of networked connections. Over the next 10 years, the Internet of Things has the potential to provide $1.9 trillion in value to cities worldwide. The International Telecommunications Union

(ITU) predicted that the "Internet of Things" will link all of the world's things in a sensory and cognitive way in a 2005 study. The ITU has defined four aspects of the Internet of Things (IoT): item identification, sensors and wireless sensor networks, embedded systems, and nanotechnology. IoT is defined generally and does not apply to just one field, making its definition ambiguous. As a last point, it may be described as the mix of smart gadgets providing a massive amount of data while interfacing with other devices, things, and surroundings. These data may be transformed into practical activities that provide objects control over and command and improve quality of life and Figure 1 lists the IoT parts.

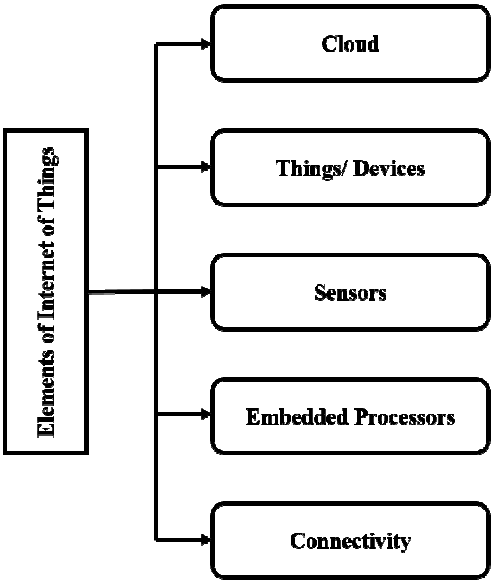


Figure 1: Represented the Different Elements of IoT.

Elements of IoT

The elements of IoT can be grouped into three categories: Hardware, Middleware, and Presentation [2]:

i. Hardware

Sensors, actuators, and embedded systems are the three key hardware elements that are fundamental to the Internet of Things.

ii. Middle Ware

The on-demand storage and processing tools for data analytics are implied by middleware technology. This is a software element or a group of related layers that sits between the engineering and application levels. The principal objective is to conceal the specifics of various technical sophistication while enabling the programmer to unilaterally create a certain IoT-enabled application.

iii. Presentation

Since it includes human engagement with the environment, visualization is crucial in IoT systems. Therefore, visualization must be easy to comprehend, and interpretation tools must work across a wide range of platforms. It must be simple to utilize for a variety of purposes. This section discusses certain enabling technologies that can put this same aforementioned component

into action. The idea of smart homes, smart environments, smart cities, and a smart nation using smart gadgets can only be realized via effective IoT deployment.

Technologies Involved in IoT

i. Wireless Sensor Networks

a. WSN Hardware:

In areas where standard infrastructure-based networks are almost unworkable, wireless sensor networks (WSN) provide a new paradigm of real-time embedded systems and have numerous potential applications in our everyday lives. The primary sensor node, which only automatically sends to the actuator controllers if internet access is available, is made up of a transceiver, a tiny embedded CPU, a power supply, operational capabilities, and very little storage. The architectural element of a sensor node is shown in Figure 1. When receiving data from sensor nodes, the actuator often has more computation and processing capability along with longer battery life. Then it takes activity to alter how the physical worlds behave. Although the actuator can provide more battery life than the sensor nodes, both the sensor nodes and actuators have bandwidth and energy source restrictions. Typically, surveillance and tracking are the two basic categories into which WSN applications fall. In both the public and private sectors, several monitoring and tracking systems are in use. WSN is crucial to the Internet of Things (IoT) sensing operations [3].

b. WSN Protocol Layer:

To create a network for any kind of application, Sensor Nodes are often installed at random and in an ad hoc way with a wireless connection. In WSN operations, communication between the sensor nodes and ultimately to the sink node is crucial. In developing a sensor network architecture, routing, and MAC protocols are thus crucial. The energy use of each node has a serious influence on the network's lifespan. Node failures and the ensuing decline in network performance are exceedingly regular occurrences. Therefore, the three-tier architecture at the sink node must be able to connect to the Internet and interact with the outside world.

c. Secure Data Aggregation/Fusion:

To monitor the occurrences, sensor networks are often used in hostile settings. The sensor nodes exchange sensor data, which is then transferred to centralized and decentralized systems for analysis. Failures of nodes occur often in wireless sensor networks. However, each node's ability to self-organize keeps the network activity for a longer period. So, to increase the network lifespan, a reliable data collection system is needed. Security is a crucial problem for the dependable transmission of data to the sink node at the same time. There are a lot of suggested cryptographic methods in the literature. However, the majority of the methods, regretfully, rely on public key cryptography. Private Key algorithms may be created in the future to preserve the security and privacy of data [4].

d. WSN Middleware Technology:

A system that unifies service-oriented architecture, sensor networks, and cyber infrastructure and makes its rapid deployment available to all heterogeneous sensor applications. For the development of sensor applications, a platform-independent technology, such as open sensor web architecture (OSA), is necessary [5].

ii. RFID Communication:

RFID uses electromagnetic and electrostatic coupling on the Radio Frequency (RF) component of electromagnetic waves, which were first employed for identifying stationary objects like people, animals, and stationary objects like stationary objects. A cheap and its successor organization, EPC worldwide, was established in an auto-ID center of MIT and may be used in the Internet of Things to identify billions of items. The outcome of these efforts is the adoption of RFID in the supplier relationships of retailers like Wall Mart and Metro. The development of RFID and related infrastructural technologies has made it very difficult for merchants to see the IoT in action. RFID has been the primary technique for designing microchips for wireless data interaction throughout the years as embedded communication has developed technologically. Both the cost and standards have improved with passive RFID. RFID is being utilized to handle apparel items, tools in factories and other businesses, books in libraries, and other goods in addition to supply chains. The tag may also be used for radio frequency identification (RFID) or quick response codes to identify physical things (QR). Active RFID readers can initiate the conversation and have a battery of their own. Among the many uses, active RFID tags are mostly used in port containers for cargo monitoring [6].

iii. IP Protocol:

Every device or network node in the internet of things of the future must utilize the Network protocols and have an IP address. By giving all of the smart things IP addresses, IPv6 will play a crucial role. Everything may be handled employing Internet services and apps at any time, from any location. However, there is currently no clear understanding of how to classify IPv6 effectively, allowing for the subdivision and public distribution of public IP numbers [7].

iv. Things on the Web:

The World Wide Web (www) is conceptually a cornerstone of the IoT since it is a vast infrastructure of intelligent items. The phrase "web of things" has recently been used in association with web 2.0 technologies that employ asynchronously JavaScript and XML, as well as the HTTP protocol (Ajax). As embedded processors in the Internet of Things (IoT) use fewer resources than conventional web clients, using Ajax in web 2.0 minimizes communications time and costs efficiently between the server and client. For instance, a PC or mobile phone's browser and its services are normally addressed by URLs and administered through a straightforward interface. While web 2.0 is a collaborative two-way communication system, web 1.0 is a one-way passive communication network that solely offers read-only materials.

Users may take an active role on the internet through podcasting, blogging, tagging, social bookmarking, and other approaches. Additionally, web 3.0 is rapidly approaching. Web 3.0 uses a virtual mall as one example. It is the concept of a semantic web, where data is organized methodically and understood by both computers and people. Many believe it to be the result of combining semantic internet technology with artificial intelligence. Web 3.0 employs semantic web technologies, decentralized databases, machine learning, natural language processing, and other methodologies to create a common framework for integrating data from many sources. The user may use a website to travel to a virtual marketplace, where they can explore the shelves or shops, choose what they want, and then pay for it. The IoT must be practically implemented in the web 4.0 vision [8].

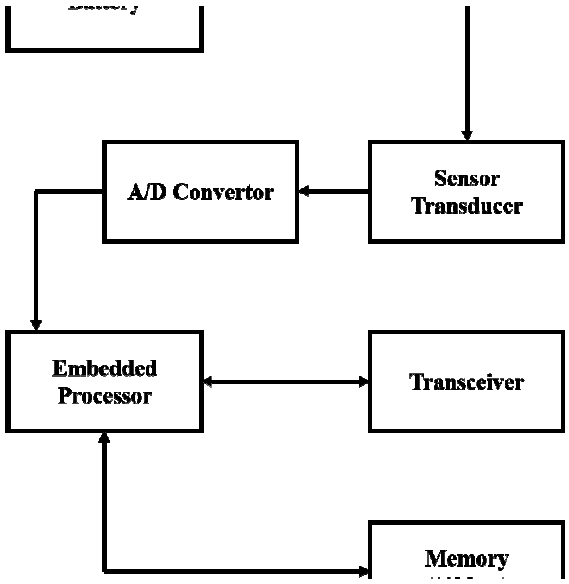


Figure 2: Represented the Architectural Components of a Sensor Node.

The Internet of Things (IoT) is the interconnection of physical items with electronics built into its design to enable communication and the detection of interactions between them or with the natural atmosphere. IoT-based technology will provide higher levels of services in the future years, effectively altering how individuals go about their everyday lives [9]. Just a few industries where IoT is well established include enhancements in medicine, power, gene treatments, agriculture, smart cities, and smart homes. In other words, the Internet of Things (IoT) is a network of linked computer devices that were already implanted in commonplace items and allow them to transmit and receive messages [10]. As of right presently, there are more than 9 billion "Things" (physical devices) linked to the Internet. This figure is expected to exceed a staggering 20 billion shortly. The main components used in IoT are mentioned below [11]:

i. Low-power Embedded Systems:

Maximum performance and low battery usage are opposed criteria that are crucial when manufacturing electrical devices.

ii. Sensors:

The main component of all IoT applications is a detector. It is a physical apparatus that measures and recognizes specific physical quantities and transfers them into signals that may be supplied with provided inputs to processing or control units for analytical purposes. There are numerous kinds of sensors in use, some of which are listed below:

1. Temperature Sensors
2. Image Sensors
3. Gyro Sensors
4. Obstacle Sensors
5. RF Sensor
6. IR Sensor

7. MQ-02/05 Gas Sensor
8. LDR Sensor
9. Ultrasonic Distance Sensor

iii. Control Units:

It is a compact computer component that consists of a microprocessor, or processing core, reminiscence, and programmable input/output devices, or peripherals, on an individual integrated circuit. It performs all systematic reasoning and handles the bulk of the operations for IoT devices.

iv. Cloud Computing:

Massive quantities of information are gathered by IoT devices, and this data has to be kept on a trustworthy storage server. Cloud computing is advantageous in this situation. Since the information has been gathered and learned from, it is now easier for us to identify fundamental problems like electrical problems as well as mistakes.

v. Availability of Big Data:

We are aware that the Internet of Things largely utilizes sensors, particularly in real time. The use of these technological devices will lead to a large influx of big data as they become progressively prevalent among all industries.

vi. Networking Connection:

In a world where each physical thing is characterized by an IP address, internet access is essential for communicating. According to the IP name, there are, nevertheless, a limited amount of addresses accessible. This naming mechanism will no longer be workable due to the increasing number of devices. To represent each actual thing, investigators are thus searching for an appropriate naming scheme. There are two ways of building IoT:

1. Establish a distinct network with solely physical things.
2. Expand the Internet even further, but doing so needs cutting-edge technology like tenacious cloud computing and quick huge data storage (expensive).

IoT will expand in reach and grow more complicated in the not-too-distant future. In terms of "anytime, anywhere, anything in a connection," it will alter the globe.

IoT Enablers [12]:

1. **RFIDs:** Employs radio waves to monitor the tags that are connected to each physical item electronically.
2. **Sensors:** Instruments that can detect changes in the environment (ex: motion detectors).
3. **Nanotechnology:** These are, as their name indicates, very tiny devices, often with sizes under a hundred nanometres.

S. Villamil et al. illustrated that most processes and devices today use the internet of things, an emerging technology that has the potential to improve people's quality of life by making it easier to access certain information and services. The main goal of this paper is to provide a broad overview of the internet of things employing data from recently published papers. The analysis of the most important recent publications and the variety of internet of things technology

applications that's what give this paper its added value. The internet of things technology stands out as a facilitator in commercial and industrial performance, but more pressingly in improving the quality of life, as a result of the analysis of the current literature. The internet of things is a tool that can solve the difficulties associated with security, computing power, and data mobility, provided that the development of other technologies proceeds as predicted [13].

Internet of Things in this paper and the integration of various technologies and communications solutions is the primary enabling factor of this encouraging paradigm. The most pertinent applications are distributed intelligence for smart things, wired and wireless sensors, actuator networks, upgraded modulation schemes shared with the Next Generation Internet, and identification and tracking technologies. Any significant advancements in the Internet of Things, as one can easily imagine, must necessarily be the result of synergistic efforts made in a wide range of disciplines, including telecommunications, informatics, electronics, and social science. This questionnaire is designed for people who want to learn more about this complicated discipline and help shape it in light of the current complicated topic. A variety of Internet of Things paradigms are reported, and supporting technologies are reviewed. What becomes clear is that the scientific community will continue to confront pressing concerns. Those that are the most important are discussed in greater depth [14].

The Internet of Things (IoT) has received a lot of research attention recently. IoT is viewed as a component of the future Internet and will include billions of intelligent, talkative "things." A heterogeneously connected network of devices will make up the Internet of the future, further extending the boundary lines of the globe with both real and virtual elements. The connected things will gain new capabilities thanks to the Internet of Things (IoT). The concepts, architecture, underlying technology, and applications of IoT are methodically examined in this study. First, several definitions of IoT are introduced. Next, emerging techniques for IoT implementation are discussed. Third, some open aspects associated with IoT applications are explored. Finally, the principal challenges that the research community needs to address are researched, along with potential solutions [15].

A cutting-edge blockchain-based architecture throughout the Internet of Things (IoT) framework for the educational system may be an alluring way to improve information dissemination for all users of the 5G network. The primary subject of study in wireless networking could have been how to enable wireless communication. When the Internet first started, it was established by downloading web pages to establish relationships between computers. Furthermore, it seems that there are high-speed, intelligent, powerful networks with a variety of modern technologies, such as low power consumption, etc., that may link to one another in the modern world. IoT features on physical objects are permitted to store and handle Blockchain and IoT data at any time. Developing a fresh virtualization foundation based on blockchain across the Internet of Things architecture is one of the challenging issues in the field of mobile communications. The purpose of this study is to determine the connection between a recent study for a Blockchain-based education sector and the internet of things as well as maintaining cryptographically safe data online. An effective online interaction system between students, teacher educators, employers, developers, coordinators, recruiters, and accreditors is accomplished by this research's improved blockchain and IoT.

DISCUSSION

The concept of combining computers, sensors, and networks to monitor and control devices in human life has been around for decades. The recent confluence of today's dominant and cutting-edge technologies and market needs is ushering in a new virtual platform for the "Internet of Things". In today's human era, IoT is all set to make a place in a revolutionary and security-connected world. With the presence of this technology, a relationship will be established between various objects and the environment and people also get more strongly connected with this relationship. The idea that there will eventually be a vast array of Internet-connected objects could fundamentally alter how people view being "online." Despite the potential significance, this vision may face several obstacles, particularly those relating to security, privacy, information sharing, and standards, as well as legal, regulatory, and human rights concerns.

A wide assortment of stakeholders must take into account a complicated and constantly changing collection of technological, social, and policy elements when it comes to the Internet of Things. The Internet of Things is here now, and it must be taken into account to achieve maximum advantages and reduce its risks. Because it represents a developing component of how individuals and organizations are likely to utilize and integrate Internet and network connection into their personal, social, and economic lives, the Internet Society is concerned with the IoT. Engaging in a divisive debate that contrasts the promises of IoT with its perceived attacks will not lead to solutions to maximize the benefits of IoT while minimizing risks. Instead, educated communication, conversation, and engagement among several stakeholders will be required to devise the most productive course of action.

A critical requirement of an IoT is that the things in the network must be interconnected. IoT system architecture must guarantee the operations of IoT, which bridges the gap between the physical and the virtual worlds. The design of IoT architecture involves many factors such as networking, communication, business models and processes, and security. In designing the architecture of IoT, the extensibility, scalability, and interoperability among heterogeneous devices and their business models should be taken into consideration. Because things may move geographically and need to interact with others in real-time mode, IoT architecture should be adaptive to make devices interact with other things dynamically and support unambiguous communication of events. In addition, IoT should possess a decentralized and heterogeneous nature. In IoT, service-oriented architecture (SOA) might be imperative for the service providers and users. SoA ensures interoperability among heterogeneous devices in multiple ways. Figure 3 provides a generic SoA, which consists of four layers with distinguished functionalities as below:

- Sensing Layer is integrated with available hardware objects to sense the statuses of things;
- The network Layer is the infrastructure to support wireless or wired connections among things;
- The service Layer is to create and manages services required by users or applications;
- Interfaces Layer consists of the interaction methods with users or applications.

The SoA treats a complex system as a set of well-defined simple objects or subsystems. Those objects or subsystems can be reused and maintained individually; therefore, the software and hardware components in an IoT can be reused and upgraded efficiently. Due to these advantages, SoA has been widely applied as a mainstream architecture for wireless sensor networks. When

SoA is applied in IoT, it is designed to provide extensibility, scalability, modularity, and interoperability among heterogeneous things; in addition, the functionalities and capabilities are abstracted into a common set of services. Figure 3 provides an example of SoA proposed for IoT, and the details of its components are discussed below:

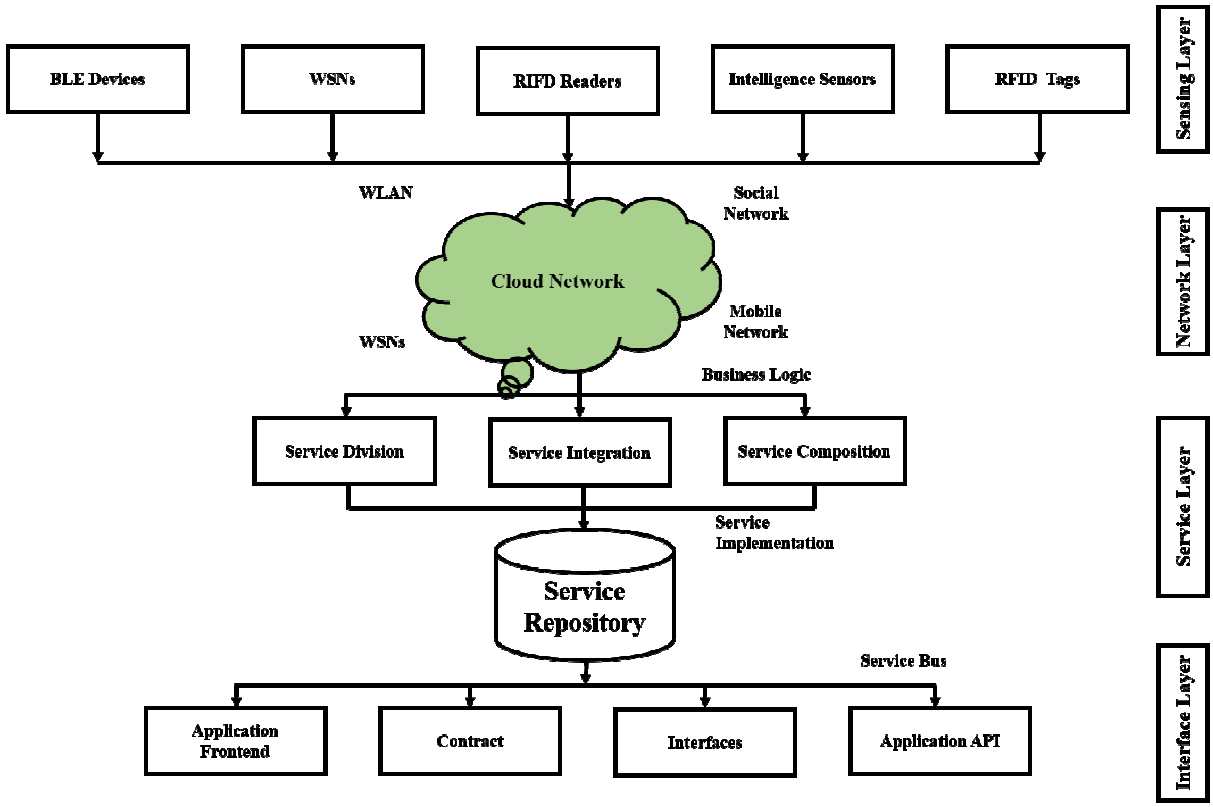


Figure 3: Represented the Service-oriented architecture for IoT.

IoT is expected to be a worldwide physical inner-connected network, in which things are connected seamlessly and can be controlled remotely. In the sensing layer, the smart systems on tags or sensors can automatically sense the environment and exchange data among devices. In the past few years, advanced sensing and communication technologies made things with RFID or sensors more versatile and accessible, which extends the capability of IoT significantly in the sense that things can be uniquely identified and the surrounding environments can be monitored for various purposes and applications. Every object in IoT holds a digital identity and can be easily tracked in the digital domain. The technique of assigning a unique identity to an object is called a universal unique identifier (UUID). In particular, UUID is critical to successful service deployment in a huge network like IoT. The identifiers might refer to names and addresses.

In determining the sensing layer of an IoT, the following aspects should be taken into consideration:

i. Cost, Size, Resource, and Energy Consumption

The items may have sensing components like RFID tags or sensor nodes. Intelligent devices need to be made with the least amount of resources and money possible since complicated system applications need a lot of sensors.

ii. Deployment

Depending on the needs of the applications, the deployment of the sensing objects may be one-time, gradual, or random.

iii. Heterogeneity

The Internet of Devices (IoT) may be quite diverse due to a range of things with various characteristics.

iv. Communication

For objects to be retrievable and accessible, sensors must be able to communicate.

v. Network

The networks are set up as multi-hop, mesh, or ad hoc systems.

As the scale of IoT increases, a large number of hardware and software components can be involved; therefore, IoT should also possess the following features:

i. Energy Efficiency

Sensors should be active all the time to acquire real-time data. This brings the challenge to supply power to sensors; high energy efficiency allows sensors to work for a longer period without the discontinuity of service.

ii. Protocols

Different things existing in IoT provide multiple functions of systems. IoT must support the coexistence of different communications such as WLAN, ZigBee, and Bluetooth.

From the perspective of hardware design, the main issues of hardware design are wireless identifiable systems, ultra-low cost tags, and smart/mobile sensors as mentioned in Figure 4.

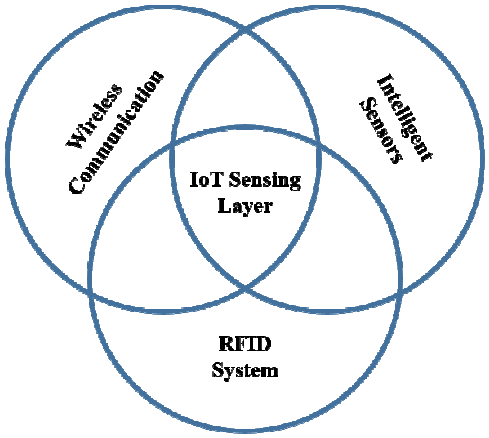


Figure 4: Represented the Functions of the sensing layer in IoT.

CONCLUSION

The Internet has changed drastically the way humans live, moving interactions between people at a virtual level in several contexts spanning from professional life to social relationships. The IoT has the potential to add a new dimension to this process by enabling communications with and among smart objects, thus

leading to the vision of ‘‘anytime, anywhere, any media, anything” communications. To this purpose, we observe that the IoT should be considered as part of the overall Internet of the future, which is likely to be dramatically different from the Internet we use today. It is clear that the current Internet paradigm, which supports and has been built around host-to-host communications, is now a limiting factor for the current use of the Internet. It has become clear that the Internet is mostly used for the publishing and retrieving of information regardless of the host which such information is published or retrieved from and therefore, information should be the focus of communication and networking solutions. This leads to the concept of data-centric networks, which has been investigated only recently.

According to such a concept, data and related queries are self-addressable and self-routable. In this perspective, the current trend, which we have highlighted, of assigning an IPv6 address to each IoT element to make it possible to reach them from any other node of the network, looks more suitable for the traditional Internet paradigm. Therefore, the Internet evolution may require a change in the above trend. Another interesting paradigm that is emerging in the Internet of the Future context is the so-called Web Squared, which is an evolution of Web 2.0. It is aimed at integrating web and sensing technologies to enrich the content provided to users. This is obtained by taking into account the information about the user context collected by the sensors deployed in the user terminals. From this perspective, serve that Web Squared can be considered as one of the applications running over the IoT like the Web is today an important application running over the Internet. In this paper, the author has surveyed the most important aspects of the IoT with emphasis on what is being done and what issues require further research. Indeed, current technologies make the IoT concept feasible but do not fit well with the scalability and efficiency requirements they will face. The author believes that, given the interest shown by industries in IoT applications, in the next years addressing such issues will be a powerful driving factor for networking and communication research in both industrial and academic laboratories.

REFERENCES

[1] P. P. Ray, “A survey on Internet of Things architectures,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.

[2] B. (Kevin) Chae, “The evolution of the Internet of Things (IoT): A computational text analysis,” *Telecomm. Policy*, 2019, doi: 10.1016/j.telpol.2019.101848.

[3] J. Virkki, “Reliability of WSN Hardware,” *Int. J. Embed. Syst. Appl.*, vol. 1, no. 2, pp. 139–10, Dec. 2011, doi: 10.5121/ijesa.2011.1201.

[4] P. Zhang, J. Wang, K. Guo, F. Wu, and G. Min, “Multi-functional secure data aggregation schemes for WSNs,” *Ad Hoc Networks*, 2018, doi: 10.1016/j.adhoc.2017.11.004.

[5] J. Hwang and H. Yoe, “Study on the context-aware middleware for ubiquitous greenhouses using wireless sensor networks,” *Sensors*, 2011, doi: 10.3390/s110504539.

[6] K. Singh *et al.*, “Localization of Life Safety Vests in an Aircraft Using Backscattering RFID Communication,” *IEEE J. Radio Freq. Identif.*, 2020, doi: 10.1109/JRFID.2020.3005248.

[7] A. Tyagi, “TCP/IP Protocol Suite,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, 2020, doi: 10.32628/cseit206420.

[8] B. Negash, T. Westerlund, and H. Tenhunen, “Towards an interoperable Internet of Things through a web of virtual things at the Fog layer,” *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2018.07.053.

[9] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*. 2019. doi: 10.1109/ACCESS.2019.2924045.

[10] N. H. Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of things (IoT) and the energy sector," *Energies*. 2020. doi: 10.3390/en13020494.

[11] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of internet of things in healthcare: a systematic literature review and classification," *Univers. Access Inf. Soc.*, vol. 18, no. 4, pp. 837–869, Nov. 2019, doi: 10.1007/s10209-018-0618-4.

[12] D. Henriques, R. F. Pereira, R. Almeida, and M. Mira da Silva, "IT governance enablers in relation to IoT implementation: a systematic literature review," *Digit. Policy, Regul. Gov.*, vol. 22, no. 1, pp. 32–49, Dec. 2019, doi: 10.1108/DPRG-02-2019-0013.

[13] S. Villamil, C. Hernández, and G. Tarazona, "An overview of internet of things," *Telkomnika (Telecommunication Comput. Electron. Control.*, 2020, doi: 10.12928/TELKOMNIKA.v18i5.15911.

[14] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[15] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, 2015, doi: 10.1007/s10796-014-9492-7.

CHAPTER 2

MODERN APPROACHES OF IOT FOR CYBER SECURITY

Ms. Renuka Bhagwat, Assistant Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- renuka@presidencyuniversity.in

ABSTRACT

The Internet of Things (IoT) as a business enabler has developed into a standardized set of use cases solving pressing operational issues that deliver operational and economic benefits across many industries, including healthcare, retail, financial services, utilities, public transit, and manufacturing, despite being relatively new as a cybersecurity discipline. IoT cyber-attacks are nothing new, but as IoT becomes even more pervasive in our daily lives and communities, it becomes more important than ever to take cyber protection seriously. As a consequence, there is a genuine need to protect IoT, which has led to a need for profound comprehension of vulnerabilities to and attacks against IoT infrastructure. In addition to analyzing and characterizing attackers and intrusions against IoT equipment and services, this paper attempts to categories different challenge categories.This paper discusses IoT devices and their application and also discusses possible cyber-attacks on different IoT environments then the prevention and recommended steps are discussed to avoid damage caused by various attacks. In future, this paper will separate the proper information about IoT and its threat.

KEYWORDS: Cyber-security, Cyber-Attack, IoT, Information Technology, IoT Devices, IoT Services.

INTRODUCTION

Technology is developing quickly these days and has a huge impact on our lives. Everywhere has easy access to the internet. Around us, there are several internet-connected gadgets, including computers, laptops, connected devices, cellphones, etc. The Internet of Things (IoT) [1] has gained more traction in recent years, and a variety of IoT-related application domains have been released on the market, including those for smart farming, traffic control, home automation, manufacturing governance, environmental monitoring, defense systems, and home automation. Many sensors, actuators, gateways, circuits, hardware, and routers connect among themselves using wired and wireless communication methods in a variety of Internet of Things applications. According to a Cisco white paper, more than 50 billion IoT devices will be connected to the internet by 2020.

Anything (IoT devices) can be connected using a variety of communication technologies, including radio frequencies identification, Zig-Bee, Bluetooth, Bluetooth Low Energy, wirelessfidelity, worldwide-interoperability for microwave access, wireless-personal area networks, near fieldcommunication, Ethernet cables, coaxialcable, mobile communication technology, and many more. These technologies depend on the infrastructure that is already in place, whether it is wired or wireless. Extensible messaging presence protocol, representational state transfer (RESTFUL) services, advanced message queuing protocol, restrained application protocol, message queuing wireless communication transport, multicast domain name system, domain name system service discovery (DNS-SD) [2], IPv6 over low-power wireless personal area networks (6LowPAN), internet protocol-version-4 (IPv4)/internet protocol-version-6 (IPv6),

routing protocol, data transmission domain name system, DNS-SD When these gadgets are close to us and transmit the data via a network, security is crucial. IoT gadgets are often applied in industries as well. As a result, it's crucial to take into account the possibility of cyber-attacks and vulnerability in the IoT ecosystem and to put the suggested precautions into operation.

Key Concepts and Interaction of IoT

IoT was defined in a variety of ways by several people and organizations. The idea of IoT is not new. Internet was also once used to link individuals, thus the term "the Internet of People." Before a few years ago, the government, academic institutions, and business areas did not have widespread access to the internet. Machine-to-machine connection, or M2M, was developed so that machines may interact with one another using wired or wireless technology to make choices together and complete tasks. Another name for it is Sensor Network. Since everyone can now access the internet for a cheap cost, the term "Internet of Things" refers to any IoT items (clouds, web servers, nodes, sensors, machines, and apps) that have a direct internet connection and transfer data to other objects through the internet. "Internet of Everything" was the moniker given by Cisco. It was given the moniker "World Size Web". The IoT idea was referred to as "Sky-net" in the Terminator movie [3].

The IoT is an extension of the Internet into the physical world for interaction with physical entities from the surroundings. Entities, devices and services are key concepts within the IoT domain, as depicted in Figure 1. They have different meanings and definitions among various projects. Therefore, it is necessary to have a good understanding of IoT entities, devices and services.

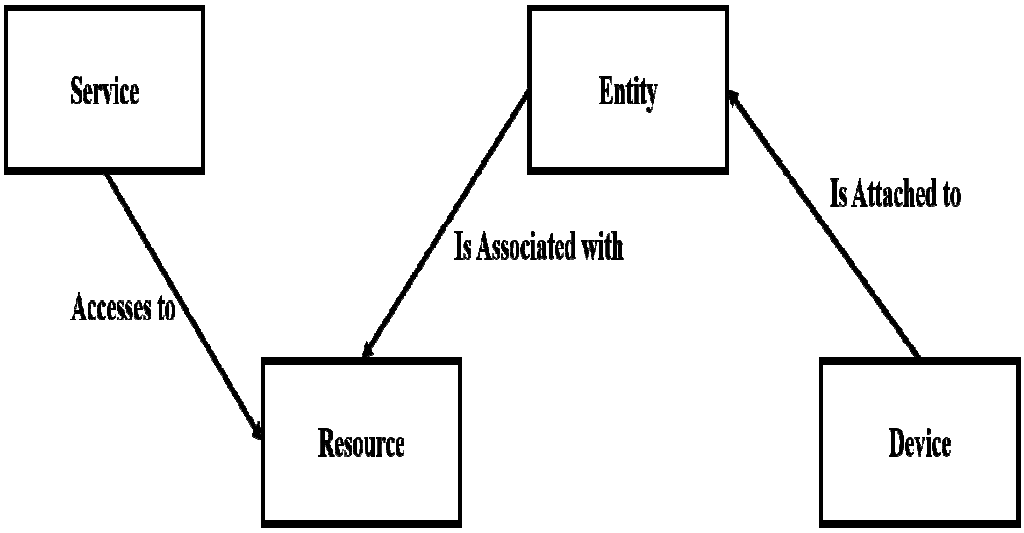


Figure 1: Represented the IoT Model: Key Concepts and Interactions.

An IoT entity might be a person, an animal, a vehicle, a member of a supply chain, an electronic device, or closed or open surroundings. Hardware elements known as devices, such as mobile phones, sensors, actuators, or RFID tags, which enable the entities to communicate with the digital world, make it feasible enable entities to communicate with one another. Machine-to-Machine (M2M) communication is the most widely used IoT application at the moment [4]. M2M is currently extensively used in power, aviation, retail, public service management, nutrition, water, oil, and other sectors to track and manage users, equipment, and manufacturing procedures in the worldwide market, among other things. M2M apps are predicted to have 12

billion connectivity by 2020 and produce 714 million dollars in revenue. In addition to all the advantages of IoT applications, several security risks are seen. For various reasons, interconnected equipment or gadgets are very desirable to cybercriminals.

i. Since the majority of IoT devices are abandoned by people, it is simple for an assailant to physically access them.

ii. The majority of Internet of Things (IoT) components operate through wireless networks, where an offender may eavesdrop and collect confidential details.

iii. The majority of Internet of Things (IoT) components lacking the power and processing resources required to support complicated security protocols.

Let's talk more about IoT-related topics now. Things are primarily classified as virtual and physical items in the information realm. Things may communicate with one another over a communication protocol and have distinct identities. Environmental threats, sensors, electrical and electronic devices, actuators, etc. are examples of physical things, while Twitter, Facebook, and other IoT apps are examples of virtual things that may be stored, processed, and retrieved [5].

Therefore, the Internet of Things (IoT) is a network of interconnected physical and virtual objects (devices, cars, buildings, and other items with electronics, software, sensors, network connectivity, etc.) that enables those certain objects to gather and exchange data following the description given in. As a result, the Internet of Things (IoT) is an ecosystem that uses various communication technologies to link processes and individuals with real or imagined things like sensors.

Many more individuals would participate in IoT by accessing IoT web/mobile apps including CRM systems, remote monitoring or repair, supply chain management, and position tracking. E.g.: In location tracking applications, GPS sensor nodes periodically send their location data to their configured servers, where it is processed and archived in databases. Mobile applications and web apps then offer user interfaces through which users can access this data and take the appropriate steps or decisions based on the needs of the application.

The authors claim that to safeguard user information and provide resistance against hostile acts, a smart home environment's security design principles and technologies should include security-enhancing technology. Additionally, argue that a gateway design is best suited to provide resource-constrained devices cyber security. They also conclude that only freshly created gadgets that will be included in a future smart house installation will be compatible with the solutions now available for the deployment of cyber defense in smart homes [5].

i. Security Frameworks

A plethora of competing security frameworks for smart homes have emerged to tackle the security attacks that threaten the privacy and safety of smart home residents. For instance present a traffic monitoring and inspection solution, called IoT-Guard. The authors utilize Bro IDS to detect abnormal behaviours in an IoT environment. The main drawback of their framework though is the requirement to forward all router's traffic to IoT Controller and link each IoT device with the IoT Watchdog to target and monitor particular IoT devices using device-specific IoT protocols. The IDS framework is based on Anomaly Behavior Analysis and tries to provide security for existing and hardly changeable smart home installations. Focus is given to measuring the activities of sensor devices installed in a smart house, and detecting any anomalies in the

quantity and quality of the collected measurements. The limitation of their work relies on the ability to apply their analysis only on primitive IoT devices without direct internet access. Where agents inside the smart home environment make observations and implement intended behavior.

This model requires minimal engagement by the user and it is focused on threat detection. However, it neglects the detection of vulnerable devices within the smart home. Furthermore, the reasoning process, namely the process of deciding what actions to perform to reach a goal, is taking place in the Cloud layer. Finally, the aforementioned framework was not tested against live data, i.e., operating in real-time. There, the authors propose a whitelist-based intrusion detection technique specific to IoT devices. The proposal aims to prevent IoT devices to get entangled in botnets activities, so it blocks at the gateway level DNS lookups to malicious sites. However, this solution is only applicable to IP-based IoT devices and networks. A network layer architecture is required for the protection of a smart home against external threats and the mitigation of attacks from compromised devices.

The authors recommend the implementation of a policy-based framework to restrict malicious traffic. The adopted policies will follow a white-listing approach based on the observed and predictable patterns in network traffic of the IoT devices. The main drawback of this proposal is that each different-purpose IoT device exhibits distinct patterns, requiring a monitoring period of the legitimate usage for each IoT device to construct its network pattern. Nevertheless, the work is in the preliminary stage and presents only considerations for designing novel security following a rule-based approach, where every IoT device is allowed a specific behaviour, namely a specific set of allowed connections, to fulfill its intended functionality [6].

The gateway enforces these rules with traffic filtering and anomaly detection techniques. An apparent drawback is the required definition of the communication rules, whereas in the case of the lack of which by the manufacturer or certification authority, should be provided by the end-users. A different approach where the authors propose a blockchain-based solution for decentralized security and privacy in a smart home environment. Specifically, they utilize a local and private blockchain to control and audit the communications internal and external to a smart home. This way an access control policy to the IoT devices and their data is enforced. However, the proposed mechanism exhibits a relatively large overhead regarding traffic, processing time and energy consumption, as it requires each smart home to be equipped with a high-resource miner for the administration of the blockchain.

ii. Emerging Advancements

Nowadays, the absence of IoT standards and the intrinsic complexity demand for proper security layers constitute the need for holistic IoT security solutions imperative. Apart from some notable exceptions, such as where the authors propose a methodology to validate and certify different technological solutions in large-scale conditions and where the cyber security aspect regarding the communication between IoT devices and external entities is addressed, there is still a long way until the total armor of the IoT. Several research papers, derived from the work done in various EU funded projects, exist in the literature mainly focusing on crucial aspects of the IoT domain, such as the interoperability in different IoT environments and for heterogeneous test beds, privacy in terms of authorization and sensitive information handling, codification and smart applications towards an open IoT ecosystem [7].

Nevertheless, there are numerous open issues for further discussion, with the most prominent one being security in IoT. GHOST project aims to close this security gap by providing a generic,

hardware-agnostic, security solution for smart home installations. It takes into account multiple different protocols and monitors the behaviour of all installed IoT devices along with the activity of the smart home gateway. The system automatically handles detected security events, while self-defending mechanisms have also been employed to ensure its normal operation. It requests user intervention only when this is required, while a lot of effort has been concentrated on the usability of the interfaces used for user interaction. Additionally, GHOST solution has been designed upon the restriction that it should be functional while running on limited hardware resources, an evident constraint for smart home gateways [8].

The developed algorithms are performance efficient and require minimal resources. In a few cases where additional hardware resources are required, a lot of attention has been given to preventing sensitive personal data of smart home inhabitants leave the gateway, and thus any privacy implications are eliminated. Finally, while blockchain technology has been employed, there is no requirement for significant hardware resources. A modular architecture has been implemented, that enables the blockchain-related components, to either connect to external blockchain nodes or run a local lightweight node inside the smart-home gateway.

DISCUSSION

IoT security and privacy threats have increased as a result of the IoT's exponential expansion. Many of these threats are caused by hardware flaws brought on by hacker cybercrime and inappropriate system resource use. The IoT must be designed in a manner that makes simple and secure use control possible. For consumers to fully benefit from the IoT and avoid privacy and confidentiality threats, they must have the competence to do so. As was previously said, the majority of IoT equipment and services are vulnerable to a variety of typical threats, including viruses and denial-of-service assaults. Simple precautions won't be enough to protect against this kind of dangers and address system weaknesses; instead, it's important to ensure ensuring policies are used smoothly and are backed by reliable protocols.

A detailed knowledge of a system's assets is necessary for the security development process, which is followed by the detection of potential threats and vulnerabilities. It is important to define the system assets and the threats they should be defended against. Assets were outlined in this study as all valuable items in the system, both physical and intangible, that need to be safeguarded. IoT assets in general include things like system hardware, software, data, and information, as well as things like service-related assets like service reputation. It has been shown that to allocate effective system mitigation resources, it is essential to understand the risks and system weaknesses. Additionally, being aware of prospective assaults helps system engineers decide where money should be allocated more wisely. The most well-known threats have been classified as DoS, physical assaults, and privacy attacks. In this research, three basic sorts of invaders individual assaults, organized groupings, and intelligence agencies were covered. Each sort of attacker has a varied risk tolerance, finance resources, skill set, and motive.

It is crucial to research the different categories of attack perpetrators and identify those that are most likely to target a system. It is simpler to understand which danger may take advantage of which cybersecurity vulnerabilities when all threats and their associated actors have been described and documented. Generally speaking, it is thought that IoT intruders have limited physical compromise power in addition to full DY intrusion capability. Assuming physical compromise attempts do not scale, they will, at worst, only have a minor impact on the whole population of IoT devices. Therefore, IoT architecture must be built to handle hacked devices

and be capable of identifying such situations. It is established that to accomplish their aims or objectives, attackers use a variety of tools, methods, and strategies to exploit vulnerabilities in a system. It's critical for an institution to comprehend the intentions and capabilities of prospective attackers to limit any harm. More research is required to close the information gaps about risks and cybercrime, offer the essential measures to minimize likely assaults and decrease both prospective threats and their effects.

CONCLUSION

In the near future, industrial IoT-based networks will expand rapidly. The primary difficulties in adopting IoT-based Big Data for cyber security are the detection of malware threats and software piracy. The author propose a hybrid deep learning-based strategy for malware and pirated content detection. First, a Tensor Flow neural network has been suggested to use software plagiarism detection to identify elements of the original software that have been copied. To research the suggested strategy, we obtained the source code files of 100 programmers from GCJ. The original code is cleaned of noise and further preprocessed to capture high-quality features, which have auxiliary tokens. Then, TFIDF and LogTF weighting algorithms are used to zoom in on the contribution of each feature in terms of source code similarity. The specified deep learning algorithm is then fed the weighting values as input. We also propose a revolutionary approach based on convolutional neural networks and color picture visualization to identify malware using the Internet of Things. To better visualize the properties of the virus, it have converted the malicious software files into colored graphics. The next fed a deep convolution neural network these malware properties that were shown. Experimental findings demonstrate that, compared to state-of-the-art procedures, the combined strategy retrieves the highest level of classification results. Although the tokenization technique pulls keywords from the source code, it hides the basic structure of the code. To record the syntactic and control flow of the source code, the Abstract Syntax Tree and Control Flow Graph feature is used. It will try to take advantage of these features to find unauthorized versions in the future. Malware detection is a big problem for the unknown group of malwares. Additionally, it will attempt to provide an algorithm that can find malware in families containing unknown malware.

REFERENCES

[1] A. Nauman, Y. A. Qadri, M. Amjad, Y. Bin Zikria, M. K. Afzal, and S. W. Kim, “Multimedia internet of things: A comprehensive survey,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2964280.

[2] W. Jin and D. Kim, “Improved resource directory based on DNS name self-registration for device transparent access in heterogeneous iot networks,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2935239.

[3] L. Urquhart, H. Schnädelbach, and N. Jäger, “Adaptive Architecture: regulating human building interaction *,” *Int. Rev. Law, Comput. Technol.*, 2019, doi: 10.1080/13600869.2019.1562605.

[4] R. Buyya and A. V. Dastjerdi, *Internet of Things: Principles and Paradigms*. 2016. doi: 10.1016/C2015-0-04135-1.

[5] H. Ning, *Unit and Ubiquitous Internet of Things*. CRC Press, 2016. doi: 10.1201/b14742.

[6] L. Kaušpadienė, S. Ramanauskaitė, and A. Čenys, "Information security management framework suitability estimation for small and medium enterprise," *Technol. Econ. Dev. Econ.*, 2019, doi: 10.3846/tede.2019.10298.

[7] N. A. Sears, "Existential Security: Towards a Security Framework for the Survival of Humanity," *Glob. Policy*, 2020, doi: 10.1111/1758-5899.12800.

[8] I. Atoum and A. Otoom, "Holistic performance model for cyber security implementation frameworks," *Int. J. Secur. its Appl.*, 2016, doi: 10.14257/ijsia.2016.10.3.10.

CHAPTER 3

AN EVOLUTION OF INTERNET OF THINGS SECURITY FOR CYBER-ENTITIES

Dr. Veena C S, Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- veena.cs@presidencyuniversity.in

ABSTRACT

The Internet of Things (IoT) is a new paradigm for networks that attempts to link omnipresent objects in various heterogeneous networks. The across-space interactions that occur when a physical item is mapped as its corresponding cyber-entity provide special security difficulties to the IoT's cyber entities. This chapter takes into account the unit and ubiquitous IoT to address the issues with cyber security, presents the suggested security approaches following the cyber-entity activity cycle, and further develops a safe interaction solution for various known colloquially with both security and privacy relevant factors. The main objective of this chapter is to introduce the new grounded theory approach to derive integration criteria for the reviewed frameworks, models, and methodologies. Then, we propose a new architecture for the integration of the reviewed frameworks, models, and methodologies. This chapter covered information about the uses of the IoT in cyber security. First it defines the system architecture and the cyber entity domains such that UUIoT and its model after that cyber entity domains such that the unit domain, and ubiquitous domain, and after that, there is to describe the security challenges in UUIoT.

KEYWORDS: Cyber Security, Data Sensor, IoT, UUIoT, Information Security, Sensor Node.

INTRODUCTION

In the Internet of Things (IoT), a physical item is mapped as one or more cyber-entities for ubiquitous interconnection across heterogeneous networks, and this is quickly becoming a commonly used network paradigm. In encounters where several cyber-physical-social features are given to the cyber-entities in cross-space settings, the cyber-entities play crucial roles in developing connectedness with the related physical objects. IoT system models have mainly been investigated, and security concerns have surfaced to spark considerable inquiry. Systemic security foundations and tactics, networks-based cryptographic security techniques, and security solutions geared toward Internet of Things applications make up the majority of appropriate security efforts. As a result, system security, network security, and application security may be used to separate related tasks[1], [2]. Network security concentrates on detection and networking-based communications like radio frequency identification and wireless sensor networks to design cryptographic techniques, including key distribution, digital signatures, and access control; Application security serves for IoT applications to address the security issue. System security primarily considers an IoT Operating system to identify security challenges, customize security frameworks, and provide security guidelines. The cyber-entities have significant problems while establishing safe connections with consideration to the aforementioned national security concerns.

1. Increasing the Domains of Information Security

In addition to physical things being mapped into cyberspace, numerous cyber-entities are appearing for ubiquitous communication and communication. In comparison to the Internet, the IoT's cyber-entities have a greater variety, which makes security issues more challenging.

2. Cyber Entities

It may exist in a dynamic activity cycle with varied roles becoming taken into account. For instance, in one case, a cyber-entity has finished its cycle of activity and is now temporally offline. While the cyber-entity may still be active in other circumstances, such irregular activity cycles create difficulties for security measures.

3. Heterogeneous Cyber Entity Interaction

These interactions go beyond just cyber-physical problems, and across-space interactions specifically depend on the related social qualities. The social interactions between cyber-entities that are both individual- and group-aware should be paid attention to during secure communications.

1.1. System Architecture and the Cyber-entity Domains

i. Overview of the Unit and Ubiquitous IoT (UUIoT)

Unit IoT and Ubiquitous IoT are both terminologies used in the U2IoT architecture. The Unit IoT is a single IoT application, meanwhile, the Ubiquitous IoT consists of several associated Unit IoTs with concerns for the country, industry, and area. Figure 1 depicts a tiered model of the U2IoT system, which encompasses the perception, network, and application layers.

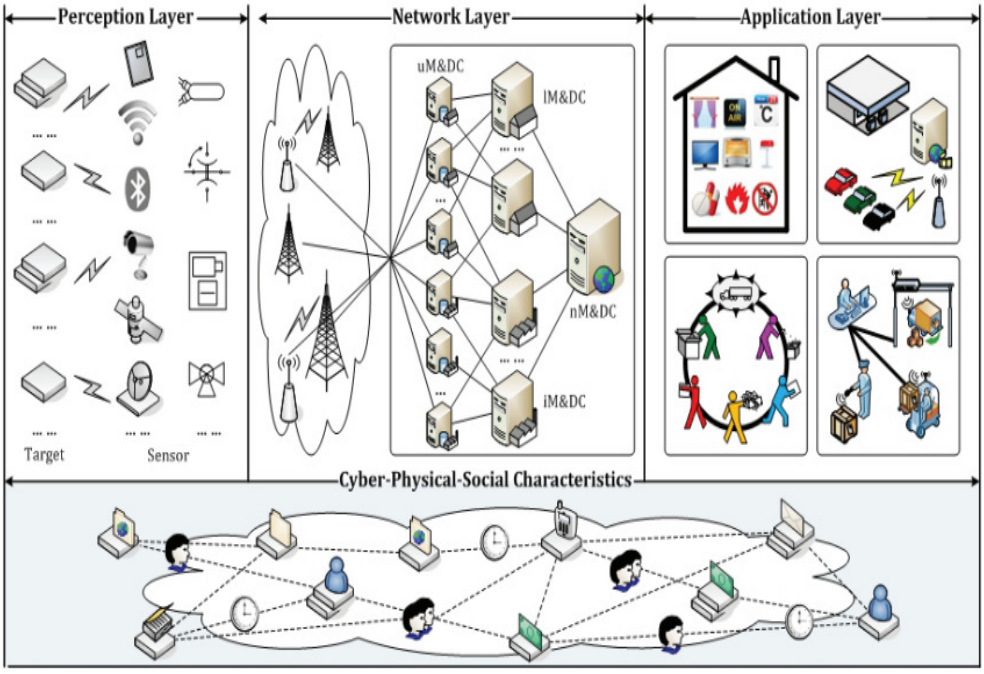


Figure 1: Represented the Layered UUIoT System Model.

The perception layer enables the transformation of physical items into cyber-entities and includes generic sensors for target recognition and the liberalization of physical objects. The most

common sensing technologies are Zig-Bee, RFID, Wi-Fi, Bluetooth, infrared induction, GPS, and radar. Keep in mind that sensors may be coupled to either mechanical or electrical actuators, such as buttons and valves, to carry out the designated instruction. Numerous system components, such as interfaces, routers, gateways, and communication channels, are included in the network layer. Keep in mind that the management and data centers serve as communication hubs on networks. The municipal, industrial, and national management and data centers may have direct or indirect control over a unit management and data center in such a situation. On the Internet, WSNs, mobile communications technology, and telephone networks, heterogeneous computing configurations may be created. By using safe data coding, fusion, mining, and aggregation methods, this layer enables the link between the heterogeneous networks and delivers dependable data transfer. The application layer offers functional services to enable IoT applications and includes local, industrial, and national governance and data centers for local, industrial, and national IoTs.

A National IoT is the combination of numerous Local IoT and Industrial IoT within a country. In more concrete terms, a Local IoT comes to realize connections among Unit IoTs in a geographic region; an Industrial IoT manages Unit IoTs in an industry or industry chain, such as commuting and telecommunications; and a National IoT. Additionally, this layer takes into account service integration, global supervision, and global collaboration. In IoT applications like smart homes and smart grids, standard protocols like restricted protocol stack, wireless application protocol, and service composition technologies like service-oriented architecture, and cloud computing, may be used. The two basic types of ubiquitous things in the U2IoT are physical goods and cyber-entities. A cyber-entity is an abstraction being used to convey information like session identifiers and social relationships through interconnections, while a physical item is something that possesses an objective presence. The cyber-entities are given a variety of cyber-physical-social traits[3]–[5].

a. Space-Time Consistency

Any time, any location, and any mode are possible for a cyber-entity to engage with other cyber-entities. The cyber-entity is free to join or quit exchanges at any time without interfering with already running sessions. In heterogeneous networks, space-time registration, synchronizing, and correlation should be taken into account.

b. Multi Identity Co-existence

Depending on its uses, a cyber-entity might have several identities, including a core identity and various temporary or helper identities. Identifiers or non-identifiers may be used to characterize such a multi-identity. For instance, a person's biological traits, such as their fingerprint and iris, serve both non-identifiers for unique recognition whereas a tagged object is allocated an identifier such as an electronic product code, or EPC for identification in RFID systems. Other cases allow for the combination use of non-identifiers and non-unique identifiers for object representation.

c. Dynamic Interaction

According to wireless links, a cyber-entity may adapt to changing environment. The cyber-entities are connected either directly or indirectly, and ubiquitous interactions are developed to facilitate further advanced information processing.

d. Social Awareness

It is important to provide cyber-entity full-fledged social qualities that reflect the social interactions with the related physical things. The social qualities take into account things like behavior formalization, affiliation connection modeling, and ownership control management. It should be noted that the goal of social awareness is to exhibit social links amongst cyber-entities that are both individual and group aware.

1.2. The Cyber Entity Domains in the U2IoT

Architecturally, the U2IoT includes three main cyber-entity domains: unit domain, ubiquitous domain, and logical domain.

i. Unit Domain

The cyber-targets, cyber-sensors, and uM&DCs make up the unit domain, which is equivalent to the cyber-entities in the unit IoT. Real-time goal data collecting, environmental monitoring, and fundamental information management are continually accomplished in this sector. The term "cyber-targets" generally refers to two separate things: first, the data that has been sensed about physical, chemical, and biological parameters in the environment (such as temperature, gas attentiveness, and blood pressure); second, the data that is currently available (such as a quick response code) attached to physical objects. Depending on whether an internal power source is present, the cyber-sensors may operate in active or passive modes.

Radars, cameras, and resistance temperature detectors are a few examples of physical devices that active cyber-sensors may actively probe for data collection. Without actively interacting with the actual things, the passive cyber-sensors collect data. Infrared sensors and resistance detectors for temperature are examples of common passive cyber-sensors (RTDs). Keep in mind that the two distinct kinds of cyber-sensors may use the same sensing technology. For instance, a passive 13.56 MHz RFID tag is activated by the reflected laser signals for supply chain management, whereas an active 2.4 GHz RFID tag for identification in electronic toll collection (ETC) contains an onboard battery.

The unit and widespread domains are connected utilizing the uM&DCs, which serve as intermediary network elements. To offer intelligent services, information retrieval, and real-time event response for the Unit IoT, they may manage the interactions between cyber-targets and cyber-sensors, conduct data storage, fusion, or mining on the sensed data, and extract informative information.

ii. Ubiquitous Domain:

The heart of the ubiquitous Internet of Things is the ubiquitous domain, which is a collection of several unit domains. The cyber-entities in this area essentially include different management and data centers, such as iM&DC, iM&DC, and nM&DC, to handle Local IoTs, Industrial IoTs, and National IoTs. Grid computing may be used for network management, and the iM&DCs manage the loosely linked and disseminated Local IoTs in this manner. For data collecting in numerous places, the separate iM&DCs may be combined in a cluster configuration.

Industrial IoTs that are concentrated on certain industries or businesses and investments are managed hierarchically by iM&DCs. The associated Industrial IoTs are connected with unique linkages, and layered data aggregation across the many sectors may be conducted via multi-agent-based collaborative management. The utilities often use the nM&DCs to supervise Local

IoT and Industrial IoT throughout a continent and to execute arbitration in the event of a disagreement. To offer coordination services, an nM&DC may interface with the connected iM&DCs/lM&DCs or other uM&DCs.

1.3. Cyber Security Challenges in the U2IoT

i. Enhanced Cyber Security Requirements

The U2IoT should take into account the more stringent cyber security standards, such as the CIA Triad, authority, non-repudiation, and privacy protection.

I. CIA Triad

Takes into account the primary standards for data availability, integrity, and confidentiality. A physical item should be protected against inappropriate correlation with the relevant cyber-entities and social qualities.

II. Authority

Primarily speaks about authentication and authentication. However, advanced needs must be taken into consideration.

III. Multi-Access Authority

Single sign-on (SSO) may be used to create a multi-access authority that is consistent with it, allowing a single authorization action to gain the matching access authorization without needing to repeat the identity verification.

IV. Multi Semantic Authority

According to the heterogeneous networks, multi-semantic dependent identification and authentication should be constructed.

The adoption and distribution of the "Internet of Things (IoT)" for remotely monitoring and managing different modules have caused architectural modifications in contemporary organizations. The industrial automation processes in smart industries constitute the most common context in which IoT technology makes the most sense. The Industrial IoT (IIoT) environment is offered with a trustworthy "Next Generation Cyber Security Architecture (NCSA)" in this study that can identify and stop cybersecurity vulnerabilities and dangers. The methods of sending crucial real-time information between equipment without human involvement are enhanced by automation. It suggests an analytical process that may be used to safeguard the network traffic and the entities participating in wireless IIoT communication. When a network session has been created, it features an automatic cyber-defense authentication system that spots and stops security assaults. The defensive mechanism creates an identity token that is cryptographically classified and authenticated by a virtual gateway system to achieve the necessary degree of cybersecurity in the network. The suggested NCSA lowers operational management expenses while enhancing efficiency in the IIoT environment [6].

The result of the Internet of Things (IoT), computing is now more omnipresent than ever in our society and every aspect is linked to the Internet. The Cloud, where business intelligence and intelligence truly exist, is gradually becoming more dependent on this tsunami of connectedness and data capture. By adopting the idea of utility computing, whose benefits are apparent for any organization, cloud computing has undoubtedly revolutionized the way computation resources and services may be utilized and accessed. The security concerns concerned with its use,

however, prevent its broad acceptance despite the advantages in terms of flexibility, money savings, and support for new services. The IoT and Cloud computing information revolution might be disastrous from a safety standpoint since any item may end up being remotely hackable and hence controlled by bad actors. In contrast to the academia, which mostly emphasizes IoT and cloud security as distinct topics, the authors provide an up-to-date and systematic overview of cloud security problems in the IoT age. We provide a comprehensive vision of where security problems arise and what their possible repercussions may be. Because cyber-sports originate from clouds, we contend that securing IoT devices alone would be insufficient [7].

The Industrial Internet of Things (IIoT) is now an important factor in industrial systems because of the Internet of Things' quick growth and widespread adoption. The proliferation of IoT devices has facilitated the ability to diversify and decentralize energy systems, and the Energy Internet enables the connection of dispersed energy customers and producers. However, the current conventional energy trading paradigm encounters issues including inadequate scalability, vulnerabilities to cyber-attack, and poor processing efficiency as the number of organizations participating in energy transactions increases and the kinds of transactions diversify. We suggest BC-ETS, a reliable and effective Blockchain-based Energy Trading Scheme, to solve these problems. The energy trading concept in BC-ETS is split into two layers, which can both preserve privacy and establish a balance between supply and demand for electricity. Additionally, a credibility-based equity verification method is created to significantly boost the system availability to accommodate the relatively low computational capacity of the underlying IoT equipment in the energy internet. The research suggests that BC-ETS can satisfy the security criteria and performs better than other comparable energy trading systems [8].

The growth of the Internet of Things has resulted in several revolutionary new applications, such as intelligent cities, cyber-physical systems, and the Internet of Vehicles (IoV). On the IoV, vehicles are comprised of various electronic intelligent sensors or devices used to obtain data and communicate the necessary information with the surroundings. One of the major concerns about the implementation of these sensors or devices is data vulnerability: thus, it is necessary to present a solution that provides Security, Trust, and Privacy (STP) to communicating entities and to secure vehicle data from malicious entities. In modern vehicles, the Controller Area Network (CAN) is utilized as a fundamental scheme for controlling the interaction among the Electronic Control Unit (ECU) of the in-vehicle networks. However, there are not enough security features that support data encryption, authorization, and authentication mechanisms to secure the network from cyber or malicious attacks like Denial of Service (DoS), and Fuzzy attacks[9], [10].

DISCUSSION

All of the projects we looked at lacked a strategy for disaster recovery. Additionally, it is critical to underline the absence of contingency planning in the leading projects given the increased dangers arising from IoT-linked devices and services as well as the failure to conduct economic impact evaluations from IoT cyber hazards. The amount of data produced by IoT devices poses some challenges across a range of industries, including machine learning, ethics, and business models. Simultaneously, it is essential to devise innovative new approaches to optimization and decision-making when developing and building the cyber security architecture for intricately connected IoT systems. A significant portion of the study is application-focused and inherently multidisciplinary, necessitating hybrid studies across many school subjects. This allowed for the development of cyber security designs that include macroeconomic effect assessments in IoT verticals that pass legal, security, and widespread understanding criteria.

IoT Devices and Applications

Working with IoT Devices:

i. Collect and Transmit Data

Sensors are often deployed for this purpose; they are used whenever necessary in various application fields.

ii. Actuate Device based on Triggers

Actuator devices indicate which action should be taken if a condition has been fulfilled or if a trigger is engaged in keeping with user expectations.

iii. Receive Information

Users and devices may obtain specific information from routers and switches for analysis and processing.

iv. Communication Assistance

As shown in Figure 2, which shows the two networks or communication between different or more IoT devices on the same or different Networks, communication assistance is a manifestation of communication. A variety of communication protocols, such as Message queuing telemetry support (MQTT), Constrained Application Protocol, Zig-Bee, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), etc., may do this.

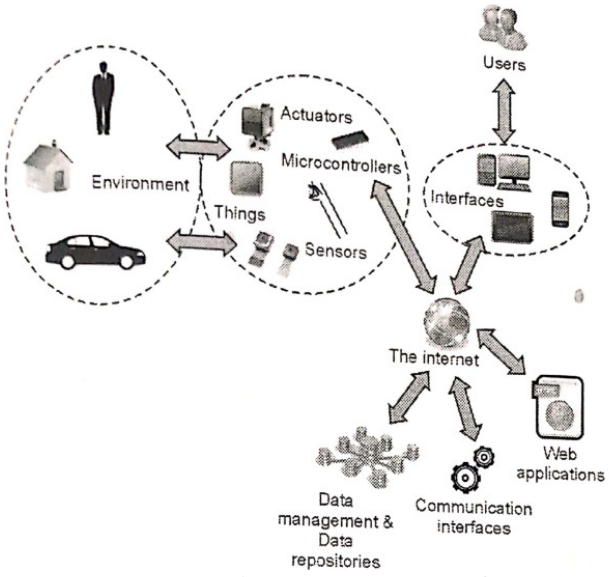


Figure 2: Illustrated the Working Phenomena of the Internet of Things.

Characteristics of IoT:

i. Extremely efficient and scalable

ii. IP-based addressing won't be appropriate shortly.

iii. IoT is made feasible by the prevalence of physical items that do not require IP.

iv. Generally speaking, devices use less electricity. They need to be set up to go to sleep automatically when not in use.

v. A device that is now linked to another device may not remain so in the future.

vi. Sporadic connection - Internet of Things (IoT) devices aren't constantly online. Devices that are not in use will occasionally be turned off to save frequency band and battery life. Otherwise, connections might become unreliable and end up being ineffective.

Desired Quality of any IoT Application:

i. **Interconnectivity:**It is the fundamental prerequisite for every IoT infrastructure. Any device on any network should be able to maintain connectivity since only those on the same network can interact with one another.

ii. **Heterogeneity:**IoT-enabled devices may come in a variety of forms, such as various hardware and software configurations, network topologies, or connections, but despite this heterogeneity, they should be able to communicate and interact with one another.

iii. **Dynamic in Nature:**IoT devices might dynamically react to their changing environments, including various situations and prefaces [11].

iv. **Self-adapting and Self-configuring Technology:**a security camera, as an example. It should be adaptable to operate in various climatic conditions and lighting scenarios (morning, afternoon, or night).

v. **Intelligence:**In the Internet of Things, gathering data alone is not sufficient; knowledge must be extracted from the created data. For instance, sensors provide data, but the value of that data depends on how well it is understood. Therefore, one of the essential elements of IoT is intelligence. Because data processing is essential to every IoT deployment because, without it, we wouldn't be able to conclude the data. Big data is therefore one of the IoT field's most enabling technologies.

vi. **Scalability:**Every day, more and more components (devices) are linked to the IoT zone. So, the growth should be manageable by an IoT setup. It may either enhance capabilities in terms of computing power, storage, etc. by multiplication with simple cloning or horizontally via scaling.

vii. **Identity:**IoT devices each have their personality like an IP address. This identification is useful for monitoring, communicating, and finding out how things are doing. Any system's security and safety will suffer if it does not have identification since without differentiation, we can't tell which networks are linked to which or with whom we need to speak. Therefore, there should be technology that clearly and appropriately distinguishes between IoT networks and devices.

viii. **Safety:** When the gadgets are linked to the Internet, a user's private information may be compromised. Data security is therefore a significant concern. The user can suffer a loss as a result. The vast IoT network's equipment may potentially be in danger. The safety of the equipment is thus essential.

ix. **Architecture:**For goods from many manufacturers to operate in the IoT network, it should be hybrid.

CONCLUSION

To develop common strategies and integrate current standards, this chapter synthesizes existing material. This result includes a mapping of the activities, methodologies, and techniques used to evaluate the effect of cyber risk. As a consequence, a new set of design principles and criteria that are tailored specifically for IoT cyber risk are produced. The recommended design principles provide suggestions for enhancing cybersecurity recovery. The design principles make it possible to visualize IoT cyber risk and provide enterprises operating in this field with best practices. The new design principles provide new sets of cyber security evaluation criteria by mapping relationships between various aspects of IoT devices. The design ideas discussed here may be used to evaluate the financial effects of IoT compromises and to suggest improvements for IoT hardware. National and international networks, especially for developing recovery plans, may benefit from the design concepts.

REFERENCES

[1] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Res.*, 2016, doi: 10.1108/IntR-07-2014-0173.

[2] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security 'Hands-On,'" *IEEE Secur. Priv.*, 2016, doi: 10.1109/MSP.2016.4.

[3] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of Things Security : Layered classification of attacks and possible Countermeasures," *Electron. J. Inf. Technol.*, 2016.

[4] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things Security Device..A review-04," *Int. J. Comput. Sci. Inf. Secur.*, 2016.

[5] T. M. and J. Al-Muhtadi, "Internet of Things Security based on Devices Architecture," *Int. J. Comput. Appl.*, 2016, doi: 10.5120/ijca2016908191.

[6] C. Vijayakumaran, B. Muthusenthil, and B. Manickavasagam, "A reliable next generation cyber security architecture for industrial internet of things environment," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, p. 387, Feb. 2020, doi: 10.11591/ijece.v10i1.pp387-395.

[7] M. De Donno, A. Giaretta, N. Dragoni, A. Bucchiarone, and M. Mazzara, "Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era," *Futur. Internet*, vol. 11, no. 6, p. 127, Jun. 2019, doi: 10.3390/fi11060127.

[8] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, and M. Guizani, "Towards secure and efficient energy trading in IIoT-enabled energy internet: A blockchain approach," *Futur. Gener. Comput. Syst.*, vol. 110, pp. 686–695, Sep. 2020, doi: 10.1016/j.future.2019.09.027.

[9] B. Russell and D. Van Duren, *Practical Internet Of Things Security*. 2016.

[10] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2015.2460333.

[11] V. Bhanumathi and K. Kalaivanan, "The Role of Geospatial Technology with IoT for Precision Agriculture," *Stud. Big Data*, 2019, doi: 10.1007/978-3-030-03359-0_11.

CHAPTER 4

AN ANALYSIS OF PRIVACY AND CYBERSECURITY CONCERNS WITH THE INDUSTRIAL INTERNET OF THINGS

Dr. Veena C S, Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- veena.cs@presidencyuniversity.in

ABSTRACT

Industry 4.0 is the result of research that has received a lot of attention over the last several decades. As a result, there is now a significant paradigm change in the industrial and manufacturing enterprises. However, this presents a challenge for cybersecurity and emphasizes the necessity to tackle potential attacks aimed at different industry 4.0 pillars. However, several aspects need to be investigated before offering a tangible answer, also including industry-wide privacy concerns and cybersecurity concerns.

KEYWORDS: Computer Science, Cyber Security, Industry 4.0, Information Technology, Internet of Things.

INTRODUCTION

By connecting manufacturing equipment over the internet with the aim of enhancing production and efficiency, the numerous organizations using I4.0, also known as Industrial Internet or Internet of Things, is steadily expanding. Cybersecurity (CS) risks are a main consideration for these internet-based companies, making it one of the biggest problems to be solved. I4.0 places a strong emphasis on CS as a means of maintaining organizational competitiveness. The amount of cyber-attacks conducted at vital infrastructure has an impact on every aspect of corporate operations and on the identities of firms. Hyper-connectivity between smart networks and smart devices creates a significant opportunity for hackers in the I4.0 age, who can identify potential weak areas and unsecure access points in networks and even sometimes devices as well. These cyber-attacks disrupt an organization's operational functions, but they also have an effect on society as a whole and, in certain occasions, the national psyche of the victim nations[1], [2].

According to CISCO's 2018 annual report on CS, 31% of firms experienced cyber-attacks on operational technology, and 38% of enterprises estimated that cyber-attacks will extend past information technology to operational technology. This study found that 75% of professionals said CS should be a top priority. Comparatively, just 16% of specialists felt that their organization was prepared to handle CS issues. This issue appears to be caused by inadequate technical and administrative competencies as well as an insufficient understanding of CS hazards.

CS is now gaining importance for Europe and a handful of other international organizations. For instance, IEC has released rules about CS and privacy as well as potential techniques of putting these concepts into practice. To assist the European digital market in solving current CS difficulties, the ESCO has similarly gathered all regulatory requirements and recommendations. Despite these measures, several security concerns are announced every day, particularly in relation to I4.0. This underscores the need of researching cyber-security, particularly in the context of the I4.0 paradigm. In additionally, a thorough analysis of potential security risks

affecting I4.0 and potential defenses is required. By learning about potential risks, practitioners will be better able to take prompt preventative action. In light of the above-mentioned information, this paper seeks to provide a thorough analysis of CS risks targeting IIoT, along with their effects and available defenses. The term "IIoT" refers to a network of sensors, tools, and other components that are linked to industrial software packages for things like production, manufacturing, and energy management[2], [3].

This interconnectedness makes it easier to gather, distribute, and evaluate data, which may lead to improvements in productivity and quality as well as other financial advantages. The benefits of adopting IIoT are many. To start, it is one of the cornerstones of I4.0. Additionally, it is the primary impetus for the I4.0 revolution. The remainder of the paper is arranged as follows: The IIoT architecture and I4.0 categorization are covered in the next part, along with a detailed discussion of several essential terms for a better comprehension of the topic. The study methodology, the postulated framework, potential risks to IIoT layers, the effects of such threats, and viable countermeasures will all be covered in Section 4. The conclusion of the essay will then be presented after a thorough analysis of our data.

Understanding IoT in Industry 4.0 initiatives

The Industrial Internet Consortium advocates for an entirely automated, networked production line which thus includes the consumer as a decision-maker and gives them the freedom to modify their preferences throughout production. Additionally, IIC enables the use of situations with human-controlled visualization, intervention management, and highly automated rules engines. The IIC supports disaster response plans and cloud computing platforms. Disaster recovery plans, however, are just discussed briefly in a schematic with no explanation of the specifics or how they will be performed. The problem of having recovery strategy in place is not automatically answered by just addressing it. Cloud integration in I4.0 is a major topic in the most recent UK report from the Department for Culture, Media, and Sport. While some initiatives are backed by real examples of how the strategy can be put into practice, also including cloud data centers from Amazon, IBM, and Microsoft, or the cloud skills initiative to train the public service in digital skills and say with certainty the development of larger cloud technical skills, other initiatives are not clearly defined. In certain cases, this could be advantageous since standards with broad definitions allow for more flexibility in adapting as needs change.

The integration of IoT in I4.0 does, however, need a specific area of concentration, as shown by real implementations. The DCMS also mentions creating a real-time platform for communicating information on missing people and suspects as well as digital real-time shareable records for healthcare. Real-time CPS-IoT systems for I4.0 are not discussed in this study on the UK's digital sector, which covers the characteristics of independent cognitive judgments in great depth and lists particular initiatives, programmer, and funding sources. The study places a lot of emphasis on proactive cyber security and general customer data protection, but it misses other huge threats, such as those related to unannounced failures, for which recovery management is essential since such failures cannot be predicted in advance. There are no specific plans for real-time embedded applications or recovery strategies identified in the current Industrial Value Chain Initiative[4], [5].

Industry 4.0 encourages cloud computing cooperation with the Internet of Services and suggests cloud-based security networks, although it does not include recovery strategies. The NIT project

focuses on the development of market connections and is a very long-term prognosis for IoT and I4.0. This effort offers fresh perspectives on I4.0 by maintaining that the integration of the supply chain and future business success depends on the development of markets for new technologies. However, the NIT forecasting does not evaluate the vulnerabilities with real-time cloud networks and, more significantly, does not provide solutions for strategies for recovery planning.

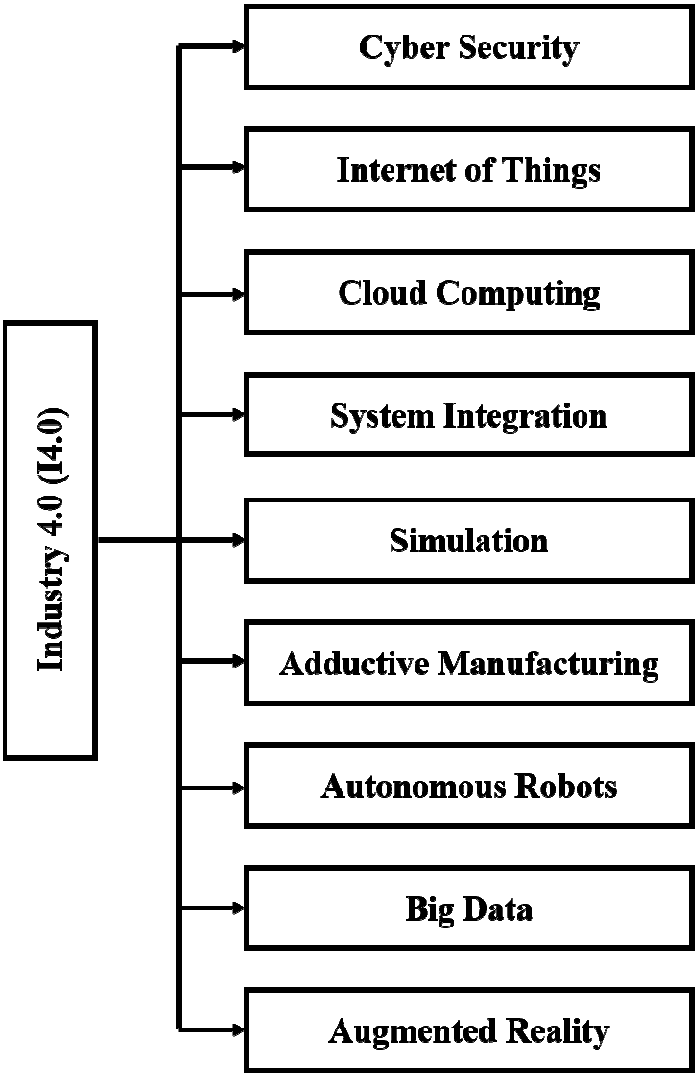


Figure 1: Represented the Digital Transformation of Industry 4.0.

The term I4.0 also known as industrial internet has brought a great revolution in the industry also shown in Figure 1. It originated in Germany when the German government promoted the computerization of the manufacturing industry. The idea behind I4.0 was to connect all the participants using the internet so that they could exchange information with each other. This idea is based on a cyber-physical system, a system of computational elements collaborating in a coordinated and controlled way. I4.0. provides better business gain and has accelerated productivity a lot. It has impacted almost every field of life; proponent of I4.0 considers it as the third wave of innovation. Below we discuss some definitions of I4.0 from the current literature for a better understanding. "The industrial internet is an IoT, machines, computers, and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes, and it is redefining the landscape for business and individuals alike". "I4.0 is

a collective term for technologies and concepts of value chain organization. Within the modular structured Smart Factories of I4.0, CPS monitors physical processes, creates a virtual copy of the physical world, and makes decentralized decisions. Over the IoT, CPS communicates and cooperates with other CPS and humans in real-time. Via the IOS, both internal and cross-organizational services are offered and utilized by participants of the value chain". I4.0 is the interaction between IoT and CPS which includes embedded systems, sensors and actuators, hardware, and software along with the connection to other systems. Figure 2 describes the perspective of I4.0 that is inevitable to compete in today's' fast-paced economy and to satisfy heterogeneous customers.

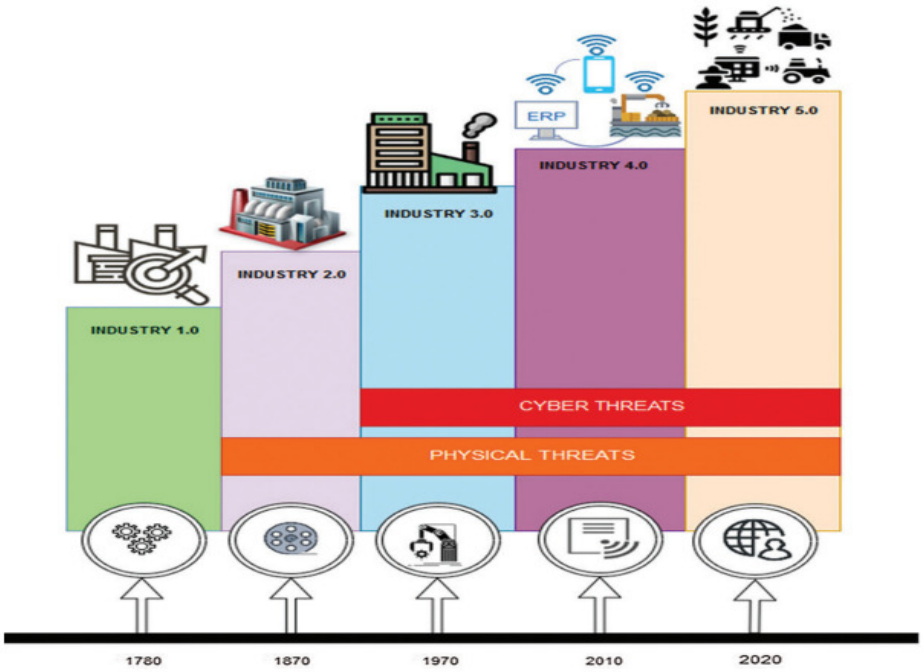


Figure 2: Represented the Evolution of Industry 4.0.

Industrial Internet of Things (IIoT)

IoT is a network of connected devices that are communicating with each other through the internet. When the same IoT is applied in industrial settings, it becomes IIoT. Researchers have used the term I4.0 and IIoT interchangeably. However, we have taken IIoT as one of the pillars of I4.0. Below we present some definitions of IIoT from literature. Industrial Internet: a short-hand for the industrial applications of IoT, also known as the IIoT. The IIoT is the use of IoT technologies in manufacturing. The IoT represents a scenario in which every object is embedded with a sensor and is capable of automatically communicating its state with other objects and automated systems within the environment. Each object represents a node in a virtual network, continuously transmitting a large volume of data about itself and its surroundings. In general, the terms IoT apply to expand network access and computational capabilities to objects, devices, sensors, and things that are not typically considered computers. These smart objects require minimal human involvement in the creation, sharing and consumption of information; they also have connectivity to remote data collection, analysis, and management capabilities. Group of infrastructures, interconnecting connected objects and allowing their management, data mining and access to data they generate where connected objects are sensor and actuators carrying out a specific function that can communicate with other equipment.

Smart manufacturing is where Industry 4.0 (I4.0) sprang from and is what it is led by. The routine operations of enterprises and people's lives would undergo profound changes and transformations as a result of the fourth industrial revolution, or I4.0. The sustainability of the possible development systems and operations is important since these significant changes influence all sectors and industries globally. The social component is noticeably undervalued in the I4.0 sustainability-related studies, according to the most recently published literature. The few studies that focus on this topic often look at the so-called "techno-centric" approach. The purpose of this research was to examine the I4.0 construction project management (PM) field from a 'worker-centric', socially responsible perspective. To do this, five essential facets of the new I4.0 project manager's role specifically relevant to the construction sector were investigated. This was done via a questionnaire distributed sent to 100 Gulf Cooperation Council (GCC) area building project managers. The overall study findings demonstrated that professional and academic credentials were crucial during the process of adjusting to the new I4.0 approaches.

Adopting Industry 4.0 (I4.0) is a strategy to improve production and efficiency while gaining competitiveness via technological innovation. To improve industry readiness, Indonesia created I 4.0 (Industry 4.0 readiness index Indonesia) in 2018. It is less accurate and thorough in capturing I4.0 readiness, particularly in the element of manufacturing operations. I4.0 only offers a small number of questions to gather substantial data while measuring I4.0. The goal of this research was to improve I 4.0 in the area of industrial operation to create a complete I4.0 index. The study thoroughly investigated journal papers and several other I4.0 indexes used in various countries to examine concerns in the I4.0 readiness index. The paper also established a complete I4.0 index with key indicators covering the life cycles of smart products including the sources, collecting, storage, analysis, and transfer of data (designing, planning, monitoring, quality, and maintenance). This model is anticipated to provide a significant improvement to Indonesia's INDI 4.0. The I4.0 phenomenon will surely have an impact on all nations, and more investigation into this issue and other vital factors impacting I4.0 readiness is necessary to finish this study. To solve the gaps, inadequacies, and weaknesses in this study, new academic research is required.

The emergence of the fourth industrial revolution, also known as I4.0, from the advancement in several technologies is viewed not only to promote economic growth but also to enable a greener future. The 2030 Agenda of the United Nations for sustainable development sets out clear goals for the industry to foster the economy while preserving social well-being and ecological validity. However, the influence of I4.0 technologies on the achievement of the SDG has not been conclusively or systematically investigated. By understanding the link between the I4.0 technologies and the SDGs, researchers can better support policy makers to consider the technological advancement in updating and harmonizing policies and strategies in different sectors that is education, industry, and governmental with the SDGs. To address this gap, academic experts in this paper have investigated the influence of I4.0 technologies on the sustainability targets identified. The results indicate that the majority of the I4.0 technologies can contribute positively to achieving the UN agenda. It was also found that the effects of the technologies on individual goals vary between direct and strong, and indirect and weak influences. The main insights and lessons learned from the mapping are provided to support future policy.

Industrial Automation and Control Systems (IACS) have traditionally been largely cut off from standard digital networks like business ICT settings. A zoned design was employed when

interconnection was necessary, and firewalls and demilitarized zones were deployed to isolate the main parts of the management system. IACS is undergoing architectural transformations as a result of the acceptance and implementation of "Internet of Things" (IoT) technologies, including the verification of industrial systems. This essay examines the definition of Industrial IoT (IIoT) and its connections to ideas like cyber-physical technologies and Industry 4.0. In this work, an IIoT definition is developed, and associated partial IoT taxonomies are investigated. It provides a framework for IIoT analysis that may be used to characterize and list IIoT devices while investigating system designs and security risks. The paper's conclusion identifies certain gaps in the body of knowledge [6].

Modern production is more sophisticated and data-driven than ever before. In the era of the Industrial Internet of Things, a smart production unit may be seen as a potent linked industrial system with materials, materials, equipment, tools, inventories, and services that can exchange data and interact with one another (IIoT). This IIoT refers to connected devices, sensors, and many other machineries that may be networked in an industrial setting to provide remote access, efficient monitoring, improved data collection, analysis, and sharing, among other benefits. IIoT is key to Industry 4.0 because it uses big data and analytics to alter cyber-physical systems and production processes. An understanding of the IIoT and the underlying technologies is given in this paper. The main advantages and characteristics of IIoT in manufacturing are explained in detail. Diagrams are used to highlight the smart transformations that IIoT culture has brought about in the industrial sector. All scattered and outsourced processes may be monitored with the use of IIoT, which can also verify the circumstances connected to product storage and delivery and consult data on items in warehouses. As a result, IIoT is transforming the industry by changing how industrial companies handle their everyday business to boost productivity and efficiency.

The Internet of Things (IoT) concept has important applications in industrial environments. The Industrial Internet of Things (IIoT), also known as Industry 4.0, is an emerging technology that has the potential to revolutionise manufacturing and production through the use of a significant number of networked embedded sensing devices and the integration of cutting-edge computing technologies like fog/cloud computing and artificial intelligence. An enhanced level of interconnectivity that characterises the IIoT presents an opportunity for cybercriminals as well as the sectors that use it. One of the main barriers preventing the general use of IIoT technology at the moment is IoT security. Unsurprisingly, these worries have caused the amount of published research to increase exponentially over the last several years. We believe it's crucial to do a thorough review of the existing academic literature in the sector to conclude the different security needs and their popularity. Our second contribution is an analysis of how the relatively new Fog computing paradigm might be used to meet these needs and so increase the security of the IIoT [7].

Compliance is receiving increased attention as a result of industrialization and the modernization of industrial processes. Different industrial sectors must adhere to a variety of rules to be productive and competitive. By incorporating all requirements imposed by laws and standards, compliance seeks to satisfy regulations. Standards support interoperability across the many technologies that are employed by every device, application, and service at various levels. For development to be sustainable and long-lasting, they aid in the creation of international customers for certain sectors. This study provides an autonomous monitoring and government institutions and frameworks verification system and emphasizes the significance of the

successful outcome and ongoing verification in the industrial Internet of Things. In this paper, we concentrate on the operational, security, and safety implications of the industrial Internet of Things. We define a variety of standards and industry standard recommendations that are utilized to extract enterprise quantifiable indicator points for security, safety, and compliance. Additionally, a metric model is offered as the cornerstone for the criteria, standards, and indicators required for compliance verification. Additionally, we demonstrate the monitoring and guideline compliance verification framework prototype that will be used to demonstrate how an industrial Internet of Things use case complies with security standards [8].

The order to achieve a renewable energy industry and the aims of sustainable development, industrial output is crucial. Therefore, from the perspective of sustainable development, the embryonic transformation of industrial production caused by digitization into a so-called the Industrial Internet of Things (IIoT) is of significant importance. The environmental aspect of sustainable development is discussed in this study, with a particular emphasis on three areas: resource efficiency, sustainable energy, and transparency. The three environmental concerns are covered in a state-of-the-art literature study of IIoT-enabled techniques. This study is contrasted with the results of a survey among Chinese industrial businesses that looked at what participants expected from the adoption of IIoT solutions in terms of sustainability. Because of its robust industrial sector, ambitious goals for industrial digitization, high relevance, and pressing need for greater sustainability, China has been selected as the case study. A questionnaire used for direct on-site interviews and distribution through email was utilized to conduct the survey. It targeted big and medium-sized businesses, mostly in Liaoning Province, and had participants as its sample size.

DISCUSSION

To inform individuals of the dangers involved with using these devices, this research highlights the main security issues with IoT systems. IoT hazards have been divided into many groups for easier understanding. Additionally, a thorough comparison of each class is included. Network attacks are those that involve malicious activity being injected into a network to steal information packets and slow the network down. Attackers use side-channel assaults to concurrently attack security and privacy. Attackers who use cryptanalysis get access to the decryption key to transform encrypted text into plaintext. Attackers use the restricted resources available in access-level assaults to steal or modify the data. While in ip spoofing, attackers may read the message but do not alter it, active attacks include attackers reading and altering the message packets.

Attackers use a variety of tactics in strategy-level assaults to insert malicious malware into IoT devices. Physical assaults are those that involve physical contact and intentionally hurt hardware; logical attacks, on the other hand, are those that can be carried out remotely. IoT assaults are divided into internal and external attacks depending on the location of the adversary. An attacker might be an insider with knowledge of the targeting IoT system or an outsider with no knowledge of the system. In assaults when the hardware has been hacked, the attacker tampers with it to take data. Software assaults include the deliberate introduction of harmful applications onto the system to allow unauthorized entry. Hackers may access these IoT web apps, databases, or servers because of bad coding. Firmware assaults are those launched as a result of outdated firmware not being present.

CONCLUSION

By linking billions of heterogeneous gadgets in real time, I4.0 has sparked a huge change in basically every aspect of life. Different I4.0 pillars, such as autonomous robotics, simulation, cyber-security, IIoT, horizontal and straight up and down integration, augmented reality, etc., have been addressed by researchers. It was not feasible to examine the privacy and cybersecurity concerns affecting all of the I4.0 pillars in a single study. We have thus emphasized IIoT, one of the key pillars of I4.0, in our study. We have given a thorough description of I4.0's four-layer design. The possibility of CS attempts is one of the biggest difficulties I4.0 faces. We have covered all potential assaults on each tier of the IIoT, their effects, and proposed solutions to address this issue. This exhaustive review of the literature attempts to provide readers with a more comprehensive understanding of IIoT architecture and indeed the potential threats posed by each layer of the IIoT. It will assist IIoT researchers and practitioners in studying potential threats and their remedies. A thorough framework which it offers an overview of potential security and privacy concerns, as well as the methods of attacks and solutions, is established based on a review of the current cybersecurity and privacy problems affecting IIoT. We want to use the road to achieving Industry 4.0 situations in the future to study how it affects the mitigation of computer privacy and security concerns.

REFERENCES

[1] E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *2016 International Wireless Communications and Mobile Computing Conference, IWCMC 2016*, 2016. doi: 10.1109/IWCMC.2016.7577060.

[2] J. Bhatia, T. D. Breaux, L. Friedberg, H. Hibshi, and D. Smullen, "Privacy risk in cybersecurity data sharing," in *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, 2016. doi: 10.1145/2994539.2994541.

[3] I. J. Perez-Arriaga, "The Transmission of the Future: The Impact of Distributed Energy Resources on the Network," *IEEE Power Energy Mag.*, 2016, doi: 10.1109/MPE.2016.2550398.

[4] R. Ruiz and R. Winter, "Lazarus: Data leakage with PGP and resurrection of the revoked user," *J. Cyber Secur. Mobil.*, 2016, doi: 10.13052/jcsm2245-1439.521.

[5] S. J. Shackelford, "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk," *Chapman Law Rev.*, 2016.

[6] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018, doi: 10.1016/j.compind.2018.04.015.

[7] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020, doi: 10.1109/COMST.2020.3011208.

[8] A. Bicaku, M. Tauber, and J. Delsing, "Security standard compliance and continuous verification for Industrial Internet of Things," *Int. J. Distrib. Sens. Networks*, vol. 16, no. 6, p. 155014772092273, Jun. 2020, doi: 10.1177/1550147720922731.

CHAPTER 5
AN INTRODUCTION TO CYBER SECURITY WITH INTERNET OF THINGS

Mr. Nipun Sharma, Assistant Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- nipun.sharma@presidencyuniversity.in

ABSTRACT

The Internet of Things (IoT) is growing very quickly. It is a group of interconnected devices that may receive information from the outside world, analyse it, and, if required, manage external equipment in addition to supplying information for decision-making. These devices are linked through the Internet and other networks. The objective is to make both private and public life more cozy, secure, and effective. But there are growing cybersecurity threats, just as with any quickly developing Internet technology. Considered are the most notable cyber events in the IoT industry, the causes of such incidents, and potential solutions to strengthen IoT cybersecurity. In future, this paper will separate the proper information about the uses of internet of things in cyber security and this chapter elaborated that the different elements of IoT.

KEYWORDS: Cyber Security, Data Sensor, IoT, UUIoT, Information Security, Sensor Node.

INTRODUCTION

We can't help but love our smart devices and by 2030, there will likely be billions more operational technology (OT) and Internet of Things (IoT) devices in use, totalling approximately 24 billion. We value how they improve the quality and simplicity of our lives as individuals. We have instant access to information and we can interact with each other. They are necessary. Businesses appreciate smart IoT devices because they enable continuous consumer interaction and data collection. Manufacturers, energy companies, and supply chain organizations all enjoy IoT and however, this type of IoT is called operational technology.

The term "industrial control system" has OT roots (ICS). Industrial control systems, which also integrate instruments and networking capabilities, can be used to efficiently drive robots, wind turbines and cargo ships. If an IoT device is used to power a physical system, such as a part of a power grid or a device on a factory floor, it is called an OT device. Cyber criminals are fond of IoT and OT devices, which is a problem. Maybe even more than us. The fundamental problem with IoT and ICS devices is that they make it possible for individuals or organizations to conduct sophisticated cyber-attacks. Hackers will use whatever means necessary to attack a company, a neighbourhood, or even an entire country. This argument is often made by cyber security professionals who claim that IoT increases the potential attack surface for criminals. Since they are aware of it, security experts manage the incoming security threats.

The IoT/ICS Device

IoT and ICS are examples of device end points. In other words, they are the last link in the communication chain that starts with a person or robot and ends at cloud data centres and

platform centres. IoT and ICS hardware were not invented overnight. They are designed, built and managed just like any other computer. Description of the components inside a typical IoT device.

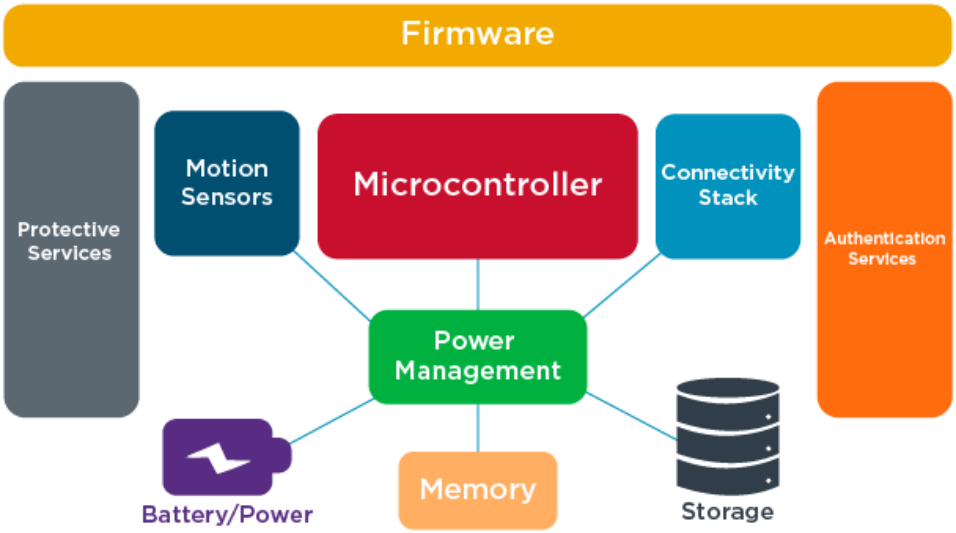


Figure 1: Represented the Different Elements in IoT Devices.

As shown in Figure 1 above, any IoT device has each of these elements inside:

i. Firmware:

Read-only memory embedded in the device provides low-level control of the hardware. It can be updated, but usually not programmed. Communicates between each of the elements in the device as well as other networked devices.

ii. Protective services:

A portion of the device's firmware or operating system provides security functionality, including the ability to isolate processes so that they can't be used to defeat security, and encryption.

iii. Motion sensors:

The combined hardware and software are used to track how the device is moved. This can include the detection of simple movement (e.g., moving the device back and forth, or up and down), or satellite connectivity (e.g., Global Positioning System or GLONASS).

iv. Microcontroller:

The processor is used to run the software and provide the "brains" of the unit.

v. Connectivity stack:

Responsible for providing network connectivity. Networking capabilities can include Bluetooth, mobile (e.g., 3G, 4G, 5G), Zigbee, LoRA, SigFox or WiFi.

vi. Authentication Services:

When included, provides the ability for the IoT device to verify and validate users, network traffic or processes.

vii. Power management:

If the device requires significant use of power, functionality that manages power usage, as well as the charging of the device.

viii. Battery/power:

The physical capability to store power, as well as receive power from a remote source.

ix. Memory:

The working "muscle" of the IoT device, is that it provides the ability to store working data, machine code and information that is then addressed by the processor.

x. Storage:

Provides the ability to capture and keep data for relatively long periods. Such information can include storing the location(s) the IoT device wearer/operator took the device, information about other devices that have connected with it and information entered by the user. Such information can be added actively (e.g., by the user programming the IoT/OT device on purpose), or passively (e.g., by the device capturing the motions and actions of the wearer/user). It doesn't matter if that device is a webcam, the smartwatch or the Raspberry pi device your local water utility company developed to control devices for your community water supply, the elements remain the same.

The IoT Ecosystem

Each of these components must be created and kept up-to-date for an IoT/ICS device to function effectively and safely. To put it another way, companies and developers must make sure to provide high-quality hardware and software for IoT/OT devices. As you'll see, software and hardware engineers work cooperatively sometimes not so closely to ensure that IoT and other processor architectures are compatible with each others. To build IoT solutions and control devices, a full IoT ecosystem already exists. The components listed in Table 1 make up this ecosystem.

Table 1: Represented the IoT Ecosystem.

Sr. No.	Element	Description
1.	Software developers	• The people who develop the software that runs IoT devices.
2.	Hardware engineers	• The people who create the hardware devices, including processors and microcontrollers.
3.	Network connectivity	• Service providers, local LANS and mobile networks (including 4G and 5G) are responsible for transporting

Sr. No.	Element	Description
		data and keeping us connected.
4.	Platforms	Cloud-based services that collect and handle the terabytes, petabytes, and exabytes of data generated by IoT devices might be among them.
5.	Data analysts and scientists	Individuals who process IoT device data to provide usable, actionable information.
6.	IT workers and managers	In charge of controlling end points and IoT network traffic throughout the device lifespan and for maintaining the IoT infrastructure.
7.	Cybersecurity workers and managers	The people in charge of controlling cyber threats, implementing IoT security rules, and enabling data protection methods.
8.	AI and machine learning	Services that are often linked to IoT/ICS data to aid in automating device operation, data gathering, and information processing.

Common Threats

Many times, mistakes or omissions occur as developers create the IoT/ICS hardware and software. No one is perfect.

However, these mistakes can result in the following flaws:

i. **Inadequate default settings:** IoT devices that contain default settings may include default passwords and other settings that cannot be changed.

ii. **Non-existent upgrade paths:** Sometimes, it is impossible to update the firmware or other information itself, making the device permanently toxic to healthy IoT networks.

iii. **The use of inappropriate technology:** Many times, organizations will place powerful software onto an IoT device, even though such computing power is not necessary. For example, IoT manufacturers have placed complete Linux operating system on an IoT device, when only a portion was necessary. As a result, once the IoT device was compromised, it became a powerful weapon in the hands of an attacker.

IoT security is one of the major cybersecurity challenges today. Several challenges exist. IoT and OT devices can also provide a rich breeding ground for attackers who want to conduct Distributed Denial of Service (DDoS) attacks, such as through botnets.

A botnet is a large collection of devices that have fallen under the control of a centralized attacker or group of attackers. A botnet can include tens of thousands, or even millions of devices. Attackers can use these botnets to wage DDoS attacks or introduce malware to new victims. Many of the security breaches that find their way into the news are the results of botnets.

IoT devices can also be used to introduce new forms of malware, which attackers then use to compromise more organizations. Service providers of all types, from cellular network providers to cloud providers and finance companies, continue to be concerned about these security risks.

Types of Cybersecurity Threats

IoT devices that are not properly developed or secured can result in the conditions found in Table 2.

Table 2: Represented the Different Conditions in IoT.

Sr. No.	Condition	Description
1.	Service disruption	• Manipulating an IoT device or devices to make an essential service (e.g., a power generating dam, the water system, a database) completely unavailable.
2.	Data theft	• Gaining improper access to personally identifiable information (PII), such as names, user accounts, social security, national health ID numbers, telephone numbers and residence addresses. Increasingly, organizations and individuals alike are concerned about the use – and misuse – of personal information.
3.	Data or service manipulation	• Where the attacker can make arbitrary changes to the settings of a device, which can cause loss of life, loss of service, damage to the device itself or damage to other devices.
4.	Non-compliance	• Governments worldwide have enacted laws designed to protect privacy. Such laws include the European Union General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPPA), and the California Consumer Privacy Act (CCPA), among many others.

Notable IoT Attacks

As the number and intensity of IoT attacks increase, several notable attacks have been made public. Here are a few examples in Table 3.

Table 3: Represented the Notable IT Attacks.

Sr. No.	Attack	Description
1.	Mirai botnet (Dyn attack)	• In 2018, the Mirai botnet created such a large volume of garbage traffic (just over 1 Tbps) that much of the internet was inaccessible in various countries.
2.	Stuxnet	• In 2010, attackers disabled the centrifuges used in Iran that were being used to create fissile nuclear material.
3.	Brickerbot	• In 2017, an attack that did more than just clog network traffic or misconfigure devices. This particular attack actually "bricked" the infected device, making it no longer usable.
4.	Abbot / St. Jude Hackable Pediatric Pacemakers	• In 2017, attackers demonstrated the ability to manipulate the firmware of over 465,000 implanted pacemakers, making it possible to drain the pacemaker battery, steal sensitive data or even change life-saving settings on the pacemaker itself.

The Future of IoT Cybersecurity

Additional technological and personnel solutions do exist. Here are a few ways IT professionals can improve their security posture when it comes to IoT devices.

i. **Enhance monitoring of devices:** The use of intrusion detection systems (IDS), as well as a security information and event management (SIEM) system can help so can the practice of information sharing. Using cybersecurity threat intelligence (CTI), it is possible to profile attackers and more intelligently position security controls for IoT and ICS devices.

ii. **Add security features:** Features such as the functionality that encrypts all stored and transmitted data can help. Enhanced authentication schemes can also help control connections. Additionally, workers can learn how to better partition and segment IoT traffic so that it can be easily controlled and managed. This way, they can respond better to security breaches.

iii. **Follow IoT and ICS standards:** The National Institute of Standards and Technology (NIST) has published many cybersecurity standards, including Recommendations for IoT Device Manufacturers. It has also provided a helpful page that outlines its Cybersecurity for IoT Program.

IoT and ICS/OT devices will be in our lives for the foreseeable future. It is up to cybersecurity professionals to make sure that these devices will continue to help us conduct business and enjoy life, rather than be a problem.

LITERATURE REVIEW

M. Roopak et al. discussed that in this chapter, we present deep learning models for IoT (Internet of Things) networks' cyber security. The Internet of Items (IoT) network is a promising technology that integrates both living and non-living connections between different. IoT deployment is expanding quickly, but there are still security gaps, making it vulnerable to many cyber-attacks. For any network to succeed, the network must be secure; otherwise, consumers may be hesitant to utilize this technology. Many IoT networks have recently been impacted by DDoS (Distributed Denial of Service) attacks, which may have caused significant losses. To identify DDoS attacks, we suggested deep learning models and tested them employing the most recent CICIDS2017 datasets, which delivered the greatest accuracy of 97.16%. The proposed models are also compared to machine learning methods. The use of algorithms for deep learning for IoT cyber security is also subject to open research problems, which are listed in this study [1].

K. Kimani et al. illustrated that work is being done to make the electric system more intelligent to make it more receptive to consumers' energy demands and to deliver increased effectiveness and reliability of power systems. The energy needs of the 21st century are expanding quickly because of population expansion. One of the enabling technologies for a smarter grid network is the Internet of Things (IoT). One of the biggest issues is security as IoT-linked devices continue to increase quickly. Since the devices are online, the smart grid is exposed to serious assaults. An IoT-based smart grid provides the largest attack surface for an IoT-focused cyber-attack since it might encompass millions of nodes. Given the potential cascading effects of shutting down the electricity grid and the fact that a large portion of the devices in our homes, offices, hospitals, and trains depend on electricity to operate, a cyber-attack on a smart grid would just have devastating effects on the dependability of widespread infrastructure. When only one piece of the grid is hacked, so this whole system is open to assault. Such cyber-attacks on the supply of energy may bring whole cities to a standstill, resulting in enormous both financial and economic losses. Because of this, security must be carefully considered before IoT-based smart grid networks are extensively deployed. The main obstacles and security problems impeding the development of IoT-based smart grid networks are addressed and looked into in this research [2].

R. Ande et al. stated that the IoT has expanded into a variety of spheres of daily life in recent years, including smarthomes, smartcities, agriculture, offices, and businesses. Lighting, locks, and industrial machinery are examples of mundane physical objects that may now be a part of the IoT ecosystem. To boost the safety, effectiveness, and comfort of our lives, the Internet of Things has reimagined how critical and non-critical systems are managed. IoT technology has a significantly good influence on our lives as a consequence. IoT systems have drawn unnecessary attention from criminal users that seek to exploit defects in IoT systems to gain a personal advantage, known as cyber security attacks, in addition to these good aspects. The paper is appropriate for researchers, practitioners, and students, especially those from industries like computer networking, information technology, or electronics. The paper opens by proposing IoT as the product of communication capabilities' 200-year history. IoT began to be used by customers around 2014. The first IoT devices were almost always local closed IoT networks, which were followed by huge networks like smart cities. Next Generation Internet, or NGI, is an expansion of NGI that includes human values. This evolutionary introduction is followed by a comparison of IoT designs and also an introduction to some of the methodologies that make up each architectural layer. Finally, the paper wraps up with possible future advancements. Security

problems inside each architectural layer are examined, as well as various mitigating measures [3].

A. Shivanathan et al. embellish in their study that Internet of Things (IoT) devices that are procured from a wide range of companies and deployed in significant numbers are subject to increasing cybersecurity vulnerabilities. Therefore, it's becoming increasingly crucial for network operators to control these devices. Existing network monitoring systems analyse traffic using specialist acceleration on managed switches or thorough packet inspection in software, but these technologies may be difficult, costly, rigid, and unsustainable. In this study, we use the SDN paradigm together with machine learning to take advantage of adjustable flow-based telemetry and customizable data-driven models to control IoT devices thus according to their network activities. We examine the traffic patterns of actual consumer IoT devices that were gathered in our lab over six months, and we identify a set of car traffic (per-device) whose time-series characteristics computed at multiple timescales describe the network characteristics of different IoT device types, as well as their operating states and conditions. We create a multi-stage infrastructure of inference models that automatically differentiate IoT devices from non-IoTs, describe various IoT device kinds, and determine their operational conditions. We leverage actual traffic traces to train our models, test their effectiveness, quantify the trade-off involving performance and cost of our technology, and show how our watching scheme can be used in application to spot lifestyle patterns [4].

P. Radanliev et al. illustrated that new kinds of cyber dangers become sparked by the Internet of Things (IoT). Therefore, a consciousness of IoT cyber security posture is important before integrating new IoT products and services. This paper employs the expression security posture to describe an organization's ability to evaluate, stop, and react to cyber threats. Because there are currently no self-assessment procedures for calculating IoT cyber risk assessment, there is a gap in the state of the art. An empirical evaluation of the techniques to cyber risk management is carried out to fill this gap. Following conclusions and comments on a transformation pathway that describe how IoT systems might attain the target state with either a new goal-oriented dependency model, the results and key findings from the study are provided as the contemporary and target risk posture for IoT systems. The cyber security target that satisfies the general security needs of an institution is referred to as the target state. Goal-oriented dependency programming is identified as the leading method among the risk management models explored in academics, which examines and adapts multiple choices for IoT risk assessment. The novel goal-oriented dependencies model outlined in this paper allows for the quantitative self-evaluation of the IoT cyber risk posture and the measurement of unmanageable possible risks in complex IoT systems.

I. Kotenko et al. stated that sophisticated methods to look into the software of current IoT gadgets to ensure their security. Computer simulation is one of the most popular techniques that has consistently been demonstrated to be successful. But as IoT systems grow in size, their connections get more complex, and their components become more diverse, their job must be automated and intellectualized. To do this, a presumption is maintained that machine-learning techniques may be used for static analysis of IoT systems. A study was an attempt that reflects the study's ontology and aims to support the hypothesis provided. The following are the main contributions to the work: organizations to meet static analysis stages for IoT systems and decision-making of machine-learning problems throughout the form of codified models; review of all publications in the field and analysis of findings; confirmation of the suitability of

machine-learning monitoring systems for each static data analysis; and the proposal of an intelligent conceptual model concept for the static analysis of IoT systems. The uniqueness of the results is a consideration of the entire horizontal analysis process, consideration of each stage from the standpoint of the full set of machine-learning answers, and codification of the stages and quick fixes in the form of data transformations.

A. Rasool et al. illustrated that with the flexible architecture that clouds computing offers, data and resources may be distributed across many different places and accessed from either a variety of industrial settings. Utilizing, storing, and sharing resources including data, services, and solutions for industrial applications have mostly altered as a result of cloud computing. In the last ten years, companies have started shifting to cloud computing to take advantage of greater performance, reduce premiums, and more extensive access. Additionally, the internet of things (IoT) has significantly improved when cloud computing. However, this quick shift to the cloud brings up several security issues and difficulties. The following are some of the research's findings: We present a thorough analysis of the supporting cloud-based IoT architecture, services, arrangements, and security models; the normative framework of cloud security concerns throughout IoT into four major categories, which are discussed in great detail; we identify and examine the most recent developments in cloud-based IoT attacks; we recognize, discuss, and analyses significant security vulnerabilities in each category and preemptive measures; and finally, we present a comprehensive study of the cloud security concerns.

M. Gunduz et al. discussed that one of the most important uses for the Internet of Things is the smart grid. The advancement of smart grid cyber-physical systems goes hand in hand with the development and use of information and communications technologies in conventional power systems. Smart grid systems powered by IoT are crucial infrastructures that feature intricate patterns and crucial components. They contain communication systems that, should the secrecy, integrity, or availability of the transmission be compromised, might result in gaps in national security, disturbances of the peace, fatalities, or serious economic harm. These massive systems might be subject to cyber-attacks. As a result, there is a lot of research being done in corporate, government, and academia to strengthen smart grid security. To increase protection against cyber-attacks in smart grid applications, security strategies are crucial. We give an extensive survey that is backed up by a careful examination of prior studies. Additionally, recent trends and defenses in cyber security for smart grids are highlighted. The risks and possible remedies associated with an IoT-based smart grid are investigated in this study. We provide a thorough analysis of the smart grid's cyber-security condition while concentrating on various types of cyber-attacks. We specifically focus on the investigation and debate of network vulnerabilities, attack defenses, and security needs. In addition to offering a roadmap for future research on cyber-security in smart grid applications, our purpose is to provide a thorough understanding of the vulnerabilities and answers [5].

DISCUSSION

Domains of Internet of Things

IoT includes trillions of sensors, trillions of intelligent systems, and millions of applications, to name a few. Domains for Applications. Currently, IoT may be found in four widely used domains [6]:

i. Manufacturing/Industrial business - 39.9%

ii. Healthcare - 31.31%

iii. Security - 8.2%

iv. Retail - 9.1%

IoT Energy Domain

In the realm of energymanagement and control, the Internet of Things is crucial. Smart Energy System is the term referring to such a system. IoT apps take into account several energy management capabilities for both home and professional usage and also shown in Figure 1.

i. Residential Energy:

The cost of electricity is rising along with technology's exponential growth. Consumers look for means of lowering and controlling their energy costs. IoT offers a sophisticated method to evaluate and improve how a gadget and a home's complete system are used. To reduce energy consumption, devices could simply be turned on or off or their settings changed [7].

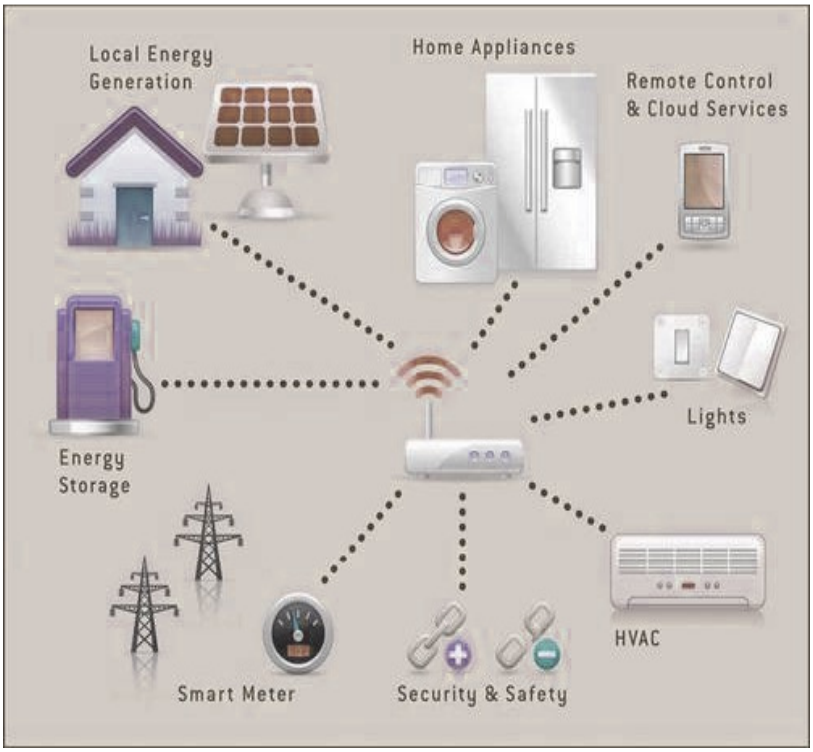


Figure 1: Display the Different IoT Energy Domains.

ii. Commercial Energy:

Energy waste has a significant influence on the cost of production for all corporate organizations. IoT offers a particular method for sustaining a high quality of care at a minimal cost. IoT systems provide a powerful way to control energy consumption costs and maximize business productivity. It identifies energy problems in a complicated corporate network in almost the same way it identifies functional problems and offers solutions.

iii. Reliability:

By delivering information and taking action, IoT technology maintains the system's dependability. It anticipates risks to system stability and performance, mitigating losses like damaged equipment, downtime, and accidents [8].

There are many Modern Applications used in this technological era which are mentioned below:

1. Smart Grids and energy saving
2. Smart cities
3. Smart homes/Home automation
4. Healthcare
5. Earthquake detection
6. Radiation detection/hazardous gas detection
7. Smartphone detection
8. Water flow monitoring
9. Traffic monitoring
10. Wearable
11. Smart door lock protection system
12. Robots and Drones
13. Healthcare and Hospitals, Telemedicine applications
14. Security
15. Biochip Transponders (For animals on farms)
16. Heart monitoring implants (Example Pacemaker, ECG real-time tracking).

DISCUSSION

Modern society depends on the internet of things gadgets to provide us with vital and on-demand services. IoT devices are practically everywhere in our everyday lives, including schools, smart cities, transportation, and houses. Due to better data processing methods and advanced analytic approaches based on IoT, the use of internet of things devices has favorably influenced enterprises. This helps to establish a more efficient and reliable institution infrastructure. As a consequence, several enterprises in both the public and private sectors implement various laws to safeguard their internet of things systems from cyber security risks. In this document, I've suggested several options to safeguard confidential information for academic and commercial organizations. Future work will focus on finding creative ways to provide users with numerous levels of cyber security knowledge simple control placed above a white protecting internet of things devices from cyber security risks. Furthermore, it should be recognized as an urgent necessity to standardize the data gathering and sharing processes used by internet of things devices that are linked to the internet. With the help of this initiative, there will be greater internet of things gadgets in use worldwide while fewer network security dangers are there. The

advantage of internet of things devices should really be clear to users, who should also capable of adapting to changes in the new technology.

REFERENCES

[1] M. Roopak, G. Yun Tian, and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2019, pp. 0452–0457. doi: 10.1109/CCWC.2019.8666588.

[2] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.

[3] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustain. Cities Soc.*, vol. 54, p. 101728, Mar. 2020, doi: 10.1016/j.scs.2019.101728.

[4] A. Sivanathan, H. Habibi Gharakheili, and V. Sivaraman, "Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 60–74, Mar. 2020, doi: 10.1109/TNSM.2020.2971213.

[5] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Networks*, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.

[6] X. Jia *et al.*, "IRBA: An Identity-Based Cross-Domain Authentication Scheme for the Internet of Things," *Electronics*, vol. 9, no. 4, p. 634, Apr. 2020, doi: 10.3390/electronics9040634.

[7] E. Aydin and D. Brounen, "The impact of policy on residential energy consumption," *Energy*, 2019, doi: 10.1016/j.energy.2018.12.030.

[8] T. Cui and S. Li, "System movement space and system mapping theory for reliability of IoT," *Futur. Gener. Comput. Syst.*, 2020, doi: 10.1016/j.future.2020.01.040.

CHAPTER 6

AN ELABORATION OF FRAMEWORK OF CYBER SECURITY WITH ENERGY INTERNET

Dr. Anilloy Frank, Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- anilloy@presidencyuniversity.in

ABSTRACT

Through the orchestration of cyber-physical structures, coordinating dispersed technologies, operations and maintenance and forecasting frameworks across all energy players, and smart local energy infrastructure, personalized regional solutions may be supported. The multi-objective optimization of many success factors may greatly benefit from unprecedented access to innovative data streams, information, and controls. To facilitate the widespread adoption of cyber-physical networks, this research provides a detailed and critical analysis of the current standards and also suggests areas to concentrate on. Even though that current protocols and specifications are very fragmented, our research indicates that many of them can satisfy the needs of the SLES applications and infrastructures. Due to the growing necessity of information security and personal privacy, several standards have also been developed to safeguard these areas. The study proposes that the sector would have to provide more accessible and safe online products and services. Information can be added on the minimal functionality and security demands for apps should be made available to the authorities and government. To guarantee that the components of the SLES ecosystem have a satisfactory security level by design, conformance tests and certifications should also be in place and conducted by an impartial third party.

KEYWORDS: Energy Internet, Embedded System, Internet of Things, Sensor Devices, Smart Homes.

INTRODUCTION

The Rambus IoT Security Framework is a series of embedded software toolkits that provide a wealth of security protocols, such as TLS and IPsec, to cost-sensitive devices that have an inadequate ability to secure the internal SoC. The IoT Security Framework offers a standard API that includes the required cryptography and certificate capabilities. It was created for Internet of Things (IoT) devices and cloud-based applications. Designers can still choose either FIPS 140-2 or FIPS 140-3 level 1 certified or DPA-protected crypto libraries, depending on the particular demands of the application. The FIPS TLS toolkit offers a FIPS-compliant software package that enables development teams to securely access any popular cloud service for their device in conjunction with a pre-integrated FIPS library as displayed in Table 1.

Table 1: Represented the Software Packages for Security Control Access.

Sr. No.	Solution	Description
1.	DPA Resistant Software Libraries	Provides the professional cryptographic library needed to secure connected devices.

2.	Secure Boot	Provides tools for integrating security into an embedded device's system boot sequence. Uses strong cryptography to protect the boot process of SoCs and application processors.
3.	FIPS TLS Toolkit	FIPS compliant TLS 1.3 implementation for embedded devices.

Over the last several years, there's been a rise in security assaults on smart grids. These assaults have increased environmental worries and caused substantial yield losses. The smart grid's present security posture is insufficient to fend off all current and future security intrusions. The idea of Energy Internet (EI) and its implementation will dramatically increase the security of the dc microgrid. EI is envisioned as an integrated solution with power flow and multidirectional communication methods for strengthening the smart grid. Real-time data collection and analysis are accomplished using IoT technology to support intelligent energy management. EI makes ensuring that all aspects of the energy industry are fully linked, including production, transmission, distribution, operations, service providers, markets, end users, and regulators. It makes it possible to gradually switch from non-renewable to alternative energy sources, supporting energy management schemes like those that aim to improve the environment and the economy. The term "EI" may also be used to describe a software platform that controls, monitors, and manages the whole smart grid with an emphasis on interconnectedness across all power systems. In addition to intelligent energy management, automated misdirection and adjusting of energy consumption, energy security, asset depreciation control, and availability of smart energy options to clients, it offers new energy efficiency. EI is envisioned as the technology that would improve the smart grid and make it even smarter with the use of IoT for the whole future smart grid infrastructure as display in Figure 1.

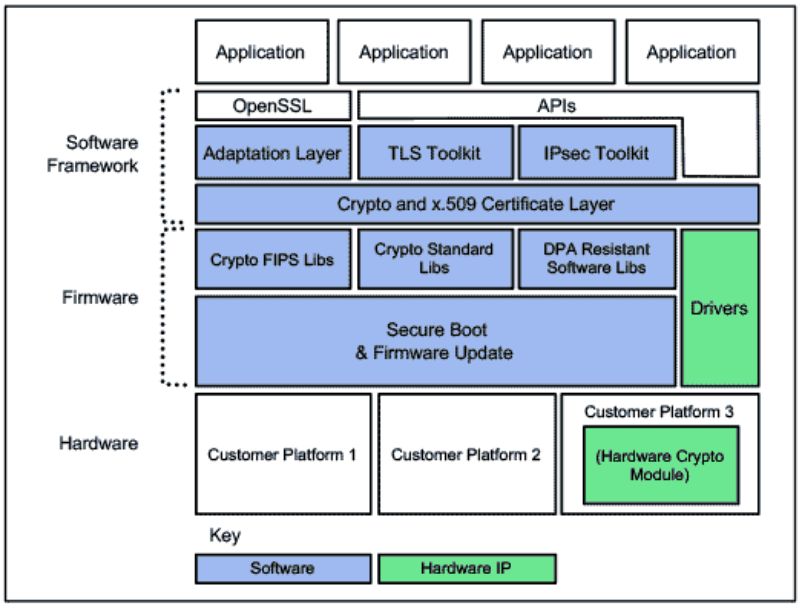


Figure 1: Represented the Future Smart Grid Infrastructure.

Sensing and actuating are vital factors of many assets in the energy domains, where they are significant enablers for improving operational and communication efficiency. The ability of IoT in EI to manage energy well promotes the quick identification of security problems and assaults. However, it is extremely difficult to develop a framework that is completely safe and effective when detecting and preventing security flaws and attacks in EI owing to the complexity of the IoT. The capacity to leverage IoT to manage and monitor all of the operations and features of the smart grid is one of the key elements of EI. Even if research on EI security is still in its early stages, the impact of security software frameworks is developing in the industry. The EI has significant problems as a result of security assaults on assets, data, networks, users, and applications. We need to research and find solutions for these security assaults as well as other issues like risk management and network assurance.

The cyber-security methodology for the IoT-based EI that we provide throughout this study takes into consideration the current security issues with the smart grid. An identity-based security mechanism (I-ICAAAN), a secure communication protocol, and an effective security system for energy management are all included in the proposed framework (ISSEM). Integrity, confidentiality, availability, authenticity, authentication and nonrepudiation security aspects are represented by I-ICAAAN. End-to-end security in EI is provided by integrating the security parameters to support components, data, and events in EI. This is capable of mitigating security vulnerabilities and assaults and resolving the difficulties with security misconfiguration including session mismanagement confronting the smart grid. To communicate securely amongst all components of the EI, the secure communication protocol makes advantage of the I-ICAAAN. The security state of the EI is evaluated and analysed using the ISSEM. To examine the security behaviours of the energy components as suggested in this work, an Intelligent Security Unit for Energy Management (ISUEM) that is controlled by the ISSEM is integrated into a resource management device called an Energy Router. The suggested framework will aid in minimizing security issues inherent in the current EI design as well as bolstering the smart grid's security measures.

Our main contributions are:

- **i.** Recognizing cyber-attacks on the smart grid.
- **ii.** Advising I-ICAAAN, which considers numerous security requirements for privacy and security.
- **iii.** Outlining a secure communication protocol that enables data transmission in a safe manner and guards against different security threats.
- **iv.** Recommending an ISSEM that incorporates an ISUEM to boost the energy router's security capabilities;
- **v.** Outlining a framework for cyber security that makes use of the I-ICAAAN, secure communication protocol, and ISSEM to tackle the scale-up analysis and remediation of significant smart grid security vulnerabilities.

The I-ICAAAN offers the EI a platform for security and privacy. All components in EI are certified and registered by default using identification and authentication security settings. The secure communication protocol is tested using an Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, while the I-ICAAAN is principally assessed using

theoretical analysis. Nash equilibrium is used to examine and evaluate the ISSEM because it has characteristics that make it possible to analyse how different players interact and produce outcomes.

Energy Internet Architecture and Security Requirements

Energy Internet represents a new convergence between communication, energy and the internet. In this section, we first examine a simple Energy Internet architecture from which we identify and present the Energy Internet security requirements. The Energy Internet architecture is made up of elements that are capable of providing security and privacy to components, data and events in Energy Internet thereby supporting energy management.

i. Energy Internet Architecture

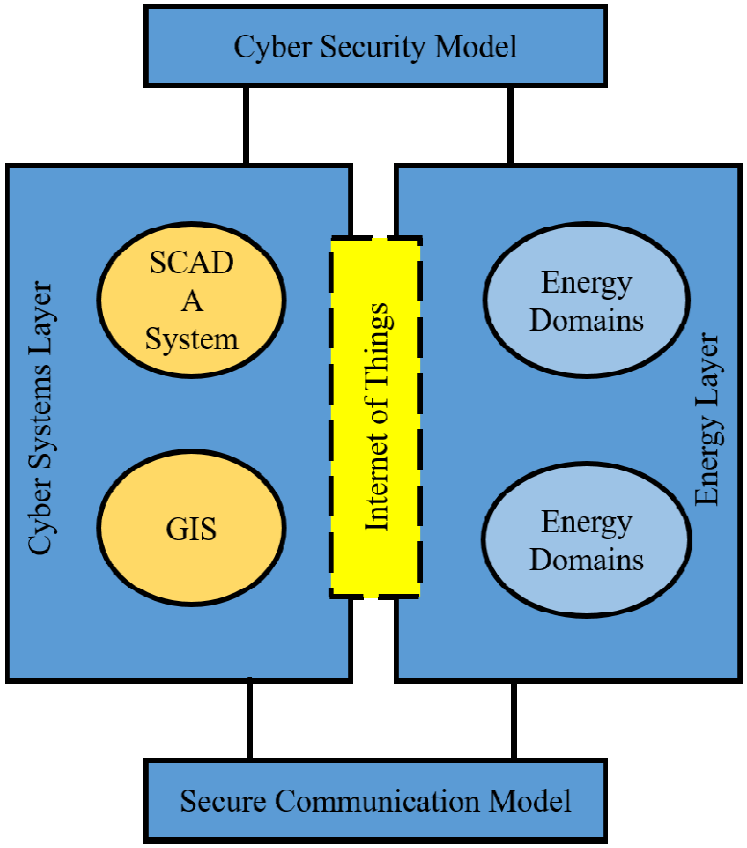


Figure 2: Represented the Effectiveness of Energy Internet.

As shown in Figure 2, we describe the energy architecture to ensure its effectiveness in securing and maintaining privacy across all its components. It should be noted that IoT serves as the underlying element that supports the EI architecture. We present the interconnected elements of the EI architecture, which rely on the IoT for connection and interaction with one another. These elements include:

1. Cyber Systems Layer

2. Energy Layer
3. Cyber Security Model
4. Secure Communication Model.

These elements contribute to the security of the energy internet. Brief descriptions of the elements are given below:

a. Cyber Systems Layer:

This element is responsible for providing, overseeing and monitoring the cyber systems across the EI. Two major supporting technologies of this element are supervisory control and data acquisition (SCADA) system and geographic information system. The SCADA system is used for monitoring and controlling operations in EI. Using IoT-based SCADA provides improved monitoring and timely decision-making in the smart grid. The GIS is used for analyzing and processing real-time geographic data to enhance the management of energy and reduce maintenance cost and time. Real-time data from the grid are displayed by the GIS to optimize the performance of the smart grid network. IoT is characterized by energy efficiency and is considered an enabler responsible for providing all connections and interactions that are utilized by these supporting technologies and other elements in the EI. The changing resource constraints such as system resources, operations and performance in Information and Communication Technologies (ICT) have been addressed by IoT for adequate decision-making and support, thereby preventing any negative impact on the EI architecture. The proposed framework will assist in providing end-to-end security and privacy to this layer for efficient energy management support.

b. Energy Layer:

This element is responsible for energy management across the energy domains and energy resources [35] of the EI. With the help of IoT, the energy layer is managed smartly and intelligently. In this paper, we use the smart grid energy domains and introduced three additional entities to support the security and privacy of the EI. These additional entities include:

1. Regulator/Legal
2. Cyber Security Change Authority (CSCA)
3. Cyber Security Assurance Authority (CSAA).

The regulator/legal will monitor, enforce and automate energy compliance across the energy domains. Both the CSCA and CSAA are cyber security authorities of the EI. The CSCA is a cyber-security authority assigned to authorize and deal with change specifications within the agreements made on cyber security. It is assigned collectively by the energy domains, excluding the CSAA. The agreement is made by the concerned/associated domains (including regulators/legal and excluding CSAA). The CSAA is presented as an entity assigned to monitor the cyber security performance and changes associated with the EI. It is assigned collectively by the energy domains, excluding the CSCA. In addition, one of the energy components utilised by the EI architecture is the energy router which is presented as a concept in energy internet that controls energy flow and information exchange. The energy router uses a communication

module for communication amongst power components. Thus, the energy router is utilized in the proposed secure communication model and it is sub-divided into the following:

1. Renewable energy sources (high rates)
2. Non-renewable energy sources
3. Energy storage.

Renewable energy sources include wind, solar, rain, waves, tides and geothermal heat while non-renewable energy sources include petroleum, coal and natural gas. Furthermore, IoT ensures that all energy sources are inter-connected for efficient energy management.

c. Cyber Security Model

This element provides end-to-end security and privacy to all layers in the EI. It models and assesses the relationship and dependencies between the Functional Security Area (FSA) and Logical Security Area (LSA) of the EI as shown in Figure 2. The emergence of IoT enables the adoption of an extensive approach to cybersecurity for privacy and security improvement in smart grid [37]. With the support of IoT, the FSA interacts with the LSA in real-time to improve energy management. Major entities in FSA are briefly described as follows:

1. **Asset:** This consists of all the energy infrastructure.
2. **Data:** This represents a set of values and information.
3. **Network:** This provides the pathway for connection, communication and services.
4. **Software:** This represents energy applications and programs.
5. **Users:** These are energy operators and customers.

d. Secure Communication Model

EI's complete architecture is coordinated via communication. A secure communication model is described to enable end-to-end secure data flow in EI given the range of communication methods accessible in the smart grid. All locations are constantly accessible since IoT has made it possible for components to communicate with one another without the need for human intervention. Reliability, availability, security, and maintainability are the essential metrics for communication in EI. To guarantee the dependability, availability, security, and maintainability of communication in the EI, the secure communication model offers the security and privacy concerns necessary. End-to-end secure communication is one of the most important factors to take into account when designing an EI architecture because it helps prevent security attacks like DoS attacks, replay attacks, MITM attacks, impersonation attacks, Sybil attacks, false data injection attacks, and repudiation attacks. To provide end-to-end secure energy flow in EI, the secure communication model also offers communication security to the energy router. The key elements of the secure communication paradigm are briefly described below:

1. Intrusion Detection System (IDS):

To detect harmful behavior during communication and operations in EI, this is either a hardware or software component. To fight against possible security flaws and attacks on IoT-based applications, the IDS is used as an extra component.

2. Firewall:

This might be a hardware or software solution that can monitor and regulate network traffic following the security guidelines necessary for efficient energy management. A firewall is used to offer access control and assist communication security due to the sensitivity of the enormous quantity of data on components and events acquired by IoT in every setting.

3. Historian Server:

This corporate server contains data and resources from businesses to help energy management. The historical server is used in this study to enhance data security in EI.

4. Secure Programmable Automation Controllers (Secure PACs):

These securely integrate the capabilities of Programmable Logic Controllers (PLCs) with Remote Terminal Units (RTUs). In support of SCADA systems or remote controllers for energy applications, they serve as local control systems. IoT allows the automation of the smart grid via PACs.

5. Simulation Server:

The operations of the actual systems are replicated by this virtual server. To conduct security tests and investigations, it replicates the energy environment.

6. Sensors and Actuators:

The operations of the actual systems are replicated by this virtual server. To conduct security tests and investigations, it replicates the energy environment.

The number of devices being deployed and the wide range of applications for which they are used have both grown significantly in the Internet of Things. Their size, computing capabilities, storage capacity, and energy all vary considerably. An Internet of Vulnerabilities has been established by the rapid advancement and incorporation of IoT in several fields and aspects of our everyday life. Security and privacy are not being effectively addressed in the race to create as well as deploy IoT devices. IoT devices are susceptible to cyber-attacks, which put user and system privacy and protection at risk since many of them are heavily restricted. This survey offers a comprehensive overview of IoT in terms of application areas, security architectural approaches, current IoT security and privacy challenges, as well as an examination of previous research on IoT security and privacy that are comparable to this one. The study also offers an in-depth taxonomy of IoT attacks based on the three-layer architecture, including the perception, network, and application levels, as well as a prescription of how these assaults may affect CIA goals in sample devices. The paper also provides mitigations and countermeasures, using a diversified strategy rather than a per layer strategy. To provide researchers access to the most current research on pressing issues related to protecting the IoT ecosystem, open research fields are also addressed [1].

Industrial Internet of Things (IIoT) has emerged as a crucial area of research and development that holds the potential to improve the productivity of real-time data gathering, recording, analysis, and administration of all machine activity, as well as likely to be resolved quality and lower costs. Traditional IIoT relies on centralized systems that may be accessed via single points of failure and other types of cyber-attacks. To shift traditional structures into distributed ones, blockchain technology evolved. Blockchain technology is used in contemporaneous industrial settings because it may provide high levels of security, minimal processing complexity, P2P

communication, transparent logging, and decentralization. The current study suggests using a private blockchain mechanism for a practical process in a cement plant. This mechanism provides a low power consumption, scalability, and a lightweight cryptography scheme; it can also effectively manage access to vital information generated by sensors and actuators. Additionally, to guarantee safe authentication, scalability, speed, and energy efficiency, our blockchain network employs proof of authentication as an agreement method so instead of proof of work. Our test results demonstrated that the suggested framework combines excellent performance, high levels of protection, and scalability for smart industrial facilities.

The variability and absence of transparency in the processing of the evidence, and computer forensics are crucial in the IoT paradigm. Additionally, cross-border legalization hinders this operation concerning cloud forensic difficulties. This necessitates the establishment of an IoT forensic framework that facilitates distributed computing, independence, and transparency of scientific analysis of digital evidence from a global context. To do this, we provide a methodology for Forensic investigation that takes care of the aforementioned problems. The Internet-of-Forensics (IoF) suggested solution involves taking into account a blockchain-specific IoT infrastructure for digital forensics. The investigative process is publically seen, including all related personnel in a single framework. It handles the investigative process, including chain-of-custody and evidence chain, using a blockchain-based case chain. In a consortium, concerns with cross-border regulation are resolved by consensus. Additionally significant are the transparency and simplicity of forensic references. Reduced complexity is produced via the programmatic lattice-based cryptographic primitives. It highlights the advantages of power-conscious devices and amplifies the uniqueness of the suggested solution. IoF may be utilized by independent security operation centers, cyber-forensic investigators, and manually started shreds of evidence underneath chain-of-custody for crimes committed by humans since it is general. Security services are ensured following the framework. IoF is tested and contrasted with different blade frameworks. Results and analysis demonstrate that IoF is effective in terms of sophistication, time, memory and CPU use, fuel efficiency, and energy analysis.

The next scientific and technical transformation for interactions between omnipresent elements in cyber-physical-social settings is being ushered about by the Internet of Things (IoT), an emerging network paradigm. By facilitating the relatively stable interconnection of the existing science and engineering system for an unavoidable infrastructure reconfiguration, the IoT has a consequence on it. In this paper, we investigate a modernized scientific and technology paradigm for the Internet of Things. The Internet of Thinking (IoTk) is specifically used to establish a novel cyber-physical-social-thinking (CPST) space, and a framework for science and technology is afterwards proposed that needs to take into account both the scientific and technological aspects. We describe the current framework of science and technology from the standpoint of traditional Chinese culture, where the Five Elements share characteristics with the restructured cyber-physical science in the IoT. To further highlight the electrochemical analysis of the IoT, we introduce a hypothetical smart city scenario and talk about its key enabling technologies, such as resources development, energy management, database administration, session management, encryption and privacy, loop control, space-time consistency, nanotechnology, and paper physics technology. It turns out that the framework of existing research and technology will be the foundation for innovation for the communities of both academia and industry [2].

The power cyber-physical systems (PCPSs) are taking use of all facets of societal concerns as they get more sophisticated and diversified. A PCPS is a cutting-edge system that tightly

incorporates systems for computing, telecommunication, control, and power. The Internet of Energy, which is the energy resource of the future, is created through the integration of PCPS and the Internet of Things. Similarly, the interconnectedness of large components and the significant interactions within them have created several security concerns. As a result, this work presents a study of the analysis and evaluation of the security and dependability of PCPS. Models for a broad cyber-Attack are created by putting into consideration the dangerous uncertainties, and a double-loop security defensive architecture is developed. According to this structure, the characteristics of each kind of cyber-attack are used to improve security control scenarios. Finally, the issue is shown just use a separately stimulated dc motor exhibiting uncertainty [3].

An emerging kind of energy system is the "energy internet." It achieves the integration of business, informational, and energy flow. The Energy Internet is encouraging more and more breakthroughs in business and service models. In this paper, we provide a complete analysis of the Energy Internet from an economic standpoint. We start by outlining the phases of energy systems' development. Energy systems have mostly gone through four phases since their invention during the second industrial revolution: decentralized energy system, centralized energy system, distributed energy system, and smart & connected energy system. The fourth growth stage of energy systems is characterized creatively by the energy internet. Presume, micro grid, Virtual Power Plant (VPP), smart grid, and smart energy are a few more important Sources of energy Internet ideas that are introduced. The commercial benefits of the Energy Internet are then explored from the standpoint of energy big data analytics. Last but not least, the Energy Internet business areas of research are highlighted from five key dimensions: strategic problems, data issues, behavior problems, security challenges, and regulatory issues [4].

Software Defined Networking (SDN), a new network model, has gained widespread acceptance. SDN has been successfully employed in a variety of network domains, including data centers, WAN, corporate, optical networks, and energy Internet, due to its inherent benefits. SDN-based energy Internet systems are one of them that are getting becoming more and more attention. However, several issues and obstacles are also progressively attracting attention. The current conventional electric energy market model will no longer be applicable since the SDN-based energy Internet has a distributed architecture for renewable energy. Due to its decentralization, coordinated autonomy, and non-comparability, the blockchain has swiftly grown and been deployed in a variety of fields. We suggest a blockchain-based SDN-based distributed energy stock exchange for the internet. Under the presupposition of privacy protection, the suggested approach successfully matches the transaction objectives in a balanced way. Finally, we completed a thorough, methodical security and applicability examination of the suggested remedy, further demonstrating that the system satisfies our design objectives [5].

A. Saini et al. stated that the adoption of Internet of Things into the smart grid infrastructure has significantly improved, and as a result, demand for cyber security is rising quickly. All of the security flaws in the current smart grid are carried over to the energy internet, also known as the integrated internet-based smart grid and energy resources. The smart grid's security architecture can no longer satisfy the 21st-century energy industries' security requirements. In this paper, we provide a cyber-security paradigm that may allow effective power management in the EI while offering sufficient security and privacy. The proposed framework certifies security and privacy in the EI using an identity-based failsafe mechanism, a secure communication protocol, and an intelligent security system for energy management. The assessment of our suggested intelligent

security system for energy management based on secure event allocation uses the Nash Equilibrium solution of game theory. Theoretical study and formal verification demonstrate that our suggested architecture improves security and privacy for IoT-based energy internet [6].

S. Hussain et al. illustrated that idea called the "energy internet" which aims to efficiently capture, regulate and manage energy resources with the use of information and communication technologies. Connecting the smart grid to the Internet increases the flexibility of the system and allows for better utilization of energy resources. For the operation and administration of the Energy Internet, a scalable and reliable information and communication infrastructure are essential. An energy router (ER), also known as a communications router and used to manage or route electrical energy, routes data packets rather than energy packets. This study provides a comprehensive analysis of the development of the Energy Internet in terms of its architecture, different ER types, and the advantages and disadvantages of its use. This study also includes a comprehensive overview of the design and architecture of different types of ERs. The benefits of the Energy Internet have been highlighted as well as the difficulties of implementing it on a large-scale distributed architecture with the use of renewable energy sources. The potential of the Energy Internet to provide reliability and security guarantees is discussed at the end [7].

Y. Kabalci et al. illustrated that the notion of "energy internet," which was only just unveiled, intends to advance smart grids by combining various energy sources into a system that is very adaptable and efficient. To research the growth of energy internet-based IoT applications, we have thoroughly examined Internet of Things applications enabled for smart grids and environmental sensings, such as smart cities, smart homes, smartmetering, and energy management infrastructures. Since the IoT is regarded as one of the most significant driving forces of the energy internet, these applications represent potentially major areas of the energy World Wide Web idea. Additionally, we addressed certain crucial research topics and spoke about the difficulties, unresolved obstacles, and potential future directions for something like the energy internet idea [8].

DISCUSSION

With the inerrability of cutting-edge technologies, the importance placed on distributed renewable systems, and their applicability in energy-sharing networks, the future of the Energy Internet looks promising. Via in-depth analyses of the conceptual model, model structure through to the introduction of a new concept called Energy Intranet, and processes of the Energy Internet, we have presented the Energy Internet as a continued expansion of a transitional generation system in this study. Given the abundance of possibilities, we anticipate that necessary changes to the current laws and regulations will be made to allow the conversion of existing grid-based power systems into the Energy Internet. According to the present objectives, there will likely be a regulatory push towards promoting energy storage, electronic payments, and future technologies like blockchains and vehicle-to-grid. The study's findings place a significant emphasis on the early cohabitation of the Energy Internet and legacy grid, succeeded by the gradual national scaling-up of the Energy Internet, which might cause upheaval in the whole electrical sector. All of these factors have always had the potential to drastically alter how power is generated, distributed, and used.

Other Explanation of the Internet of Things (IoT)

The Internet of Things (IoT) is a network of linked things, sometimes referred to as smart gadgets. The item might be a remote control, a heart rate monitor, or a car equipped with

sensors. This refers to gadgets that may gather and send information across a network and have been given an IP address. With the aid of embedded technology, the components interact with the outside world as seen in Figure 1; this enables them to make judgments. Considering that these instruments may now digitally portray themselves.

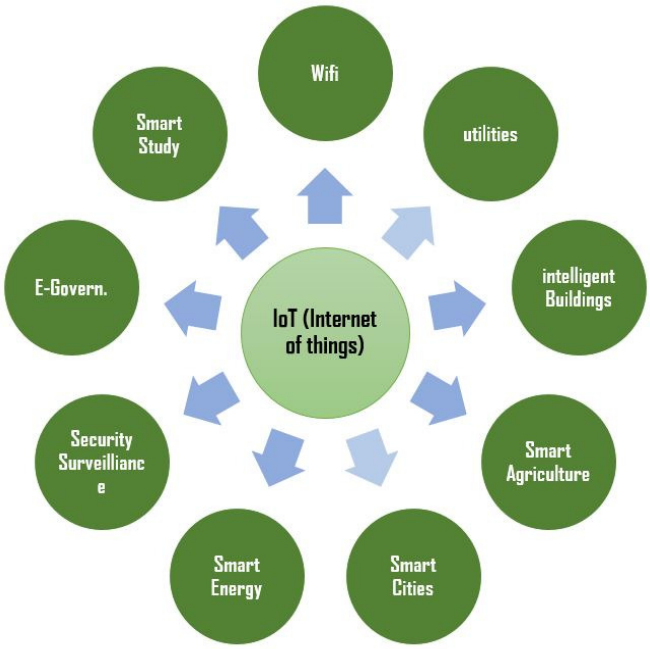


Figure 1: Illustrated the Representation of IoT in Different Areas.

Or, to put it another way, "The internationally dominant technology functions as a single key to downsizing this whole cosmos to a little connected and interdependent hamlet, while IoT consists only specific terms that accurately express its meaning".

- **Internet:** Inter connectivity-For global connection
- **Things:** Embedded system devices-sensors, actuators, RFID tags, QR codes and so many others.

i. For sensing the data

ii. Collecting the data

iii. Sending the data

The technology behind the Internet of Things, then, allows enables things to independently connect between themselves through the internet using gadgets rather than computers. The most important and frequently employed phrase in IoT is "Smart," which refers to automation. Automation is the act of reducing steps involved or intervention while enhancing machine intelligence to execute every operation that IoT is capable of someone doing on its own [9]. IoT creates a network of interconnected artificial objects, comprising furniture, automobiles, household appliances, and even connection with other living things like plants, mammals, and so on.

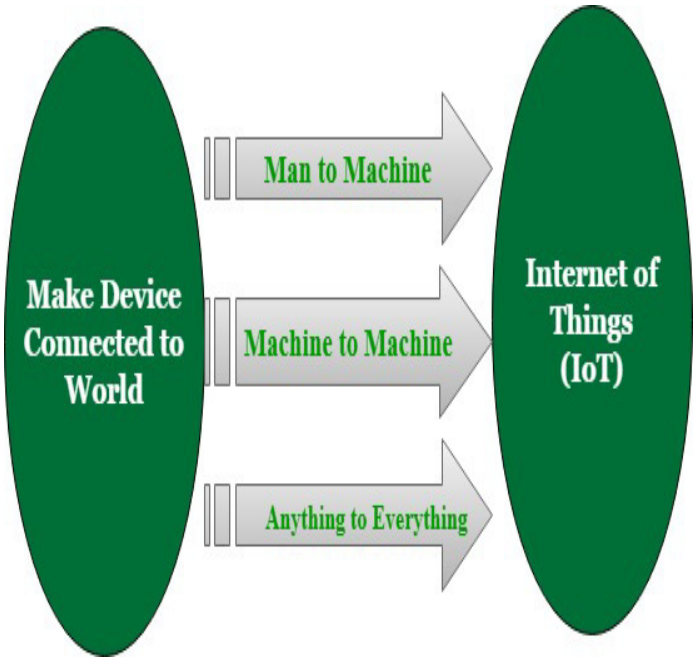


Figure 2: Illustrated the Communication of Devices with IoT.

Some communication devices in IoT are also shown in Figure 2:

i. Sensors:

Devices that transform motion, temperature, and other physical characteristics into electrical currents. The crucial IoT enablers are smart sensors. Imagine an automated farm management system that only indicates the prevailing crop status, such as "four crops need water. Now I'm going to pour it," before meeting the crop's request [10].

This wonder is because of the IoT technology behind it,

A. The plant pot's temperature controller, which is attached, determines the low temperature.

B. Following that, it initiates microprocessor platforms like Raspberry-Pi and Arduino boards.

C. It receives sensor signals with internet connections like Wi-Fi and Bluetooth.

D. Following that, it notifies the user, and a motion sensor attached to that same tap activates so that the water can be poured.

ii. Actuators:

Devices that are different from sensors. It converts electrical instructions into motions of the body. Transducers, which change from one kind of energy into another, include both actuator and sensor components. The most critical component of IoT is the sharing of data. Therefore, sensors and actuators are necessary for this situation [11].

iii. RFID Tags:

Wireless microchips are being employed to tag everything over them for automated, one-of-a-kind authentication. It may be found on credit cards, vehicle ignition keys, and many other

items. IoT's primary objective is the connectedness of things, hence RFID tags and IoT technology work alongside one another and are utilized to offer a unique identify for the linked "things" in IoT.

CONCLUSION

One of the most important factors affecting the environment and the energy systems is the supply structure. A sustainable multi-energy system will be achieved by the continuing development of the Energy Internet, which will bring together dispersed energy sources and different types of energy, including electricity, gas, heating, and cooling. This system will also be underpinned by the data internet. This study examines three instances of connected energy systems, each using modern operation and planning techniques, utilizing the examination of an Energy Internet architecture. The primary issues of optimum connection, cyber systems, uniform standards, and large-scale demonstrations are addressed by four main avenues of future study. Even though development into the Energy Internet is still in its early stages, it is now one of the most significant energy-related subjects, making it valuable for the research community to investigate. We have developed identity-based security features, a secure communication protocol, and an intelligent security system for energy management for both the IoT-based Energy Internet (ISSEM). The framework facilitates improved energy management on the Energy Internet and offers sufficient security and confidentiality to components, data, and events. We demonstrated the secure communication protocol's superiority over current similar schemes and resilience against a variety of security assaults using the AVISPA tool and computational methods. The demonstration using Nash equilibrium demonstrates that the ISSEM is accurate. The evaluation's findings demonstrate how effective and safe our suggested structure is for the Energy Internet. We want to provide safe and portable key exchange protocols as part of our continuing efforts to secure unicast, multicast, and broadcast communications in the Energy Internet.

REFERENCES

[1] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, “A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures,” *Computers*, vol. 9, no. 2, p. 44, May 2020, doi: 10.3390/computers9020044.

[2] H. Ning and H. Liu, “Cyber-physical-social-thinking space based science and technology framework for the Internet of Things,” *Sci. China Inf. Sci.*, vol. 58, no. 3, pp. 1–19, Mar. 2015, doi: 10.1007/s11432-014-5209-2.

[3] H. Ge and Z. Zhao, “Security Analysis of Energy Internet with Robust Control Approaches and Defense Design,” *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2806941.

[4] K. Zhou, S. Yang, and Z. Shao, “Energy Internet: The business perspective,” *Appl. Energy*, vol. 178, pp. 212–222, Sep. 2016, doi: 10.1016/j.apenergy.2016.06.052.

[5] X. Lu *et al.*, “Blockchain-Based Distributed Energy Trading in Energy Internet: An SDN Approach,” *IEEE Access*, vol. 7, pp. 173817–173826, 2019, doi: 10.1109/ACCESS.2019.2957211.

[6] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for Internet of Things-based Energy Internet," *Futur. Gener. Comput. Syst.*, vol. 93, pp. 849–859, Apr. 2019, doi: 10.1016/j.future.2018.01.029.

[7] S. M. S. Hussain, F. Nadeem, M. A. Aftab, I. Ali, and T. S. Ustun, "The Emerging Energy Internet: Architecture, Benefits, Challenges, and Future Prospects," *Electronics*, vol. 8, no. 9, p. 1037, Sep. 2019, doi: 10.3390/electronics8091037.

[8] Y. Kabalci, E. Kabalci, S. Padmanaban, J. B. Holm-Nielsen, and F. Blaabjerg, "Internet of Things Applications as Energy Internet in Smart Grids and Smart Environments," *Electronics*, vol. 8, no. 9, p. 972, Aug. 2019, doi: 10.3390/electronics8090972.

[9] L. Xing, "Reliability in Internet of Things: Current Status and Future Perspectives," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6704–6721, Aug. 2020, doi: 10.1109/JIOT.2020.2993216.

[10] S. Ratnaparkhi *et al.*, "WITHDRAWN: Smart agriculture sensors in IOT: A review," *Mater. Today Proc.*, Dec. 2020, doi: 10.1016/j.matpr.2020.11.138.

[11] S. Malik, S. Ahmad, and D. Kim, "A Novel Approach of IoT Services Orchestration Based on Multiple Sensor and Actuator Platforms Using Virtual Objects in Online IoT App-Store," *Sustainability*, vol. 11, no. 20, p. 5859, Oct. 2019, doi: 10.3390/su11205859.

CHAPTER 7

A DEVELOPMENT OF PRIVACY, SECURITY PROPERTIES IN INTERNET OF THINGS

Dr. Anilloy Frank, Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- anilloy@presidencyuniversity.in

ABSTRACT

With time, interest in the Internet of Things is growing and The Internet of Things is expanding rapidly because of how inexpensive sensors are. Many sectors, including healthcare, manufacturing, agriculture, and transportation, are using this technology more and more. However, when it comes to the Internet of Things' future, security and confidentiality are two major worries. It is almost difficult to protect these "things" that are linked to the Internet using ordinary resource-intensive defenses since the preponderance of them are basic devices with constrained hardware capabilities. In this chapter, we go over the value of protecting Internet of Things networks, lay on the floor the security problems, and quickly go over some of the literary criticism alternative alternatives. In Future this chapter illustrates the security, privacy and other properties of IoT these properties are responsible for creating a secure chain it provides some information for other researcher and students for their research and study.

KEYWORDS: Internet of Things, Privacy, Security, Technology, Verification.

INTRODUCTION

Since the first network was created in 1972, many different topologies have been used for computer networks. The idea is the same whether using IPv6-enabled wearable sensors for medical monitoring or the traditional pair of wires used in industrial facilities to connect sensors and actuators in systems that drive operations. Multiple sensors should be able to be securely connected via any of the following: Ethernet, Bluetooth, Zigbee, or a traditional 4-20 electric circuit. It is conceivable to assume that the Internet of Things was founded when operations and information technology merged. In actuality, OT advances aimed at making field equipment "smart" have a direct impact on the industry's increased use of Fieldbus technology, which is one of the versions. However, the challenge is getting the different versions to communicate with each other, which requires a common communication network such as the Internet Protocol (IP) [1].

The Internet of Things can be integrated into two different ways: Greenfield and Brownfield. Greenfield IoT implementations account for the bulk of Internet of Things (IoT) deployments in sectors such as healthcare, agriculture, and transportation that have not previously used network technologies. On the other hand, a brownfield implementation aims to connect Internet-connected devices with an already connected infrastructure, such as fieldbus technology in the process automation industry. In both scenarios, establishing a clear communication structure is critically necessary to increase system security and reduce risk.

On October 21, 2016, a massive Distributed Denial of Service (DDOS) [2] attack pulled down several websites including Twitter, Amazon, Netflix, Airbnb, and GitHub. DNS service provider

Dyn is apparently targeted by the spyware, known as Mirai. The Japanese word for "future" is Mirai. Mirai exploits IoT device flaws such as factory default settings to turn Linux-running devices into digital weapons. IP cameras and digital video recorders (DVRs) were considered separate groups in this attack. This is possible because many manufacturers of Internet of Things (IoT) devices retain user-defined passwords in the firmware, making it easier for hackers to access them via Telnet or Transport Layer Security (SSH).

In 2010, a specific piece of malware was written to target nuclear power plants. This malware was known as stuxnet. Even though most nuclear research organizations prevent the formation of the well-known air gap, the programmable logic controller (PLC) in charge of uranium enrichment centrifuges was infected using a poisoned Universal Serial Bus (USB) [3] flash drive. The centrifuge suffered physical damage as a result of the high acceleration, deceleration rate, and faster than normal spin for extended periods. Apart from Iran, this attack also affected some other countries, they were also hurt. Other countries such as the Philippines and India also felt the impact.

Building blocks of IoT Security

Security was not a priority when most network protocols were developed. Thus, network security is often the result. Additionally, predators may be able to undermine the system due to the diversity of network components. One way to deal with this problem is to put network devices into trusted and untrusted groups. For the former category the "root of trust" can be as simple as a verification key issued by the manufacturer. These reliable gadgets use encryption technologies, secure key management, and secure communication protocols. Verification techniques are used to decide whether untrusted devices are secure enough to join the trusted group. Because it is so difficult to differentiate between these groups of products based on type, manufacturer, or even use, the line separating reliable equipment from untrustworthy equipment is often invisible. The verification process is often dynamic and open to modification over time or in response to network threats. The collection of device features that prove to be reliable and resistant to manipulation is the basis of trust. For example, the Secure Booting function of root-of-trust devices. Another example is the verification facility, which verifies claims using cryptographic methods. An IoT device can have several different trust bases.

Running application software reliably and mitigating security risks are primarily the responsibilities of the Trusted Execution Environment (TEE). Another responsibility of this component is to isolate process execution from other processes using the same hardware. The second part is the secure communication channel, which employs traditional encryption methods to protect the confidentiality and integrity of data moving between network devices. The third component of the system is the authentication process, which consists of key distribution and authentication protocols as well as key symmetric or asymmetric keys. The fourth component is the verification process, which includes the verification logic and the verification key provided by the manufacturer. The keys and data received from the sensors must be stored securely by the devices. The pinnacle is the ability to gather all relevant information including time and place.

IoT Device Lifecycle

Before we can talk about IoT security, we must first understand the several phases of an IoT device. The lifetime of an IoT device is shown in Figure 1. It starts with building the software component of the IoT device, which uses an application programming interface (API) or

software development kit (SDK) to hide the complexity. The actual parts of the gadget are manufactured using various tools. We cannot stress enough how important proper settings are for the long life of an IoT device. In this step, many settings are done for various components including CPU, System on Chip (SoC) and Operating System (OS) [4]. The next step is field deployment, which involves making sure the link is built correctly and also shown in Figure 1. The gadget is protected by regular upgrades. The final truth that older appliances must face is retirement.

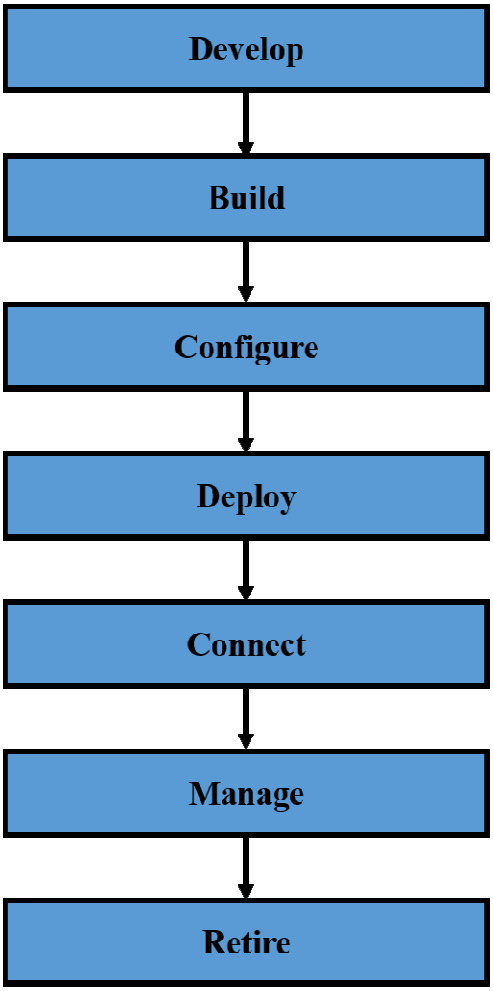


Figure 1: Represented the Typical Lifecycle of IoT Device.

End-to-End IoT Security

When discussing communications network security, end-to-end consideration is important. The key elements in the end-to-end security journey of IoT device communications. The data received from the sensors and sent to the gateway is usually encrypted by the IoT device. Sometimes, after encryption, this data may be stored locally. The data will be subjected to some analysis and then decrypted by the gateway before being encrypted once again and shared with the cloud. When the data is received, the cloud instance will decrypt it once again and do some analytics before encrypting it again to enable database storage (DB).

Frameworks for the Internet of Things have been developed to improve nodes' portability. The Internet of Things framework is a fantastic tool for hiding network complexity and type. However, whether from an authenticating, privacy, or confidentiality point of view, an IoT framework must be created to facilitate end-to-end secure between nodes. In truth, end-to-end security is carried out in a variety of ways across a wide range of frameworks. In Table 1, some of these contradictions were indeed underlined.

Table 1: Represented the IoT Framework and its Security Approach.

Sr. No.	IoT framework	Security approach
1.	Open Connectivity Foundation (OCF)	Tackles the security using three strategies: • Access control • Message encryption • Device lifecycle management. • Issue: (no security interoperability with other frameworks such as All Joyn or UPnP)
2.	Data Distribution Service (DDS)	Security is achieved through three techniques: • Message security enveloping • Security tokens • Security plugin modules to add on services, such as authentication, access control and encryption.
3.	AllSeen Alliance/AllJoyn	End-to-end security in the application layer using leaf nodes.
4.	Universal Plug and Play (UPnP)	Security was not in the initial design and it was added later as an optional service through the IoT management and control architecture.
5.	Lightweight Machine 2 Machine (LWM2M)	It achieves security using a secure message exchange with the Datagram Transport Layer Security (DTLS) and an access control list using the bootstrap server.
6.	One Machine to Machine (OneM2M)	By design, it has the capability of performing authorization, access control, data protection as well as privacy preservation.
7.	Open Platform Communications-Unified Architecture (OPC-UA)	OPC-UA is designed with security in mind. Distribute security functions over two layers, namely: the session layer and the secure channel layer. The former is the one responsible for authentication and access control, whereas

		the latter is taking care of message encryption, using Transport Layer Security (TLS) and HyperText Transfer Protocol Secure (HTTPS).

The platform abstraction layer, also known as the connectivity and hardware abstraction layer, the node interaction layer, and the data object layer are the three tiers that make up the Internet of Things framework. These three layers are shown in Figure 2. The data object layer is used to conceptually and physically map a node to a device. It is also responsible for managing the node Access Control List (ACL). The communication between nodes is handled by the second layer. The end-point security context must be obtained in this layer. The last three sub-layers that may be divided into the platform layer are the network, sensor, actuator, and security layers. IoT networks mostly adhere to the same Internet tiers strategy. This will enable the usage of older industrial Internet of Things protocols like Fieldbus on top of IP. The application layer is replaced by the IoT framework layer as the lone differentiation.

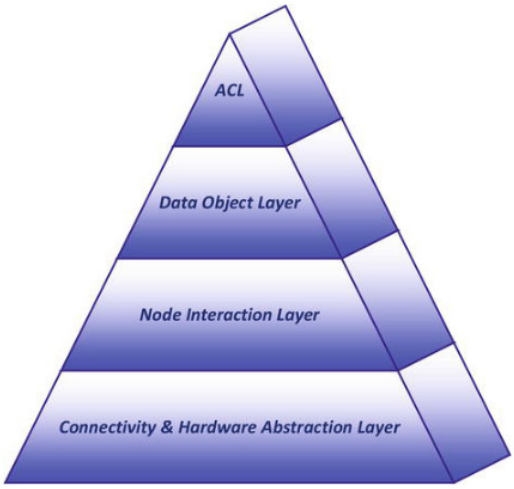


Figure 2: Represented the Layers of IoT Framework.

LITERATURE REVIEW

P. Fremantle et al. illustrated that the Internet of Things (IoT), which refers to the Internet-connected proliferation of tiny objects, is posing new difficulties for the development of private, secure infrastructures. With a heavy emphasis on how these issues are addressed in IoT middleware, this paper analyses the existing research on the problems and answers to security and confidentiality in the Internet of Things. Since many systems are constructed using existing middleware and these systems inherit the underlying security characteristics of the middleware framework, we concentrate on IoT middleware. There are three key portions to the essay. We first provide a matrix of IoT security and privacy issues. This matrix serves as the foundation for a comprehensive evaluation of the literature that identifies the needs for IoT platforms and middleware. Second, we give a systematic literature assessment of the middleware that is currently available and how various middleware techniques address security. To assess, we make use of the first phase's needs. Finally, we come to a set of findings and suggest more research in this area [5].

M. Ammar et al. illustrated that the Internet of Things (IoT), which encompasses anything from small wearable gadgets to massive industrial systems, has a tremendous impact on many aspects of our everyday life. As a result, several IoT applications have been created and implemented using various IoT frameworks. An IoT framework is an ensemble of standards, protocols, and guiding principles that make it easier to create IoT applications. These applications' success largely rely on the ecosystem features of the IoT framework, with a focus on the security measures used in it, where concerns about security and privacy play a crucial role. In this paper, the security of the seven major Internet of Things frameworks is assessed. We describe the suggested architecture, the specifications for creating third-party smart applications, the associated hardware, and the security precautions for each framework. Comparing security architectures reveals that although various approaches were deployed to provide other security features, the same requirements were utilized to establish a secure connection [6].

M. Yu et al. discussed that the number and diversity of Internet of Things (IoT) devices have expanded considerably as a result of the thriving IoT industrial environment. IoT devices are extensively utilized in a wide range of industries relating to daily living, including smart homes, smart apparel, smart manufacturing, smart transportation, and smart medical care. IoT device security flaws are evolving constantly as a result of it. Security flaws will proliferate, causing serious hazards to user privacy and property. The study context, including Protocol stack, device components, and attack surfaces, is initially reported in this publication. We examine one of the most recent studies on IoT device detection and prevention, mitigation, and related tasks. Then, using an examination, we highlight the current challenges and potential. Finally, we project and evaluate future paths for research regarding IoT device vulnerability methods of analysis [7].

R. Roman et al. illustrated that using centralized architectures, where central organizations collect, process, and deliver information, services can be offered in the Internet of Things. Distributed architectures, which allow entities at the network's edge to communicate and operate together in real-time, are an optional accessory. Knowing this distributed technique's advantages and limitations in terms of features as well as security and privacy issues is essential for comprehending the usefulness and sustainability of this approach. The objective of this research is to demonstrate that the distributed strategy offers both attractive traits and strengths as well as a variety of challenges that need to be handled [8].

IoT devices, sensors, and Radio-Frequency Identifications (RFIDs) are increasingly being used for recreation purposes. For example, in commuting where vehicles are monitored, in taxi services, in healthcare where patients' health conditions are monitored, in smart homes, smart grids, and smart automobiles, etc. Due to this, attackers are targeting certain networks or protocols for economic profit, and adversaries are attempting to harm the organization's reputation or steal intellectual property. The injection vulnerabilities have been increasingly dangerous security hazards for web applications over the last twenty years or more. Implementing IoT or Web of Things (WoT) communication channels presents new security issues for security professionals or researchers. Each of these protocols, including RestAPI, WebSockets, and Message Queuing Telemetry Transport (MQTT), has a unique set of security problems. Accordingly, the use of phoney devices, the lack of authentication in WebSocket connections, and the usage of RestAPI without its validation may all compromise user privacy. We have created a Personal Home Pages (PHP) application for the identification of new IoT network nodes. With this, significant security flaws in the core protocols of WoT will be resolved along with the protection of user privacy and data [9].

The ordinary life is adopting the Internet of Things. Unfortunately, the security of IoT devices is often neglected. We choose to focus on access control among the wide range of security concerns affecting the developing IoT because controlled access is essential for establishing privacy, trust, and other security properties. This paper analyzes the suitability of various IoT access control systems for access control purposes by classifying them according to their architecture for example centralized, hierarchical, federated, and distributed. According to the results of our investigation, the community ignores hierarchical and federated structures, while many proposals lack important features like audit and revocation. Finally, we provide an architecture-based taxonomy and outline potential future study areas with an emphasis on hybrid architectures, usability, flexibility, privacy, and server-less permission revocation techniques.

The Internet of Things (IoT) intends to create a civilization where objects in the real world and online can communicate and work together. IoT produces a variety of vast, multi-source, heterogeneous, and sparse datasets due to the involvement of so many wireless sensor devices. Data acquisition is typically used to reduce the volume and dimensionality of data, manage the volume of data flows, and extract useful information from raw data before using these data to further strengthen IoT services and provide significant advantages over traditional is done for extraction. Despite numerous studies on IoT data fusion, there is a lack of in-depth evaluation and discussion of it with a focus on various IoT application areas, especially with regard to security and privacy. In this paper, we explore the characteristics of IoT data, put forward several requirements for IoT data fusion, such as privacy and security concerns to group IoT applications across different domains, and provide an in-depth analysis of the situation Lets take the art of data fusion across major IoT application domains. We are specifically using the IoT data fusion paradigm as a benchmark to assess and compare the effectiveness of current data fusion techniques. We highlight unresolved research concerns, highlight exciting new research areas, and list research challenges based on the exhaustive survey [10].

The Technology for face resolution and authentication is essential to maintaining human identity both offline and online. The rise in technologies dependent on face recognition and resolution in the existing Internet of Things (IoT) and big data environment puts additional demands on computing, communication, and storage resources. To increase computing resources and save bandwidth, we have suggested the fog computing-based understandingof the concept and resolution framework. However, the attributes of a system based on fog computing have certain security and privacy difficulties. To address the aforementioned problems, we provide a security and privacy preservation approach in this work. We explain the foundation for face detection and resolution based on edge computing and briefly discuss the concerns about privacy and security. Then it is suggested that data encryption, data integrity checking, and authentication and session key agreement schemes be used to address the problems with confidentiality, integrity, and availability in face identification with face resolution procedures. Finally, we put a simulation system into place to assess how safety precautions affect system performance. In the meanwhile, we assess and investigate the suggested scheme's security attributes from the perspective of logical paper that presents the implementation and the confidentiality, consistency, and availability attributes of information systems [11].

The wide range of cutting-edge technologies, such as Internet-of-Things, cloud computing, edge computing, big data, and intelligence-accelerating chips, have recently enabled the connectivity of a large number of various equipment for particular uses. Based on the key characteristics of techniques, networking technologies have transformed into future intelligent

networks (FINs). FINs integrate intelligence into solutions that enable generating and optimising policies, freeing security management from the management and configuration burdens, and enhancing the successfulness of self-learning from real-time network data. In FINs, low responsiveness is achieved at the expense of computational complexity that is more than what individuals' or Internet of Things (IoT) device capabilities can handle. Computing-intensive intelligence duties are envisaged to be offloaded to more potent smart objects with intelligent computing technology to accomplish a new generation of delay-sensitive, function-intelligent, and computing-intensive services. However, since the data were being duplicated or divided before being sent to edge devices, and since these devices serve a variety of functions and have large and diverse computer resources, there are unidentified security and privacy disadvantages that could potentially shut down the network system, compromise the privacy of network elements, harm data assets, or result in unfair incentive improvements. In this post, we go over the design problems for FINs' data privacy and security [12].

The future where physical items are online multiplayer into information networks to provide cutting-edge and intelligent services to people is what the Internet of Things (IoT) is going to bring about. For dependable data fusion and mining, right management with context awareness, and improved user privacy as well as information security in the IoT, trust management is crucial. It aids in consumer adoption and consumption of IoT services and apps and assists customers in overcoming perceptions of uncertainties and danger. However, there is currently no systematic research on trust maintenance in IoT in the literature. In this paper, we look at the properties of trust, provide goals for IoT trust governance, and conduct a literature review on recent developments in trustworthy IoT. Furthermore, by pushing out a research model for integrated trust management in IoT, we examine big questions, identify research roadblocks, as well as identify future research trends [13].

The Large-scale Internet of Things (IoT) devices receive huge amounts of information from everywhere at all times, which may violate people's privacy, especially when the systems are used in places where people are receiving medical attention receive care or go about their regular daily existence. Protecting privacy is important, so weak detection is often required where privacy requirements are high. However, previous research has shown that strong security often requires strong identification, especially in authentication processes. Therefore, finding an appropriate balance between security and privacy remains a difficult issue. This inspired us to create an authentication technology that protects the privacy and is responsible for IoT enddevices with weak identities. It contains a modified version of Small Group Signatures on Shamir's Secret Sharing Scheme. We consider three common attacks while analyzing the security features of our approach, and we use the Prove if tool to verify the formal security. Our authentication mechanism is practical in operation, as shown by experiments deploying implementations in the MacBook Pro and Intel Edison development platforms [14].

DISCUSSION

In this, we have discussed the origins of the IoT and how this has posed a major challenge to standardisation and a single overall vision. This, in turn, has given rise to challenges for security and assurance in the IoT. Arguably the most significant challenge, but also the most fundamental, is to encourage standardisation and coordination in the IoT. This is not only difficult in terms of process and technology, but also politics. There needs to be consideration of all stakeholders and their conflicting views on the IoT. The Platform for Privacy Preferences

Project project shows the difficulties involved in gaining consensus and trust between parties that have different visions and interests. The Platform for Privacy Preferences Project project was laudable but faced considerable difficulties. An analogous system for the IoT would certainly be beneficial, but it is challenging to ensure that the outcomes are relevant and acceptable to all.

If there is to be a protocol, analogous to Platform for Privacy Preferences Project, to communicate how data are captured, processed, stored, and transmitted, and offer users a way to have choice and control regarding their data, lessons must be learned from the Platform for Privacy Preferences Project project. It is important that, for any standard to be successful, the project should be mindful of the politics involved. Privacy advocates may see the development as industrial subterfuge, a criticism that was levelled at the Platform for Privacy Preferences Project project; the protocol should not allow services to create an illusion of privacy whilst gathering personal data. It should be recognised that any standard is likely to be only part of a solution, and as such, implementing the standard alone may not provide adequate protection. Therefore it is recommended that the standard should be used together with other privacy-enhancing tools. Any standard should be developed in line with legal and regulatory compliance. If there is no compliance requirement or financial implication to not implementing the protocol, the business case for the protocol will fail. To maximise the probability of industry adoption and user acceptance, any protocol for managing consent in the IoT should be:

A. Developed around firmly agreed principles, to ensure there is no mission creep and that the objectives are clear;

B. Simple, economically efficient, and implementable;

C. Mindful of any impact on current and future business models;

D. Co-developed with industry bodies (service and infrastructure providers) and user representative groups;

E. Developed in line with legal and regulatory compliance. If there is no compliance requirement or financial implication to not implementing the protocol, the business case for the protocol will fail.

CONCLUSION

Authentication and identification in IoT systems are fundamental for security and privacy. Systems based upon biometric identification, possibly combined with a token, may prove advantageous compared to existing systems, but care must be taken to ensure that the system is secure yet frictionless. Significant progress has been made in the battle to ensure the authenticity of devices, streams, and services in the IoT. In particular, the development of Physical Unclonable Functions (PUFs), can play a role in device authentication. A PUF has a complex and unpredictable yet repeatable mapping system of inputs to outputs. For efficient authentication, the function needs to be easy to evaluate and repeatable, and for security purposes, it needs to be difficult to predict. Some weaknesses have been observed, such as ageing, which can make PUF responses unreliable, and improved schemes using enhanced challenge-response are being developed. PUFs are being combined with embedded Subscriber

Identity Modules (eSIMs) to provide authentication and access control. The eSIM is used to address issues of scalability, interoperability, and compliance with security protocols.

Other areas requiring urgent attention include the need to adapt existing SSO mechanisms or create new ones that better fit the IoT. Although some approaches address this need, proposing a hybrid architecture that combines all mechanisms through specially crafted middleware [6], this topic still needs research. There is also a need for a standardised communication platform and architecture, with unified security considerations in intelligent transport systems, prioritising the incorporation of security in each layer of the architecture. Attacks are feasible from the physical layer, through to the network layer, to the facilities layer by altering the ECUs, before finally affecting applications such as windscreen wipers and door locks. Various Industrial IoT attacks have also shown SCADA vulnerabilities such as slow updates and authentication holes, paving the way for further attack vectors on the network. This raises a need for a secure and reliable architecture that can protect an Industrial IoT from network to endpoint devices, which governs the functioning of an industry.

REFERENCES

[1] B. Devlin, "Internet protocol," *SMPTE Motion Imaging Journal*. 2020. doi: 10.5594/JMI.2020.2984962.

[2] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Int. J. Distrib. Sens. Networks*, 2017, doi: 10.1177/1550147717741463.

[3] O. H. Halvorsen and D. Clarke, "Universal Serial Bus," in *OS X and iOS Kernel Programming*, Berkeley, CA: Apress, 2011, pp. 141–172. doi: 10.1007/978-1-4302-3537-8_8.

[4] M. Silva, A. Tavares, T. Gomes, and S. Pinto, "ChamelIoT: An Agnostic Operating System Framework for Reconfigurable IoT Devices," *IEEE Internet Things J.*, 2019, doi: 10.1109/JIOT.2018.2863545.

[5] P. Fremantle and P. Scott, "A survey of secure middleware for the Internet of Things," *PeerJ Comput. Sci.*, vol. 3, p. e114, May 2017, doi: 10.7717/peerj-cs.114.

[6] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002.

[7] M. Yu, J. Zhuge, M. Cao, Z. Shi, and L. Jiang, "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices," *Futur. Internet*, vol. 12, no. 2, p. 27, Feb. 2020, doi: 10.3390/fi12020027.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.

[9] S. Murawat *et al.*, "WoT Communication Protocol Security and Privacy Issues," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 3, 2020, doi: 10.14569/IJACSA.2020.0110319.

[10] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in internet of things:

Towards secure and privacy-preserving fusion," *Inf. Fusion*, vol. 51, pp. 129–144, Nov. 2019, doi: 10.1016/j.inffus.2018.12.001.

[11] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1143–1155, Oct. 2017, doi: 10.1109/JIOT.2017.2659783.

[12] F. Wang, B. Diao, T. Sun, and Y. Xu, "Data Security and Privacy Challenges of Computing Offloading in FINs," *IEEE Netw.*, vol. 34, no. 2, pp. 14–20, Mar. 2020, doi: 10.1109/MNET.001.1900140.

[13] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014, doi: 10.1016/j.jnca.2014.01.014.

[14] Z. Wang, "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 342–348, May 2018, doi: 10.1016/j.future.2017.09.042.

CHAPTER 8

AN EVOLUTION OF DATA AGGREGATION FOR THE INTERNET OF THINGS IN SMART CITIES

Dr. A Maheswari Senthil Kumar, Assistant Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- a.maheswari@presidencyuniversity.in

ABSTRACT

The Internet of Things is a contemporary, cutting-edge system that promises to link a wide range of digital equipment with the Internet, delivering many new services in the framework of a smart city. These devices are packed with various sensing, actuation, and processing capabilities. Smart city efforts are being made possible internationally because of the alluring IoT services combined with big data analytics. By enhancing transport and infrastructure systems, lowering traffic congestion, managing waste, and enhancing human life quality, these services are altering cities. Additionally, we provide us with a summary of the most recent global collaborations and measures taken to advance IoT in the context of smart cities. Finally, to offer recommendations for future study, designers identify several concerns.

KEYWORDS: Application Layer, Cloud Computation, Data Aggregation, Internet of Things, Sensors.

INTRODUCTION

Over the last decades, the prevalence of emerging wireless technologies and internet-based systems such as cloud computing has promoted the blooming of the Internet of Things (IoT), offering more convenience and flexibility in our various daily applications. IoT is defined as the network of smart, distributed, self-organized, and energy-constrained sensors and everyday physical devices that can provide specific functionality without human intervention through the Internet. IoT is a networked interconnection between multiple heterogeneous systems. As illustrated in Figure 1, the architecture of IoT-based systems includes four layers: sensing layer, networking layer, cloud computing layer, and applications layer. Every layer of IoT architecture provides self-governing functionality and scalability. In the following, the four-layer architecture of IoT is described.

i. Sensory Layer

This layer is where different sensors and IoT devices gather data from the monitoring area and transfer it to the sink. The monitoring area is home to millions of IoT devices that have been set up to create a self-organized, multi-hop topology. In a basic IoT system with sensors, a sink, and management nodes, the sensors gather data from the monitoring area and then send it in a multi-hop fashion to the sink. Through management nodes, system administrators may keep an eye on and regulate the operation of IoT devices. It should be mentioned that certain IoT devices are vulnerable to failure since they are located in a particular region. Additionally, certain gadgets' energy runs out more quickly than others. Therefore, it is crucial to use energy-efficient approaches for IoT data aggregation.

ii. **Networking Layer**

The networking layer is in charge of offering effective topologies for data transmission between source and destination devices. IoT topologies should enable high data transmission rates for source devices, however owing to various topologies, these systems are subject to limitations in terms of throughput, energy use, and malicious assaults.

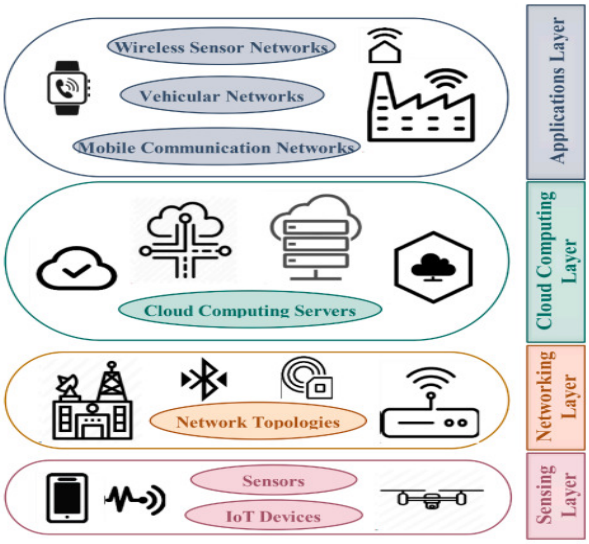


Figure 1: Represented the Layered architecture of IoT.

iii. **Cloud Computing Layer**

The ability to handle massive amounts of data more rapidly and precisely has been made feasible by advancements in cloud computing technology. Data is received, processed, and decided upon by the cloud computing layer, which then sends the results to other tiers. Although cloud computing is the preferred method for IoT-based systems to store and analyse data, other techniques favour edge and fog to maximise costs and performance. The main goal of using edge or fog architecture in the data aggregation process is not to replace the cloud, but rather to manage system heterogeneity, cope with distant IoT devices, and distinguish important data from generic data. The necessity for huge data aggregation in IoT applications drives techniques away from cloud computing and toward fog or edge computing.

iv. **Applications Layer**

This layer includes a variety of applications, including wireless sensor networks, smart grids, smart homes, smart cities, and smart healthcare. Anyone may use a smart gadget to communicate with people whenever and wherever they are. IoT applications are also utilised to keep an eye on environmental conditions and emergencies. To effortlessly take use of IoT capabilities in their everyday lives and industries, user-friendly interfaces are required. Since 1999, the Internet of Things (IoT) has advanced at an incredible rate, enabling smart technologies-based communication between people and virtual worlds. Figure 2 shows the installed base of IoT-

connected devices from 2015 to 2025 globally. The number of IoT-connected devices is predicted to reach more than 75 billion by 2025. People cannot imagine living in a connected world without IoT devices and the services they provide.

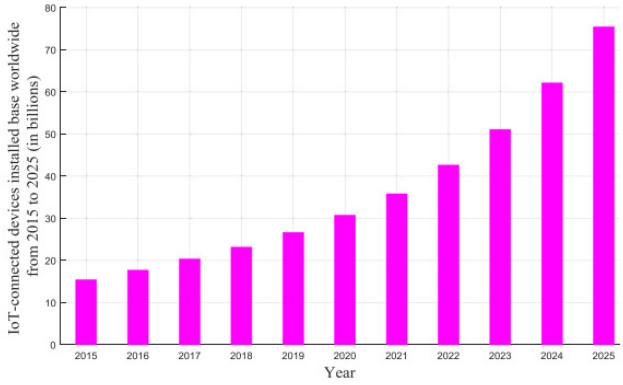


Figure 2: Represented the IoT-connected devices installed base worldwide from 2015 to 2025 (in billions).

IoT is used in many facets of daily life and business. IoT applications may be categorized into six categories, as indicated in Figure 3: industrial, agricultural, transportation, smart buildings, security, and healthcare systems. To gather data from the monitoring domain and provide it to the sink, monitoring systems and IoT devices are linked to the network in these applications. The Internet of Things is now a feasible technology for a variety of applications because to characteristics like cheap cost, adequate functionality, and high error tolerance. Here, IoT applications are briefly discussed and divided into the following categories:

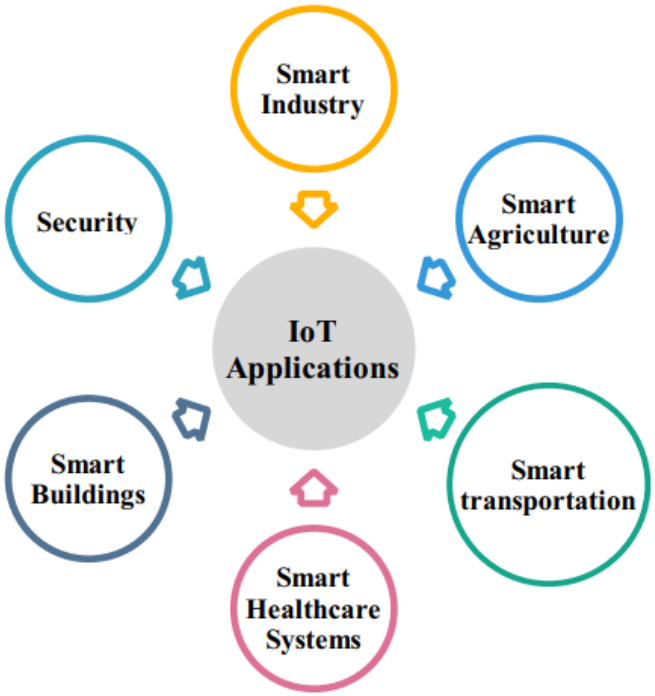


Figure 3: Represented the IoT Applications.

i. Industry

In industrial settings, a variety of IoT devices are used to monitor production processes and boost productivity. Real-time functional parameters, increased throughput, and decreased organisational expenses have been achieved by using IoT-based industrial management systems. Additionally, sensors may gather environmental data in dangerous locations like gas pipelines and mines, transfer it to a sink, and ensure employee safety via real-time alerts. The creation of interoperable, intelligent, and energy-efficient factories is referred to as Industry 4.0 and is regarded as the cornerstone of the IoT-based industry.

ii. Agriculture

Smart sensors and IoT devices may turn on and off automatically at certain periods to perceive environmental data in realtime. A monitoring area is equipped with hundreds of sensors that operate together as a self-organizing, multi-hop network to collect environmental data and transmit it to cloud computing servers for further analysis and decision-making. In addition, IoT-based technologies are utilized to remotely manage farms and greenhouses as well as automate the process of monitoring agricultural settings.

iii. Transportation

Networks based on the internet of cars are referred to as smart transportation systems. To control traffic, provide trip information, lessen environmental pollution, increase safety, and improve conventional transportation systems, these systems incorporate cutting-edge information technology and electronic sensors.

iv. Smart buildings

IoT systems provide automated building control and security capabilities by integrating digital technology and network connection protocols. Comfort, energy efficiency, dependability, and ecologically responsible living are all made possible through intelligent building management. IoT devices may be connected to the system in smart buildings through remote communication networks or short-range wireless connections, enabling users to operate their house or workplace from a distance. For a smart building to have the same qualities as conventional buildings and to enable effective equipment communication, IoT devices must be diversified and scalable.

v. Healthcare Systems

IoT has developed into a smart technology in recent years for delivering healthcare services, keeping an eye on old patients' behavior and vital signs without interfering with their everyday activities, and enhancing surgical operations. Humans' heart rates, blood pressure, and sleep patterns may be sensed by smartphones, clocks, wristbands, and other wearables, which can then be used to monitor their health remotely in realtime. Additionally, IoT-based robots may advise ways to help users' health practices. Patient comfort, safer procedures, better hospital administration, and the provision of more precise pharmaceuticals are some of the important IoT applications' contributions to smart healthcare systems.

vi. Security

IoT-based security systems are characterized as a collection of instruments for preventing theft and general safety, including security for communications, protection from fire, first aid, and risk factor monitoring. Security systems keep an eye on both the internal and exterior settings, gather important information, and alert the user in an emergency.

All spheres of life have steadily shifted toward a "smart" contemporary civilization thanks to the Internet of Things and cloud computing's strong development, widespread use, and convergence of new ideas and technology. The area of smart cities has been increasingly impacted by these technologies. The conventional urban system, which has been passed on from generation to generation since antiquity, operates in an exceptionally inefficient and laborious manner, and information across the systems has never been efficiently exchanged and integrated. A smart city system is based on the Internet and cloud computing has been suggested, with the backing of these two technologies. In-depth research has been conducted on multiple levels on system architecture, application software implementation, application support platforms, diverse transmission networks, and common sensors. Sensor networks are often positioned in poor communications settings in the Internet of Things-based smart city systems, which typically results in data communication failure. An optimal issue is whether the sensor decides to communicate again after an unsuccessful information transfer. The experiment findings demonstrate that the system is capable of knowing information interchange, fusion, and sharing throughout multiple sensing subsystems, resolving the communication island problem of the past, and addressing the requirement of smart cities [1].

Model scheme of an enterprise energy efficiency management platform based on the Internet of Things is examined, and the dynamically collected energy consumption data is reviewed using Internet of Things technology and data mining technology, to address the current predicament of complicated energy-consuming equipment and large energy consumption in the current enterprise. They provide help for making judgments on corporate energy efficiency management practices and the creation of initiatives for energy conservation and emission reduction. The current state of energy efficiency management in buildings is reviewed in this chapter, along with its pain points, which include installation dilemmas, high software development costs, upgrade challenges, protracted debugging cycles, and closed systems. To address these challenges, intelligent power transmission monitoring accessed via the Internet of Things is introduced. Through case studies, we investigate the system's real value in energy efficiency information management. Through the Internet of Things, it may acquire scattering data, compile it into vast data, and then utilize data analysis and processing to locate the relevant data. It is simple to promote and use, has a good usage impact, excellent practicality, and a sensible design.

The dominance of sensors and the Internet in the previous age of the Internet of Things offers a solution to a diverse range of everyday issues. Smart cities, smart healthcare systems, intelligent buildings, industrial automation, and smart environments are a few samples of such applications. However, there are several problems with real-time IoT sensor data, including one with a flood of dirty sensor data and a maximum resource cost. To create informed insight into unseen data patterns for quick decision-making, this chapter discusses how to handle IoT sensor data, fuse it with data from multiple sources, and conduct analysis. This paper discusses methods for processing data, including data demising, outlier recognition, imputation for missingdata, and data aggregation. The requirement of machine learning and other data fusion techniques, such as

direct fusion, related semantic segmentation, and identity announcement data fusion, are also discussed in depth. To handle multiple difficulties in IoT sensor networks and environmental data analysis, this study also tries to deal with data analysis integration with new advancements, such as cloud applications, fog computing, and advanced analytics. In conclusion, this study has provided the first comprehensive review of Iot data processing, fusion, and research methodology.

The potential to be fatal for infrastructure, the environment, and human life. The development of the required earthquake-resistant smart city (DRSC) settings is now conceivable because of recent developments in the Internet of Things and big data analytics technology. Through the application of IoT and big data analytics technologies, we demonstrate and explain the new reference design and philosophy of a disaster-resilient smart city in this paper. A general solution for disaster preparedness initiatives in smart city motivations is provided by the suggested architecture. To build an efficient DRSC environment that enables both real-time and asynchronous analysis, the Hadoop Ecosystem and Spark are combined. Data collection, dataaggregation, data pre-processing, big data analytics, and application servers make up the environment's implementation strategy. For the validation and analysis of the system to detect and create warnings for a massive fire, city pollution level, evacuation routes route, and the collection of information about natural catastrophes, a range of datasets are used. Throughput and batch processing are used to evaluate the system's efficiency, which highlights the suggested architecture's increased quality. Additionally, the main challenges of working are noted and described briefly [2].

A smart city was pioneered by the Internet of Things (IoT), which was inspired by the explosive expansion of linked heterogeneous devices. The goal of the many factors that comprise the design of smart cities is to improve the quality of life for urban residents. These elements encompass smart transportation, smart communities, smart healthcare, smart grid, etc. Real-time processing needs and the exponential rise of data, however, prevent the implementation of smart cities. As a result, we here suggest an experimental method for smart cities that integrates Big Data analytics. The embedded smart city provides services for two main features. First off, it makes it easier to use urban big data for creating, building, and administering smart cities. Second, it requires night before going to bed management and processing to improve the standard of urban services. The suggested architecture's three layers are responsible for managing real-time data, aggregating data, and providing services. By including data normalization and data filtering procedures throughout into suggested job, offline and online data processing operations are further sped up. We were able to determine the threshold values essential for urban planning and municipality operation management by evaluating verified datasets. Analysis of current works' throughput and processing times indicate that the new job will perform better overall[3].

The process of gathering big data using Internet of Things (IoT) ubiquitous technology is often privacy-invasive and leads to surveillance, profiling and discriminatory measures against residents, which is a major challenge for citizens in building sustainable smart cities. reduces the busyness of Nevertheless, there is great potential for monitoring and regulating smart city infrastructure more effectively and sustainably, thanks to real-time data analytics and information gathered from IoT devices. The study topic and problem addressed in this paper is the privacy-enhancing aggregation of dispersed sensor data such as household energy usage or traffic data. Citizens can choose the degree of privacy they want by reducing the quality of the

data shared at the cost of less accurate data analysis services. Real-world data from two smart city pilot projects are used to assess the proposed technology and its general applicability. Secrecy is enhanced under grouping, while maintaining the accuracy of the baseline scenario. Fairness on privacy among group members with comparable privacy preferences is shown to be greatest when the impact of privacy is assessed by one group member versus another group member. There are opposites of different grouping techniques. The most privacy is achieved when privacy options are grouped by proximity. The impact of the strategy on the design of incentive systems is examined [4].

The rise of the Internet of Things (IoT) and the development of ubiquitous communication devices have played an important role in the feasibility of smart city plans. Cities have the potential to become smarter thanks to wireless sensor networks (WSNs), a key enabling technology in the Internet of Things. Due to the increasing number of WSN applications that allow remote monitoring and tracking in smart cities, WSN has attracted great interest in recent years. Object tracking sensor networks are one of the most interesting uses of WSNs in smart cities for detection, monitoring and tracking (OTSN). Smart cities of the future will face new and fascinating challenges as a result of the integration of OTSNs into urban areas. These difficulties mostly center on the issues of active surveillance and monitoring in smart cities. In this paper, we outline the key features of OTSN, a monitoring and tracking program to be used with smart city content. In addition, we talked about the analysis, comparison and classification of OTSN. Research issues related to object retrieval position estimation, energy reservation, object detection, object motion, accuracy in tracking, sensor node collaboration, data aggregation, and energy reservation are also explored. Researchers can use this evaluation as a benchmark for building smart cities in the OTSN environment in the future. Finally, we provide suggestions for further studies [5].

A huge business opportunity is being presented in the development of the new era of smart cities by the recent advances and developments in the Internet of Things (IoT) industry. The concept of smart city is highly preferred as it combines multiple regulations such as smart parking, intelligent transportation, smart healthcare etc. to enhance the quality of life for the residents. Real-time data processing and rational decision-making capabilities pose significant threats to the intensification of complex urban environments. As a result, we suggest a Big Data Analytics-based framework for smart cities in this chapter. The suggested design is a general approach to smart urban planning and has been validated through the analysis of a variety of datasets. Examination shows that the suggested scheme provides significant incentives in social development systems to improve the current smart urban architecture, and we examine the reliable data on Hadoop server to validate the threshold limit value [6].

Internet of Things, which is growing in importance for the future of humans and robots, will be the basis for the next wave of information and applications. IoT services are an important component in creating smart environments in homes, structures and cities. Several issues including governance, compilation and storage for huge generated data have been raised in the era of a large number of connected things and devices with rapid growth rates. Cloud computing, also known as the Cloud of Things (CoT), was introduced in IoT to help solve some of these problems. COT provides almost unlimited cloud services to improve large-scale IoT systems. When creating and implementing a COT platform, several elements must be taken into account. Asymmetry of many objects is one of the most important and difficult issues. By implementing suitable "middleware" that stands between objects and applications as a consistent platform for

communication across objects with different interfaces, operating systems, and architectures, this issue can be resolved. The primary goal of this paper is to look into middleware techniques for CoT. To do this, we first outline the primary properties and characteristics of middleware. Then, we examine the different structure types and service areas. Next, we introduce several middle wares that are acceptable for COT-based platforms, and finally, we analyze several existing difficulties and problems with the design of COT-based middle wares [7].

DISCUSSION

This Chapter discusses the platform-related technical difficulties in supporting flexible IoT analytics for smart cities. A new technological trend for IoT analytics is to transfer data processing from either the cloud to the network edges since the number of IoT devices in a smart city is dramatically increasing and quick reaction time is strongly desired by more or smarter city use cases. We highlight this new technological trend and highlight how use cases might profit from it using two real-world platform implementations, namely City Data and Analytics Platform and Geelytics. Geelytics now focuses more heavily on the edge side, whereas City Data and Analytics Platform focus more on the cloud side. Geelytics, however, is meant to complement City Data and Enterprise Applications rather than replace it as an alternate option. Geelytics, for instance, excels at processing stream data both at the cloud's edge and in the cloud, however, it is not a viable option for handling large-scale historical files in the database, which is City Data and Analytics Platform's forte. To construct a more sophisticated and integrated platform for IoT analytics that can make use of both edge computing and cloud computing, it makes good sense to merge City Data and Analytics Platform with Geelytics. In the near future, that was one of the phases. Additionally, we are continuing to improve Geelytics' job assignment algorithms to provide mobility-aware IoT monitoring for moving devices like flying drones and linked autos.

CONCLUSION

We are focusing on semantic interoperability in the long run to allow enhanced IoT analytics that may make use of data from diverse data sources across various application domains. Relevant data for a smart city may originate from a variety of sources, including neighbouring IoT systems, the same IoT system, or even more conventional IT systems with contents that may have been contributed by people. Regardless of the specific data format, standardization will enable us to communicate with a wide range of data sources while preserving data integrity across systems. Using an ontology-defined common language, the semantics may be clearly described. Standardized solutions are necessitated for IoT to succeed, whether they are de facto conventions created as part of industry agreements or open source communities, or official standards. The OMA NGSI Context interfaces, which are the foundation of Fiware Platform, are used in CiDAP.

Additionally, we are actively taking part in the oneM2M standards. In the end, crucial functions created and investigated in our research prototypes need to be included in the standards. Gaps in standardization must be found and filled while different schemes must be brought into alignment. We have included fundamental semantic capabilities into oneM2M to provide semantic interoperability. Based on this, we conducted an experiment to demonstrate how semantic data may be utilized to transform oneM2M IoT data into the NGSI data format that is used by FIWARE. The idea of mediation gateways will now be used to generalize the strategy. We would also want to take into account the security and privacy concerns in IoT analytics for smart

cities for the next work. Although we have made considerable progress toward safe component-to-component communication in both CiDAP and Geelytics, this is still the first step in ensuring security. The IoT analytics platform is now globally distributed with the extended farther down to the edges, such as mobile base stations, IoT gateways, and even certain endpoint devices as well.

REFERENCES

[1] D. Jiang, "The construction of smart city information system based on the Internet of Things and cloud computing," *Comput. Commun.*, vol. 150, pp. 158–166, Jan. 2020, doi: 10.1016/j.comcom.2019.10.035.

[2] S. A. Shah, D. Z. Seker, M. M. Rathore, S. Hameed, S. Ben Yahia, and D. Draheim, "Towards Disaster Resilient Smart Cities: Can Internet of Things and Big Data Analytics Be the Game Changers?," *IEEE Access*, vol. 7, pp. 91885–91903, 2019, doi: 10.1109/ACCESS.2019.2928233.

[3] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. 2016. doi: 10.1201/b10867.

[4] S. Bennati and E. Pournaras, "Privacy-enhancing aggregation of Internet of Things data via sensors grouping," *Sustain. Cities Soc.*, vol. 39, pp. 387–400, May 2018, doi: 10.1016/j.scs.2018.02.013.

[5] M. S. Adam, M. H. Anisi, and I. Ali, "Object tracking sensor networks in smart cities: Taxonomy, architecture, applications, research challenges and future directions," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 909–923, Jun. 2020, doi: 10.1016/j.future.2017.12.011.

[6] M. Babar and F. Arif, "Smart urban planning using Big Data analytics to contend with the interoperability in Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 77, pp. 65–76, Dec. 2017, doi: 10.1016/j.future.2017.07.029.

[7] A. Farahzadi, P. Shams, J. Rezazadeh, and R. Farahbakhsh, "Middleware technologies for cloud of things: a survey," *Digit. Commun. Networks*, 2018, doi: 10.1016/j.dcan.2017.04.005.

CHAPTER 9

AN EVOLUTION OF DATA AGGREGATION FOR THE INTERNET OF THINGS IN SMART CITIES

Dr. A Maheswari Senthil Kumar, Assistant Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- a.maheswari@presidencyuniversity.in

ABSTRACT

The Internet of Things is a contemporary, cutting-edge system that promises to link a wide range of digital equipment with the Internet, delivering many new services in the framework of a smart city. These devices are packed with various sensing, actuation, and processing capabilities. Smart city efforts are being made possible internationally because of the alluring IoT services combined with big data analytics. By enhancing transport and infrastructure systems, lowering traffic congestion, managing waste, and enhancing human life quality, these services are altering cities. Additionally, we provide us with a summary of the most recent global collaborations and measures taken to advance IoT in the context of smart cities. Finally, to offer recommendations for future study, designers identify several concerns.

KEYWORDS: Application Layer, Cloud Computation, Data Aggregation, Internet of Things, Sensors.

INTRODUCTION

Over the last decades, the prevalence of emerging wireless technologies and internet-based systems such as cloud computing has promoted the blooming of the Internet of Things (IoT), offering more convenience and flexibility in our various daily applications. IoT is defined as the network of smart, distributed, self-organized, and energy-constrained sensors and everyday physical devices that can provide specific functionality without human intervention through the Internet. IoT is a networked interconnection between multiple heterogeneous systems[1], [2]. As illustrated in Figure 1, the architecture of IoT-based systems includes four layers: sensing layer, networking layer, cloud computing layer, and applications layer. Every layer of IoT architecture provides self-governing functionality and scalability. In the following, the four-layer architecture of IoT is described.

v. Sensory Layer

This layer is where different sensors and IoT devices gather data from the monitoring area and transfer it to the sink. The monitoring area is home to millions of IoT devices that have been set up to create a self-organized, multi-hop topology. In a basic IoT system with sensors, a sink, and management nodes, the sensors gather data from the monitoring area and then send it in a multi-hop fashion to the sink. Through management nodes, system administrators may keep an eye on and regulate the operation of IoT devices. It should be mentioned that certain IoT devices are vulnerable to failure since they are located in a particular region. Additionally, certain gadgets' energy runs out more quickly than others. Therefore, it is crucial to use energy-efficient approaches for IoT data aggregation[3], [4].

vi. **Networking Layer**

The networking layer is in charge of offering effective topologies for data transmission between source and destination devices. IoT topologies should enable high data transmission rates for source devices, however owing to various topologies, these systems are subject to limitations in terms of throughput, energy use, and malicious assaults.

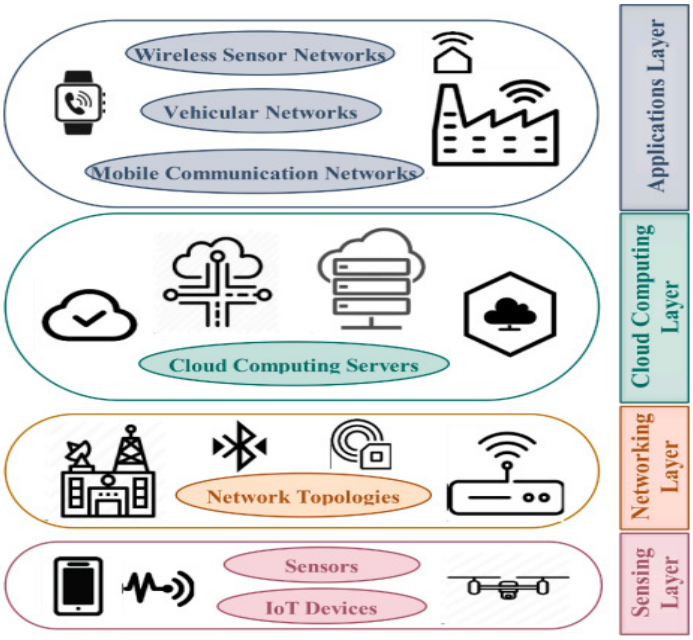


Figure 1: Represented the Layered architecture of IoT.

vii. **Cloud Computing Layer**

The ability to handle massive amounts of data more rapidly and precisely has been made feasible by advancements in cloud computing technology. Data is received, processed, and decided upon by the cloud computing layer, which then sends the results to other tiers. Although cloud computing is the preferred method for IoT-based systems to store and analyse data, other techniques favour edge and fog to maximise costs and performance. The main goal of using edge or fog architecture in the data aggregation process is not to replace the cloud, but rather to manage system heterogeneity, cope with distant IoT devices, and distinguish important data from generic data. The necessity for huge data aggregation in IoT applications drives techniques away from cloud computing and toward fog or edge computing.

viii. **Applications Layer**

This layer includes a variety of applications, including wireless sensor networks, smart grids, smart homes, smart cities, and smart healthcare. Anyone may use a smart gadget to communicate with people whenever and wherever they are. IoT applications are also utilised to keep an eye on

environmental conditions and emergencies. To effortlessly take use of IoT capabilities in their everyday lives and industries, user-friendly interfaces are required.

Since 1999, the Internet of Things (IoT) has advanced at an incredible rate, enabling smart technologies-based communication between people and virtual worlds. Figure 2 shows the installed base of IoT-connected devices from 2015 to 2025 globally. The number of IoT-connected devices is predicted to reach more than 75 billion by 2025. People cannot imagine living in a connected world without IoT devices and the services they provide.

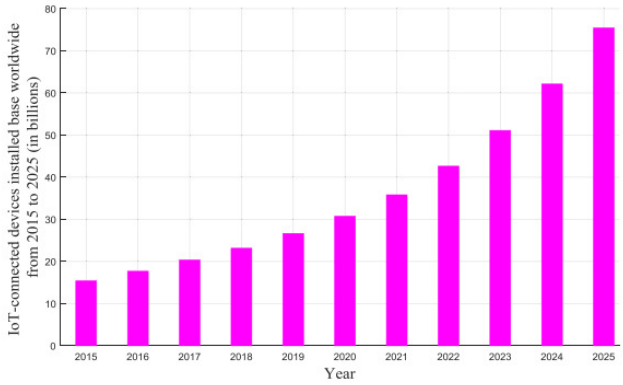


Figure 2: Represented the IoT-connected devices installed base worldwide from 2015 to 2025 (in billions).

IoT is used in many facets of daily life and business. IoT applications may be categorized into six categories, as indicated in Figure 3: industrial, agricultural, transportation, smart buildings, security, and healthcare systems. To gather data from the monitoring domain and provide it to the sink, monitoring systems and IoT devices are linked to the network in these applications. The Internet of Things is now a feasible technology for a variety of applications because to characteristics like cheap cost, adequate functionality, and high error tolerance. Here, IoT applications are briefly discussed and divided into the following categories:

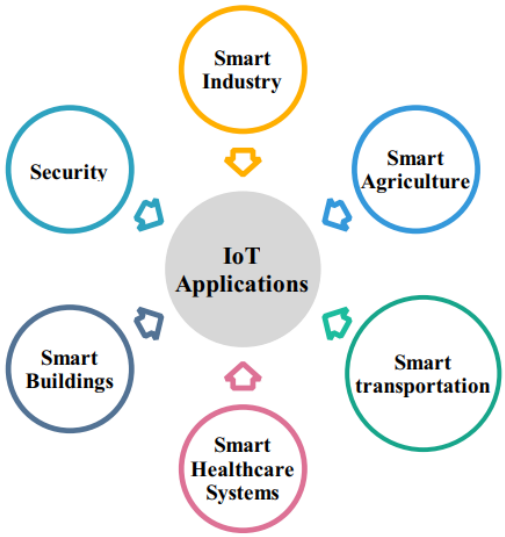


Figure 3: Represented the IoT Applications.

vii. Industry

In industrial settings, a variety of IoT devices are used to monitor production processes and boost productivity. Real-time functional parameters, increased throughput, and decreased organisational expenses have been achieved by using IoT-based industrial management systems. Additionally, sensors may gather environmental data in dangerous locations like gas pipelines and mines, transfer it to a sink, and ensure employee safety via real-time alerts. The creation of interoperable, intelligent, and energy-efficient factories is referred to as Industry 4.0 and is regarded as the cornerstone of the IoT-based industry.

viii. Agriculture

Smart sensors and IoT devices may turn on and off automatically at certain periods to perceive environmental data in realtime. A monitoring area is equipped with hundreds of sensors that operate together as a self-organizing, multi-hop network to collect environmental data and transmit it to cloud computing servers for further analysis and decision-making. In addition, IoT-based technologies are utilized to remotely manage farms and greenhouses as well as automate the process of monitoring agricultural settings.

ix. Transportation

Networks based on the internet of cars are referred to as smart transportation systems. To control traffic, provide trip information, lessen environmental pollution, increase safety, and improve conventional transportation systems, these systems incorporate cutting-edge information technology and electronic sensors.

x. Smart buildings

IoT systems provide automated building control and security capabilities by integrating digital technology and network connection protocols. Comfort, energy efficiency, dependability, and ecologically responsible living are all made possible through intelligent building management. IoT devices may be connected to the system in smart buildings through remote communication networks or short-range wireless connections, enabling users to operate their house or workplace from a distance. For a smart building to have the same qualities as conventional buildings and to enable effective equipment communication, IoT devices must be diversified and scalable.

xi. Healthcare Systems

IoT has developed into a smart technology in recent years for delivering healthcare services, keeping an eye on old patients' behavior and vital signs without interfering with their everyday activities, and enhancing surgical operations. Humans' heart rates, blood pressure, and sleep patterns may be sensed by smartphones, clocks, wristbands, and other wearables, which can then be used to monitor their health remotely in realtime. Additionally, IoT-based robots may advise ways to help users' health practices. Patient comfort, safer procedures, better hospital administration, and the provision of more precise pharmaceuticals are some of the important IoT applications' contributions to smart healthcare systems.

xii. Security

IoT-based security systems are characterized as a collection of instruments for preventing theft and general safety, including security for communications, protection from fire, first aid, and risk factor monitoring. Security systems keep an eye on both the internal and exterior settings, gather important information, and alert the user in an emergency.

All spheres of life have steadily shifted toward a "smart" contemporary civilization thanks to the Internet of Things and cloud computing's strong development, widespread use, and convergence of new ideas and technology. The area of smart cities has been increasingly impacted by these technologies. The conventional urban system, which has been passed on from generation to generation since antiquity, operates in an exceptionally inefficient and laborious manner, and information across the systems has never been efficiently exchanged and integrated. A smart city system is based on the Internet and cloud computing has been suggested, with the backing of these two technologies. In-depth research has been conducted on multiple levels on system architecture, application software implementation, application support platforms, diverse transmission networks, and common sensors. Sensor networks are often positioned in poor communications settings in the Internet of Things-based smart city systems, which typically results in data communication failure. An optimal issue is whether the sensor decides to communicate again after an unsuccessful information transfer. The experiment findings demonstrate that the system is capable of knowing information interchange, fusion, and sharing throughout multiple sensing subsystems, resolving the communication island problem of the past, and addressing the requirement of smart cities [5].

Model scheme of an enterprise energy efficiency management platform based on the Internet of Things is examined, and the dynamically collected energy consumption data is reviewed using Internet of Things technology and data mining technology, to address the current predicament of complicated energy-consuming equipment and large energy consumption in the current enterprise. They provide help for making judgments on corporate energy efficiency management practices and the creation of initiatives for energy conservation and emission reduction. The current state of energy efficiency management in buildings is reviewed in this chapter, along with its pain points, which include installation dilemmas, high software development costs, upgrade challenges, protracted debugging cycles, and closed systems. To address these challenges, intelligent power transmission monitoring accessed via the Internet of Things is introduced. Through case studies, we investigate the system's real value in energy efficiency information management. Through the Internet of Things, it may acquire scattering data, compile it into vast data, and then utilize data analysis and processing to locate the relevant data. It is simple to promote and use, has a good usage impact, excellent practicality, and a sensible design.

The dominance of sensors and the Internet in the previous age of the Internet of Things offers a solution to a diverse range of everyday issues. Smart cities, smart healthcare systems, intelligent buildings, industrial automation, and smart environments are a few samples of such applications. However, there are several problems with real-time IoT sensor data, including one with a flood of dirty sensor data and a maximum resource cost. To create informed insight into unseen data patterns for quick decision-making, this chapter discusses how to handle IoT sensor data, fuse it with data from multiple sources, and conduct analysis. This paper discusses methods for processing data, including data demising, outlier recognition, imputation for missingdata, and data aggregation. The requirement of machine learning and other data fusion techniques, such as

direct fusion, related semantic segmentation, and identity announcement data fusion, are also discussed in depth. To handle multiple difficulties in IoT sensor networks and environmental data analysis, this study also tries to deal with data analysis integration with new advancements, such as cloud applications, fog computing, and advanced analytics. In conclusion, this study has provided the first comprehensive review of Iot data processing, fusion, and research methodology.

The potential to be fatal for infrastructure, the environment, and human life. The development of the required earthquake-resistant smart city (DRSC) settings is now conceivable because of recent developments in the Internet of Things and big data analytics technology. Through the application of IoT and big data analytics technologies, we demonstrate and explain the new reference design and philosophy of a disaster-resilient smart city in this paper. A general solution for disaster preparedness initiatives in smart city motivations is provided by the suggested architecture. To build an efficient DRSC environment that enables both real-time and asynchronous analysis, the Hadoop Ecosystem and Spark are combined. Data collection, dataaggregation, data pre-processing, big data analytics, and application servers make up the environment's implementation strategy. For the validation and analysis of the system to detect and create warnings for a massive fire, city pollution level, evacuation routes route, and the collection of information about natural catastrophes, a range of datasets are used. Throughput and batch processing are used to evaluate the system's efficiency, which highlights the suggested architecture's increased quality. Additionally, the main challenges of working are noted and described briefly [6].

A smart city was pioneered by the Internet of Things (IoT), which was inspired by the explosive expansion of linked heterogeneous devices. The goal of the many factors that comprise the design of smart cities is to improve the quality of life for urban residents. These elements encompass smart transportation, smart communities, smart healthcare, smart grid, etc. Real-time processing needs and the exponential rise of data, however, prevent the implementation of smart cities. As a result, we here suggest an experimental method for smart cities that integrates Big Data analytics. The embedded smart city provides services for two main features. First off, it makes it easier to use urban big data for creating, building, and administering smart cities. Second, it requires night before going to bed management and processing to improve the standard of urban services. The suggested architecture's three layers are responsible for managing real-time data, aggregating data, and providing services. By including data normalization and data filtering procedures throughout into suggested job, offline and online data processing operations are further sped up. We were able to determine the threshold values essential for urban planning and municipality operation management by evaluating verified datasets. Analysis of current works' throughput and processing times indicate that the new job will perform better overall.

The process of gathering big data using Internet of Things (IoT) ubiquitous technology is often privacy-invasive and leads to surveillance, profiling and discriminatory measures against residents, which is a major challenge for citizens in building sustainable smart cities. reduces the busyness of Nevertheless, there is great potential for monitoring and regulating smart city infrastructure more effectively and sustainably, thanks to real-time data analytics and information gathered from IoT devices. The study topic and problem addressed in this paper is the privacy-enhancing aggregation of dispersed sensor data such as household energy usage or traffic data. Citizens can choose the degree of privacy they want by reducing the quality of the

data shared at the cost of less accurate data analysis services. Real-world data from two smart city pilot projects are used to assess the proposed technology and its general applicability. Secrecy is enhanced under grouping, while maintaining the accuracy of the baseline scenario. Fairness on privacy among group members with comparable privacy preferences is shown to be greatest when the impact of privacy is assessed by one group member versus another group member. There are opposites of different grouping techniques. The most privacy is achieved when privacy options are grouped by proximity. The impact of the strategy on the design of incentive systems is examined [7].

The rise of the Internet of Things (IoT) and the development of ubiquitous communication devices have played an important role in the feasibility of smart city plans. Cities have the potential to become smarter thanks to wireless sensor networks (WSNs), a key enabling technology in the Internet of Things. Due to the increasing number of WSN applications that allow remote monitoring and tracking in smart cities, WSN has attracted great interest in recent years. Object tracking sensor networks are one of the most interesting uses of WSNs in smart cities for detection, monitoring and tracking (OTSN). Smart cities of the future will face new and fascinating challenges as a result of the integration of OTSNs into urban areas. These difficulties mostly center on the issues of active surveillance and monitoring in smart cities. In this paper, we outline the key features of OTSN, a monitoring and tracking program to be used with smart city content. In addition, we talked about the analysis, comparison and classification of OTSN. Research issues related to object retrieval position estimation, energy reservation, object detection, object motion, accuracy in tracking, sensor node collaboration, data aggregation, and energy reservation are also explored. Researchers can use this evaluation as a benchmark for building smart cities in the OTSN environment in the future. Finally, we provide suggestions for further studies [8].

A huge business opportunity is being presented in the development of the new era of smart cities by the recent advances and developments in the Internet of Things (IoT) industry. The concept of smart city is highly preferred as it combines multiple regulations such as smart parking, intelligent transportation, smart healthcare etc. to enhance the quality of life for the residents. Real-time data processing and rational decision-making capabilities pose significant threats to the intensification of complex urban environments. As a result, we suggest a Big Data Analytics-based framework for smart cities in this chapter. The suggested design is a general approach to smart urban planning and has been validated through the analysis of a variety of datasets. Examination shows that the suggested scheme provides significant incentives in social development systems to improve the current smart urban architecture, and we examine the reliable data on Hadoop server to validate the threshold limit value [9].

Internet of Things, which is growing in importance for the future of humans and robots, will be the basis for the next wave of information and applications. IoT services are an important component in creating smart environments in homes, structures and cities. Several issues including governance, compilation and storage for huge generated data have been raised in the era of a large number of connected things and devices with rapid growth rates. Cloud computing, also known as the Cloud of Things (CoT), was introduced in IoT to help solve some of these problems. COT provides almost unlimited cloud services to improve large-scale IoT systems. When creating and implementing a COT platform, several elements must be taken into account. Asymmetry of many objects is one of the most important and difficult issues. By implementing suitable "middleware" that stands between objects and applications as a consistent platform for

communication across objects with different interfaces, operating systems, and architectures, this issue can be resolved. The primary goal of this paper is to look into middleware techniques for CoT. To do this, we first outline the primary properties and characteristics of middleware. Then, we examine the different structure types and service areas. Next, we introduce several middle wares that are acceptable for COT-based platforms, and finally, we analyze several existing difficulties and problems with the design of COT-based middle wares [10].

DISCUSSION

This Chapter discusses the platform-related technical difficulties in supporting flexible IoT analytics for smart cities. A new technological trend for IoT analytics is to transfer data processing from either the cloud to the network edges since the number of IoT devices in a smart city is dramatically increasing and quick reaction time is strongly desired by more or smarter city use cases. We highlight this new technological trend and highlight how use cases might profit from it using two real-world platform implementations, namely City Data and Analytics Platform and Geelytics. Geelytics now focuses more heavily on the edge side, whereas City Data and Analytics Platform focus more on the cloud side. Geelytics, however, is meant to complement City Data and Enterprise Applications rather than replace it as an alternate option. Geelytics, for instance, excels at processing stream data both at the cloud's edge and in the cloud, however, it is not a viable option for handling large-scale historical files in the database, which is City Data and Analytics Platform's forte. To construct a more sophisticated and integrated platform for IoT analytics that can make use of both edge computing and cloud computing, it makes good sense to merge City Data and Analytics Platform with Geelytics. In the near future, that was one of the phases. Additionally, we are continuing to improve Geelytics' job assignment algorithms to provide mobility-aware IoT monitoring for moving devices like flying drones and linked autos.

CONCLUSION

We are focusing on semantic interoperability in the long run to allow enhanced IoT analytics that may make use of data from diverse data sources across various application domains. Relevant data for a smart city may originate from a variety of sources, including neighbouring IoT systems, the same IoT system, or even more conventional IT systems with contents that may have been contributed by people. Regardless of the specific data format, standardization will enable us to communicate with a wide range of data sources while preserving data integrity across systems. Using an ontology-defined common language, the semantics may be clearly described. Standardized solutions are necessitated for IoT to succeed, whether they are de facto conventions created as part of industry agreements or open source communities, or official standards. The OMA NGSI Context interfaces, which are the foundation of Fiware Platform, are used in CiDAP.

Additionally, we are actively taking part in the oneM2M standards. In the end, crucial functions created and investigated in our research prototypes need to be included in the standards. Gaps in standardization must be found and filled while different schemes must be brought into alignment. We have included fundamental semantic capabilities into oneM2M to provide semantic interoperability. Based on this, we conducted an experiment to demonstrate how semantic data may be utilized to transform oneM2M IoT data into the NGSI data format that is used by FIWARE. The idea of mediation gateways will now be used to generalize the strategy. We would also want to take into account the security and privacy concerns in IoT analytics for smart

cities for the next work. Although we have made considerable progress toward safe component-to-component communication in both CiDAP and Geelytics, this is still the first step in ensuring security. The IoT analytics platform is now globally distributed with the extended farther down to the edges, such as mobile base stations, IoT gateways, and even certain endpoint devices as well.

REFERENCES

[1] C. Pavel and F. Vlad, "Trends in the Evolution of Mobile Commerce," *Quaestus*, 2016.

[2] G. Greenleaf and S. Livingston, "China' s New Cybersecurity Law – Also a Data Privacy Law?," *Priv. Laws Bus. Int. Rep.*, 2016.

[3] S. J. Shackelford, "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk," *Chapman Law Rev.*, 2016.

[4] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. 2016. doi: 10.1201/b10867.

[5] D. Jiang, "The construction of smart city information system based on the Internet of Things and cloud computing," *Comput. Commun.*, vol. 150, pp. 158–166, Jan. 2020, doi: 10.1016/j.comcom.2019.10.035.

[6] S. A. Shah, D. Z. Seker, M. M. Rathore, S. Hameed, S. Ben Yahia, and D. Draheim, "Towards Disaster Resilient Smart Cities: Can Internet of Things and Big Data Analytics Be the Game Changers?," *IEEE Access*, vol. 7, pp. 91885–91903, 2019, doi: 10.1109/ACCESS.2019.2928233.

[7] S. Bennati and E. Pournaras, "Privacy-enhancing aggregation of Internet of Things data via sensors grouping," *Sustain. Cities Soc.*, vol. 39, pp. 387–400, May 2018, doi: 10.1016/j.scs.2018.02.013.

[8] M. S. Adam, M. H. Anisi, and I. Ali, "Object tracking sensor networks in smart cities: Taxonomy, architecture, applications, research challenges and future directions," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 909–923, Jun. 2020, doi: 10.1016/j.future.2017.12.011.

[9] M. Babar and F. Arif, "Smart urban planning using Big Data analytics to contend with the interoperability in Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 77, pp. 65–76, Dec. 2017, doi: 10.1016/j.future.2017.07.029.

[10] A. Farahzadi, P. Shams, J. Rezazadeh, and R. Farahbakhsh, "Middleware technologies for cloud of things: a survey," *Digit. Commun. Networks*, 2018, doi: 10.1016/j.dcan.2017.04.005.

CHAPTER 10

AN EVOLUTION OF INTERNET OF THINGS PROTOCOLS IN CYBER SECURITY

Mrs. Varalakshmi K R, Assistant Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- varalakshmi.kr@presidencyuniversity.in

ABSTRACT

The internet of things is a hot idea that involves connected items so they may interact among themselves across networks. Protocols are used to control this connection and make sure that data and information are sent correctly while adhering to the regulations set out by the different standards organizations. The bothersome topic of how to improve the protection of these interactions emerges as telecommunications go forward. The goal of this chapter is to present the current state of the major protocols that control communication among interconnected objects inside this IoT domain, to list each protocol's shortcomings and any current solutions, and to compare these existing techniques in terms of their features and capabilities and traits.

KEYWORDS: Communication, Cyber Security, Internet of Things, Protocols.

INTRODUCTION

The Internet of Things is a recent phenomenon that involves attaching devices to converse and exchange data. This communication is controlled by protocols, where a convention is a collection of guidelines for specifying a certain kind of communication. There are eight basic sorts of protocols that control communication between devices in the Internet of objects:

A. Infrastructure (e.g., 6LowPAN, IPv4 / IPv6, RPL)
B. Identification (e.g., EPC, uCode, IPv6, URIs)
C. Comms / Transport (e.g., Wifi, Bluetooth, LPWAN)
D. Discovery (e.g., Physical Web, mDNS, DNS-SD)
E. Data Protocols (e.g., MQTT, CoAP, AMQP, Websocket, Node)
F. Device Management (e.g., TR-069, OMA-DM)
G. Semantic (e.g., JSON-LD, Web Thing Model)
H. Multi-Layer Frameworks (e.g., Alljoyn, IoTivity, Weave, Homekit)

First, we must provide a solution to the following questions: How do the protocols function and how do they interact with one another? What errors have been found in each protocol? What are the numerous attack and threat categories that have an impact on these protocols? And lastly, what are the current alternatives and steps that must be taken to reduce the degrees of impact? The structure of this essay is as follows: To ensure the security, integrity, and privacy of the personal information, we will first define each protocol, analyze its design, list its flaws, and provide any suggested alternatives that are already available. Then, to compare worldwide data

on energy usage, typologies used, and security the most important factor we give a table summarizing each protocol's properties. Finally, we'll discuss our ambitions and upcoming projects.

Protocols of IoT

IoT protocols and standards can be broadly classified into two separate categories.

1. IoT Network Protocols

IoT network protocols are used to connect devices over the network. These are the set of communication protocols typically used over the Internet. Using IoT network protocols, end-to-end data communication within the scope of the network is allowed. Following are the various IoT Network protocols:

i. HTTP (Hyper Text Transfer Protocol)

The most effective IoT network protocol is Hyper Text Transfer Protocol. The backbone of data transmission via the web is this protocol. When there is a lot of data to be released, it is the most popular protocol for IoT devices. The HTTP protocol is not favoured, nevertheless, due to its cost, battery life, energy efficiency, and further limitations. One use for the HTTP protocol is additive manufacturing and 3D printing. It allows computers to network 3D printers to produce three-dimensional objects and prototypes for predetermined processes.

ii. Lo-Ra-Wan (Long Range Wide Area Network)

It is a low power, long-range protocol that can detect signals below background noise. Battery-powered devices may be wirelessly connected to the Internet using Lo-Ra-Wan in local or worldwide networks. Millions of low-power, low-memory devices are utilised in smart cities, where this communication protocol is mostly employed. The Lo-Ra-Wan IoT protocol's practical use case is smart street lighting. This protocol may be used to link the streetlights to a Lo-Ra gateway. The gateway then establishes a connection with a cloud programme that automatically regulates light bulb intensity depending on environmental illumination, which aids in lowering power usage throughout the day.

iii. Bluetooth

One of the most popular short-range communication technologies is Bluetooth. It is a typical IoT protocol for transmitting wireless data. This short-range, low-power, low-cost, wireless transmission protocol is safe and ideal for use between electrical devices. The BLE (Bluetooth Low Energy) protocol is a low-energy variant of the Bluetooth standard that is crucial for tying together Internet of Things (IoT) devices. In smart wearable's, smartphones, and other mobile devices where little data pieces may be transmitted without requiring a lot of power and memory, Bluetooth protocol is primarily employed. Bluetooth is the most user-friendly device communication standard for IoT devices.

iv. Zig-Bee

An IoT technology called Zig-Bee enables the communication between intelligent items. It often appears in home automation. Zig-Bee is utilised with applications that enable low-rate data transmission over short distances and is more well-known for usage in industrial environments. Urban regions that provide minimal power usage employ the Zig-Bee communication

technology for street lights and energy metres. Additionally, it is used in smart homes and security systems.

2. IoT Data Protocols

Low power IoT devices are connected via IoT data protocols. Without requiring an Internet connection, these protocols provide point-to-point communications with the hardware on the user side. IoT data protocols use cellular or cable networks for connectivity. Several IoT data protocols include:

i. Message Queue Telemetry Transport (MQTT)

One of the most popular protocols for IoT devices, MQTT provides remote device monitoring and gathers data from a variety of electronic devices. It facilitates event-driven message exchange across wireless networks since it is a subscribe/publish protocol that operates over Transmission Control Protocol (TCP). MQTT is mostly utilised in low-cost, power- and memory-intensive devices. Examples include text-based chat applications, smart watches, auto sensors, and fire alarms.

ii. Constrained Application Protocol (CoAP)

CoAP is a limited device internet utility protocol. The client may use this protocol to communicate requests to the server, and the server can use HTTP to communicate responses to the client. It uses less space and uses UDP (User Datagram Protocol) for implementation which is lightweight. The protocol use the EXL binary data format (Efficient XML Interchanges). The CoAP protocol is mostly utilised in microcontrollers, mobile devices, and automation. The protocol requests services and resources from the application's endpoints, such as home appliances, and then returns a response.

iii. Advanced Message Queuing Protocol (AMQP)

AMQP is a routing and queuing software layer protocol for message-oriented middleware environments. It provides smooth and secure data sharing between connected devices and the cloud and is utilised for dependable point-to-point connections. The three components of AMQP are Exchange, Message Queue, and Binding. These three elements work together to provide a safe and effective communication exchange and storage. Additionally, it aids in demonstrating how one message relates to another. The banking sector is the principal application for the AMQP protocol. The protocol keeps track of every message sent by a server until it is successfully delivered to all intended users and destinations.

iv. Machine-to-Machine (M2M) Communication Protocol

It is an open industry standard designed to provide IoT device remote application administration. M2M communication technologies employ open networks and are economical. It establishes a setting in which two computers may converse and share information. This protocol promotes machine self-monitoring and enables systems to change in response to their surroundings. Smart homes, automatic vehicle registrations, vending machines, and ATMs all employ M2M communication protocols.

v. Extensible Messaging and Presence Protocol (XMPP)

The XMPP has a distinctive design. It exchanges messages in real time via a push method. XMPP is adaptable and can effortlessly incorporate changes. Extensible Markup Language

(XML) was used in the development of XMPP, which functions as a presence indicator by displaying the availability state of the servers or devices sending or receiving messages. XMPP is used in online gaming, news websites, and Voice over Internet Protocol in addition to instant messaging programmes like Google Talk and WhatsApp (VoIP).

Advantages and Disadvantages of Internet of Things

a. Advantages of IoT:

The internet of things provides several benefits in day-to-day operations in the commercial world. Below are a few of its advantages:

- **Efficient Resource Utilization**

If we are aware of the functioning and operation of each gadget, we can monitor natural resources and use them more efficiently.

- **Reduce Human Effort**

As IoT devices collaborate and communicate with one another and do many tasks on our behalf, they reduce human effort.

- **Save Time**

Since it requires less human effort, time is unquestionably saved. The main resource that an IoT platform can save is time.

- **Increase Security**

If we create a system where all of these components are linked, we can increase security and efficiency [1].

b. Disadvantages of IoT include:

While the Internet of Things enables several advantages, it also generates a sizeable number of difficulties. Below are a few of the IoT challenges:

i. **Security**

Due to network connectivity and interconnectedness, IoT systems need security. Despite security precautions, the system is not very controllable and is vulnerable to several network assaults.

ii. **Privacy**

The Internet of Things system offers significant personal data in great detail, even without the user's active engagement.

iii. **Complexity**

The huge technology to IoT system's design, development, maintenance, and enablement are rather challenging.

IoT Applications Include

i. Smart City or Smart Home

Both concepts seem like they could only exist in science fiction literature or television programs. Since they were introduced in the television series The Jetsons, smart cities have captured our attention. The following attributes are expected to be present in the smart home:

ii. Smart Kitchen Appliances

A smart kitchen would increase the home's functionality and attractiveness to potential buyers. A few elements of the smart kitchen are as follows.

iii. Smart Plate

It will have Wi-Fi, cameras, and weight sensors. What you consume will be observed by the dish. If you overload, it notifies you and can link with your smartphone personal fitness plan.

iv. Drop

This option enables you to choose the meal you want to prepare, and with the aid of a smart measure, you may customize the recipe to your preferences. Additionally, most of the time in the recipes Drop offers, just one bowl is used. It also guarantees minimal cleanup after cooking.

v. Smart Fridge

This would entail a built-in artificial intelligence that could communicate with certain other appliances in the smart home or smart kitchen. A 29-inch front screen is available for taking notes or entering information about the refrigerator contents.

vi. Smart Cooker

When this product is available, you will no longer have to worry about burning your breakfast since you can change the settings for cooking temperature and cook time, regardless of where you are.

- **Thermostat with Learning Capabilities***:* can figure out the homeowner's daily schedule and change the temperature appropriately.
- **Smart Lock***:* A key-less lock that can be opened with a smartphone app is just one of many such gadgets that may make life much simpler all around your house and many more such devices that can make life around your home much easier. A smart city is an urban system that uses information and communications technology to make the infrastructure more interactive make infrastructure more efficient more importantly, make the infrastructure more accessible [2]so that it is available when we need it a smart city is the need of the hour because of:

- A swiftly increasing metropolitan population
- Quickly diminishing store of natural resources
- Environmental and climatic changes

The Internet of Things (IoT) is expanding quickly, and its wireless technology has several security concerns Because IoT protocols are varied, tailored to specific requirements, and widely used in a variety of application areas, they provide difficult security challenges. We conclude

from this study that a standardized formalism that applies to all IoT protocols is required. In this review, we provide a general strategy with dual difficulties. To compare IoT protocol stacks, our first task is to identify common elements that may be used to design a general methodology. We compare various IoT protocols based on five biggest factors: their range, interoperability, openness as a protocol, topology, and security procedures. The second issue we think about is how to broadly categorise core IoT threats, irrespective of the protocol in use. This method, which again is broken down into three parts: attacks focused on packets, attacks focusing on the protocol, and attacks focusing on the whole system, reveals significant risks across various IoT protocols. Additionally, it identifies the processes that vary between the two schemes and leaves them both open to attack. Furthermore, we take a few insights and takeaways from this Trans disciplinary research.

A network of sensors, actuators, and networking devices used for communication and control is known as the Internet of Things (IoT). Because IoT devices have limited resources, an efficient routing protocol is needed to convey sensed data from source to destination. One of the most popular routing protocols in Internet of Things networks is the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL). In the Cooja simulator built on the Contiki platform, the performance of the RPL protocol is assessed using three distinct mobility models: Manhattan Grid (MG), Gaussian Markov (GM), and Random Waypoint (RW) at various scaling levels. For analysis, the common Quality of Service metrics Packet Delivery Ration, Average Power, and Hop Count is taken into consideration. The Manhattan Grid model offers higher QoS performance by maintaining the functioning nature of RPL ideally, according to a thorough experimental examination of RPL when subjected to various mobility models and scalability [3].

Future industrial settings will make use of the Internet of Things (IoT) paradigm to track asset activity and increase an enterprise's performance efficiency and agility. Any physical thing may be included in the IoT and linked to the Internet according to the IoT idea. As a result, the IoT will include a diverse spectrum of embedded devices, each of which will use a different protocol to share data. The effective deployment of a full IoT solution is challenged by the inclusion of such a large variety of diverse entities inside the IoT system. It is essential to devise an architecture that spans the gap between the lower levels of IoT services and the physical devices to solve the heterogeneity issue in the IoT domain. In this study, we provide an ontological strategy for connecting devices using various protocols and combining them into the IoT ecosystem [4].

Internet of Things (IoT) has attracted a lot of interest over the last ten years because it includes intelligent gadgets like smart sensors and actuators, which allow a variety of applications that enhance our everyday lives. IoT networks are, however, facing a variety of network performance issues as a result of the large number of diverse and resource-constrained devices that often operate in hostile settings while communicating across error-prone and lossy radio channels. In this setting, effective IoT network management is required to guarantee high network performance. This has sped up the creation of various frameworks and standards for managing IoT networks. This chapter presents a thorough analysis of key works on IoT network management. The study reviews current approaches for managing IoT low power networks and provides a taxonomy of such approaches. Additionally, this paper contrasts several requirements-based research suggestions for managing IoT low power networks. This report concludes by outlining the remaining obstacles to effective administration of IoT low power networks.

Internet of Things (IoT) is discussed in general terms in this paper, with a focus on enabling technologies, protocols, and application-related challenges. The most recent advancements in RFID, smart sensors, communication technologies, and Internet protocols allow the Internet of Things. The fundamental idea is to create a new class of applications by having smart sensors work together directly without human intervention. The present Internet, mobile, and machine-to-machine (M2M) technology boom may be seen as the beginning of the Internet of Things. The Internet of Things (IoT) is anticipated to link physical things to enhance intelligent decision-making in the next years, bridging various technologies to open up new applications. This paper begins by giving a broad overview of the IoT. Then, we provide a high-level review of a few technical aspects relating to the IoT enabling technologies, protocols, and applications. Our goal is to provide a more thorough summary of the most important protocols and application issues compared to other survey papers in the field so that researchers and application developers can quickly understand how the various protocols work together to deliver desired functionalities without having to read through RFCs and the standards specifications. We also provide a brief review of some of the most important IoT problems that have been discussed recently in the literature and a description of relevant research. We also investigate the connections between the IoT and other cutting-edge technologies, such as big data analytics, cloud computing, and fog computing. We also discuss how IoT services need to be more horizontally integrated. To show how the various protocols discussed in the paper work together to offer desired IoT services, we next give thorough service use-cases [5].

The everyday performance of industrial and commodity operations is being redefined by the Internet of Things (IoT). The combination of sensors, efficient processing, and the widespread use of various wireless technologies on IoT platforms make it possible for people to engage with their physical surroundings in great detail. In order to make it easier for researchers and developers to monitor and operate diverse IoT devices, numerous distinct IoT platforms have been established in response to the rapid growth of IoT. By offering APIs, IoT platforms serve as a link between consumers and basic IoT functionality in general. IoT platforms have a broad range of applications, thus they vary greatly in their topologies and designs. As a result, the right setup, execution, and protection of IoT solutions provide a problem for IoT administrators, developers, and researchers (i.e., IoT users). We next plan to investigate how the various IoT platforms address security and privacy risks impacting the most basic security services of confidentiality, integrity, availability, and access control, rather than identifying new dangers affecting IoT. We also provide solutions that these platforms may use to improve security and privacy for the IoT solution. Finally, we go through the benefits and drawbacks of each IoT platform so that IoT administrators, developers, and researchers (i.e., IoT users) may choose the best platform to employ when putting their IoT ideas into practice. As far as we are aware, this is the first thorough study to compare various IoT systems using the standards established in this work.

The volume and velocity of data continue to grow quickly as Internet of Things (IoT) devices proliferate. For communicating IoT data, IoT systems generally depend on messaging protocols, and there are several frameworks but rather protocols that allow various message patterns. It becomes extremely difficult to choose a lightweight, dependable, scalable, interoperable, extensible, and secure messaging protocol since Iot applications often have limited computing resources and processing capacity. To handle device heterogeneity as well as various message exchange patterns, IoT systems often use numerous messaging protocols. Additionally, the fundamental commonalities across the various messaging frameworks or protocols in use today

for IoT data exchange inside IoT systems point to the possible eventual interoperability. Because IoT systems make it easier for scattered, heterogeneous entities to communicate with one another, current messaging formats' compatibility will become more critical in streamlining the creation and implementation of IoT systems. We provide a thorough analysis of the current messaging protocols that may be implemented in IoT systems in this study. Humans underline the protocols' unique methods and their adaptability to use in diverse IoT scenarios throughout the whole research. We also discuss the difficulties, benefits, and drawbacks of various communications technologies in the context of the Internet of Things [6].

The major issues facing the Internet of Things are privacy and security (IoT). IoT is confronting several difficulties, including incorrect device updates, a lack of effective and reliable security mechanisms, user ignorance, and well-known active device monitoring. We examine the history of IoT systems and security measures in this work, identifying various security and privacy concerns, methods used to secure the elements of IoT-based surroundings and systems, appropriate security solutions, and the best privacy modeling techniques required and suitable for various layers of IoT-driven applications. In this study, we suggested a novel IoT layered model that is stretched and general with layers of identification and privacy and security characteristics. Implementation and evaluation of the suggested IoT system with cloud and edge support. The IoT nodes created by Amazon Web Service (AWS) as virtual machines are the bottom layer. The middle layer's (edge) implementation used the Green Grass Edge Environment on AWS together with a Raspberry Pi 4 hardware kit. To construct the top layer, we used the cloud-enabled IoT ecosystem in AWS (the cloud). Between each of these levels, there were security procedures and crucial management sessions to guarantee the confidentiality of the users' information. To facilitate data flow across the levels of the suggested cloud/edge-enabled IoT paradigm, we built security certificates. The suggested system architecture not only eliminates potential security flaws, but it can also be utilised in conjunction with the best security measures to mitigate the cybersecurity risks that each of the three layers of cloud, edge, and IoT faces [7].

The IoT protocols enable a variety of features to accomplish the quick, dependable, and secure implementation of any IoT system. They may be thought of as the manifestation of various IoT architectural layers in use. This chapter examines the five-layer IoT architecture and the mapping of various IoT protocol types to the five-layer IoT architecture for the sake of simplicity and comprehensive knowledge. It describes the fundamental characteristics and features of a few IoT protocols that fall under several categories. Physical Layer Protocols, Link Layer Protocols, and Network/Routing Layer Protocols are three sub-layers into which the IoT protocols may be divided. Several well-known Physical Layer protocols are advanced. On the other hand, protocols that integrated both Physical and Link layer features include IEEE 802.15.4, IEEE 802.11ah, BLE, and ZigBee.

Internet technology is always evolving, which has made. The internet of things (IoT) will be the focus of several computer engineering research areas. First, the review paper provides a short overview of the alternative protocols preceding discussing the selection of an application layer protocol in an IoT system integration. The debate is then launched starting comparing various protocols' overhead and message management strategies, which have an impact on traffic management. This study's major contribution focuses only on IoT applications by simplifying comparisons across session layer protocols. Platforms and standards for the Internet of Things are continually being upgraded. IoT makes it possible for devices used in applications like healthcare, smart homes, and advanced robotics to link and coordinate their actions. Several

protocols have been explored to provide efficient communication for devices with constrained resources. However, there is more study to be conducted in this area to determine the best procedure to use in certain scenarios. In addition to demonstrating the graphical and tabular compression, the study compiles the findings of prior studies that examined application-layer protocols in the IoT context experimentally.

DISCUSSION

The phrase "IoT" is increasingly widely used. This paper will examine what it is, how it works, and how it makes life easier in general. Starting, let's define the Internet of Things. A group of interconnected electronic devices known as the "Internet of Things" may communicate with one another online (IoT). IoT may be characterised in a variety of ways, but at its core, this technology allows us to control several electrical devices from a single device over the Internet. In this situation, the electronic devices used with IoT technology have to include sensors that enable them to recognise electrical impulses and modify their operations appropriately. The identified data was also sent to the other device through the Internet. IoT will make daily life incredibly simple and accurate. Today, this technological industry offers a tonne of job opportunities, and various developments are underway. IoT items with internet connectivity include smart speakers, smart TVs, smart watches, smart speakers, and Google Home and Amazon Alexa gadgets. IoT networking protocols are required for communication to take place between the various IoT system components. The IoT networking protocols will thus need to perform several tasks. They enable simultaneous communication between an IoT of different devices[8].

Messages must be efficiently transported between devices with various requirements sensors and actuators, but also data processing and storage devices. In theory, they inhibit coupling between devices, making it impossible for them to be dependent on one another. Additionally, they provide scalability by enabling the addition or removal of devices from the IoT ecosystem without impacting the deployment as a whole. Ensuring communications security in exposed contexts, such as industrial IoT, is a further consideration. As a result, the device level of cybersecurity must also be addressed. Whether there are barriers like latency or firewall problems, the network protocols make it simple for devices to connect. The Internet of Things (IoT) includes wirelessly connected industrial machinery, personal gadgets, and sensors. Since there are so many different use cases, settings, and industries, no one solution stands out.

Since there are several standards targeted at various markets and using various communication protocols, this situation is often complicated, making it difficult to choose the best technology for an IoT application. IoT devices are often linked to the Internet over an IP network regularly. This cannot be done, however, with systems that use battery-operated, distant, and resource-constrained devices.

CONCLUSION

Every connected item in the Internet of Things (IoT) transmits packets of data, which need dependable connection, storage, and security. An organization's ability to manage, monitor, and secure enormous amounts of data and communications from scattered devices is challenged by IoT. But in a cloud-based setting, this problem need not be a barrier. Cloud computing allows IoT solutions to expand internationally and across several physical locations while cutting communication latency and allowing for faster response from devices in the field. This is in addition to scaling and extending a solution in one place. In addition to services to run and

protect endpoints, gateways, platforms, and applications as well as the traffic moving across these levels, AWS now provides a full range of IoT services with comprehensive security. This integration makes it easier to utilize and manage securely interconnected devices and data, enabling businesses to take advantage of IoT's creativity and efficiency while still prioritizing security. With a variety of security services, AWS gives companies a defense in depth strategy as well as a simpler, quicker, and more inexpensive route to complete, continuous, and scalable IoT security, compliance, and governance solutions.

REFERENCES

[1] S. H. Rahaman and S. Biswas, "Advantages of Internet of Things (IoT) and It's Applications in Smart Agriculture System," *Int. Res. J. Adv. Sci. Hub*, 2020, doi: 10.47392/irjash.2020.181.

[2] A. Zhang and R. V. P. Kandubai, "Access control schema for smart locks using a wifi bridge: An exploration of a smart lock access control system based around the SimSim retrofitting smart lock," in *ACM International Conference Proceeding Series*, 2020. doi: 10.1145/3449301.3449331.

[3] K. Kabilan, N. Bhalaji, C. Selvaraj, M. Kumaar B, and K. P T R, "Performance analysis of IoT protocol under different mobility models," *Comput. Electr. Eng.*, vol. 72, pp. 154–168, Nov. 2018, doi: 10.1016/j.compeleceng.2018.09.007.

[4] M. Mahmoodpour, A. Lobov, and M. Lanz, "Configurator module to integrate different protocols for IoT solution," in *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, IEEE, Jul. 2018, pp. 67–73. doi: 10.1109/INDIN.2018.8471983.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[6] E. Al-Masri *et al.*, "Investigating Messaging Protocols for the Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 94880–94911, 2020, doi: 10.1109/ACCESS.2020.2993363.

[7] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, Jun. 2020, doi: 10.3390/app10124102.

[8] S. J. Shackelford, "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk," *Chapman Law Rev.*, 2016.

CHAPTER 11

AN ELABORATION OF INTERNET OF THINGS ARCHITECTURE FOR CYBER SECURITY

Mrs. Sowmya C S, Assistant Professor
Department of Electronics and Communication Engineering, Presidency University, Bengaluru, India
Email Id- sowmya.cs@presidencyuniversity.in

ABSTRACT

The term "Internet of Objects" (IoT) refers to a broadly dispersed network of things in which all data is sent to the internet via Radio Frequency Identification (RFID) tags and sensing devices. Since IoT does not need any feeling of connectedness and seems to be one of the biggest waves of revolutionary, security is required. However, the difficulties related to the safety of things have expanded along with the IoT's fast growth. This chapter focuses mostly on the idea of IoT, architecture, and security challenges with proposed solutions and suggested other investigation fields.

KEYWORDS: Cyber Security, Data Sensor, IoT, Information Security, Sensor Node.

INTRODUCTION

Many IoT attacks have used actuators, such as printers, as launch points into a business's network. An IoT security architecture is a blueprint that illustrates all components of the IoT infrastructure for all IoT projects and details how to secure each component.

Security Architecture for IoT Solutions

When you design and architect an IoT solution, it's important to understand the potential threats and include appropriate defenses. Understanding how an attacker might compromise a system helps you to make sure that the appropriate mitigations are in place from the start [1].

Security in IoT

It's helpful to divide your IoT architecture into several zones as part of the threat modeling exercise:

A. Device
B. Field gateway
C. Cloud gateway
D. Service

Each zone often has its own data and authentication and authorization requirements. You can also use zones to isolate damage and restrict the impact of low trust zones on higher trust zones.

Each zone is separated by a *trust boundary,* shown as the dotted red line in the following Figure 1. It represents a transition of data from one source to another. During this transition, the data could be subject to the following threats:

A. Spoofing
B. Tampering
C. Repudiation
D. Information disclosure
E. Denial of service
F. Elevation of privilege

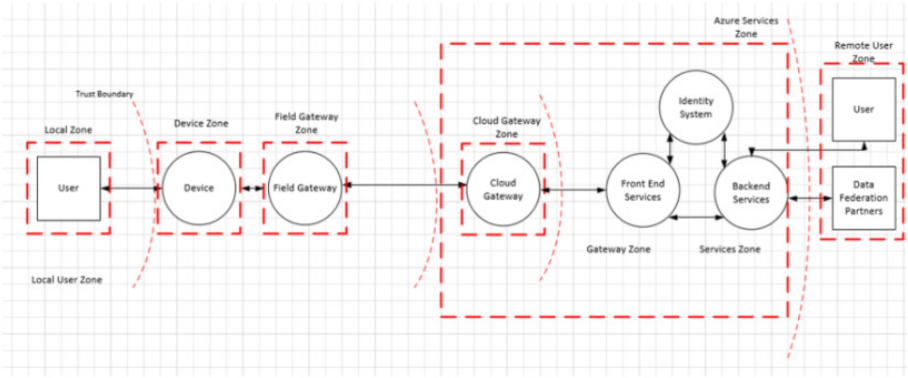


Figure 1: Represented the Architecture of IoT.

You can use STRIDE to model the threats to each component within each zone. The following sections elaborate on each of the components and specific security concerns and solutions that should be put into place. The remainder of this paper discusses the threats and mitigations for these zones and components in more detail. As you explore the interaction patterns, look at *device control* and *device data* with the same level of attention. Device control refers to any information provided to a device to modify its behavior. Device data refers to information that a device emits to any other party about its state and the observed state of its environment[2], [3].

Threat modeling for the Azure IoT Reference Architecture

This section uses the Azure IoT reference architecture to demonstrate how to think about threat modelling for IoT and how to address the threats identified as identified in Figure 2:

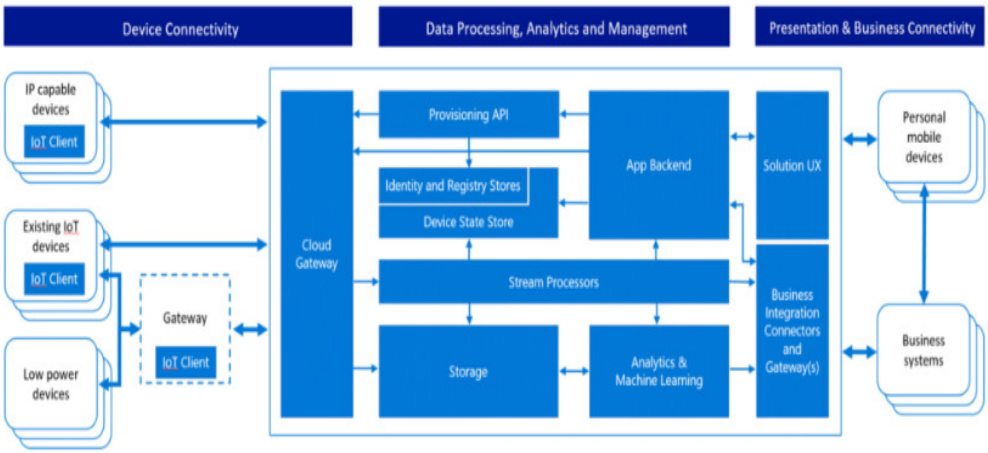


Figure 2: Represented the Azure IoT Reference Architecture.

The following diagram provides a simplified view of the reference architecture by using a data flow diagram model: The architecture separates the device and field gateway capabilities. This approach enables you to use more secure field gateway devices. Field gateway devices can communicate with the cloud gateway using secure protocols, which typically require greater processing power than a simple device, such as a thermostat, could provide on its own. In the Azure Services Zone in the diagram, the Azure IoT Hub service is the cloud gateway.Based on the architecture outlined previously, the following sections show some threat modelling examples [4]. The examples focus on the core elements of a threat model:

A. Processes
B. Communication
C. Storage

Processes

Here are some examples of threats in the processes category. The threats are categorized based on the STRIDE model:

i. Spoofing

An attacker may extract cryptographic keys from a device, either at the software or hardware level. The attacker then uses these keys to access the system from a different physical or virtual device by using the identity of the original device.

ii. Denial of Service

A device can be rendered incapable of functioning or communicating by interfering with radio frequencies or cutting wires. For example, a surveillance camera that had its power or network connection intentionally knocked out can't report data, at all.

iii. Tampering

An attacker may partially or wholly replace the software on the device. If the device's cryptographic keys are available to the attacker’s code, it can then use the identity of the device.

iv. Tampering

A surveillance camera that's showing a visible-spectrum picture of an empty hallway could be aimed at a photograph of such a hallway. A smoke or fire sensor could be reporting someone holding a lighter under it. In either case, the device may be technically fully trustworthy towards the system, but it reports manipulated information.

v. Tampering

An attacker may use extracted cryptographic keys to intercept and suppress data sent from the device and replace it with false data that are authenticated with the stolen keys.

vi. Information Disclosure

If the device is running manipulated software, such manipulated software could potentially leak data to unauthorized parties.

vii. Information Disclosure

An attacker may use extracted cryptographic keys to inject code into the communication path between the device and the field gateway or cloud gateway to siphon off information.

viii. Denial of Service

The device can be turned off or turned into a mode where communication isn't possible which is intentional in many industrial machines.

ix. Tampering

The device can be reconfigured to operate in a state unknown to the control system outside of known calibration parameters and thus provide data that can be misinterpreted

x. Elevation of Privilege

A device that does a specific function can be forced to do something else. For example, a valve that is programmed to open half way can be tricked to open all the way.

xi. Spoofing/Tampering/Repudiation

If not secured which is rarely the case with consumer remote controls, an attacker can manipulate the state of a device anonymously. A good illustration is a remote control that can turn off any TV.

The following Table 1, shows example mitigations to these threats. The values in the threat column are abbreviations:

A. Spoofing (S)
B. Tampering (T)
C. Repudiation (R)
D. Information disclosure (I)
E. Denial of service (D)
F. Elevation of privilege (E)

Table 1: Represented the Mitigation Threats.

Component	Threat	Mitigation	Risk	Implementation
Device Cloud Gateway	TID	TLS (PSK/RSA) to encrypt the traffic.	Eavesdropping or interfering with the communication between the device and the gateway	Security on the protocol level (MQTT/AMQP/HTTP/CoAP). With custom protocols, you need to figure out how to protect them.
External Entity	TID	Strong pairing of the external	Eavesdropping the connection to the device.	Securely pairing the external entity to the device NFC/Bluetooth LE.

Device		entity to the device	Interfering the communication with the device	Controlling the operational panel of the device (Physical)
Device to Device	TID	(D)TLS (PSK/RSA) to encrypt the traffic.	Reading data in transit between devices. Tampering with the data. Overloading the device with new connections	Security on the protocol level (MQTT/AMQP/HTTP/CoAP. With custom protocols, you need to figure out how to protect them. The mitigation for the DoS threat is to peer devices through a cloud or field gateway and have them only act as clients towards the network. The peering may result in a direct connection between the peers after having been brokered by the gateway
Device IoT Hub	TID	(D)TLS (PSK/RSA) to encrypt the traffic	Eavesdropping or interfering the communication between the device and the gateway	Security on the protocol level. With custom protocols, you need to figure out how to protect them. In most cases, the communication takes place from the device to the IoT Hub (device initiates the connection).
Field Gateway Cloud Gateway	TID	TLS (PSK/RSA) to encrypt the traffic.	Eavesdropping or interfering the communication between the device and the gateway	Security on the protocol level (MQTT/AMQP/HTTP/CoAP). With custom protocols, you need to figure out how to protect them.

Communication

Here are some examples of threats in the communication category. The threats are categorized based on the STRIDE model:

i. **Denial of Service**

Constrained devices are generally under DoS threat when they actively listen for inbound connections or unsolicited datagrams on a network. An attacker can open many connections in parallel and either not service them or service them slowly, or flood the device with unsolicited traffic. In both cases, the device can effectively be rendered inoperable on the network.

ii. Spoofing, Information Disclosure

Constrained devices and special-purpose devices often have one-for-all security facilities such as password or PIN protection. Sometimes they wholly rely on trusting the network, and grant access to information to any device is on the same network. If the network is protected by a shared key that gets disclosed, an attacker could control the device or observe the data it transmits.

iii. Spoofing

An attacker may intercept or partially override the broadcast and spoof the originator.

iv. Tampering

An attacker may intercept or partially override the broadcast and send false information.

v. Information Disclosure

An attacker may eavesdrop on a broadcast and obtain information without authorization.

vi. Denial of Service

An attacker may jam the broadcast signal and deny information distribution.

Storage

The following Table 2, shows example mitigations to the storage threats:

Table 2: Represented that the Mitigations to the Storage Threats.

Component	Threat	Mitigation	Risk	Implementation
Field Gateway OS image	TRID		Tampering with OS /replacing the OS components	Read-only OS partition, signed OS image, Encryption
Field Gateway storage (queuing the data)	TRID	Storage encryption, signing the logs	Reading data from the storage, tampering with telemetry data, tampering with queued or cached command	BitLocker

			control data. Tampering with configuration or firmware update packages (destined for devices or field gateway) while cached or queued locally can lead to OS and/or system components being compromised	
Device OS image	TRID		Tampering with OS /replacing the OS components	Read-only OS partition, signed OS image, encryption
Device storage	TRID	Storage encryption, signing the logs	Reading data from the storage, tampering with telemetry data. Tampering with queued or cached command control data. Tampering with configuration or firmware update packages while cached or queued locally can lead to OS and/or system components being compromised	Encryption, message authentication code (MAC), or digital signature. Where possible, strong access control through resource access control lists (ACLs) or permissions.

The adoption and deployment of the "Internet of Things (IoT)" for remotely monitoring and managing specialized instruments from the outside world, architectural changes are occurring in contemporary companies. The industrial automation techniques in smart industries are the primary context in which IoT technology makes the most sense (Industry 4.0). The Industrial IoT (IIoT) environment is offered with a trustworthy "Next Generation Cyber Security Architecture (NCSA)" in this study that can recognize and stop cybersecurity threats and vulnerabilities. The methods of sending crucial real-time information between equipment without human involvement are enhanced by automation. It suggests an analytical methodology that may be used to safeguard the network traffic and the entities concerned in wireless IIoT communication. When a network session has been created, it includes an automated cyber-defense authentication system that identifies and stops security assaults. The defensive technique creates an identity token that is cryptographically encrypted and authenticated by a virtual gateway system to achieve the requisite degree of cybersecurity in the network. The suggested NCSA lowers operational management expenses simultaneously enhancing security in the IIoT environment [5].

Internet of Things" (IoT) refers to a network foundation comprising distinguishable objects that interchange data online. One use case for something like the Internet of Things is a smart house. Home appliances might be monitored and managed remotely in a connected home. For IoT systems, this increases the need for trustworthy information security. The difficult IoT security procedures of authorization and authorization must be taken into account. For instance, illegal access to a home's smart home system, such as cyberattacks, may be dangerous by activating sensors and actuators, which could then allow a thief access. To prevent unwanted access, this study employs multi-factor registration as an additional layer of protection. One of them is facial recognition, which has lately gained popularity attributable to its non-intrusive identification techniques and ease of use with cameras linked to the majority of popular smartphones and laptops. The shortcomings of internet And mobile phone smart home systems have been examined in this paper, and we provide proposals on how to make them better by adding the essential system modules and increasing user registration and log-in authentication. We provide an agile methodology for putting such a system into practice. To the best of our knowledge, the proposed software architectures that IoT smart home administration does not include facial recognition and primarily detection as part of the authentication procedure [6].

The Internet of Things has reached the industry. Allowing connectivity from production plants to the Internet requires appropriate security mechanisms to protect against cyber attackers. In this paper, we propose a security architecture for a gateway connecting sensors and automation components from assembly lines with Internet or cloud-based systems. A Trusted Platform Module (TPM) is used for protecting the cryptographic keys used in secure communication protocols and to protect against illegitimate firmware manipulation. As proof of concept, we implemented the key protection functionality with a TPM for the Open Platform Communications Unified Architecture protocol. In a field test, gateways have been installed together with wireless sensors in production plants. Two significant results concerning the sustainability objectives of secure remote production, namely, reduction of chemical waste and reduction of electrical energy consumption have been demonstrated.

Industrial Automation and Control Systems (IACS) have previously been largely cut off from traditional digital networks like business ICT settings. A zoned design was employed when interconnection was necessary, and firewalls or heavily militarized zones were deployed to

safeguard the main parts of the management system. IACS is undergoing architectural changes as a result of the acceptance and application of "Internet of Things" (IoT) technologies, including increased connection to industrial systems. This essay examines the description of Industrial IoT (IIoT) and its connections to ideas like cyber-physical systems and Industry 4.0. In this work, an IIoT definition is proposed, and associated partial IoT taxonomies are analyzed. It provides a framework for IIoT analysis that may be used to characterize and list IIoT devices while investigating system designs and security risks. The paper's conclusion outlines certain gaps in the existing body of knowledge [7].

Several application domains, the Internet of Things (IoT) is bringing about a trans-disciplinary revolution. But security and privacy issues are impeding a wide-scale deployment of IoT-enabled infrastructure that is dependable and robust (IoT-CIs). This study offers a complete architectural architecture that addresses the primary security and privacy issues associated with IoT-CIs and cyber-physical systems to close this gap. Through the use of cutting-edge technologies like software-defined communications and network function virtualization, the architecture is designed to give IoT systems and networks the ability to make autonomous security decisions. It also equips them with the capability of reacting intelligently and procedurally to security threats by relying on monitoring techniques and cyber-situational tools [8].

The most important uses for the Internet of Things is the smart grid (IoT). The advancement of smart grid cyber-physical systems (CPS) goes hand in hand with the development and use of information and communications technologies (ICT) in conventional power systems. Smart grid systems powered by IoT are crucial infrastructures that feature beautiful designs and crucial components. They contain communication systems that, should the secrecy, and availability of the communication be undermined, might result in gaps in national security, disturbances of the peace, fatalities, or significant financial harm. These massive systems might be subject to cyber-attacks. As a result, there is a lot of research being done in business, government, and academia to improve smart grid security. To increase protection against cyber-attacks in smart meters, security strategies are crucial. We give an extensive survey that is backed up by an extensive evaluation of prior studies. Furthermore, latest developments and capabilities in cyber security for smart grids are highlighted. The risks and possible remedies associated with an IoT-based smart grid are investigated in this study. We provide a thorough analysis of the smart grid's cyber-security condition while concentrating on various types of cyber-attacks. We specifically focus on the investigation and debate of network vulnerabilities, attack countermeasures, and security needs [9].

The Blockchain and the Internet of Things are regarded as two important technologies. IoT applications may be executed remotely with more flexibility thanks to lower latency and a larger connected system number. IoT devices often lack the processing power and storage space necessary to enable strong security and encryption techniques. The Internet of Things is struggling with several issues, including inadequate interoperability, security flaws, privacy concerns, and a lack of industry standards. IoT cyber-attacks may affect the security and privacy of the energy trading industry. To offer decentralization and authentication, this paper provides a mechanism for adding a fundamental interface to the security gateway architecture of an Internet of Things device. It improves the IoT infrastructure's lack of present anonymity and adaptability. Applying suitable cryptographic techniques to the data before sending it to distant services improves the dependability of the data delivered to such services.

The Industrial Internet of Things (IIoT) has emerged as a key area of research and development that has the opportunity to enhance the productivity of real-time data gathering, recording, analysis, and administration of all machine activity, as well as likely to engender quality and lower costs. Traditional IIoT relies on centralized systems that may be attacked via isolated failure points and other types of cyberattacks. To transform traditional structures into autonomous ones, blockchain technology has evolved. Cryptographic protocols are used in contemporary industrial settings because they may provide high levels of security, minimal processing complexity, P2P communication, transparent logging, and democratization. The current study suggests using a permissioned blockchain mechanism for an industrial application in a cement plant. This mechanism provides low consumption, scalability, and a lightweight security scheme; it can also efficiently control access to vital data produced by sensors and actuators. Due to its effectiveness in processing cryptographic algorithms, a low-power ARM Cortex-M processor is used, which means quicker computational performance of the suggested design. Additionally, our blockchain network employs proof of authentication (PoAh) as a consensus method in place of proof of work (PoW) to guarantee safe authentication, scalability, speed, and energy efficiency. Our test findings demonstrate that perhaps the suggested framework delivers excellent performance, high levels of security, and scalability across smart industrial systems. Additionally, we were able to effectively integrate blockchain technology with the industrial internet of things devices, giving these devices access to blockchain technology's capabilities and effective prevention against typical cyber-security threats.

DISCUSSION

We are all aware that the Internet of Things is a technology that is essential to the development of technology in our contemporary society. To simplify the IoT architecture, it has been broken into many layers that work together to create a vast, linked network where every device is in some way or another connected to every other device. This gives us a better grasp of how the Internet of Things operates and all of its terminology, but even with all these advantages, security is a crucial component of the IoT that shouldn't be disregarded. This paper outlines several security concerns that affect the IoT architecture and are prevalent at every tier. The paper also highlighted a few security standards and procedures that may be used at different levels and how they improve security at different layers. We can therefore conclude that IoT is serving our purpose in creating a smart environment for the advancement of our civilization as we enter the next generation of technology, but to make the best use of this technology for our advancement, the security flaws present in IoT layers must also be given a high priority.

CONCLUSION

End-to-end security mechanisms for wireless networks and the internet of things have received a lot of attention recently. A massage is supported from the point of origin to the point of destination via an end-to-end security protocol. The sender nodes don't need any further encryption processes since routing information is delivered in a plain manner because this sort of protocol is utilised at the network layer or application layer. On the other side, it implies that connecting layer protocols for end-to-end security cannot sustain a network's accessibility. The difficulties surrounding new models that have been proposed for the internet of things' security architecture have been examined in the current paper. Analyzing the investigated methods reveals that each of them has specific traits that boost resistance to particular assaults. Finally, adopting them maintains network performance and sustainability while supplying security.

REFERENCES

[1] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Res.*, 2016, doi: 10.1108/IntR-07-2014-0173.

[2] S. J. Shackelford, "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk," *Chapman Law Rev.*, 2016.

[3] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. 2016. doi: 10.1201/b10867.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2017.2683200.

[5] C. Vijayakumaran, B. Muthusenthil, and B. Manickavasagam, "A reliable next generation cyber security architecture for industrial internet of things environment," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, p. 387, Feb. 2020, doi: 10.11591/ijece.v10i1.pp387-395.

[6] R. F. Al-Mutawa and F. Albouraey, "A Smart Home System based on Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, 2020, doi: 10.14569/IJACSA.2020.0110234.

[7] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018, doi: 10.1016/j.compind.2018.04.015.

[8] A. Molina Zarca *et al.*, "Security Management Architecture for NFV/SDN-Aware IoT Systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8005–8020, Oct. 2019, doi: 10.1109/JIOT.2019.2904123.

[9] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Networks*, vol. 169, p. 107094, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.

CHAPTER 12
AN ELABORATION OF MIDDLEWARE PLATFORM OF WEB OF THINGS

Dr. Rajbhadur Singh, Assistant Professor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id- rajbhadurs.soeit@sanskriti.edu.in

ABSTRACT

Through the development of Web-based guidelines and technology, the Web of Objects is an active research area that attempts to promote the simple access and administration of smart things' digital representations. It has been acknowledged that although tremendous study has gone into lower-level networks and software technologies, modelling and implementing products for the Web of Things has received less consideration. We talk about the framework's conformity to the REST principles and the critical development options. Finally, we provide us with a report on the test activities we implemented as part of the Smart Santander European Project to determine the effectiveness of our infrastructure in real-world applications of smart cities.

KEYWORDS: Internet of Things, Network, Platform, Software, Web.

INTRODUCTION

Embedded technology and wireless network have developed so much that computing has become more ubiquitous. Many applications have been developed for people to require data from devices like sensors and cameras. This trend has driven the development of the Internet of Things (IoT) which makes things accessible through the internet. In the IoT, different manufactures and operators develop their systems, which makes data sharing and collaboration difficult. As a result, the concept of the Web of Things has been proposed to abstract things into web resources. However, current WoT solutions focus more on up-layer research by adapting existing web technology to the WoT scenarios [1].

In fact, in the Smart BUPT system we implement earlier, we find that there are still some practical issues when implementing the concept. For example, a large number of things are legacy devices, which possess constrained capabilities compared with traditional web servers. In addition, it is necessary to manage the status of running resources after the resource discovery process. To tackle these problems, we propose a middleware-based network architecture for the web of things which can be applied to deploy devices on large scale. In addition, we have realized the practical problems and considered them in the designation. The rest of the paper is organized as follows: Chapter II presents the challenges when implementing the WoT. Chapter III introduces the architecture and solutions to practical problems [2].

To facilitate the deployment and integration of a large number of things, standard solutions like WSDL and WADL have been proposed to reduce the cost of connecting and interoperating. However, such standard protocols are usually applied to traditional web resources that are hosted on servers with strong capabilities. In contrast, resources are hosted on constrained devices like sensors and actuators in the web of things. It would be difficult to implement complex protocols directly on them. Meanwhile, things in the WoT are highly dynamic and unstable due to their physical attributes [3].

i. Device Accessibility

In the process to integrate things into the WoT, the primary task is to make various devices accessible. Many types of researchon the Internet of Things ignore a practical problem that many legacy devices do not process basic communication and computing capabilities. It would be necessary to extend these capabilities to legacy devices. In addition, it is also essential to reduce the use expense with a uniform access interface. This would require the translation from a specified data format to a uniform one. Fortunately, solutions like EEML [4] and SensorML [5] have provided us with references. However, it is still necessary to make some adaptions to meet the WoT requirements. Besides, the accessible device also has to provide stable data sources. Influenced by the physical attributes, resources in the WoT cannot be as stable as a traditional web resource. Such instability includes Mobility: the access address of resources may change when hosting devices move about; Reachability: the hosting device may be located in a local network and cannot be reached directly from a public network; Resource constraint: the performance of resources can be influenced by limited power or bad network condition. Many solutions like Reverse [6], Mobile IP [7] and dynamic DNS have been proposed to tackle such problems.

ii. Resource Exposition

Compared with the Internet of Things, the WoT concentrate more on the explosion of the resource. Several web protocols such as SOAP and Restful Web Service can be used for exposition, mashup and integration of things. To support such protocols, the things have to process the capabilities to deploy embed servers themselves. It is rather difficult for many legacy devices. Some systems like cosm propose to collect the data to a central repository and then expose them. However, such a method will increase the delay in acquiring real-time data. In addition, storing the data in a remote location also results in security problems. Another challenge that the WoT has to deal with is resource search. On one hand, a search service should be provided to the users to filter the resources matching requirements. On the other hand, the access address of resources should also be provided. Considering the dynamic character of WoT resources, it is essential to maintain the availability of the resource.

iii. Life Cycle Management of Resource

In the WoT, maintaining the status of resources is quite important. The status can be changed as hosting devices join, move and leave. Firstly, the process of device joining is supposed to include device discovery and registration. Some existing research like UPnP, JiNi have focused on this process. Other propositions like HTTP compression also provide a reference in the WoT context. However, in some application scenarios, we find that such protocols are too complex for implementation and a lighter protocol is more suitable. Secondly, the running status of resources is supposed to be monitored after devices have joined. Status like normal, suspended and left should be maintained according to different situations. To deal with such problems, we propose a middleware-based network architecture for the web of things. We also implement the architecture in a SMART HOME system for demonstration. It is detailed in the following sections.

Use Cases

Deep Integration

In this use case, an integrated and holistic view of a factory is established to improve decision-making across different departments and to reduce overall complexity. This includes the interlinking of diverse data sources such as sensor measurements for example, temperature, vibration, pressure, and power, the manufacturing execution system for example, work orders, material needed for production, incoming material number, business processes, workforce, and so on. Although much of this data is already captured by IT systems, it remains largely inaccessible in an integrated way without investing the significant manual effort. Thus, the objective of this use case is to make all data available in a unified model to support the user's factory planners, machinists, controllers, field technicians, and so forth in decision-making. For example, consider the following scenarios:

A. A factory planner needs input from diverse sources regarding order plans, machine maintenance schedules, workforce availability, and so on.

B. A field technician must quickly troubleshoot an onsite industrial asset, and is seeking a solution that combines a summary of the problem, including difficulty and time estimates; links to relevant manuals and necessary parts; additional physical tools to resolve the problems and the current location of these tools; and, if the problem is difficult to resolve, additional support from people with the necessary expertise.

C. During production, a machinist needs to know which tools are required to perform the task at hand, the location of these tools and materials, and the quality control standards to have adhered to.

Horizontal Integration

This use case extends the vertical integration of all factory operations into the horizontal dimension, knitting together the relevant players in a manufacturing supply chain the raw materials and parts suppliers, logistics, inventory of supplied goods, production process, warehouses and distributors of finished products, sales and marketing, customers through an interconnected networks of Internet of Things (IoT) devices and external information sources such as social media and web services, overseen via an overarching semantic-enabled engine. Some examples include the following:

A. A smart factory manager wants to optimize the supply chain and warehouse facilities to ensure that the right amount of raw material is always available in the warehouse to support production processes. Because the factory produces customized products, allowing customers to choose their food products' ingredients, it is difficult to estimate the amount and type of raw material required to fulfil customer orders. However, efficient data-mining and machine-learning techniques that harness social media data can provide insights into ongoing trends and customer preferences, which will help the warehouse manager optimize the supply chain and ensure that the right amount of raw ingredients are always available in the warehouse to replenish the processing machine at the food production factory.

B. A production manager in a manufacturing unit needs an integrated view of the supply chain, including raw materials and the distribution network, to optimize internal manufacturing processes. A horizontal integration of smart factory production processes,

supply, and the distribution network including fleet management data and external datasets such as traffic congestion, weather, and social media is required to build an optimal strategy for the production of perishable food products. Using this integrated information, the production manager can adapt internal business processes on the fly.

Autonomous System

This class of use cases deals with enabling factory devices to cooperate to achieve the factory's overall objectives and the following are just a few examples:

A. Self-organization:

When a production order comes down to the factory, machines can communicate and exchange information with one another to organize resources to complete the orders on time. Resource allocation is determined at runtime, rather than pre-allocated, depending on the machines' current conditions, including the current factory workload at the factory, machine availability and maintenance schedule time, backlog of customer orders, and machine capacity. Moreover, resource allocation could consider external electricity rates data to achieve the goal of reducing the factor's energy consumption and carbon footprint.

B. Flexible manufacturing:

Decentralized control is very useful when the market demands lead to the introduction of new machines in factories. The new machines can participate by simply announcing their services and features during the resource allocation process. This illustrates the flexibility and adaptability of a factory, where new machines can be integrated into a plug-and-produce fashion according to market demands with minimal downtime.

C. Fault tolerance

The highly dynamic and self-organization features result in a fault-tolerant system faulty sensors can be replaced by discovering new sensors with similar functionality to prevent downtime during the production process.

Service Composition and Business Process Management Middleware

The Service Composition and Business Process Management (SC-BPM) middleware will be responsible for composing services and managing business processes. Initiatives have emerged for supporting business process modeling such as Business Process Modeling Notation (BPMN) and Web Services Business Process Execution Language (WS-BPEL). We chose WS-BPEL as a reference to describe the SC-BPM.

i. BPM Engine

Business Processes are described and modelled in BPEL and stored as XML documents. The BPM engine can create an instance of the process according to the BPEL document and execute the workflow after it has been initialized. During the runtime of the process, the BPM engine will manage and store the state information and the control information in persistent storage. The BPEL engine will execute the business process invoking the web services according to the business logic defined by the BPEL program.

ii. Service Binding and Invoking

When the business process begins execution, the BPM engine will bind and invoke the needed web services. Within GaaS's scope, the devices are exposed as RESTful web services via gateways, so an HTTP binding is processed in the WS-Adaptor.

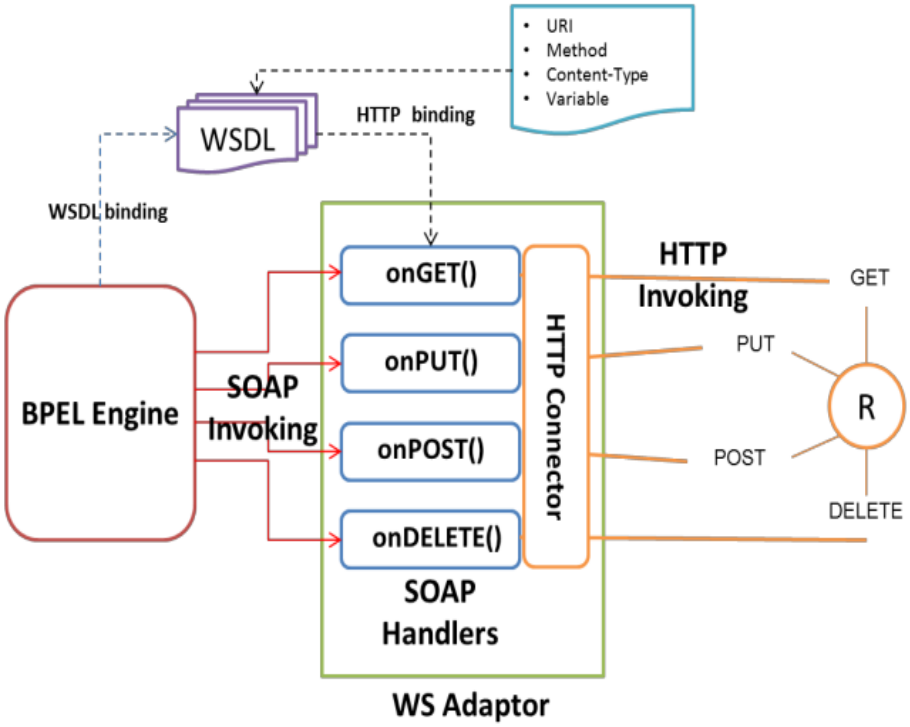


Figure 1: Represented the GaaS's scope Structure.

If the BPM engine prepares to invoke a RESTful web service inside its workflow, it will bind to the specified WSDL file to check which SOAP web service handler to invoke with URI, representation and other attribute parameters. Then the engine will invoke the handler in SOAP message, and the handler will invoke the RESTful web service on the gateway by binding the request to an HTTP request with URI, method, content-type and the parameter. The gateway will respond to the adaptor in HTTP with representations, and the adaptor will transfer the data into POX and respond to the BPEL engine with SOAP message. Figure 2 illustrates the process of a service binding and invoking.

iii. Eventing

This component is an implementation of the WS-Brokered Notification standard, implementing publish and subscribe functionality, to distribute information about events of interest. Both push and pull type delivery are supported and both involve the role of "Consumer" and "Producer". The Evening component acts as an intermediary between a Producer and the entity that has an interest in the generated events. For example, a heart-rate detection device could propagate sensor data via WoT Gateway through the Evening component acting as a Producer and some third-party application could subscribe to this event as a Consumer to monitor the heartrate of an elderly person.

Gateway as a Service (GaaS)

The basic idea of designing the architecture of GaaS is to map the three-layered cloud computing stack into GaaS as presented in Figure 1. WoT Infrastructure layer is a mapping from IaaS which provides basic IoT infrastructure, such as the embedded devices and web gateways. The web gateway is the core which will bridge different types of sensors, actuators and other devices into the Internet. All data and capabilities of the devices are abstracted as web resources and are opened with web services APIs. We assume that the devices are provided and shared by individuals and device manufacturers, and all these devices connect to the GaaS via a web gateway. We assume also that the web gateways are mainly provided by the GaaS providers or operators and are partly shared by third parties for large-scale and scalable deployment. As the first layer of GaaS, WoT infrastructure layer focuses mainly on the boundary between the physical and digital realm.

The service and Business Operation layer is a mapping from PaaS which provides service composition and business process management middleware. The Business Process Management System (BPMS) is the core that will manage the business process execution. The web services from distributed gateway can be composed with other services and they will provide data from devices to be integrated into business processes by BPM engine. As the second layer, the Service and Business Operation layer focuses mainly on the boundary between digital resources and business services.

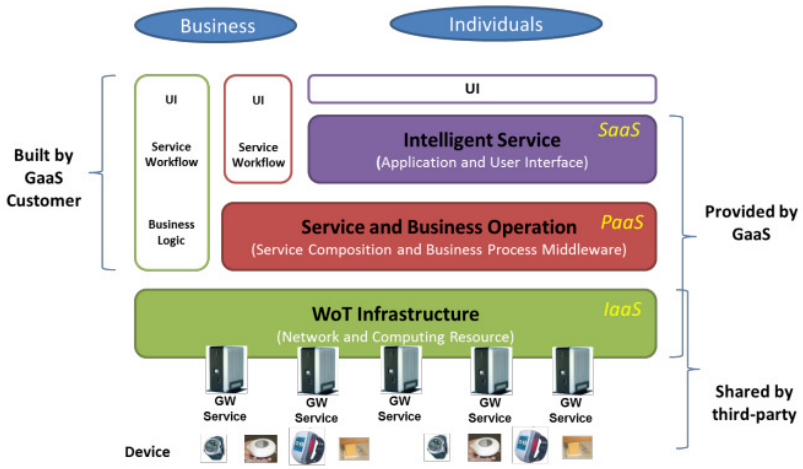


Figure 2: Represented the Concepts pf GaaS.

The intelligent Services layer is a mapping from SaaS which provides a collection of intelligent applications and user interfaces for end users. End users can directly access the services on their own demand by payment. Additionally, the services can also be provided separately by a third-party. As the top layer of GaaS, the Intelligent Service layer focuses mainly on the boundary between delivered applications and end users. Based on the GaaS concept, GaaS customers can consume services and build their own software at different levels. For example, the business customers, such as SMEs can build their own IT-based business platform, including business logic, service workflow and UI, based on the first and second layer of GaaS. Then they can provide their own customized service to their own end-users. On the other hand, individual developers can build their own applications, mainly UI programs, on their demands based on the second layer with easy-to-use programmable APIs. Then it is much easier for them to create smashup applications.

LITERATURE REVIEW

R. Sardar and T. Hanees illustrated that the Web of Things is a more advanced and promising architecture for the Internet of Things that enables smart objects to interface not only with the Web but also with the Internet. To be included in the World Wide Web, it enables users to exchange and produce information as well as provide capabilities for data aggregation and analysis over a network. Despite these developments, it has revealed several security issues that must be resolved for WOT to be successfully deployed on a wide and diverse commercial scale. Through a review of previously published empirical investigations, the authors of this work study the most prominent security concerns associated with WOT, such as unauthorized access, eavesdropping, denial of service attacks, tampering and impersonation. We have also talked about some of the methods that can be used to solve security related problems keeping in mind the size and dynamics of the network. To educate users about protective measures and prevent security threats from exploiting system flaws, the authors attack threat analysis and modeling techniques. An essential understanding of how some existing processes and algorithms can be used to enhance security is provided by the authors. According to the study's findings, WoT security methodology is still in its infancy, and further research is needed to address these problems.

J. Provoost et al. illustrated that the use of open web standards and semantic technologies, the Web of Things (WoT) allows for the open sharing of information collected by sensors placed in urban settings, allowing for better integration with other web-based data. Convenience is available and knowledge is progressed. As with WoT, artificial intelligence is important for understanding dynamic urban systems (AI). AI allows the analysis and transformation of data generated by WOT-enabled sensory observations to characterize and predict current and future conditions in space and time. This study analyzes the effects of WoT and AI in smart cities by taking into account a practical issue: forecasting parking availability. Weather forecasting web services as well as traffic cameras have been deployed as WOT sensors. AI analytics uses machine learning (ML), which builds predictive models using neural networks and random forests [8].

F. Antoniazzi et al. stated that the Web of Things (WoT) is the most recent iteration of the Internet of Things and, as the name implies, demands the use of Web protocols and protocols for device interoperability across the Internet. Only a few speculative strategies to combat the segmentation of the IoT world via the use of semantics have now been offered by scholars and industry. This new development, called Semantic WoT, is based on a WoT implementations created using the Semantic Web stack's capabilities. Through the use of a common ontology for representing devices, this paper demonstrates a workable realization of the WoT in its Semantic flavour. We characterize the ontology as a dynamic ontology since it also incorporates patterns for interrelations between devices. The proposed dynamic setup can promote interoperability at the required times by allowing on the one hand smart discovery and on the other hand instrumentation and automatic engagement through the semantic information available. A real example will provide a demonstration of idea and overall evaluation [9].

N. Tran et al. stated that the more physical items may now connect to the Internet and provide their services as resources on the Web courtesy to technological advancements. In order to effectively exploit the coming Web of Things, search engines are essential because they connect users and apps with the resources they require to execute. Due to the variety of Web of Things resources most systems use, developing them is a difficult and varied task. A separate kind of

search engine is required for each resource combinations in the query grievance procedure, each with its own set of technological difficulties and application circumstances. The creation of new systems and the examination of the state of the art are both challenged by this variability. We give a systematic analysis of Web of Things search engines in this paper, highlighting the variety of settings that these systems might take. On the basis of this model, we provide an analytical framework for investigating the growth and state of the field as shown by 30 exemplary works. We explore unresolved difficulties in our research's conclusion in an effort to close the gap between current advancements and the ideal Web of Things Search Engines [10].

J. Martins et al. represented that the novel and developing idea known as the "Web of Things" standardizes device communications on upper-layer protocols and describes how the Internet of Things may be linked using widespread web technologies. Upper-layer protocols may usually provide the requisite contact points for a high level of interoperability, even for devices that can only interact via proprietary vendor technologies. Making effective, hypermedia-enriched applications programming interfaces (APIs) that can transfer real Things into virtual ones and reveal their features to others is one of the main development obstacles for this novel idea. The following six hypermedia APIs are evaluated in-depth in this paper. the Web Thing API from Mozilla, the Media Types for Hypertext Sensor Markup from the IETF, the JSON Hypertext Application Language from the IETF, the Constrained RESTful Application Language from the IETF, the Web Thing Model from everything, and the Web of Things [11].

M. Khan et al. illustrated that the Web of Things (WoT) has a serious influence on how effectively and transparently the things linked to the Internet of Things are represented. As a result, it makes online communication between individuals and smart devices pervasive and frictionless. We proposed a WoT-based emerging sensor network (WoT-ESN), which gathers information gathered by sensors, routes sensor data to the web, and integrates iot technologies into the web using a representational state transfer (REST) infrastructure, in light of the significance of WoT. The suggested WoT-ESN architecture is evaluated using a home automation scenario. Through computer simulations of the energy usage of different home appliances, device discovery, and response performance, the home kit scenario is put to the test. The simulation findings demonstrate that the suggested strategy greatly reduces both the power usage and the reaction time of the kitchen appliances [12].

M. Noura et al. illustrated that the Internet of Things' (IoT) primary objective is to build a highly connected world for a variety of application industries. However, the predicted investment's future is seriously jeopardized by the IoT's lack of interoperability. Schema.org provides semantic interoperability for the purposes of organising various forms of data on the Web. Ongoing report concentrated on extending this language for the IoT area to enable semantic interoperability for the Web of Things. One of the main challenges in developing this vernacular is the automatic identification of the essential themes from updated knowledge in IoT applications. We created knowledge extraction for the WoT (KE4WoT) to automatically identify the most crucial topics from literary works ontologies of three different IoT application domains, such as smart home, smart city, and smart weather, in positioned to capitalize on the domain-specific knowledge encoded in IoT publications. Despite the importance of mechanically identifying the relevant subject for iot.schema.org, no study has, as far as you know, addressed this issue. The study demonstrates that the main IoT ontology issues may be used as keywords to appropriately define the existing ontologies [13].

A. García Mangas et al. stated that one of the biggest issues the Internet of Things is now dealing with is interoperability issues brought on by the variety of protocols and platforms (IoT). The Web of Things (WoT) is an architectural approach to addressing this problem that relies on using the Web to guarantee interoperability. One of the most important WoT projects at the current is a collection of building blocks that might potentially act as the WoT's foundation, and it is being coordinated by the World Wide Web Consortium. In this paper, an experimental framework built on the WoT is described, along with a selection of unique and practical protocol binding implementations. The fact that all protocol binding implementations support all interaction variables from the WoT model. This model is one of the primary surprises. By using the W3C WoT architecture and interaction model, the framework is particularly suitable for developing WoT applications for devices on all levels of the pervasive computing concept. The low-level patterns and specifics of a functional Python implementation for the binding templates are also given. By developing a benchmark application across several environments and hardware platforms, the behavior of the architecture and the protocol connections is investigated. Finally, conclusions about the best procedures for each circumstance and interaction phrase are drawn from the data [14].

R. Kumar et al. illustrated that the blockchain and the Internet of Things (IoT) are regarded as highly effective, well-liked technologies. A centrally controlled database called blockchain is used for transactional purposes. In contrast to IoT, which relates to the spread of linked machines by having provided information through the Internet, it offers novel directions for data storage and management. Even though blockchain requires real-time data application and IoT describes processes to store and manage information overloads safely and effectively, a hybrid of the two technologies seems promising. The Industrial IoT is a result of the Industrial IoT's significant impact on manufacturing companies, which are undergoing a digital revolution (IIoT). Additionally, the IIoT sector and its pertinent difficulties are examined. A description of blockchain technology is also supplied. After that, the IIoT and blockchain are consolidated, and a structural design proposal for BIIoT is made. The use of IIoT with blockchain for BIIoT industrial applications is also explored, with some struggles. As a result, this paper gives a summary of all pertinent open research paths in blockchain and IIoT. This study demonstrates how the recommendation BIIoT is used to create a redundant, traceable, secure, intricately interconnected IIoT environment. Moreover, the BIIoT system makes it possible for us to interact with one another within a decentralized, shaky peer-to-peer network without the need for a dependable third party.

K. Kimani et al. discussed in his study the electrical grid more intelligent in order to make it more responsive to consumer energy demands and to deliver increased efficiency and reliability of power systems. The energy needs of the 21st century are expanding quickly due to the population expansion. One of the enabling technologies for a smart grid network is the Internet of Things (IoT). One of the biggest issues is security as the IoT linked devices continue to expand quickly. Since the equipment are online, the smart grid is vulnerable to significant assaults. An IoT-based smart grid provides the largest security vulnerabilities for an IoT-focused cyber-attack since it might include millions of nodes. Given the potential cascading effects of shutting down the electricity grid and the fact that the majority of the devices in our homes, offices, hospitals, and trains depend on electricity to operate, a cyber-attack on a smart grid would just have devastating effects on the dependability of widespread infrastructure. When only one piece of the grid is hacked, the whole system is open to assault. Such assaults on the supply of energy may bring whole cities to just a standstill, causing significant financial and economic

losses. Because of this, security must be carefully considered before IoT-based smart grid networks are extensively deployed. The main obstacles and security concerns impeding the development of IoT-based smart grid infrastructures are addressed and examined in this study [15].

L. Sciullo et al. stated that the Internet of Things (IoT) has grown chaotically, creating a fragmented market with a vast array of devices, technologies, and applications. As a result, many system implementations experience encountered interoperability problems. An innovative approach to providing interoperability across IoT systems and application domains is the Web of Things (WoT) architecture, which again was recently put out by the W3C consortium. The academic and industrial communities must widely accept W3C WoT solutions for to result in an effective improvement, which calls for the creation of complete and well-defined support tools to facilitate the deployment of W3C WoT applications. Additionally, much like well-known app stores, the WoT Store enables the discovery and operation of third-party WoT programmers that communicate with the available Things once more in an intuitive manner. With the support of two assessment studies, we confirm the framework's functionality. First, we illustrate the Thing discovering and the ability to deploy WoT applications that synchronize the operations of several, incompatible Wireless Sensor Networks using a small-case testet. Second, we show the platform's extensibility and the capacity to aggregate and monitor the data streams generated by the WoT apps with a minimum of user input via a mixed real/simulated large-scale frequently mistaken scenario [1].

DISCUSSION

With this chapter, we've taken a step closer to making the Web of Things. by developing RESTful APIs to connect any other Web content with the services provided by real-world technologies and things including electronic materials, wireless sensor networks, and home appliances. We have discussed two methods for integrating devices here to Web using REST: a direct connectivity based on developments in embedded computing and a resource-constrained device-based Smart Gateway approach. By implementing these techniques on two separate platforms, we have further shown them. Finally, we demonstrate how the development of cyber-physical mashups may be substantially aided by an eco-system of RESTful devices. In the meanwhile, connecting devices over the Web and REST provides a highly flexible and formidable method for quickly designing a wide range of applications. REST services do, however, have certain restrictions, and they don't always provide straightforward solutions to issues. For instance, REST's fundamental openness paradoxically makes it more difficult to create complicated services. REST services are ideally suited for basic and discontinuous services, which comprise the majority of services accessible on embedded systems.

However, their limits become apparent when it comes to modelling services that demand complicated input and provide complex outputs. However, the RESTful method has several benefits for smaller and far more user-focused apps, including light and easy usage, the ability to browse services, and a considerably looser coupling. For us, this is essentially the kind of application that mashups are most suited for. Offering a substrate of Web-oriented and RESTful embedded devices is only a first step toward a worldwide Web of Things. Even though authentic devices support Web Servers and Web pages, finding them requires different search techniques than finding textual information on the Web. For searching real-world services, context data, in particular, such as location, time, and kind of usage, is essential. As a result, it will be important to develop a scalable dynamic search engine that takes into consideration the physicality of real-

world services. Similarly, creating mashups that use web services and those that use real-world services are not exactly the same.

CONCLUSION

The integration of sensors into the web is made possible by semantic sensor web technologies that are now operational, but the underlying paradigm is centered on sensors rather than on objects and their high-level states. Incorporating the LOD cloud, a rapidly expanding and open repository of semantic global information, into existing methodologies is also lacking. Spitfire contributes to the creation of a Semantic Web of Things by delivering abstractions for objects, basic search and annotation capabilities, and the embedding of objects and sensors into the LOD cloud. The adoption of IoT technologies will be considerably sped up by the use of linked data principles, which make sensor data readily available for applications through current especially making on the web.

By using an operational prototype to actualize a representative use case, we show the sustainability. Spitfire will gain from any improvements achieved in these fields implicitly since it is in sync with the most exciting developments on the web and IoT sides. We must wait and see how people will utilise the Semantic Network of Things since it was difficult to forecast the variety of contemporary web apps when the web was already developed. It is therefore difficult to foresee if a Semantic Web of Things would be embraced as widely as the web is now. LOD's early extensive use by governments, the media, the biological sciences, geo information systems, and online corporations is one instance. It is obviously advantageous include the sensor data in this data pool since that allows for integration with information gathered from other sources. For instance, monitors and the data they provide may be connected to user-generated, geographic, accessible, and other sorts of information.

REFERENCES

[1] L. Sciullo, L. Gigli, A. Trotta, and M. Di Felice, “WoT Store: Managing resources and applications on the web of things,” *Internet of Things*, vol. 9, p. 100164, Mar. 2020, doi: 10.1016/j.iot.2020.100164.

[2] S. H. Browne *et al.*, “Wirelessly observed therapy compared to directly observed therapy to confirm and support tuberculosis treatment adherence: A randomized controlled trial,” *PLOS Med.*, vol. 16, no. 10, p. e1002891, Oct. 2019, doi: 10.1371/journal.pmed.1002891.

[3] S. Murawat *et al.*, “WoT Communication Protocol Security and Privacy Issues,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 3, 2020, doi: 10.14569/IJACSA.2020.0110319.

[4] M. I. Ramírez-Rojo, R. D. Vargas-Sánchez, B. del Mar Torres-Martínez, G. R. Torrescano-Urrutia, J. M. Lorenzo, and A. Sánchez-Escalante, “Inclusion of ethanol extract of mesquite leaves to enhance the oxidative stability of pork patties,” *Foods*, 2019, doi: 10.3390/foods8120631.

[5] C. Malewski, I. Simonis, A. Terhorst, and A. Bröring, “StarFL - a modularised metadata language for sensor descriptions,” *Int. J. Digit. Earth*, 2014, doi: 10.1080/17538947.2012.739663.

[6] F. Reid, "HTTP," in *Network programming in .NET*, 2004. doi: 10.1016/b978-155558315-6/50005-0.

[7] C. E. Perkins, "Mobile IP," *IEEE Commun. Mag.*, 1997, doi: 10.1109/35.592101.

[8] J. C. Provoost, A. Kamilaris, L. J. J. Wismans, S. J. van der Drift, and M. van Keulen, "Predicting parking occupancy via machine learning in the web of things," *Internet of Things*, vol. 12, p. 100301, Dec. 2020, doi: 10.1016/j.iot.2020.100301.

[9] F. Antoniazzi and F. Viola, "Building the Semantic Web of Things Through a Dynamic Ontology," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10560–10579, Dec. 2019, doi: 10.1109/JIOT.2019.2939882.

[10] N. K. Tran, Q. Z. Sheng, M. A. Babar, and L. Yao, "Searching the Web of Things," *ACM Comput. Surv.*, vol. 50, no. 4, pp. 1–34, Jul. 2018, doi: 10.1145/3092695.

[11] J. A. Martins, A. Mazayev, and N. Correia, "Hypermedia APIs for the Web of Things," *IEEE Access*, vol. 5, pp. 20058–20067, 2017, doi: 10.1109/ACCESS.2017.2755259.

[12] M. Khan, B. Silva, and K. Han, "A Web of Things-Based Emerging Sensor Network Architecture for Smart Control Systems," *Sensors*, vol. 17, no. 2, p. 332, Feb. 2017, doi: 10.3390/s17020332.

[13] M. Noura, A. Gyrard, S. Heil, and M. Gaedke, "Automatic Knowledge Extraction to Build Semantic Web of Things Applications," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8447–8454, Oct. 2019, doi: 10.1109/JIOT.2019.2918327.

[14] A. García Mangas and F. J. Suárez Alonso, "WOTPY: A framework for web of things applications," *Comput. Commun.*, vol. 147, pp. 235–251, Nov. 2019, doi: 10.1016/j.comcom.2019.09.004.

[15] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.

CHAPTER 13
AN INTRODUCTION OF INTERNET OF THINGS BASED SENSORS

Dr. Devendra Singh, Assistant Professor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id- devendras.soeit@sanskri.edu.in

ABSTRACT

The Internet of Things (IoT) has recently created the ability for multiple smart sensors to connect to numerous everyday objects with ease, intelligence, and efficiency through wireless signals. Current revelations in sensing technology have facilitated the IoT's quick growth. This study suggests a three-phase approach to raise the quality of the IoT system technologies' customer experiences. The outcomes of the numerical tests suggest that the suggested technique is capable of accomplishing the objective of this chapter.

KEYWORDS:

IoT Sensors, IoT Devices, Networking, Optical Sensors, Rule Engine.

INTRODUCTION

Sensors are everywhere. They're in our homes and workplaces, our shopping centres and hospitals. They're embedded in smart phones and an integral part of the Internet of Things (IoT). Sensors have been around for a long time. The first thermostat was introduced in the late 1880s and infrared sensors have been around since the late 1940s. The IoT and its counterpart, the Industrial Internet of Things (IIoT), are bringing sensor usage to a new level[1], [2].

Broadly speaking, sensors are devices that detect and respond to changes in an environment. Inputs can come from a variety of sources such as light, temperature, motion and pressure. Sensors output valuable information and if they are connected to a network, they can share data with other connected devices and management systems.

Sensors are crucial to the operation of many of today's businesses. They can warn you of potential problems before they become big problems, allowing businesses to perform predictive maintenance and avoid costly downtime. The data from sensors can also be analysed for trends allowing business owners to gain insight into crucial trends and make informed evidence-based decisions.

Sensors come in many shapes and sizes. Some are purpose-built containing many built-in individual sensors, allowing you to monitor and measure many sources of data. In brownfield environments, it's key for sensors to include digital and analog inputs so that they can read data from legacy sensors. "IoT sensors have become critical to improving operational efficiency, reducing costs and enhancing worker safety."

i. **Temperature Sensors**

Temperature sensors measure the amount of heat energy in a source, allowing them to detect temperature changes and convert these changes to data. Machinery used in manufacturing often requires environmental and device temperatures to be at specific levels. Similarly, within agriculture, soil temperature is a key factor for crop growth.

ii. **Humidity Sensors**

These types of sensors measure the amount of water vapor in the atmosphere of air or other gases. Humidity sensors are commonly found in heating, vents and air conditioning (HVAC) systems in both industrial and residential domains. They can be found in many other areas including hospitals, and meteorology stations to report and predict weather.

iii. Pressure Sensors

A pressure sensor senses changes in gases and liquids. When the pressure changes, the sensor detects these changes, and communicates them to connected systems. Common use cases include leak testing which can be a result of decay. Pressure sensors are also useful in the manufacturing of water systems as it is easy to detect fluctuations or drops in pressure.

iv. **Proximity Sensors**

Proximity sensors are used for non-contact detection of objects near the sensor. These types of sensors often emit electromagnetic fields or beams of radiation such as infrared. Proximity sensors have some interesting use cases. In retail, a proximity sensor can detect the motion between a customer and a product in which he or she is interested. The user can be notified of any discounts or special offers of products located near the sensor. Proximity sensors are also used in the parking lots of malls, stadiums and airports to indicate parking availability. They can also be used on the assembly lines of chemical, food and many other types of industries[3]–[5].

v. Level Sensors

Level sensors are used to detect the level of substances including liquids, powders and granular materials. Many industries including oil manufacturing, water treatment and beverage and food manufacturing factories use level sensors. Waste management systems provide a common use case as level sensors can detect the level of waste in a garbage can or dumpster.

vi. **Accelerometers**

Accelerometers detect an object's acceleration i.e. the rate of change of the object's velocity with respect to time. Accelerometers can also detect changes to gravity. Use cases for accelerometers include smart pedometers and monitoring driving fleets. They can also be used as anti-theft protection alerting the system if an object that should be stationary is moved.

vii. **Gyroscope**

Gyroscope sensors measure the angular rate or velocity, often defined as a measurement of speed and rotation around an axis. Use cases include automotive, such as car navigation and electronic

stability control (anti-skid) systems. Additional use cases include motion sensing for video games, and camera-shake detection systems.

viii. **Gas Sensors**

These types of sensors monitor and detect changes in air quality, including the presence of toxic, combustible or hazardous gasses. Industries using gas sensors include mining, oil and gas, chemical research and manufacturing. A common consumer use case is the familiar carbon dioxide detectors used in many homes.

ix. **Infrared Sensors**

These types of sensors sense characteristics in their surroundings by either emitting or detecting infrared radiation. They can also measure the heat emitted by objects. Infrared sensors are used in a variety of different IoT projects including healthcare as they simplify the monitoring of blood flow and blood pressure. Televisions use infrared sensors to interpret the signals sent from a remote control. Another interesting application is that of art historians using infrared sensors to see hidden layers in paintings to help determine whether a work of art is original or fake or has been altered by a restoration process.

x. **Optical Sensors**

Optical sensors convert rays of light into electrical signals. There are many applications and use cases for optical sensors. In the auto industry, vehicles use optical sensors to recognize signs, obstacles, and other things that a driver would notice when driving or parking. Optical sensors play a big role in the development of driverless cars. Optical sensors are very common in smart phones. For example, ambient light sensors can extend battery life. Optical sensors are also used in the biomedical field including breath analysis and heart-rate monitors.

i. **Smart Object**

The definition of Smart Object depends on its author. Nevertheless, some authors agree with other authors and therefore, we can get a premise of their definitions. Below is our premise which was created using the definitions obtained from. A Smart Object, also known as Intelligent Product, is a physical element that can be identified throughout its life and interact with the environment and other objects. Moreover, it can act in an intelligent way and independently under certain conditions. Furthermore, Smart Objects have an embedded operating system and they usually can have actuators, sensors, or both. This allows Smart Objects to communicate with other objects, process environment data, and do events. However, there are definitions that differ from the previous which was obtained from.

The definition from is very different from the previous. In, they consider as Intelligent Products the objects which are constantly monitoring, which react and adapt to the environment, which have an optimum performance, and which hold an active communication. In our daily life, we are surrounded by examples of Smart Object and there are also examples in our everyday objects like smartphones, tablets, Smart TVs, microcontrollers like Arduino, and even some coffee pots and some cars are also Smart Objects. Therefore, an object connected to the Internet and capable

of manage information can be a Smart Object. As we can see, Smart Objects can be very different from each other. A smartphone has little in common with a microcontroller and microcomputer. They only have in common some electronic components. Each one has their own sensors and actuators, their own intelligence, and their own operating system when they have one. This classification is useful to distinguish the different data that a Smart Object can give us about its architecture. Each dimension represents a quality of the intelligence. With the three dimensions, we can determine the intelligence that an object has and the type of Smart Object that it is. The three dimensions are the level of intelligence, the location of the intelligence, and the aggregation level of the intelligence.

a. **Level of Intelligence**

The first dimension is the level of intelligence. This describes how much intelligent an object can be. It is formed by three levels information handling, notification of the problem, and decision making.

- **Information Handling**

The information handling is the capacity of the object to manage the information gathered from sensors, readers, or from any other techniques. This is the most basic intelligence level and all Smart Object must have it, thus, any Smart Object must be able to manage the information that receives. Otherwise, it would not be a Smart Object and it would be just a Not-Smart Object.

- **Notification of the Problem**

The notification of the problem is the ability of an object to notify its owner under certain conditions or when an event occurs like flames detection, an unusual decrease of the temperature, or any other event like these. In this level, the objects do not have free will.

- **Decision Making**

The decision making is the highest level of intelligence that an object can have. An object has this level when it has the other two levels and it is able to take decisions by itself. It does not require any type of intervention, thus, it has free will.

b. **Location of the Intelligence**

The second dimension is the location of the intelligence and is formed by two categories according to [15], but we have added one extra category. Thus, this dimension has three categories: intelligence through the Network, intelligence in the Object, and combined intelligence. Moreover, we added a third level that combines both levels.

- **Intelligence through the Network**

The intelligence through the Network consists in that the intelligence depends totally on an external agent due to the lack of intelligence in the object. This agent can be a network where the object is connected, usually known as portal platforms, a server that runs the agents or another object that takes decisions or has the global intelligence.

- **Intelligence in the Object**

The intelligence in the Object means that the objects with this level, can process information by themselves, so, they do not need any external agent in order to be intelligent. The platforms that have objects with this level are usually called embedded platforms.

- **Combined Intelligence**

The combined intelligence is a level that does not include in their classification but they talk about it and they include it in an example graph. In this level, the object has the both intelligences. It has its own intelligence and it is capable of use the intelligence located in the Network. This platforms are usually called surrogated platforms.

c. **Aggregation Level of the Intelligence**

The last dimension is the aggregation level of the intelligence which is formed by three categories. This dimension is useful to describe the objects that are composed of several parts. Depending on the aggregation level we could say that an object is indivisible or every part is independent. For example, we can connect a Raspberry Pi with an Arduino and connect sensors or actuators to both devices. The Not-Smart Objects like the sensors or actuators, do not have their own intelligence but the Raspberry Pi and the Arduino are Smart Objects. Therefore, if we disconnected the Arduino and the Raspberry Pi, they could run independently, whereas if we disconnect the Not-Smart Objects they could not work by themselves[6]–[8].

ii. **Non-Smart Object**

In the previous section, we explained what the objects are and what elements compose this group. These elements are the objects without intelligence and objects with intelligence which are also known as Smart Objects. Due to the existence of these elements, it is essential to know how to distinguish the different type of objects and know the way in which these objects can interact with us. In this section we will address the objects of the second group, the objects without intelligence or Not-Smart Objects, and in later sections we will deepen in the Smart Objects. The Not-Smart Objects can be formed by sensors and actuators.

Sensors are electronic devices composed of sensitive cells that are able to measure physical parameters like the light fluctuation using a photoresist or, the temperature using a thermistor, to detect flames, sounds, movements, or any other fluctuation in the environment. Thus, sensors are specific physical elements that allow us to measure a concrete physical parameter or detect something of the sensor's immediate environment.

However, actuators can be mechanic actuators which allow actions over themselves or over other devices, and actions which a specific object allow to perform. Thus, we can divide actuators in two different groups: mechanic devices and actions. Examples of mechanic actuators could be motors, servomotors or hydraulic bombs, and examples of actions could be to send a message, control LEDs, and turn on lights or control the movement of a robot or any other available robot's actions.

According to the previous definitions, we could find devices that combine both types of Not-Smart Objects, they not only would have actuators and sensors but also would have both. An example of these are smartphones or any other Smart Object that are composed by sensors and actuators. Another similar example could be a microcontroller like an Arduino. The Arduino microcontroller is capable of manage almost any type of electronic device. Thus, an Arduino allows creating a system composed only of actuators, only of sensors, or both. Therefore, the Smart Objects are formed by Not-Smart Objects.

Figure 1 shows a concept map that explains the composition of the objects. This figure is useful to understand better the difference between Not-Smart Objects and Smart Objects. As we can see in figure, Not Smart Objects can be sensors or actuators, and actuators are divided into mechanic actuators and actions. Moreover, in order to improve the understand ability and this figure shows several examples of each group.

Figure 1: Represented that the Composition of Objects [6].

LITERATURE REVIEW

K. Gsangaya et al. ststed that the Production farming's sustainability relies on making the right choice is important at the right time according to the circumstances at hand and past performance. The goal of precision agriculture is to enhance agricultural output without preserving environmental quality by precisely adjusting soil and crop management to match the distinct characteristics of each area. This research study outlines the development of a wireless, portable sensor network system that can be used to remotely measure the environmental factors in an agricultural field, provide field managers warnings and information about the current predicament, and store the data for later use. Temperature, humidity, intensities, and soil moisture content are just a few of the appropriate for measuring data that are acquired by the data collection unit, which is made up of sensors and a microprocessor. By leveraging Internet of Things technology, the information collected by the sensors is wirelessly posted to that same cloud server and accessible to users through in an Internet-enabled device from anywhere in the globe. The system may be utilized in outside agricultural lands thanks to its tough and water-resistant shell, and its solar power source minimizes the need for wiring and minimizes sensor node maintenance costs. The system has effectively captured and displayed appropriate for measuring data to users, according to tests [7].

A. Khedr et al. illustrated that the one of the core components of the Internet of Things (IoT), which is utilised for a variety of applications to conduct accurate real-time observations, is the wireless sensor network (WSN). The aggregation and analyses of data are more difficult since WSN has limited resources and there is a large number of IoT data that is moving quickly. To efficiently manage the data being produced by the sensors and to evaluate the data patterns in order to get the necessary information from them, data mining-based solutions have recently been offered. Our proposal for a distributed and effective data mining method was driven by the growing need for these approaches. It not only manages the enormous and quickly produced data by the nodes, but also lengthens the life of the network. This significantly lowers the

communication overhead, extending the network lifespan in the process. The suggested method is tested using several simulations, and the findings show that by including the proposed scheme into the current protocols, the communication overhead is greatly reduced, hence extending the network lifespan and stability.

B. Hu and H. Li discussed that the as a typical Internet of Things application, home-based multi-sensor Internet of Things integrates a range of intelligent sensor devices and home appliances to provide intelligent solutions to individuals everywhere. There is less and less need for human input as families grow smarter, more complicated, and reliant on technology. Recent security breaches have demonstrated that the Internet-based, home-based Internet of Things have turned into a susceptible target, posing issues with personal privacy. For instance, eavesdroppers may learn particular devices' or sensors' identities over vulnerable public channels, allowing them the guess about a person's private life on the home area network. Authenticate is a crucial step in many secure systems' identity declaration and verification processes. Home-based Internet of Things solution needs to verify users and devices before distributing private information. Intelligent gadgets have limited capacity for processing and communication. Lightweight authenticating and key agreement technologies are thus crucial in the home-based Internet of Things to fend away known threats. This paper suggests a pairing-based cryptography-based anonymized authenticated key agreement technique. The Internet of Things network at residence that uses several sensors may carefully selected with the Internet thanks to the methodology that is suggested in this chapter.

H. Farman et al. illustrated that the limited Wireless Sensor Network built on the Internet of Things, there has been rapid growth and rising interest in effective service delivery and improved resource use in recent years (WSN). The most effective deployment of energy-conscious WSN and effective communication architecture for data transmission across embedded systems are key components of the Internet of Things. Additionally, energy-efficient clustering algorithms for routing and WSN node deployment have made significant strides in extending network lifespan. When using a clustering strategy, the network is broken into several segments, and careful consideration should be given to the hierarchical clustering process in order to maximize node reachability within the cluster and ensure effective communication with the cell tower. In this chapter, by putting into consideration various elements influencing node energy and network lifespan, we suggested a multi-criteria dependent cluster head selection technique in Internet of Things based WSN. Energy level, distance from nearby nodes, distance from the zone's center, the number of times a node previously served as zone head, and whether or not a node is merged all directly influence how well a WSN performs overall. The suggested approach works comparatively better in simulations comparison to other energy-efficient clustering algorithms already in use.

P. Sanjeevi et al. stated that the agricultural and agriculture sectors have recently evolved into a precise network of sensor connection with a new level of Internet of Things (IoT) technology. The agricultural and farming profession in a distant location may benefit from either the wide distance network in IoT that is based on wireless sensor networks (WSNs) and cloud computing. In this research, we provide an IoT-based scalable wireless sensor network architecture for

remote farming and agricultural surveillance and control. Water resource development and efficient water use are important middle managers in precision agriculture and farming (PAF). By using WSN technology with IoT, proper water irrigation control may be realized. IoT is used in PAF to handle the efficient communication of a variety of wireless sensors, enhancing farmers' production. Based on throughput maximization, delay reduction, high signal-to-noise ratio (SNR), minimal mean square error, and expanded coverage area, we have investigated the WSN structure. The outcomes of the tests have proven that the suggested technique performs more efficiently than conventional IoT-based agriculture and farming.

M. Subashini et al. stated that the environment in which crops are grown must now be continuously monitored in order to maximize yield, improve food security, and use as few resources as possible in light of global warming and quickly changing weather patterns. In this work, we created a low-cost system that would keep track of a crop's temperature, humidity, light intensity, and soil moisture and transmit that information to a server online for storage and analysis. Using this information, the system can then operate actuators to regulate growth factors. The base level of the three-tier system architecture is made up of sensors and actuators, followed by an 8-bit AVR microcontroller for data processing, and the top level is an ESP8266 Wi-Fi module for connecting to the internet server. To water the crops, the system employs relay to operate actuators like pumps, and online weather data is utilized to optimize irrigation cycles. The prototype system underwent a number of tests, and the results demonstrate the system's dependability and precision, which highlight its viability in practical applications.

S. Khan et al. stated that the patient falls that are unintentional cannot entirely be avoided. However, prompt fall detection may aid in avoiding further issues including blood loss and unconsciousness. In this work, the authors describe an integrated, cost-effective system that can categories non-fall movements as activities of daily living as well as remotely recognize patient falls in hospitals. The suggested system is a wearable gadget with a camera, gyroscope, and barometer that connects to a single board microprocessor the size of a credit card. The sensor data is examined using the k-Nearest Neighbor and Nave Bayes classifiers, and the information from the camera is employed in a visual-based classifier. When a fall is discovered, a hospital attendant is notified. According to research observations, the gadget is 95% accurate in identifying fall-related activity from some of the other types of activity. There is further in-depth explanation of other specs and needs.

R. Dogra et al. stated that the advancements in the technology, Internet of Things (IoT)-based wireless sensor networks (WSNs) have shown a tremendous growth in rendering a huge number of applications across the globe. However, it is observed that IoT-based sensor nodes suffer from energy limitations. To resolve this, cluster-based topology is adapted by the various researchers for rendering green energy-efficient solution for communication of IoT devices. In this paper, the dynamic and energy-efficient clustering for energy whole mitigation is proposed. The proposed framework is composed of the following proposed attributes; network is divided in two halves of regions, in each half, a gateway node (GN) is selected that collects data from their corresponding half region. Further, in each cluster, two cluster heads (CHs) are selected among whom one is made active at a moment (remains active until 60% of its energy is consumed) and other stays in

sleep mode. First, the GN is selected in each side of the network (divided into two halves), and later, clustering is done, and selection of two CHs in each cluster is performed. The parameters for the selection of GN and CHs include residual energy, separation between the node and the sink, the number of neighbor nodes and network's residual energy.

A. Aziz et al. illustrated that the IoT-based systems, which connect various kinds of sensors, mobile devices, and other technologies to the actual environment, are gaining popularity for usage in a broad range of applications. A reliable solution for precise data recovery at the base station (BS) with lower communication costs is offered by in-network compression and compressed sensing (CS)-based information gathering. This paper investigates the energy-efficient data collection methods for IoT-based Wireless Sensor Networks (WSNs) using CS in conjunction with routing protocols. Detailed simulation and analysis findings show that our suggested solution performs 35% better than the ECST algorithm and 93% better than the PEGASIS strategy in terms of increasing network lifespan. The suggested reconstruction approach performs better than previous reconstruction techniques as well.

J. Moon et al. illustrated that in this chapter, we modified a sensor-based smart insole to track the workload of the labor-intensive hauling of construction material that regularly takes place on construction sites. The majority of the time, the professionals on a construction site walk while they do their respective jobs. In order to seamlessly predict the weight of the building material being carried and the time it would take to complete these tasks based on the characteristics of walking, we created and installed an application software server to receive and process information from the Internet of Things sensors. A link between the signal change at the foot plantar pressure while walking and the added and the mixture of the construction material carried by the employees was proven as a result of the experimental analysis with 15 individuals utilizing the tell researchers. It has been verified that one may determine the weight of the construction material that a worker now owns by measuring the foot pressure value whilst also walking. Based on this, we were able to assess the production time with a 97% accuracy and estimate the approximate weight of the product with a 91% accuracy from either the 20 new test individuals.

DISCUSSION

We have discussed IoT sensors in this chapter, which are a modular IoT management solution that can be used to automate the functions of gathering and initiating sustainability activities. SensoMan employs sensors and actuators to gather data and, in accordance with rules specified by users in its rule engine, activate actions. It permits the use of numerous sensors attached to microcontroller boards, making the structure extendable with new sensors to cover a variety of situations. Its modules are built on open-source technologies. When linked to other SensoMan users via the social network, users may browse their boards as well as information from other users' sensors. With the assist of two scenarios that highlight the usage of the rule engine and the social network, we have shown SensoMan's use and its usefulness, and we have also performed a small-scale user research. We maintain that since the platform is built on a fundamental design and gives users the option to employ the system components that best match their needs, everyone, including those with low technical skills, would benefit from using it.

In most IoT device architectures, sensors are employed and that the Hardware of Internet of Things shown in Figure 2. Sensors are used to detect objects, machinery, and other things. A gadget that responds to a certain measurement by producing a useable output. The sensor collects a physical quantity and transforms it into a signal acceptable for electrical, mechanical, or optical processing. The qualities of any substance or instrument that allow it to determine the presence of a certain physical amount. The sensor's output is a signal that is translated into human-readable forms, such as variations in characteristics, resistance, capacitance, impedance, etc.

Figure 2: Illustrated that the Hardware of Internet of Things.

Transducer:

- Signals are transformed from one building appearance to another via transducers.
- It transforms one kind of electricity into another.
- It might function as actuators in a wide range of applications.

Sensors Characteristics:

- Static
- Dynamic

i. Static Characteristics:

It is about how the output of a sensor changes in response to an input change after steady state condition.

- Accuracy

Accuracy is the capacity of measurement device to provide a result that is reasonably closer to the actual value of the quantity being measured. It counts mistakes. Both absolute and comparative mistakes serve as a gauge. Compare the output's accuracy compared to a more advanced earlier system [19].

Absolute error = Measured value – True value

Relative error = Measured value/True value

- Range

Reveals the physical quantity's greatest and lowest values that the sensor is truly capable of sensing. There is no meaning or form of reaction outside of these ideals. For instance, the temperature measuring range of an RTD is between -200°C and 800°C.

- Resolution

Resolution is a crucial parameter when choosing a sensor. The accuracy improves with increased resolution. Threshold is the condition when the accumulating is zero to. Give the slightest adjustments to the input that somehow a sensor is capable of detecting.

- Precision

When repeatedly measuring the same amount under the same set of guidelines, a measuring device must be able to provide the same reading. It indicates agreement, NOT closer to the real value, between subsequent measurements. It has to do with the variability of a collection of measurements. It is a prerequisite for accuracy but not a sufficient one.

- Sensitivity

Sensitivity describes the proportion of small changes in the system's reaction to small changes in its process variables. It may be determined from the slope of a sensor's output characteristics curve. The tiniest quantity fluctuation will cause the instrument's measurement to alter.

- Linearity

The sensor value curve's departure from a certain straight line. The calibration curve establishes the linearity. Under static circumstances, the static calibration curve plots the environments leading vs the input amplitude. The linearity of a curve is expressed through its slope, which resembles a straight line.

- Drift

The deviation of the sensor's measurement from a given reading when it is maintained at that value over an extended length of time.

- Repeatability

The variation in measurements made sequentially under the same circumstances. The measurements must be taken over a brief enough period of time to prevent considerable long-term drift.

CONCLUSION

Our world is undergoing a change because to the Internet of Things (IoT), which is making our surroundings smarter. Sensors are fundamental to the automation of any IoT-based smart application because they enable the applications to react intelligently and dynamically. In an IoT-enabled smart environment, many kinds of sensors are presented in this study. Health, water, commuting, home appliances, waste, agriculture, livestock, and other businesses may all benefit from the deployment of IoT sensors. IoT incorporates many sorts of sensors with the capacity to connect between them intelligently and remotely in any specific smart application. In order to clarify which sensors are deployed in various IoT applications, this paper explores different IoT sensors and sensor-based IoT applications. This study will be important in the future as we create sensor-based Internet of Things applications[9], [10].

Future work will concentrate on enhancing SensoMan to provide pertinent assistance for the real-time handling of sensor data. We are also working towards a more sophisticated usage of actuators, one that goes beyond simple device activation and deactivation and incorporates additional functions, such using infrared codes to adjust the temperature of an air conditioning system. In order to draw conclusions about the data that cannot be seen when viewing or using the data independently, we are also working to provide users with an elaborated reasoning mechanism that would enable them to use sensor values in their applications in combination with machine learning techniques and other sources of information. Additionally, we plan to solve any scalability problems that could arise if the number of users, sensors, actors, and rules greatly increases. Additionally, we'll carry out a comprehensive user review of SensoMan's features. Finally, since this is a crucial newly developing sector in IoT, we will include security and data protection methods in accordance with the General Data Protection Regulation (GDPR).

REFERENCES

[1] F. J. Ferrández-Pastor, J. M. García-Chamizo, M. Nieto-Hidalgo, J. Mora-Pascual, and J. Mora-Martínez, "Developing ubiquitous sensor network platform using internet of things: Application in precision agriculture," *Sensors (Switzerland)*, 2016, doi: 10.3390/s16071141.

[2] M. Pouryazdan and B. Kantarci, "The Smart Citizen Factor in Trustworthy Smart City Crowdsensing," *IT Prof.*, 2016, doi: 10.1109/MITP.2016.72.

[3] Y. Khan, A. E. Ostfeld, C. M. Lochner, A. Pierre, and A. C. Arias, "Monitoring of Vital Signs with Flexible and Wearable Medical Devices," *Advanced Materials*. 2016. doi: 10.1002/adma.201504366.

[4] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio, and R. Prasad, "Satellite communications supporting internet of remote things," *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2015.2487046.

[5] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *Journal of Network and Computer Applications*. 2016. doi: 10.1016/j.jnca.2016.01.010.

[6] K. Lin, W. Wang, Y. Bi, M. Qiu, and M. M. Hassan, "Human localization based on inertial sensors and fingerprints in the Industrial Internet of Things," *Comput. Networks*, 2016, doi: 10.1016/j.comnet.2015.11.012.

[7] S. Park, S. Park, S. Park, and J. Byun, "Design of a mass-customization-based cost-effective Internet of Things sensor system in smart building spaces," *Int. J. Distrib. Sens. Networks*, 2016, doi: 10.1177/1550147716660895.

[8] M. Elkhodr, S. Shahrestani, and H. Cheung, "A middleware for the internet of things," *Int. J. Comput. Networks Commun.*, 2016, doi: 10.5121/ijcnc.2016.8214.

[9] P. Zhang, Y. Liu, F. Wu, S. Liu, and B. Tang, "Low-Overhead and High-Precision Prediction Model for Content-Based Sensor Search in the Internet of Things," *IEEE Commun. Lett.*, 2016, doi: 10.1109/LCOMM.2016.2521735.

[10] R. Martac, N. Milivojevic, V. Milivojevic, V. Cirovic, and D. Barac, "Using internet of things in monitoring and management of dams in Serbia," *Facta Univ. - Ser. Electron. Energ.*, 2016, doi: 10.2298/fuee1603419m.

CHAPTER 14

AN INTRODUCTION OF THE FUTURE DIRECTION AND DIFFERENT VISION FOR THE INTERNET OF THINGS

Dr. Sovit Kumar, Assistant Professor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id- sovit.soeit@sanskriti.edu.in

ABSTRACT

Wireless sensor network (WSN) technology-enabled ubiquitous sensing affects many aspects of everyday culture. Indicators of the environmental, from sensitive ecologies and natural wealth to urban settings, may now be measured, inferred, and understood. The Internet of Things (IoT) is created by the development of these devices in a powerful communication network, where the actuators and sensors seamlessly integrate with our surroundings and information is exchanged across platforms to build a commonly used performance picture. A cloud implementation based on the interconnection of private clouds and public clouds and employing Aneka is shown. We concentrate on the need of WSN, the Internet, and distributed systems in order to address the audience of technical researchers as users finally end our IoT vision.

KEYWORDS:

Intelligence Object, Optical Sensors, Sensors, Smart Sensor, Wireless Sensor.

INTRODUCTION

The Internet of Things is a futuristic idea in which mundane things are included in an Internet that permeates into actual world. Physical objects could now be controlled remotely and used as physical access points to Internet services, so they are no longer isolated from the virtual world. Computing becomes completely pervasive with an Internet of Things, an idea previously advanced by Mark Weiser in the early 1990s. Huge possibilities are really being created by this growth for the economy and for people individually. It is clearly a huge technological and social challenge, but it also carries hazards [1]–[3].

The idea behind the Internet of Things is based on the assumption that the constant advancements in communications, information, and microelectronics we have seen over recent years will continue for some time to come. In reality, processors, communications modules, and other computer equipment are being incorporated into more and more ordinary products nowadays as a result of their shrinking size, continually lowering prices, and decreasing energy usage. Since embedded communication and data technology has the potential to change the usability of these "smart" things, they play a crucial role in the Internet of Things concept. They can sense their surroundings via sensors, and with to their built-in networking features, they might talk with one another, connect to the Internet, and engage with others. By incorporating the characteristics of digital items, "digitally upgrading" traditional objects in this manner

strengthens their physical function and creates significant value. Indicators of this trend may already be seen in the increasing "computerization" and network interfaces of products like sewing machines, exercise bikes, electronic dentistry, washing machines, and photocopiers [4]–[6].

In other application sectors, Internet service may be used to remotely monitor the condition of ubiquitous items, allowing information systems to compile the most recent data about physical things and processes. This allows one to "observe" many parts of the actual world at a previously unattainable degree of detail and for a very little investment. This would enable more effective control and management in addition to a better understanding of the core processes. A broad range of corporate operations may be maximized when responses to occurrences in the real world can be automated, quick, and informed. This opens up new potential for handling challenging or urgent problems. Real-time analysis of data gathered from the physical world will probably result in the development of a number of unique commercial services, which might have a significant positive impact on both the economy and society. In the same way that people use the Web today, things will soon also communicate with each other, use services, provide data, and thus generate added value . Alternatively, the term "Internet" in the catchy phrase "Internet of Things," which stands for the above-described vision, can be interpreted in a stricter technical sense, postulating that an IP protocol stack will be used by smart things or at least by the "proxies," their representatives.

Getting IoT ready

The most basic obstacles, including that of the following, should always be met by manufacturers in order to set up the lowest layers of innovation for the IoT's horizontal nature:

- **Connectivity:**

There won't be a "winner" among the communication standards. To link the items in the IoT, a broad range of wireless and wireless standards as well as custom implementations will be utilised. Getting the many connectivity standards to communicate with one another using a single unified data currency is difficult.

- **Power Management**

The Internet of Things (IoT) will include more rechargeable or energy-harvesting devices that are more accessible and self-sufficient. Equipment that runs across lines will be required to be more energy-efficient. Making battery management simple to add to these devices and devices is the difficult part. Connectivity and energy management will be factored into wireless charging.

- **Security**

Security is essential given this same volume of data transmitted by the IoT. To protect the IoT, built-in hardware security and adoption of current connection security procedures are required. Simply getting people to utilise the built-in security on their gadgets is another hurdle. The Internet of Everything Evolution September 2013 to 2020: 50 billion connected devices.

- **Complexity**

To join the IoT, manufacturers are striving to connect objects and machinery that have never been interconnected before. More items must be linked, and this is particularly true considering the difficulty of ordinary RF programming, therefore ease of design and development is crucial. Furthermore, the average customer must be able to set up and manage their gadgets without any existing technical knowledge.

- **Rapid Evolution**

The Internet of Things is continuously improving. The sector is continually developing, and also more gadgets are being incorporated daily. The unknown is the industry's difficulty unknown equipment unknown programmers. Unidentified use cases given this, flexibility is important in every aspect of development. Microcontrollers (MCUs) in tiny, energy-efficient wireless sensor nodes and high-performance, multi-core processing for IoT infrastructure are two examples of processors and embedded processors that span the frequency range of 16–1500 MHz to handle the whole spectrum of operations. To address the diverse market demands, a broad range of wired and wireless communications solutions are required. The focus of attention for the Internet of Things and energy-efficient designs must also be delivered, which calls for an assortment of sensors, mixed-signal, and strength technologies.

Compelling Benefits of IoT

Cost reductions, increased income, and chances for innovation are just a few of the compelling business advantages and value that IoT provides that enterprises just cannot afford to ignore.

- **Cost Savings**

Costs may be decreased through increasing productivity, process efficiency, and equipment utilization. Customers and businesses stand to gain from better asset management such as via smart metres that do away with manual measurements and service enhancements e.g., remote monitoring of patients in clinical settings. According to General Electric, it would result in billions of dollars in cost savings if intelligent equipment and analytics resulted in even a small decrease in fuel usage, capital expenditures, and inefficiencies.

- **Improved Asset Utilization**

Businesses may get real-time insights and visibility across their assets and supply chains through increased asset tracking machines, equipment, tools, etc. via sensors and connection. To improvement system and utilization, for instance, they might more readily discover assets and do proactive maintenance on important pieces of equipment and infrastructure.

- **Efficient Processes**

Real-time operational analytics may help small businesses make better choices and save operational expenses. They can monitor and enhance process efficiency, save energy costs, and limit human interference by using real-time data from sensors and actuators.

- Improved Productivity

Productivity is a crucial factor that determines every organization's profitability. By providing the employees with just-in-time training, lowering the imbalance between necessary and available skills, and optimizing labour efficiency, IoT increases organisational productivity.

IoT Futures

The expected exponential proliferation of smart devices and the convergence of low-cost infrastructure, communication, and data will accelerate the IoT from a lofty notion to a reality. IoT solutions are being widely used as a result of falling device prices, ubiquitous connectivity, and a growing emphasis on operational efficiency and productivity. Only 15% of firms had an IoT solution in place as of 2012, according to a poll by Zebra Consulting and Forrester, but more than half (53%) intended to adopt one in the next two years, and another 14% planned to do so in the following two to five years. About 21% of respondents from the transportation and logistics industry said they had previously implemented an IoT solution.

- **Billions of Smart Devices are Becoming Connected**

By 2020, 50 billion linked smart devices may exist, a rapid increase in the number of these gadgets (see Figure). Machine-to-machine (M2M) communications, a crucial component of the Internet of Things, are also expanding. According to Machina Research, there will be 18 billion M2M connections by 2020, up from two billion in 2011.

- **Confluence of Low-cost technologies, Connectivity, Data and Sensors**

IoT has reached a tipping point as a result of lower sensor prices, a sharp rise in computer and processing capacity, low-cost data storage, and universal low-cost, high-bandwidth connection. As cellular M2M module prices have dropped at a pace of 15% every year and the cost of connection has fallen, with 1GB currently costing $1.50, services that need connectivity are becoming more competitive. 1 The new Internet Protocol (IPv6) standard helps with the connectivity requirements of the expanding universe of smart objects. It uses a 128-bit address to offer 340 undecillion (or 3.4 x 1038) unique IP addresses, which again is sufficient to connect the billions of smart objects that human civilisation will use in the future.

Issues and Challenges

Despite the enormous possibilities of IoT, enterprises must resolve a host of problems and obstacles that are hampering IoT's development. Organizations will need to collaborate closely with experienced suppliers to get over important obstacles, including:

- **A lack of standards and interoperable technologies**

Interoperability is hampered by the tremendous variety of vendors, technologies, and protocols adopted by each class of smart devices. Organizations find it challenging to integrate apps as well as devices that utilise various network technologies as well as operate on various networks due to the lack of agreement on how to use developing protocols and protocols to enable smart objects to communicate and interact. Organizations must also make sure that smart devices can communicate with one another and with other services[7]–[9].

- **Data and information management issues**

It is very difficult to route, capture, analyses, and use the insights produced by massive amounts of IoT data in a suitable and timely manner using existing infrastructures. Due to the sheer volume of data being gathered, advanced algorithms that can sort, examine, and extract value from data are essential. New data silos are developed as more gadgets hit the market, resulting in a complicated web of linkages between diverse sources of information. The elimination of data silos inside enterprises will also be made more difficult by the absence of global standards and conventions.

- Privacy and security concerns

The capacity of enterprises to acquire, handle, and process data will influence how much value they can get from IoT. A major worry will be preserving such data from illegal usage and assaults. Similar to how numerous gadgets are used for personal purposes, this raises considerable privacy issues since many users may not be aware of the kinds of individually identifiable information being gathered. Additionally, because the majority of gadgets only need minimum human involvement, businesses must be wary concerning hacking and other illegal mischief. A cyber-attack or malfunctioning device that causes malfunctions in the IoT ecosystem poses a substantially greater danger in the future.

- Organizational inability to manage IoT complexities

Even while IoT has a lot to offer, implementing it will need whole new levels of skills and systems that can control the ecosystems and create value for businesses. For instance, it will be important to have robust data management, storage, and analytics skills to make sense of the data influx supplied by sensors every minute. Similar to this, policymakers should handle issues with data, security, and privacy. In order to guarantee that activities of the company are successful and efficient, organisations will also need to acquire the knowledge and abilities to anticipate probable component failures and substitutions through preventive maintenance and maintenance techniques.

LITERATURE REVIEW

The Wireless sensor network (WSN) technology-enabled ubiquitous sensing affects many aspects of contemporary culture. Indicators of the environmental, from sensitive ecologies and energy wealth to urban settings, may now be measured, inferred, and analyzed. The Internet of Things (IoT) is created by the proliferation of these devices in a powerful communication network, where sensors and actuators seamlessly integrate with our surroundings and information is exchanged across platforms to build a commonly used performance picture (COP). The requirement for data-on-demand employing sophisticated intuitive searches substantially grows as we convert from the www, or static pages online, to the web2 (social networking web), and finally the web3 (ubiquitous computing web). In this study, a cloud-centric paradigm for the global implementation of the Internet of Things is presented. We explore the major enabling technologies and application areas that will likely steer IoT technology in the near future. A cloud implementation based on the interplay of private and public clouds and

employing Aneka is shown. We concentrate on the need of WSN, the Internet, and distributed computing in order to address the community of technical researchers as we wrap up our IoT vision .

Internet of Things (IoT) is quickly evolving, paving the way for the creation of a number of IoT applications that entail little to no human intervention in the processes of data gathering, transformation, knowledge extraction, and decision-making (actuation). Such IoT applications (which we refer to as autonomic) must be measured and evaluated for quality, which is difficult in the absence of any human interaction or input. The majority of Quality of Experience (QoE) definitions and existing literature place a strong emphasis on assessing application quality through the eyes of the person using the service. However, with autonomous IoT applications, bad decision-making and subsequent actions might reduce the application's quality, resulting in losses in both the economic and social spheres. We provide a vision, a survey, and potential future prospects for IoT QoE research in this study. Following a review of the QoE definitions currently in use, we cover the methods and strategies utilised in the literature to assess QoE in IoT. We identify and examine the function of data in IoT designs, which is important for assessing the Quality of Experience (QoE) of IoT applications. In order to assess the quality of experience (QoE) of autonomous IoT applications, we define and give our vision for future research as a conclusion to this work .

Internet of Things (IoT) is a potential paradigm for communication that uses sensors, embedded processors, and transceivers to formulate powerful systems for computing and communication. The apps and infrastructure must support and enhance the intelligent governance of our municipal services, jobs, and everyday lives. This paper explores the fusion of the Radio-over-Fiber (RoF) infrastructure and the eventual 6G vision of the Internet of Things. In opposition to the IoT services included in the 5G deployment, 6G IoT utilises high-density heterogeneous devices with exceedingly high capacity, providing much more resilient system design and clever algorithms based on artificial intelligence (AI). One of the most promising drivers for the exceptional qualities of flexibility and efficiency of 6G IoT systems is the RoF. This paper starts by explaining the IoT evolution path from 5G to 6G and the effectiveness of RoF and fibre optic technologies. Then, we highlight the most notable recent efforts in the many dimensions while introducing the fast growing RoF industry and corresponding relevant technologies connected to IoT-RoF convergence. Finally, we look at the obstacles that the 6G IoT system that RoF will enable in the future will face and possible solutions [8].

The wireless sensor network technologies enable ubiquitous sensing, which is used in many aspects of today's life. With this, one may perceive, interpret, evaluate, and extrapolate environmental characteristics ranging from sensitive ecologies and natural resources to metropolitan surroundings. The Internet of Things (IoT) technology revolution has occurred as a result of the exponential growth in the number of devices that are online. Actuators and sensors in any of these technologies integrate easily with the IoT ecosystem. Additionally, platforms are used to disseminate the detected information in order to build a common operational picture. A variety of IoT devices power this cutting-edge technology, enabling innovations including near field networking, embedded actuator, sensor nodes, radio frequency tags, and readers. The

Internet of Things has grown out of its infancy and created a full functioning future internet. Although several IoT technology concepts have been examined, the research community should confront and present the present incarnation of this topic. The primary enabling technologies, current and upcoming network technologies, and application areas that will drive IoT research in the near future are reviewed in this paper as we address the recent global introduction of IoT. Furthermore, all of the IoT stack's protocols are thoroughly explored, encompassing their initial, most recent, and upcoming improvements. More examples of middleware's definition, applications, categorization, and important open challenges are provided. Not only to this extent, but also in-depth analysis of IoT research history and approaches that have caught the interest of contemporary IoT researchers are included in this survey, which also covers IoT sensors and the latest recent potential application, as well as general IoT research problem.

The Internet of Things (IoT) is a brand-new paradigm that offers a number of fresh applications for the next wave of technological breakthroughs. IoT applications are almost endless and allow for simultaneous physical and digital world convergence. To fully realise the promise of IoT, there are still many issues to be solved despite the great efforts of implementation and evaluation, alliances, companies, academics, and others. Various factors, particularly enabling technologies, applications, business practices, social implications, and environmental impacts, should be taken into account while analyzing these concerns. This presentation focuses on open issues and obstacles seen from a technology standpoint. In order to promote a better appreciation of the components of the IoT, we have highlighted many views that support this paradigm. Further, this thorough analysis offers insights into the most recent developments in emerging and IoT supporting technologies. Information is given for the ones that are the most relevant. The primary goal is to provide a comprehensive investigation of the problems and obstacles that need to be resolved by future research. In order to aid future study, we provide some perspectives into certain particular developing theories. Additionally, this publication organizes the body of literature by categorizing contributions up into multiple research areas .

The present and next Internet generations are being shaped by the Internet of Things (IoT). The goal of the Internet of Things is to connect communication capabilities into a network of widely dispersed, always present, and dense heterogeneous objects. In this vision, anyone or everything may use new intelligent apps and services to adapt protected mobile networks anytime, whenever. There have been several attempts to examine the IoT-related literature for the benefit of IoT development. To fully realize the IoT's capabilities, however, there are a number of obstacles that must be resolved. In order to categories and standardize IoT research domains, this study will focus on review papers that were released between 2010 and 2019. This paper investigated 95 relevant reviews that were carefully picked from databases based on six predetermined topics. The six study categories of application, architecture, communication, problems, technology, and security are used to identify and illustrate the trends in IoT reviews. With 21% of all evaluations and a growth rate of more than 100% over the last ten years, IoT communication research has dominated the trends. As a result, this work may help future research by offering important insights into certain emergent IoT sectors .

Internet of Things (IoT) is aggressively expanding and gaining popularity worldwide. In this study, two models for the Future IoT are offered based on the restructured Unit IoT and Ubiquitous IoT. A layer model is constructed for the future IoT system architecture, and a dimension model is produced to categorise the complex IoT technologies. The IoT concept and projected stages of evolution are then described. Furthermore, it is argued that it is incorrect to think of the Internet of Things (IoT) as a new phase in the evolution of intelligence and information technology. At the meanwhile, the need for skilled staff training in colleges is established. The interaction between the Internet of Things, the science and technology system, and IoT-related disciplines is then examined. This essay highlights the issue of specializing in IoT in college and offers some solutions in the conclusion. 2012 John Wiley & Sons, Ltd. Copyright The complexity Internet of Things (IoT) technologies are categorised using a dimension model proposed in this research, and a layer paradigm for the IoT system architecture of the future is constructed. IoT vision and forecasts for its initial stages of growth are also provided. It is clarified that the idea of seeing IoT as a developing industry is incorrect .

The most frequent and devastating natural disasters is flooding. A better response to flood threats is necessary given the growing number of flood-related fatalities and financial losses seen each year and throughout the globe. It's interesting to note that in the last ten years, there have been many chances for academic research into how camera pictures and wireless sensor data from Internet of Things (IoT) networks might enhance flood control. The literature on IoT-based sensors and vision - based applications for flood mapping and surveillance has been thoroughly reviewed in this research. The work makes a contribution by outlining several key computer vision algorithms and Internet of Things sensor approaches used in the literature for real-time flood monitoring, flood modelling, mapping, and early detection systems, including the estimate of water level. The work makes further achievements by offering suggestions for more study. In particular, the paper makes recommendations on how computer vision and IoT sensor approaches might be used to improve the management and monitoring of coastal lagoons a topic that has garnered little attention in the literature .

Internet of Things (IoT) is essential to living spaces. The authors believe that telecom operators are better at providing IoT services than other companies, particularly in poorest countries where community concerns about security are the biggest roadblocks. This report discussed wireless carriers' future expectations for IoT services in emerging nations. The potential and challenges for telecom operators to provide these services were highlighted in this research. Additionally, a case study concerning telecom providers in Yemen was provided in this report. The MTN and Yemen Mobile operators were used as the sources for the case study. 73 engineers made up the study's sample population, and SPSS was utilised to analysis the information. The research found that Yemen Mobile (81.14%) and MTN (91.35%) respondents both agree that the operator's supply of IoT services opens up new revenue prospects. Moreover, the results in terms of current services that may be offered includes seven services from Yemen Mobile operator and eleven services from MTN .

The Internet of Things (IoTs) provides a future picture when computer systems, consumers, and things collaborate for comfort and financial gains by connecting digital and physical items via

modern communication technologies. Such a vision calls for constant security, privacy issues, authentication, and assault resistance. Blockchain, a decentralized ledger that keeps an accurate account of network transactions, may be used to add these attributes. In this paper, we provide a thorough analysis of how to adapt blockchain to the particular requirements of the Internet of Things (IoT) in order to create Blockchain-based IoT (BIoT) applications. We also attempt to present cogent picture of the present state-of-the-art initiatives in this area. After outlining the fundamental needs and features of IoT, the development of crypto currency is discussed. In this respect, we begin with a discussion of the core operating concepts of blockchain and how auditability, security, and decentralization are achieved in such systems. Additionally, we discuss the architectural design, security mechanisms, and most relevant BIoT applications. Our story is then developed based on the main IoT problems and the most recent steps taken to tackle them. In order to inform future BIoT researchers about the issues that need to be taken into consideration before implementing the next iteration of BIoT applications, some potential approaches are then listed .

The goal of the Internet of Things (IoT) is to turn commonplace physical things into a networked ecosystem with available at all times digital information. IoT "things" work together to provide smart and creative services on their own by integrating sensing, processing, and actuators capabilities. Different security risks produced by the IoT services' quick adoption must be properly addressed. To increase the security of IoT, a number of new and innovative technologies and strategies are presented. This paper will attempt to provide readers a current overview of the IoT security research areas that are constantly being studied. To clarify the sources of dangers in IoT, we first discuss common elements and protocols. Then, we provide a taxonomy of IoT threats and investigate the many levels of IoT security weaknesses. Then, we simply compare security protocols based on cutting-edge technologies including blockchain, fog-computing, edge-computing, software-defined networking (SDN), holomorphic and searchable encryption, but instead machine learning. Finally, security issues being covered and potential future study topics are identified for those who might be interested .

The way individuals engage in the virtual world, in their employment, and in their social connections has all been drastically altered by the internet. By allowing connections between smart things and people as well as between smart items themselves, IoT technology has given this process a fresh perspective and opened the door to conversations across any medium, at any time, from anywhere. By enabling them to communicate with one another, exchange information, and plan actions, IoT enables things to really see, hear, think, and carry out activities. The most crucial IoT components are then explored in detail, including IoT operating systems like Tiny OS, Contiki OS, FreeRTOS, and RIOT. Finally, IoT issues that academics have lately found are discussed, along with a summary of IoT applications. Findings: Research on IoT projects and literature demonstrates the overriding significance of technology in IoT initiatives, which are often propelled by technical interventions rather than novel business model developments. IoT expansion has raised a number of significant issues, notably in the areas of privacy and security. As a result, both the private sector and the public sector have started addressing these worries. Ultimately, what makes IoT intriguing is that we are still unsure about the precise use cases that might have a substantial impact on our lives. Originality/value: This

study offers a thorough literature assessment on IoT methodologies, platforms, and trends [10], [11].

DISCUSSION

The idea of an Internet of Things, where sensing and actuation functions smoothly fade into the background and new capabilities are made feasible by access to rich new information sources, is becoming closer with the proliferation of objects having communicating-actuating capabilities. The ability of users to build innovative new apps will determine how the next generation of mobile systems evolves. IoT is a perfect example of an emerging technology that may have an impact on this field by offering fresh, up-to-date data and the necessary processing power to develop ground-breaking applications.

This paper offers a user-centric cloud-based paradigm for achieving this objective by combining private and public clouds. The requirements of the end-user are prioritized in this way. We suggest a framework supported by a scalable cloud to provide the ability to leverage the IoT while allowing for the essential flexibility to fulfil the various and perhaps conflicting demands of different industries. The system keeps the networking, processing, storage, and visualization elements distinct, enabling autonomous evolution in each area while also complimenting one another in a communal setting. With Cloud at its core, the standardization that is taking place in each of these topics won't be negatively impacted. The new frameworks associated challenges, which include issues with privacy, security, and data management that must support such a platform in order for it to be genuinely viable, have been highlighted. These challenges range from the proper interpretation and visualization of the enormous amounts of data to other related challenges. By giving a comprehensive perspective of the integration and functional components that can create an operational IoT, the convergence of multinational projects is definitely expediting the development of an IoT.

CONCLUSION

The quality of life for people and the competitiveness of businesses are expected to significantly improve as little more than a result of the Internet of Things. The IoT has the possibility of allowing extensions and enhancements to fundamental facilities in commuting, logistics, security, utilities, education, healthcare, and other areas, while providing a new ecosystem for enterprise applications. This is accomplished through a widely dispersed, locally intelligent network of smart devices. With a shared knowledge of the unique nature of the opportunity, a coordinated effort is needed to propel the sector from its childhood into maturity. The distribution of services, business and billing structures, technical requirements for delivering IoT services, and the multitude of demands that these services will impose on mobile networks are all characteristic features of this sector. It is intended that through sharing a common knowledge of the IoT's features, industry participants would be better able to work together again to advance the market for the benefit of customers and society.

REFERENCES

[1] K. Lin, W. Wang, Y. Bi, M. Qiu, and M. M. Hassan, "Human localization based on inertial sensors and fingerprints in the Industrial Internet of Things," *Comput. Networks*, 2016, doi: 10.1016/j.comnet.2015.11.012.

[2] S. Park, S. Park, S. Park, and J. Byun, "Design of a mass-customization-based cost-effective Internet of Things sensor system in smart building spaces," *Int. J. Distrib. Sens. Networks*, 2016, doi: 10.1177/1550147716660895.

[3] M. Elkhodr, S. Shahrestani, and H. Cheung, "A middleware for the internet of things," *Int. J. Comput. Networks Commun.*, 2016, doi: 10.5121/ijcnc.2016.8214.

[4] Y. Khan, A. E. Ostfeld, C. M. Lochner, A. Pierre, and A. C. Arias, "Monitoring of Vital Signs with Flexible and Wearable Medical Devices," *Advanced Materials*. 2016. doi: 10.1002/adma.201504366.

[5] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio, and R. Prasad, "Satellite communications supporting internet of remote things," *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2015.2487046.

[6] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *Journal of Network and Computer Applications*. 2016. doi: 10.1016/j.jnca.2016.01.010.

[7] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) - Enabled framework for health monitoring," *Comput. Networks*, 2016, doi: 10.1016/j.comnet.2016.01.009.

[8] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, "Urban planning and building smart cities based on the Internet of Things using Big Data analytics," *Comput. Networks*, 2016, doi: 10.1016/j.comnet.2015.12.023.

[9] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networks in the context of the Internet of Things," *Comput. Commun.*, 2016, doi: 10.1016/j.comcom.2016.03.007.

[10] P. Zhang, Y. Liu, F. Wu, S. Liu, and B. Tang, "Low-Overhead and High-Precision Prediction Model for Content-Based Sensor Search in the Internet of Things," *IEEE Commun. Lett.*, 2016, doi: 10.1109/LCOMM.2016.2521735.

[11] R. Martac, N. Milivojevic, V. Milivojevic, V. Cirovic, and D. Barac, "Using internet of things in monitoring and management of dams in Serbia," *Facta Univ. - Ser. Electron. Energ.*, 2016, doi: 10.2298/fuee1603419m.

CHAPTER 15

AN EVOLUTION OF STACK ARCHITECTURE IN INTERNET OF THINGS

Dr. Ravindra Kumar, Associate Professor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id- ravindrak.soeit@sanskriti.edu.in

ABSTRACT

The Internet of Things (IoT) technology stack is nothing other than a collection of technologies, guidelines, and tools that span from the fundamental connecting of items to the apps that utilize them, the data they generate and share, and the many processes necessary to power them. The suggested strategy aims to bring together the advantages of horizontal approaches, which provide users the option to choose individual elements and create integration code, with those of monolithic vertical systems, where all IoT pieces are pre-selected, from the hardware to the cloud. Prototyping is only one of benefits of the suggested method since it is simple to turn a demonstration into a workable industrial solution. The research concluded with a real-world example that shows how the suggested stack is used to the construction of an IoT device that transforms conventional freezers into intelligent, network topologies.

KEYWORDS

Cloud, Internet of Things, Network Topologies, Stack.

INTRODUCTION

People and things are getting more and more linked as technology develops. Some of the fundamental concepts that make up such a scenario include machine-to-machine (M2M) connectivity and the Internet of Things (IoT). The IoT paradigm is built on connecting and exchanging data between applications and physical devices , connecting material things with the virtual world. The Lean Startup paradigm, a cutting-edge method of business design originating from the Lean Production Strategy, and IoT are expanding together. As a consequence, we support the process of common ones being reinvented and transformed into "smart" or "connected" products, which are physical objects with a streaming platform at their core. The personal, professional, and financial advantages for the whole society are significant as the number of these devices increases significantly[1]–[3].

In particular, wearable sensors based on low-cost, low-power microcontrollers are anticipated to be the accelerator for the Internet of Things (IoT) revolution by enabling the "smartification" of "Things" with the least possible effect on device hardware costs. But there is a striking divergence between Things and Devices. Fremantle defined Things as daily items integrated in

everyday environments, such as a vehicle, refrigerator, home, or city. Devices, which are often a component of a Thing, are sensors, actuators, or tags that have a computing unit. The "Smart Fridge," for instance, is a standard refrigerator with sensors for temperature monitoring, inventory tracking, and compressor control built into an electronic device that is often equipped with a WiFi network connectivity. On the other hand, the Smart Fridge is also required to be connected to a cloud service that allows the end user to control and communicate with the system via online or mobile interfaces in order to be useful [4]–[6].

IoT Architectures and Business Models

Two distinct business models for IoT software architectures arose with the rise of smart IoT devices: vertical and horizontal. The sensors and actuator nodes that constitute an IoT device in the vertical method are quite often linked to the Internet either directly or via a local gateway. Monolithic vertical offerings are then created by coupling these component to exclusive cloud-based services. Such a strategy benefits the end-user in two ways: it lessens compatibility issues in between different system components, and it centralizes the support center to a single source.

The complete reliance mostly on vendor for any technical modification, update, or upgrade of the final product is unquestionably a drawback. Many IoT firms that specialize on B2C (Business-to-Client) have embraced this model since it is easier to manage and sell. In this scenario, the end-user of the solution also happens to be the product's ultimate customer. On the other perspective, a horizontal approach may foster innovation and development while ensuring high levels of flexibility, scalability, and customization. For this reason, in B2B (Business-to-Business) situations when the smart product is simply created by a business and then produced by system integrators, hardware, and ICT firms, the horizontal method has been chosen. From a software perspective the major cloud providers choose extremely broad horizontal cloud-based services that are scalable to a variety of products and applications [7], [8].

Such deals, though, often don't really have anything to do with hardware. In fact, this strategy perfectly aligns with the business model of cloud providers: directing users towards a fully cloud-based, pay-per-use platform as a service (PaaS) architecture where IoT nodes are viewed as unimportant, remotely controlled objects designed to produce as many data streams as possible. Additionally, these methods are often unsuitable for the creation of a smart product that is focused on the needs of the consumer since local intelligence and computation are essential for ensuring the adoption of appropriate smart behaviors. In order to keep given services functioning even in the event of a brief network breakdown, smart goods must provide offline use and local data storage i.e. control of a smart fridge, security alarm monitoring, etc.

Regarding the hardware, prototype solutions that lower the barrier to entry for controlling and programming embedded devices for IoT applications play a significant role in accelerating the development process and meeting the industrial-grade standards. Depending on the technique used, these solutions may be divided into two categories which is solutions operating on proprietary hardware, and solutions running on generic hardware. Examples of solutions designed for proprietary hardware are Ppaper and Onion. Ppaper1 offers a line of MCU (Micro

Controller Unit) based boards that are prepared to link to a proprietary cloud and enable rapid creation of smart product prototypes using a C language comparable to Arduino.

On the MCU side, several software frameworks recently created that can operate on many IOT hardware platforms, such as Micropython3 and Zerynth4 VM (Formerly Viper VM). Micropython is an MCU-based Python interpreter that makes it simple and rapid and create embedded Python applications. Manufacturers may quickly test the functionality and peripherals of embedded devices from a serial port simulated terminal prompt by simply writing Micropython scripts on the board's serial port terminal. VIPER (Viper is Python Embedded in Realtime), a cross-platform virtual machine for MCUs that enables Written in a programming for MCU devices with real-time capabilities, a very small footprint, and low memory utilisation, was created by the authors themselves in 2014. A completely horizontal, modular, scalable, and adaptable IoT development stack is still needed in the given environment to expedite the creation of smart goods for IoT. A system that offers the capability of quickly programming embedded devices that are organically linked to cloud-based PaaS, where data governance modules, rule engines, data visualization tools, and mobile App connection frameworks are already integrated and accessible for usage.

Generic IoT stack

We suggest a common layered model similar to the OSI or the transmission control protocol (TCP)/IP models being used conventional networks in order to analyze IoT protocol stacks in depth. Our suggested approach borrows heavily from these well-known concepts while being adjusted to work with IoT protocol stacks. The seven levels of the OSI model, which are shown in, range from the physical layer to the application layer. The presentation layer and the session layer provide enough characteristics for traditional information technology (IT) networks, but they are generally explicitly defined or implemented in Internet of Things (IoT) systems. As a result, we might choose take these layers away from basic IoT stack. The TCP/IP paradigm offers a 4-layer stack, from the application layer to the network interface layer. To decide how a computer should be linked to the Internet, this model is utilized, however. Furthermore, it could be difficult to change protocols and used this architecture, such TCP to UDP[8], [9].

All IoT protocol stacks reported in this survey are compared using this methodology. From the physical layer (PHY layer) to the application layer, the model is made up of five levels. Each layer offers the following features: The radio frequency (RF) operations are specified by the physical and data-link levels, routing and security are defined by the network layer, and protocol instructions are specified by the transport and application layers.

IoT Protocol Stacks

This section presents IoT protocol stacks that have been characterized using the standards defined in the part before. For this study, we opted to emphasis on nine recently developed protocols: open stack for IoT (OS4I), BLE, Zigbee, Z-Wave, WirelessHart, LoRaWAN, and Sigfox. These protocols have all been extensively implemented, have been investigation by

researchers or hackers, and try to provide security features. We contemplated incorporating narrowband Internet of Things (NB-IoT), but we came to the conclusion that it was unnecessary for a study because of the lack of current incarnation, use, and security studies. We first define the stack structure for each protocol stack that is shown, then we provide the corresponding routing strategies, and lastly we analyze the security model. The five requirements listed herein are labelled on each stack tried to present.

IoT Attack Study

IoT devices are embedded technology devices come with a system operating system and software. Additionally, these gadgets communicate with other devices and are linked with each other. The likelihood of IoT security vulnerabilities is implied by all of these qualities, and these vulnerabilities may be assessed using the conventional confidentially, integrity, and availability principle:

- **Confidentiality**

Ability to prevent access to information by persons who are not authorized.

- **Integrity**

The ability to verify that communication system remain unaltered from the source to the destination.

- **Availability**

Information's ability to continuously be easily available by organizations with access rights. In the next sections of this work, we exclusively discuss assaults on availability that are undertaken by an attacker and exclude those attacks brought on by natural calamities.

We see IoT systems as networks of mobile networks with a particular topology or design. Every device is capable of communicating with all the other device using one or more protocols to exchange data. In addition, even if IoT devices may have a variety of software difficulties, our attention is drawn to vulnerabilities in communication and protocol. Software difficulties are often not unique to IoT but rather standard IT challenges.

Focus on Packet Security

The initial aspect of the kill chain is packet security. Getting information or maybe even taking control of a gadget represents what this phase entails. As previously stated, we purposely only take into account vulnerabilities affecting telecommunication and protocol so instead of software exploitation. As a result, this approximate analytical solution cryptographic assaults, which target transmission from and to a device. We differentiate between passive and aggressive cryptography assaults. Unlike sending a message, passive cryptographic attacks comprise stealing secrets or personal information from intercepted frames. There is no chance of compromising the network's availability or integrity since nothing is done inside of it. The secrecy is instead jeopardized by passive cryptographic attacks which thus steal data from devices via listening. Active cryptographic attacks allow an attacker to change communications

sent across the network. In order to disrupt the network, the attacker may also inject traffic by replaying or forging information. Therefore, the three principles of secrecy, integrity, and availability are the target of an active assault.

i. **Passive Cryptographic Attacks**

Traffic interception is a common risk for wireless communication systems. One way to guarantee that transferred data is shielded from unauthorized access is via encryption. Using the terminology "attacking no cryptography," "ugly cryptography," "poor cryptography," and "good cryptography," we differentiate four different types of cryptographic assaults.

ii. Active Cryptographic Attacks

Even with the best implementations of a cryptographic standard, data security cannot always be completely maintained. For a network to be secure, additional procedures are necessary. An attacker must inject incoming packets or tamper with already-existing nodes in the network to determine if these techniques are present.

LITERATURE REVIEW

Internet of Things (IoT) has emerged as one of the most significant technologies in use today. It offers the human race excellent answers in many important spheres of life. IoT refers to a group of sensors or objects in the universe that have the capacity to communicate with one another over the internet without the assistance of a person. The review's results demonstrate that early IoT designs lacked a full definition of the IoT's nature, but more modern IoT architectures express a comprehensive definition of the IoT that begins with data collecting and ends with data dissemination. The results also show that IoT design has changed significantly over time, with new solutions being added to the architectural stack to address issues with scalability, interoperability, extensibility, management, and other IoT concerns without taking security measures into account. The results show that none of the IoT designs under discussion take privacy issues into account, despite the fact that this is thought to be a crucial component of IoT viability and success. As a result, while creating IoT architecture, security and privacy solutions must be taken into account .

The horizontal integration of IoT devices, which create silos based on vendors or protocols, is what is meant by interoperability. To address this, an architectural solution for an autonomic interoperability manager (AIM) that can self-configure, self-heal, self-optimize, and self-protect is shown in this short. AIM enables collaboration and interaction amongst IoT devices with different protocols, syntaxes, and semantics, and its plugin-based autonomic, service-oriented design provides scalability and extensibility. To show how the AIM significantly lowers the average reaction time in a highly dynamic environment, we simulated a healthcare use-case using a variety of virtual IoT devices. This was done by actively pruning the network traffic and optimizing the computation resources .

Internet traffic increased substantially with the advent of the Internet of Things (IoT). Growing connection produced several network flaws and led to numerous cyber-attacks. Despite the existence of various security features, these fatalities cannot be avoided by the current network

stack. Almost all of the network weaknesses in the current wireless stack are to be eliminated by the secure network architecture proposed in this research. It is built on the Recursive Internetworking Architecture (RINA), a potential solution that has been under development for a lengthy period of time by researchers. RINA architecture's capabilities and characteristics may replace the existing communication technology with something more secure. The suggested solution was created in a closed environment, such a LAN, using the RINA architecture. It validates RINA characteristics that successfully thwart network flow assaults .

The through innovative services and seamless interaction across heterogeneous devices, the Internet of Things (IoT) is crucial in bridging the gap between the physical and digital worlds. Utilizing green initiatives for IoT is still difficult, however, since as the technology grows in scope and complexity, the present trends become less relevant. Similar to this, using 5G to provide green communication introduces additional difficulties in effectively moving vast amounts of data. This chapter proposes a plan for green IoT in a 5G network to overcome the aforementioned difficulties. Green IoT is achieved in a cluster by grouping mobile nodes. Additionally, a mobility management model is created to aid in effective handover and the selection of the best networks using multi-criteria decision modelling. Then, we create a system architecture that combines the green IoT with the 5G network. Additionally, it facilitates effective, low-energy communication with other heterogeneous networks. The proposed protocol stack, which maps Internet Protocol (IP), Medium Access Protocol (MAC), and Location Identifiers, also supports the 5G network design (LOC). Utilizing the C programming language, the suggested system is built, and a thorough mathematical and statistical analysis is done in regards to cost, energy use, and service quality .

Internet of Things (IoT) is a vast network of many heterogeneous devices that offers a variety of cutting-edge applications and solutions. IoT networks allow for the seamless interconnection of cyber and physical systems via the integration of data and services. However, there are tremendous hurdles in this field because to the variety of devices, underlying technology, and lack of standards. This research study seeks to provide a full overview of the supporting technologies and standards that make up the IoT technology stack in light among those difficulties. First, a tiered architectural approach is described, with each layer discussing current research and outstanding issues. The next section of this research study focuses on the function of software platforms in the creation and integration of IoT applications. This paper also discusses unsolved problems and provides detailed instructions for IoT stack optimization. Finally, by reviewing ongoing research and open problems in this field, the incorporation of fog/edge networks with the IoT technology stack is comprehensively examined. The primary goal of this research is to give an in-depth analysis of Internet of things, the related middleware, and the networks needed to create applications that are future-proof .

Internet of Things (IoT) presents a future Internet whereby people, computer systems, and commonplace items with sensing and actuating characteristics work together with previously unheard-of ease and financial advantages. The ubiquitous networking of devices in the framework of IoT applications will be made possible through IP-based communication channels, much as with the existing Internet architecture. These technological devices are being created in

accordance with the limitations of the sensing platforms that IoT applications are expected to use, resulting in a communications stacking that can offer the necessary power, efficiency, reliability, and Wifi connection. Mechanisms must be developed to safeguard communications made possible by such capabilities since security will be a basic enabler of most IoT applications. This research explores open research questions as well as current protocols and procedures for IoT communication security. We examine the fundamental security criteria that are met through current technologies and the protection of IoT communications, as well as the unresolved issues and development plans for the future .

Industry sources, corporate executives, and business executives all agree that the next industrial revolution, which is about to begin, has been one of the most disruptive and consequential in human history. Without a doubt, one of the foundations of this industrialization is automation. Customers generally prefer automatic versus manual systems. The Internet has become seamlessly integrated into modern life. Life alone cannot be imagined without the Internet. In this paper, we will show you an automated system that uses the Internet of Things, a rapidly expanding new Internet technology, in the real world (IoT). An IoT-based automation system improves the efficiency, speed, and security of the consumer's life. By employing a web browser and a connection to the internet, this state-of-the-art technology enables the user to fully control all of the house items and appliances from anywhere on the globe. The simulation we constructed for this study is a crude representation of a much bigger real-world system, but the concept, technique, and methodology are the same .

The automation of smart buildings and housing has greatly benefited from the Internet of Things (IoT). IoT, cloud computing, and rules-based data are additionally used in the management of smart buildings and residences to guarantee the safety, accessibility, and comfort of just about everyone who uses the space. This research showed that once radio band interference affected the commands and control signals communicated through electrical wiring, the use of IoT for intelligent home automation was more fully adopted in the twenty-first millennium. IoT is determined to improve smart home governance by trying to ensure that home electronics and appliances can be truly controlled remotely and in a practical, secure, and comfortable fashion. IoT, cloud computing, and rules-based real-time evaluation were combined by the author to investigate the case of various devices and devices for command and control purposes. Fire protection connections, security cameras, smart TVs, lighting controls, home automation, air conditioners, doors, fans, and moisture control and gas management systems are among the devices that are taken into account for this evaluation. When it comes to smart home automation without the use of IoT the above tools and equipment operate incorrectly. The use of IoT has optimized the functionality and automation of home and construction equipment and systems to ensure that they efficiently and effectively provide the security, comfort, and access needed for a smart campus, as this study concludes by telling.

Smart home devices have become increasingly popular as daily living has been smoother as a result of quick technology advancements. Almost everything has been automated and digitalized. To facilitate numerous house automation, a system for interconnecting sensors, actuators, and some other data sources is presented in this dissertation. The system, designated as q-Toggle,

relies on the robustness of an Application Programming Interface (API), the backbone of a straightforward and widely used communication scheme. Q-Toggle often embedded sensors or actuators that have upstream internet connectivity and perform the Q-Toggle API. The majority of Q-Toggle's devices are designed on Raspberry Pi boards and/or ESP8266/ESP8285 chips. A smartphone application has been developed that allows users to control a series of home appliances and sensors. The q-Toggle system is user-friendly, flexible, and can be further developed by using different devices and add-ons.

Bluetooth mesh, focuses on the Internet of Things and is based on the Bluetooth low energy protocol stack design. Even though it is still under development, it provides a fantastic option for commercial and industrial lighting applications. The Bluetooth mesh network's strengthening of confirmation message receipt is one of its main hurdles. Determine the Status of the received messages in a Bluetooth mesh network since numerous devices responding at once, as in certain lighting purposes, might cause unanticipated problems. This tendency, particularly as the number of devices in the network rises, may lower the likelihood that information will be delivered because of collisions. This paper suggests a novel method of distributing Status over time in order to improve the accuracy of receiving send and receive messages in a Bluetooth mesh network. We compare our method with an experimental Bluetooth mesh network with actual nodes in order to assess the performance of the suggested strategy. 98.84% of the Status was received for the connection with our optimum configuration, and 96.98% for those with the SC, as measured by our findings' packet-loss rate. Finally, an extensive performance assessment approach was also used to analyze the lost Status.

Artificial Intelligence (AI) is transforming school education. The study's concentration was on the use of AI and its effects in administration, education, and acquisition. It was built together around the narrative and methodology for evaluating the AI established during the initial investigation. The intention of the study was successfully realized through the employment of a qualitative research method that utilized the reviewed literature as a design and methodology. Computers, robots, and other artifacts now include human-like intelligence that is distinct from cognitive abilities, learning, flexibility, and decision-making, thanks to the research area known as artificial intelligence and in fact inventions and advancements. According to the report, AI has been generally recognized and employed in various ways in education, especially by higher education institutions. Initially, AI was demonstrated by computers and computer-related technologies. It then managed to evolve into web-based and web-based intelligent higher education, and eventually, with the use of embedded personal computers and other technologies, bipedal robots and web-based chatbots were used to perform the duties and tasks of the teaching staff to complete. Alone or together with teachers [10], [11].

DISCUSSION

The design of the sensors is the first thing to take into account. Although there may not be much of a selection when it comes to the sensors themselves, there is undoubtedly a wide range of options available when it comes to the processing and networking capabilities that are included with the sensors. Our options vary from tiny boards designed for sensor motes to 300–500 mW-consuming Arduino or Atom boards. The decision we make here is based on how much analytics

and data preparation we want to undertake at the sensor level. Second, there is the logistical challenge. We require board design skills, which may not be easily accessible, to produce a sub-mW board. Therefore, it could be wise to include a sensor in a kit with an integrated CPU that is readily accessible from vendors. Communication is the next crucial factor to take into account. The main problem with IoT nodes is electricity. The choice of networking technology is crucial since a significant portion of the total power is used for sending and receiving messages. The distance between the transmitter and the receiver, the kind of obstructions, signal distortion, background noise, and regulatory rules are the crucial elements that we need to take into account. We must choose a certain wireless networking protocol based on these important considerations. For instance, Zigbee may be used to communicate just inside a small building, but Sigfox or Lora-WAN should be used to communicate throughout a smart city. The frequency and power that may be used for transmission are sometimes subject to substantial limitations as well. Governmental organizations primarily impose these restrictions. All of these considerations must go into the decision-making process.

CONCLUSION

The first decision to be taken is whether to use a proprietary solution or an open source middleware like FiWare. Both have advantages and disadvantages. Although open source middleware is, in principle, more versatile, they could not have full compatibility for Internet of Things (IoT) devices. Even though it would be ideal, not all communication protocols and hardware may be compatible with middleware solutions. Therefore, a proprietary solution is preferable if we want stringent compatibility with certain devices and protocols. Open source solutions, however, often have lower costs and are simpler to implement. Additionally, we must decide on the communication protocol and confirm that it is compatible with the firewalls used by the participating businesses. In general, from this perspective, using a protocol based on HTTP is the best option. Additionally, we must decide between TCP and UDP. When it comes to power usage, UDP is always preferable. We also need to take into account querying languages, capability for creating dynamic warnings, and alternatives for storing sensor data streams. Let's move on to the application layer. The majority of IoT frameworks provide a substantial quantity of assistance for developing the application layer. This comprises APIs for data processing, data mining, and data visualization. These days, it's relatively simple to create data smashups and dashboards because to the substantial assistance offered by IoT frameworks. However, in this case, there is a trade-off between the resources needed and the functionalities offered. If we don't require a lot of functionality, we don't need a particularly robust framework. These decisions must be made by the programmers of the application.

REFERENCES

[1] R. F. Babiceanu and R. Seker, “Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook,” *Comput. Ind.*, 2016, doi: 10.1016/j.compind.2016.02.004.

[2] K. Lin, W. Wang, Y. Bi, M. Qiu, and M. M. Hassan, “Human localization based on inertial sensors and fingerprints in the Industrial Internet of Things,” *Comput. Networks*, 2016, doi: 10.1016/j.comnet.2015.11.012.

[3] S. Park, S. Park, S. Park, and J. Byun, "Design of a mass-customization-based cost-effective Internet of Things sensor system in smart building spaces," *Int. J. Distrib. Sens. Networks*, 2016, doi: 10.1177/1550147716660895.

[4] I. Ungurean, N. C. Gaitan, and V. G. Gaitan, "A middleware based architecture for the industrial internet of things," *KSII Trans. Internet Inf. Syst.*, 2016, doi: 10.3837/tiis.2016.07.001.

[5] D. Linthicum, "Responsive Data Architecture for the Internet of Things," *Computer (Long. Beach. Calif).*, 2016, doi: 10.1109/MC.2016.302.

[6] A. Alghadeir and H. Al-Sakran, "Smart Airport Architecture Using Internet of Things," *Int. J. Innov. Res. Comput. Sci. Technol.*, 2016.

[7] G. Marques and R. Pitarma, "An indoor monitoring system for ambient assisted living based on internet of things architecture," *Int. J. Environ. Res. Public Health*, 2016, doi: 10.3390/ijerph13111152.

[8] T. Ara, P. Gajkumar Shah, and M. Prabhakar, "Internet of Things Architecture and Applications: A Survey," *Indian J. Sci. Technol.*, 2016, doi: 10.17485/ijst/2016/v9i45/106507.

[9] A. Zimmermann *et al.*, "Decision case management for digital enterprise architectures with the internet of things," in *Smart Innovation, Systems and Technologies*, 2016. doi: 10.1007/978-3-319-39627-9_3.

[10] S. Sicari, C. Cappiello, F. De Pellegrini, D. Miorandi, and A. Coen-Porisini, "A security- and quality-aware system architecture for Internet of Things," *Inf. Syst. Front.*, 2016, doi: 10.1007/s10796-014-9538-x.

[11] Y. Xu and A. Helal, "Scalable Cloud-Sensor Architecture for the Internet of Things," *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2015.2455555.

CHAPTER 16

AN EVALUATION OF CLOUD COMPUTING IN INTERNET OF THINGS

Dr. Sundar Singh, AssistantProfessor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id- sundar@sanskriti.edu.in

ABSTRACT

The Internet of Things (IoT) connects a significant number of devices to the Internet, producing massive amounts of information. It is suggested to utilize cloud computing to store, analyze, and manage access to this data because those devices have limited resources. Since private information about users may be gathered by IoT devices and transmitted to the cloud, privacy is a key issue with this integration. Therefore, it is crucial to provide systems that let individuals handle how their data is used. An analytical and experimental assessment of the suggested method's performance against all the other methods that exist in the literature compares its outcomes in terms of delay and energy usage.

KEYWORDS:

Cloud Computing, Cloud Service, Internet of Things, IoT Devices, Sensor Network.

INTRODUCTION

The Internet of Things (IoT) was made available by latest developments in wireless communications and the simplification of electronic components, which led to a situation in which most devices are online. It is estimated that billions of items will link to the Internet in the future, offering consumer's perhaps widest range of information and services. Whereas IoT devices will be present in a variety of settings, sensor devices are often what create IoT networks possible. A Wireless Sensor Network (WSN) is made up of a number of embedded systems that each include a quad core chip, a sensor for interacting with the outside environment, and a wireless communication antenna. WSN devices often have constrained space and power sources, hence the network stack has to have a minimal processing overhead. Although certain Internet of Things (IoT) devices are also not sensors and have a limitless supply of energy, their size and processing power are often restricted. Even though most IoT devices have limited capabilities, an architecture has been developed that harnesses cloud computing to carry out a number of activities, including storing, processing, exposing, and controlling access to data produced by IoT devices. Data privacy issues are raised by this integration, also known as Cloud of Things (CoT), since information is transmitted from the user's control sphere to the cloud. Therefore, it is crucial to provide the user the tools to manage how his data is used in the cloud[1]–[3].

The CoT designs that have been researched either do not provide security methods within the IoT network, like UPECSI and Sensor Cloud, or do not assess the burden such techniques place on the limited IoT devices, like our newly described architecture, hereafter referred to as PROTeCt: A privacy infrastructure that extends UPECSI to offer security within the IoT network

is needed for the integration of the internet of things and cloud computing. Briefly stated, the UPECSI structure allows use of a gateway to collect data from the Iot environment and then employs security and privacy protocols to provide user control over his data after it has been stored in the cloud. The UPECSI does not specify any security measures for internal IoT network connections. By shifting the security and privacy controls from the gateway to the IoT devices, PROTeCt expands UPECSI. This protects the whole communications and offers precise access to the data once the cryptographic algorithms are implemented by each IoT device rather than centralized in the gateway. Since the gateway is not given access to plain-data, it is unable to compromise the system's security once an attack is successful. Additionally, a simple precursor crash does not affect the system's availability because the improved architecture doesn't somehow contain this single point of failure[4]–[6].

This approach increases network security and reliability. One or more gateways may nevertheless carry out other support functions like protocol translation even while they don't apply privacy and protection methods to the user's data. While PROTeCt enhances UPECSI security, it also places more demands on IoT devices. If these devices lack the processing ability to handle all security-related procedures, this might negatively influence network performance or even block the deployment of the network. In fact, defining the external controller by PROTeCt is one of the objectives of this study. Additionally, this paper suggests an improved approach for a secure channel that PROTeCt uses, known as Enhanced PROTeCt or EPROTeCt, in an effort to boost PROTeCt's overall performance. By using an application layer prevent the formation rather of a secure transport layer protocol, which might increase communication overhead, this strategy attempts to reduce the processing burden on IoT devices. This study makes at least three major additions to the frameworks already mentioned:

A. It discusses PROTeCt, stressing its key distinctions from UPECSI, and suggests an improved implementation for this architecture, named E-PROTeCt, which frees up the IoT devices' cryptographic processing.

B. It gives a quantitative study of the expenses associated with putting security and privacy controls in place right at the IoT devices.

C. Through simulations carried out in the ns-3 network simulator, it gives an experimental assessment of different topologies in terms of end-to-end latency and energy consumption (device life time).

The Internet of Things (IoT) is a network of connected computing devices, mechanical and digital machinery, items, animals, or people that may exchange data across a network without needing human-to-human or human-to-computer contact. To put it simply, the internet of things may refer to anything from a person with a heart monitor implant to a car with built-in sensors that warn the driver of impending danger. The Internet of Things (IoT) refers to any artificially or naturally occurring thing that may be assigned an IP address and given the capability to send data across a network. IoT has developed as a result of increased data production. There will soon be billions of linked machines and gadgets joining human users as a result of the Internet of Things Cloud

The necessity for the internet of things is clear. Precision agriculture, healthcare, energy, transportation, building management, and other sectors have all basically been overtaken by IoT. For electrical engineers and application developers, internet cloud services are offering an enormous expansion of connection alternatives. Work is being done on Internet of Things (IoT) technologies and items that will easily aid in higher growth.

However, the devices linked to the network to offer information they acquire from the environment is what makes IoT the next step to success. Greater connection of the devices alone does not assist people. By reaching out to and interacting with the world, connectivity offered by cloud services enables the gadgets to deliver vital information. Through internet cloud services, linked devices may range from small, personal devices that each person uses to large ones, so they are not only restricted to those that businesses possess.

IoT and cloud computing for Future Internet

However, it is still unclear how the gadgets would stay linked throughout. The internet of things cloud service's connection holds the key to the solution. Increased use of IoT in the cloud has sped up the creation and implementation of scalable IoT applications and business models. IoT and cloud computing are now two strongly interconnected future internet technologies, with one laying a foundation for success for the other. The integration of IoT with cloud computing has produced a number of advantages.

Providing Infrastructure

IoT in the cloud provides public cloud services, which by giving other parties access to the infrastructure, may readily assist the IoT sector. Therefore, IoT data or computational components using IoT devices may benefit from integration. Enhanced Scalability: IoT devices need a significant amount of storage in order to exchange information for beneficial uses. IoT in the cloud, such as the StoneFly Cloud Connect to Microsoft Azure, may provide clients more capacity, which can be expanded in response to user demand. Assisting clients in meeting their storage demands.

A. Increased Performance

IoT devices create a lot of data, and in order to communicate and connect with one another, they need very high performance. IoT in the cloud offers the connection required to quickly transmit information between devices and interpret it.

B. **Pay-as-you-go**

Infrastructures for Internet-based cloud computing assist IoT in making sense of the larger volume of produced data. Users need not worry about purchasing more or less storage. With Internet Cloud Computing, companies can quickly extend the storage as the quantity of data created rises and only pay for the storage they use.

Role of Cloud computing in IoT

i. Enables Remote Computing Capabilities:

IoT minimises reliance on on-site infrastructure because to its vast storage capacity. Cloud computing has been more popular as a result of ongoing advancements in internet-based technology, including the internet and the devices that enable sophisticated cloud solutions. Cloud solutions, which are jam-packed with IoT, provide businesses the opportunity to quickly and easily use remote computing services.

ii. **Security & Privacy**

With cloud technology and IoT, tasks may be completed automatically, helping enterprises significantly lower security hazards. An IoT-enabled cloud technology is a system that offers control that is preventative, investigative, and remedial. It also offers consumers excellent security mechanisms with efficient authentication and encryption. IoT goods employ protocols like biometrics to manage and secure user identities as well as data.

iii. **Data Integration**

In addition to seamlessly integrating IoT and cloud, recent technological advancements also provide real-time connection and communication. As a result, it is simple to extract real-time data on crucial business activities and carry out on-the-spot data integration thanks to constant connectivity. The volume of data created from various sources, as well as its centralised storage, processing, and analysis, may be handled by cloud-based systems with strong data integration capabilities.

iv. **Minimal Hardware Dependency**

Currently, a number of IoT solutions provide plug-and-play hosting services, which are made possible by fusing the IoT with the cloud. To support the agility needed by IoT devices, cloud-enabled IoT hosting providers do not need to depend on any form of hardware or infrastructure. Organizations may now effortlessly integrate large-scale IoT strategy across platforms and transition to Omni channel communication[7], [8].

v. **Business Continuity**

Cloud computing solutions, which are renowned for their adaptability and dependability, can guarantee company continuity in the event of any emergency, data loss, or catastrophe. Cloud services function via a network of data servers spread over many different places that store numerous copies of backup data. IoT-based activities continue to function in the event of an emergency, making data recovery simple.

vi. Communication Between Multiple Devices & Touch point

To carry out activities that are made possible by cloud solutions, IoT devices and services must connect to one another and exchange information. The cloud and IoT are able to communicate with other connected devices via offering a number of reliable APIs. Using cloud-based communication speeds up the contact and makes it more fluid.

vii. **Response Time & Data Processing**

Response times and data processing rates are often shortened and increased when edge computing and IoT technologies are coupled. For best use, IoT implementation with cloud computing and edge computing solutions is necessary. Although cloud computing services help speed up IoT development, correctly using these services presents several difficulties. There are a few challenges that need to be resolved before combining IoT with cloud.

Challenges the Cloud & IoT brings Together

i. Large Amount of Data:

Processing a lot of data may be demanding and daunting, particularly when several devices are interacting with the system at once. This may jeopardise the application's overall performance. So it is recommended to constantly check the system and back up your data.

ii. **Network and Communication Protocol:**

IoT and cloud devices use a variety of protocols to communicate across various touch points. Because it is an internet-based business, managing the shift may sometimes be challenging. In such circumstances, internet accessibility through wi-fi and mobile Internet may assist in resolving any difficulties encountered owing to connection concerns.

iii. **Sensor Network:**

Sensor networks enhance the advantages of IoT by enabling users to interpret and comprehend the IoT environment. But one of the biggest problems these networks confront is consistently digesting growing amounts of data.

Cloud Desirable for IoT

We have just spoken about the advantages of utilising the cloud for IoT so far. Let's quickly review them before examining the issues:

A. Lower infrastructure and up-front expenses

B. Pay-as-you-go for compute and storage

C. High availability and scalability of the system

D. Extended battery life for sensors and devices

E. Capability to combine a lot of data

F. Anything connected to the internet may be made "smart"

However, there are valid worries about cloud computing

i. **Ownership of the Data**

Do you or the cloud provider own the data that you keep in a company's cloud service? For Internet of Things (IoT) applications involving personal data, like healthcare or smart homes, this might be of utmost importance.

ii. **Potential Collisions**

The IoT application won't function if the connection is broken or the cloud service itself breaks. For certain IoT applications, such as smart agriculture, short-term inoperability may not be a major concern, but it could be disastrous for others. Health and safety-related apps shouldn't break for even a few seconds, much alone many hours.

iii. **Latency**

Data transmission to the cloud and command transmission back to the device both require time. These milliseconds may be crucial in certain IoT applications, such as those involving health and safety. Autonomous vehicles are a nice example. You shouldn't have to wait for the automobile to communicate with the cloud before deciding whether to swerve out of the path if a collision is about to occur.

LITERATURE REVIEW

IoT system that will automatically communicate essential information of customers once shockwave detecting sensor nodes are engaged, decreasing catastrophe evaporation rate and alerting adjoining local emergency responder's authorities about the geographical event location. P. Choudhary and P. K. Dwivedi develop a sustainable urban transport system and use a roadside component. It uses substitute routing and circumvent traffic problems, generate greater movement of vehicles through IoT, and reduce the traffic density. It also involves the use of statistical assessment techniques which would include humongous methodologies.

Scalable-Enhanced-Road-Side-Unit (SERSU), who's incorporated a wireless communication network and therefore an electromagnetic radiation responsive signalized intersections technology, environmental remote monitoring, and environmental communications network. SERSU elements were positioned anywhere along roadside without varied interruptions, with the automotive sensors component recording every produced data from the sensor. Which work at modern automotive engineering, the World Wide Web (www), and associated immediate and long term interconnections, as well as a descriptive history about the use of electronic equipment in automotive and the societal possible consequences of these advancements of an emission spectra sensor system that incorporates infrared radiations generated by motorists on the transportation surface and monitoring traffic flow and recommends alternate motor vehicles routing patterns to passengers to traffic composition .

An analogous platform that combines average new car speeds to modify the current road markings related to traffic density. That each vehicle throughout this developed framework is furnished and an On Board Device (OBD) that involves sending information to the central server through the use of the Zigbee technology, something that collects linear acceleration data and an

intelligent traffic control system for communications between urgent situation vehicles and between vehicles, reducing the pressure and continuing to increase signalized intersections predictability. The recommended analysis takes into consideration the significance of something like the vehicle based on the type of occurrence, but there is a need to protect messages from hijacking. Some shortcomings in conventional intelligent transport system have been cited as reasons to choose Radio Frequency Identification (RFID), monitoring devices, and communications technology over classical intelligent transport system. Because of the tremendous advancement of technology and computer systems, we use Computer-Human Interaction in every aspect of our everyday life. The proposal and employment of collaborative whiteboards are part of the multidisciplinary field of examination known as human-computer interaction. Human behavior, psychology, scientific method, computer technologies, software engineering, biomechanics, industrial design, sociology, and instructional sciences are just a couple of the fields that have connections to the field of human-to-human computer interaction. The user, task, tool, and environment are the four essential parts of the human-computer interdisciplinary approach. With the aid of planning, testing, and operational plans, interactive technologies are to be established. Usability is a requirement for the advancement of interactive technology. By combining the evaluation of usefulness, efficiency, and happiness, usability may well be evaluated. How well users seem to be able to do the things assigned to them while using the program is one measure of its effectiveness; efficiency and duration of the user work; The term satisfaction expresses how the respondents feel about the program after using it [9], [10].

Digital media manifestations are continuing to evolve with the aid of science and technology, ushering in a brand-new age and propelling the advancement of computer-computer communication technology. The development of the medium of interaction and associated field implementations are still understudied in the domain of visual interaction blocky graphics and related technologies. This paper concluded to examine the visual interaction development process, possible applications, and related technologies from a technical standpoint. The author addressed how to better connect the visual dependent on application with creative design in combination with the technological advancement of digital media art, and we discussed the critical components of the architecture, technology, and manufacturing methods of visual interactive works. This paper will also develop an image processing model for the communication tool of a human-computer interface, harvest boundary requires identification using the edge contour method for feature extraction combined with merge fusion technology to improve the processing of the visual language information, and create a perimeter package for the visual communication image. The network method makes the interface for human-computer interaction communication tools as efficient as possible. The test outcomes show that this approach may large and positively the integrity of its visual communication, increase the output of the interface's discriminate capability, and various performance metrics in the commenting of visual interactive works .

The multidisciplinary field of human-computer interaction has attained threshold status. The use of human-computer interaction in construction site management has increased throughout the fourth industrial revolution, which has substantially accelerated the advancement of hazard recognition in construction projects. The findings indicate that over the past 20 years, hazard

recognition has benefitted immensely significantly from the use of human-to-human interaction. In addition, several entirely new research areas have now been created as a result of this work, including the multimodal neurobiological data analysis in hazard acknowledgment experimental studies, the creation of perceptive policies and antennae, and the development of a human-computer-interaction safety management system based on big-data. Future examination courses will focus on virtual reality, biomechanics, computer vision, and computational analysis. In this study, they constructed a conceptual base that reflected the findings of previous studies and their connections, and we made submissions for the practical enhancement of human-computer communication in the area of danger assessment in the future.

Mobile devices are still perceived as restricted computing devices despite the significant advancements and improvements they have witnessed. Users nowadays are increasingly demanding and anticipate that their smartphone devices will run computationally demanding apps. Mobile cloud computing consequently combines mobile and cloud techniques to increase connectivity options by adopting offloading approaches. By offloading the task to more complex technologies with superior performance and resources, computation offloading addresses the disadvantages of smart mobile devices, also including limited battery life, computing capabilities, and storage space. The contemporary offloading frameworks and computationally offloading strategies are examined in this research along with an examination of their practices that help to maintain challenges. Additionally, it examines other significant application elements, such as the partitioning level and offloading mechanism. It concludes by highlighting the problems with offloading mechanisms in the field of mobile cloud computing that need independent investigation

The use of mobile cloud computing technologies is still in its infancy. By investigating the key variables that affect the overall choice to use mobile cloud computing in colleges and universities, this study intends to close this gap in knowledge. As a result, this experiment proposes an integrated model that incorporates seven key technological factors drawn from a review of related research as well as fresh considerations like service quality and comparative advantage that were not supposed to cover in earlier studies as crucial factors in the decision to adopt smartphone cloud services in campuses across the country. Data were gathered from several academic staff members who work in different departments of Saudi Arabia's public institutions. Quality of service, perceived utility, perceived simplicity of use, relative benefit, and trust were determined to be among the most important predictors of smartphone cloud adoption. The results also showed that Saudi institutions are still reticent to utilize mobile clouds because of security and privacy concerns. Last but not least, the results of this study provide helpful info to academic institutions, mobile cloud providers, and decision-makers to enable the successful development of m cloud computing technology .

This study support the notion that wearable sensors and mobile devices enable people to access medical care whenever and wherever they want. Outsourcing computation- or data-intensive operations to distant cloud centers might ease the long-standing limitation of computing capabilities and storage capacity on mobile devices. As a result, cloud-based mobile computing has gained recognition as a possible route for offering consumers inescapable healthcare services

in their ordinary activities. New optimization methodologies have been examined to allow mobile cloud healthcare services to be distributed more effectively and efficiently with the development and acceptance of mobile cloud computing technology in healthcare. This paper illustrates the widespread use of mobile cloud computing methodologies in several healthcare systems and, in particular, outlines the main architectural and design criteria one should keep in mind while creating a mobile cloud computing platform for healthcare situations. This paper introduces the state-of-the-art optimization algorithms on mobile cloud technology for meeting diverse priorities and achieving the ideal trade-off between multiple objectives, given the numerous factors that may impact the performance of smartphone cloud computing and even have disastrous consequences in healthcare. Finally, the security and confidentiality concerns of mobile cloud-based computing in the healthcare industry also were covered .

The Comprehensive information analysis, similar to an intelligent watering system. The system can access and examine weather data from the internet, including historical prognostications. Such data may be carefully analyzed to provide an irrigation parameter for an irrigation plan. After examining the soil's composition, another irrigation characteristic may be provided based on the soil's capacity to retain water and dirt. Additionally, before supplying parameters, the system may record and process temperature data from the air and do systematic study on a variety of factors that may have an influence on plant development. Finally, using these criteria, a day-specific irrigation plan is created. This may ensure that the plant receives the appropriate amount of water while preventing overwatering, which might drown the plant and result in waste .

The flexible architecture that cloud computing offers, data and resources may be distributed across many different places and accessed from a variety of industrial settings. Utilizing, storing, and sharing resources including data, services, and applications for industrial applications have all altered as a result of cloud computing. In the last ten years, companies have quickly shifted to cloud computing in order to benefit from greater performance, lower costs, and more extensive access. Additionally, the internet of things (IoT) has significantly improved when cloud computing was included. However, this quick shift to the cloud brought up a number of security concerns and challenges. Traditional security measures don't immediately apply to cloud-based systems and are sometimes inadequate. Despite the repeated usage and spread of diverse cyber weapons, cloud platforms' issues and security worries have been resolved during the last three years. Deep learning's (DL) quick development in the field of artificial intelligence (AI) has produced a number of advantages that may be used to cloud-based industrial security concerns .

DISCUSSION

The fusion of many technologies, particularly wireless communication, real-time analytics, pattern recognition, commodity sensors, and embedded software has led to the evolution of the Internet of Things (IoT) and cloud computing. The results of this research have shown that software product engineering has gotten less attention than other fields in this field. As a result, there is a gap in our understanding of the models, quality issues, tool chains, interdependencies, and industry assessments related to CoT software applications. This research demonstrates how improvements in some areas of software engineering will increase the dependability of

architectures. The fusion of many technologies, including wireless connectivity, real-time analytics, machine learning, commodity sensors, and embedded software has led to the evolution of the Internet of Things (IoT) and cloud computing. The results of this research have shown that software architecture development has gotten less attention than other professions in this field. As a result, there is a gap in our understanding of the models, quality issues, tool chains, interdependencies, and industry components of information to CoT software architectures. This research demonstrates how improvements in some areas of software engineering will increase the dependability of architectures.

CONCLUSION

Low-memory devices, network restrictions, inadequate processing capability, heterogeneity, ubiquity, and mass scalability are just a few of the IoT's drawbacks. The scientific and industrial communities have lately begun to pay attention to the confluence of cloud computing and IoT because it has the potential to solve these problems by using cloud infrastructure. In order to address the numerous quality difficulties that come with new developing technologies and the quality criteria that go along with them, many firms want trustworthy software structures. An analysis of 82 main research on CoT software architectures was reported in this study. Including design patterns, styles, viewpoints, and assessment procedures in terms of different quality aspects and CoT application domains, we gathered, assessed, and consolidated the available architectural knowledge in this field.

REFERENCES

[1] A. Botta, W. De Donato, V. Persico, and A. Pescapé, “Integration of Cloud computing and Internet of Things: A survey,” *Futur. Gener. Comput. Syst.*, 2016, doi: 10.1016/j.future.2015.09.021.

[2] S. Luo and B. Ren, “The monitoring and managing application of cloud computing based on Internet of Things,” *Comput. Methods Programs Biomed.*, 2016, doi: 10.1016/j.cmpb.2016.03.024.

[3] M. KUMAR, “CLOUD IOT: A COMBINATION OF CLOUD COMPUTING AND INTERNET OF THINGS,” *Int. J. Emerg. Trends Eng. Dev. Issue 6, Vol. 6 (November 2016) ISSN 2249-6149*, 2016, doi: http://rspublication.com/ijeted/2016/NOV16/33.pdf.

[4] M. Díaz, C. Martín, and B. Rubio, “State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing,” *Journal of Network and Computer Applications*. 2016. doi: 10.1016/j.jnca.2016.01.010.

[5] I. Khan and P. S. D. Sawant, “A review on integration of cloud computing and Internet of Things,” *Int. J. Adv. Res. Comput. Commun. Eng.*, 2016.

[6] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, “Internet of Things and Edge Cloud Computing Roadmap for Manufacturing,” *IEEE Cloud Comput.*, 2016, doi: 10.1109/MCC.2016.91.

[7] Q. Lele and K. Lihua, “Technical framework design of safety production information management platform for chemical industrial parks based on cloud computing and the

internet of things," *Int. J. Grid Distrib. Comput.*, 2016, doi: 10.14257/ijgdc.2016.9.6.28.

[8] C. S. Nandyala and H. K. Kim, "Green IoT Agriculture and Healthcare Application (GAHA)," *Int. J. Smart Home*, 2016, doi: 10.14257/ijsh.2016.10.4.26.

[9] Y. Benkler, "Degrees of freedom, dimensions of power," *Daedalus*, 2016, doi: 10.1162/DAED_a_00362.

[10] N. Feng, "Research on the modern intelligent healthcare platform from the perspectives of grid based cloud computing and information management system assisted internet of things technology," *Int. J. Grid Distrib. Comput.*, 2016, doi: 10.14257/ijgdc.2016.9.11.03.

CHAPTER 17

AN ANALYSIS OF IOT DEPENDENT MONITORING SYSTEM

Mr. Vishal Sharma, Assistant Professor/HOD
Department of SOMFT, IIMT University, Meerut Uttar Pradesh, India
Email id- journalistdrvishal@gmail.com

ABSTRACT

The Internet of Things is currently transforming the globe and creating numerous forms of connection. Only today's Internet of Things, which encompasses cyber-physical systems that can automatically make choices and monitor production and manufacturing processes in factories, allows for human to machine and machine to machine communications. The sensor in a wireless sensor network gathers data from the object and communicates it to the router. Depending on its intended use, that Sensor can be different. The Internet of Things will create massive amounts of information since so many gadgets will be linked to it. We must use several sorts of algorithms to extract confidential message from the created data. Wi-Fi, the internet of things, cloud computing, and cyber-physical systems all could be used to monitor and manage massive amounts of information.

KEYWORDS:

Cloud Computing, Cloud Service, Internet of Things, IoT Devices, Sensor Network.

INTRODUCTION

You may find a thorough analysis of the IoT's architecture, regulations, applications, cybersecurity, real-world usage, and anticipated advancements in. The technologies of today are constantly advancing all the time. People are gravitating towards a "always connected" system. Both wired and wireless networks are available, and support and develop for certain addressing protocols have been acknowledged and created. Scientists have recently begun investigating theories about the "Future Internet." IoT technology adoption is rising in popularity among many industries. Between 26 and 50 billion "things" will be online by the year 2020 thanks to several industrial Internet of Things (IoT) efforts that have been implemented across a range of industries, including agriculture, food processing, surveillance, and many more. IoT, which uses Android, portable technologies, and sensors, has given us a viable means for creating reliable industrial systems and applications[1]–[3].

Everyone wants to upgrade their system nowadays by tying it to the cloud. Other businesses besides those in the electronics and IT sectors are interested in connecting their manufacturing lines with IoT devices so that they may manage and monitor data in a real-time scenario from anywhere on the planet's surface without any difficulties. IIoT is the foundation for Industry 4.0 integration. IoT is a popular study field that has both potential and risks, and it is continually expanding. One of the best IoT protocols, MQTT enables the transfer of data between sensors and cloud services as well as between sensors and the Internet of Things. Almost all operations taking place within the internal environment of the industry must be observed for the workers'

increased safety. The Internet of Things (IoT) may link two physical components and enhance a communication system by introducing an intelligent component. IoT is a crucial technology that may enable a variety of practical services and applications that might assist infrastructure, health, economies, and the environment in ways we had never imagined.

Since many years, the world's population has been growing, and this has resulted in more resource waste. This resource waste is caused by a number of things, including, but not limited to, improper regulations and standards, improper application of already-existing standards, and sometimes outright contempt for such norms in both residential and commercial settings. Standards may take the form of instructions on power consumption, regulations for outdated equipment (some of which are still in use today), or standby equipment rules on power utilisation. The development, or manipulation, of sensors and the connectivity between them as well as the analytics that resulted from this new information, establishing the Internet of Things, was one strategy tried to combat these problems (IoT).

Today, practically every industry from retail to healthcare has made some kind of IoT investment, and the International Data Corporation (IDC) has already predicted that by 2025, the amount of data created would be 163 zettabytes, or ten times as much as it was in 2016. IoT devices are partly to blame for this, as Peter Newman projects that there will be more than 55 billion IoT devices linked to some kind of network by that year. In addition, investments in IoT are expected to total up to $15 trillion between 2017 and 2025. In order to establish more effective energy management within buildings, there is a rising need for IoT projects and infrastructures that are appropriate for using more clean energy[4], [5].

Edge computing is yet another approach to issues with limited resources, such as bandwidth, server resources, and the costs associated with cloud processing, all while reducing latency and adding functionality, creating a more aware system that can generate alerts in a timely manner. Edge computing is described in as a networking paradigm focused on bringing computing processes as close to the source of data as possible, which in some cases could mean the sensor itself. PTEC (predictive thermal and energy control system), a thermal and energy control prediction system in a data centre, was designed and evaluated by the authors in. The goal of the research was to determine if the PTEC could effectively monitor the data centre at a reasonable cost in terms of power consumption.

The system gathers data from the air conditioner and server fans and checks to see whether the temperature and power consumption figures are within the data center's margin of safety. To assess the effectiveness and durability of the PTEC, simulation is used to evaluate the system. According to the PTEC review, it may cut cooling and circulation energy use by up to 34% and 30%, respectively. By controlling the occasionally wasteful cooling processes, temperature and humidity sensors used in conjunction with cloud management of air conditioners can also enhance supporting infrastructure. This frees up resources on IT (Information Technologies) servers, improves performance while maintaining proper temperatures, and lowers energy usage. An open-source IoT infrastructure is used to develop a low-cost solution for energy consumption and environmental monitoring with a goal that is comparable to one of this work's case studies, the monitoring of educational facilities.

Additionally, it offers insights based on preliminary findings about a deployment within a university building using XBee devices. While this is going on, a different strategy for reducing energy consumption is put forth by using occupancy sensors in large commercial buildings to identify the occupancy patterns in specific areas and thereby create a more effective HVAC schedule pattern that can reduce energy consumption by up to 38% while maintaining thermal comfort. We can outline three of the most popular products on the market for business energy monitoring devices:

A. Smart Energy by Develco Products focuses on total building energy monitoring and offers tools to assess both energy production and consumption via the use of a variety of communication technologies, including Zigbee, Z-Wave, WLAN, Wireless M-Bus, and Bluetooth Low Energy.

B. Sense: Unlike other, more invasive sensors, Home Energy operates differently. This sensor's key unique feature is that it measures power consumption using amperage clamps or current transformers, like in this work.

C. Engage: Energy is yet another home energy consumption monitoring system that measures energy using current transformers and has the option to combine with "coming soon" smart electrical outlets, enabling both invasive and non-intrusive experiences.

Edge Monitoring in IoT

Understanding application performance at the edge and how it affects overall company performance is significant as the edge gets more intelligent. The internet of things is enabling the development of edge computing. Sensing devices that collect data on the physical environment, such as dampness, light, chemicals, and vibration, create enormous amounts of information. Cisco predicts that during the next four years, the amount of data coming from handsets and machine-to-machine modules should increase by 49% annually.

Sending such enormous amounts of information back to the cloud for processing is just not practical when the quantity of data processed every hour increases from tens to hundreds of gigabytes. The costs of failing to fulfil response time standards because of network congestion are too expensive. When demanding an action from the vehicle management system, such as slowing or decelerating, connected automobiles receiving events that might impact from the front and rear of the vehicle through lidar or ladar systems and pictures cannot risk a slow reaction time. Similarly, real-time processing of humidity, wind speed, and sound data is required for linked roads that depend on peripheral sensors to dynamically modify road signs alerting drivers of extreme weather like flash floods and fog. Congestion, collisions, and even fatalities increase with every delay.

IoT has created a Smarter Edge

When sensors are placed in countries with patchy network availability sometimes with limited cellular or satellite capacity, real-time edge computing becomes necessary. This is true for transportation and logistics and for keeping an eye on industrial equipment in far-off places include mines or oil and gas fields. Monitoring and control has just lately started to catch up with

applications as they progressively go to the edge. There was minimal need for comprehensive diagnostics when the edge was supposed to be stupid. Either sensors functioned or they didn't. They weren't a component of more complicated systems that may experience issues like thread congestion or memory shortages apart from the sensors themselves.

Performance control is necessary with a wiser edge. There is very little insight into problems experienced by remote applications and cloud infrastructure without performance monitoring; these problems happen in the shadows. Someone normally has to travel out to the region and examine if an IoT device ceases functioning, for instance, if sensors in a garage or on a platform in the Gulf of Mexico stop reacting. For maintenance, connected vehicles must be brought in. Due to the lack of visibility, it is difficult to determine which concerns need urgent action and which are more likely to have no or minimal effects on the organization [6]–[8].

The emergence of new, more complicated designs presents the largest obstacle for performance testing at the edge. More levels or tiers of edge computing are needed as there are more devices transferring information and as there is more data that has to be processed. As an example, various sensors on a factory floor may transmit data to a single gateway, which then could transfer the data to the cloud. Similar to this, a single smart garage might gather information from all throughout the buildings, analyse it at a single gateway, but then just send it to a single cloud application. However, handling parking in several garages throughout numerous neighbourhoods would presumably need adding additional computing layers at the edge, maybe necessitating a separate server and perhaps other physical resource for each neighbourhood. An end-to-end view of computing service requests, commonly referred to as financial transactions, is necessary to ensure that each layer is operating as efficiently as possible.

IoT System (EnerMon)

Since the goal is the development of an IoT System, we follow the typical IoT waterfall methodology:

i. Identification of requirements.

ii. Design of the System.

iii. System development.

iv. System Testing.

v. Implementation and Results

i. Identification of Requirements

Our system proposal can be applied from small houses to big buildings, so in this phase, a set of interviews were performed to several service employees, such as a university’s sustainability and maintenance responsibilities and individual houses owners. From this initial work, a set of requirements were identified for EnerMon:

a. Problem:

Pattern identification is important to check power consumers that might be giving problems, such as power consumption deviation from the normality that could indicate that the hardware might be malfunctioning.

b. Requirement:

Real-time monitoring of power consumption/ low interval on sending data makes it easier to test for problematic devices •

a. Problem:

It is also important that each month or week, a general vision of how each power consumer is working.

b. Requirement:

Aggregate monitoring of power consumption with filters based on different attributes.

a. Problem:

Different environments can have several consumers in different electrical phases so not only the devices must be cheap so many can be made, but they also need to be easy to install in case there is the need to change their location.

b. Requirement:

Ease of installation for changeability within different environments.

c. Requirement: Low-cost with an accuracy of 97%..

a. Problem:

Power consumption monitoring generates summative values, and as such, it is important to reduce failures to a minimum while always keeping the interval between reads within the same time frame.

b. Requirement: Robustness to failures and errors, to keep a near 100% uptime.

c. Requirement: Real-time device synchronization.

a. Problem: With different environments comes different networks infrastructures; in most usual cases, the available infrastructure would be Wi-Fi, which can have multiple issues, such as low-range or the signal strength loss when crossing walls.

b. B. Requirement: Wide area network with low frequency

System Design

a. Device Layel: LoRa (LongRange) End Device: The end devices use edge computing approaches to collect data and then sends it to the LoRa gateway without any need for a nearby, small-range communication network (e.g., Wi-Fi).

b. Communication Layer: LoRa Gateway: Receives uplinks from end devices and redirects that data to one or more application servers, while, also, sending downlinks to end devices, in case there is a need to send a command.

c. Data Layer: Application Server and Databases: Receives data from the gateways, processes that data and stores it in a database while communicating with the end-device through the LoRa gateway.

d. Information Layer: Dashboard and Analysis: The data collected is used to create a dashboard that presents information in the form of detailed graphics alongside proper filters, with the analysis done using PowerBi's dashboard alongside Python to better understand the data.

The health of patients has previously been taken into account by several researchers, who have presented an ideal and suitable alternative. Information may be transmitted more securely and quickly with the development of technologies like cloud applications, the Internet of Things, and 5G. The topic of e-health has a lot of prospects thanks to the Internet of Things (IoT). This technology has the potential to advance medical and bring about a multitude of advances. The monitoring of patients may be tremendously enhanced if you incorporate cloud computing and IoT into this workflow. In order to efficiently monitor patient status via linked sensors, it is crucial to advance both the medical business and computer science. The use of cloud computing to carry out the analysis gathered from remote patient monitoring and IoT platform has therefore been recommended owing to its ideal efficiency, speed, and validity of the data processing and categorization. A prioritizing method is utilized in this study to priorities sensitive data in the Internet of Things, and LSTM deep neural network is employed in cloud computing to categories and remotely monitor patients' symptoms, which may be regarded as an additional novel component of this chapter. The 5th generation Internet is used to communicate sensor data from the IoT platform to the cloud .

The Internet of Things (IoT) and cloud computing are two very different technologies that are both essential to our daily lives. They are anticipated to be increasingly widely accepted and used, making them crucial components of the global Internet in the future due to the amount of time we have in our jobs and the need to follow through all over every activity before a game is played at any stadium in the globe. Here, before every game, a cautious procedure is covered. In this study, it was discussed how to combine cloud computing and the Internet of Things together to build smart facilities throughout the globe. However, a number of new and current varieties of smart stadiums are discussed .

Internet of Things (IoT) and cloud computing multifactor authentication have recently been carefully examined for safe data retrieval and trustworthy access management on large-scale IoT networks. It does not, however, have a best practice for combining IoT and cloud computing together and with strong security. In this paper, we provide a brand-new authentication method for cloud servers and IoT-based architecture. In order to achieve the highest efficiency, our

authentication strategy uses lightweight crypto-modules like that of the one-way hash function and exclusive-or operation. It not only lessens the computational strain but also qualifies our tell researchers for items with restricted resources, such sensors or World Wide Web of Things (IoT) gadgets. The recommended authentication scheme's security robustness is ensured by the formal verification provided by Provera. Additionally, the performance analysis demonstrates how feasible our suggested approach is in obtaining a user-acceptable computation overhead .

The with an unpredictably high gross local consumption, the fourth industrial revolution may link ecosystems of more than 20 billion devices. By 2020, connected devices will generate over 44 ZB of raw data, posing intriguing issues in terms of privacy, connection, and scalability. The Internet of Things (IoT), which connects the physical and the digital worlds, is receiving more and more attention. Therefore, it is necessary to quantify and transform the physical world into quantifiable numbers. In the many areas, the cloud for IoT delivers priceless applications and uncommon services. Fog computing, on the contrary hand, aids in effective use, improved performance, and reduced power consumption. The IoT platforms utilized for fog and cloud computing to provide end-to-end IoT services are the main topic of this evaluation. The use of the cloud of things and fog roles to alleviate the cloud of products' difficulties is indeed offered .

The fog computing is a tool for the developing Internet of Things systems because it offers low-latency computing functions at the network edge. In this paper, we investigate how fog and external cloud computing resources are divided across Internet of Things users in a multilevel computing paradigm. To optimally distribute the finite processing capacity of fog nodes and mimic the rivalry amongst IoT users, we develop a computationally offloading game. Each user strives to achieve the greatest quality of experience, which represents how satisfied they are with the computing services they have used in regards to the reduction in processing time and energy. We demonstrate the presence of a pure Nash equilibrium and provide an upper limit on the cost of anarchy using a prospective game methodology. We further offer a near-optimal resource allocation method and illustrate that in a system with N IoT users, it accomplishes time, taking into account the fact that the time complexity to reach the equilibrium rises exponentially with the number of users. We assess the equilibrium productivity and the quality of experience of the users using numerical analyses. Our findings indicate that as compared to an existing offloading system, the suggested method provides more consumers with computing resources. We also demonstrate how our suggested approach allows for low-latency fog server virtualization for IoT applications that are night before going to bed to computation delay. A wealth of chemical industrial parks has been built one after another in many places, where lots of chemical enterprises are established. In the normal operation of those enterprises, their raw materials or products manufactured, transported and stored are usually featured by flammable, explosive or toxic properties, resulting in frequent occurrence of pollution and personal accidents and causing great threats to surrounding environment. This thesis realizes an integrated information management platform based on currently advanced cloud computing and IOT technologies, so as for integrated management of chemical industrial parks. The said platform can accomplish the whole-process, real-time and dynamic follow-up and control of chemicals and hazardous materials and also provide effective service for users' decision-making by mining and analyzing tremendous data of a chemical industrial park with Agent-middleware technology. The

information management platform is capable of assessing the safety factors of chemical enterprises at peacetime, giving necessary warning before accidents and offering effective technical support for rescue via expert system, emergency plan system, monitoring system and positioning system. The realization of chemical industrial park integrated information management platform based on cloud computing and IOT technologies will greatly improve the management level of chemical industrial parks, intensify surveillance, achieve information resource sharing and lower the probability of accident

Utilizing, storing, and sharing resources including data, services, and applications for industrial applications have all altered as a result of cloud computing. In the last ten years, companies have quickly shifted to cloud computing in order to benefit from greater performance, lower costs, and more extensive access. However, the internet of things (IoT) has significantly improved when cloud computing was included. However, this quick shift to the cloud brought up a number of security concerns and challenges. Traditional security measures don't immediately apply to cloud-based systems and are sometimes inadequate. Despite the repeated employment and spread of diverse cyber weapons, cloud platforms' issues and security worries have been resolved during the last three years. Deep learning's (DL) quick development in the field of artificial intelligence (AI) has produced a number of advantages that may be used to cloud-based industrial security concerns. The results of the proposed research include the following: a thorough analysis of the enabling cloud-based IoT architecture, services, arrangements, and security models; the characterization of cloud security concerns in IoT into four key categories, which are discussed in detail; the identification and examination of the most current revelations in cloud-based IoT attacks; and the identification, consultation, and analysis of the most staggering security threats .

With the advent of technologies such as cloud computing, Internet of Things and 5G, information can be exchanged faster and more securely. The Internet of things (IoT) offers many opportunities in the field of e-health. This technology can improve health services and lead to various innovations in this regard. Using cloud computing and IoT in this process can significantly improve the monitoring of patients. Therefore, it is important to provide a useful method in the medical industry and computer science to monitor the status of patients using connected sensors. Thus, due to its optimal efficiency, speed, and accuracy of data processing and classification, the use of cloud computing to process the data collected from remote patient sensors and IoT platform has been suggested. In this paper, a prioritization system is used to prioritize sensitive information in IoT, and in cloud computing, LSTM deep neural network is applied to classify and monitor patients' condition remotely, which can be considered as an important innovative aspect of this paper. Sensor data in the IoT platform is sent to the cloud with the help of the 5th generation Internet. The core of cloud computing uses the LSTM (long short-term memory) deep neural network algorithm .

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved with the greater generation of data. Internet of Things Cloud Service creates excessive communication between inexpensive sensors in the IoT which means even

greater connectivity. Billions of connected devices and machines will soon join human-users. IoT generates lots of data while on the other hand, cloud computing paves way for this data to travel. In this paper we try to focus on cloud providers who take advantage of this to provide a pay-as-you-use model where customers pay for the specific resources used. Also, cloud hosting as a service adds value to IoT startups by providing economies of scale to reduce their overall cost structure .

The current continuous glucose tracking devices monitor the blood glucose level and notify the user of type 1 diabetes when a designated critical threshold is exceeded. This may because the person's immune system to function at high levels until the medication is taken to lower the glucose level, elevating the risk of serious health problems if the intake is postponed. In this research, a novel strategy based on cutting-edge software and hardware techniques is suggested to overcome the latter. In particular, a deep learning approach for artificial intelligence is suggested to predict glucose levels throughout time periods of 30 minutes. Additionally, the implementation of the prediction model and its integration with the current wearable CGM model are being examined, in order to give patients with the forecast of future glucose levels. A feed forward RNN-RBM DL model based on both recurrent neural networks (RNNs) and restricted Boltzmann machines (RBM) has been regarded amongst some of the various DL methodologies in the state-of-the-art owing to its better qualities regarding increased prediction accuracy .

This research corresponds to the use of big data, cloud computing, IoT systems, and data mining technologies with in-depth discussion. This work offers a thorough assessment and assessment based on the performance measurement and computational factors. Based on communication capabilities, system component communications, features of data mining, big data, and cloud computing in IoT, the analysis and debate are framed. There has also been exploration and analysis of various communication and communication difficulties. Finally, a framework for the proper performance of the IoT protocols has been suggested based on the research and analysis [8]–[10]. The success of the present and future IoT and connected device environment depends on service provision that is defined by, among other things, scalability, ubiquity, dependability, and high-performance. The fusion of IoT with Cloud Computing (CC), also known as cloud IoT, has arisen as a new paradigm offering enhanced services specifically designed to aggregate, store, and analyses data produced by IoT in order to accomplish this attribution. IoT and cloud convergence provide potential, but they are also constrained in certain ways by things like bandwidth, latency, and connection. Due to the hierarchical, cross-layer, and dispersed character of this architecture, it is difficult to achieve an osmotic and successful convergence of IoT, edge, fog, and cloud computing. These difficulties relate to design and implementation, deployment, and assessment. In order to give chances for more detailed investigations and to hasten knowledge acquisition, this paper blends talks on all significant elements of the underlying technologies to provide a thorough understanding of the edge-fog-cloud computing paradigm. In order to obtain a thorough grasp of edge-fog-cloud, we will first explain the key needs, cutting-edge reference architectures, building blocks, components, protocols, applications, and other related computing paradigms, along with their similarities and contrasts. The role of distributed, collaborative, and privacy-preserving analytics, as well as how edge, fog, and cloud computing

interact, will be discussed next. Finally, we will provide an overview of the key edge-fog-cloud computing difficulties that must be overcome in order to fully use IoT .

DISCUSSION

The author of this work covers several research papers on various environmental monitoring systems used for varied objectives. The study's analysis and discussion provide critical suggestions for enhancing these systems. The necessity for in-depth study in these aspects has been recognized as a result of research on deep learning, managing massive data, and applying consistent classification models. We have concentrated on systems that can handle environmental difficulties, such as water, air quality monitoring, and intelligent waste management. For ecological sustainability via smart environmental monitoring, the considerable obstacles to integrating smart sensors, artificial intelligence (AI), and wireless sensor networks (WSNs) must be overcome (SEM). SEM initiatives would be strengthened by the involvement of conservation activists, regulatory entities, and widespread awareness. Techniques for pre-processing may be used to enhance the quality of sensory input. These methods, which include filtering and engineering controls, improve the data's suitability for SEM-related activities. Future research will focus on investigating other environmental consequences, such as flexible sensing, energy-harvesting sensing, marine pollution, sound pollution, etc.

CONCLUSION

The Internet of Things (IoT) guarantees that different concepts for quality of life and businesses will alter. The IoT has the potential to facilitate extensions and enhancements to fundamental facilities in logistics, transportation, education, healthcare, and security, among other areas, while creating a brand-new ecosystem for application development. This is made possible by a large-scale, locally intelligent network of smart devices. In a shorter amount of time than the Internet of Things has operated, it has impacted every area of modern life. In this work, I've presented a prototype for an IOT-based data collection and analysis system for a wide range of purposes in education and other fields. I've come to the conclusion that Industry 4.0 will be the main community for carrying out tasks in the current industry. For IoT deployment, there are three main phases: data collection, data security, and data analysis. The confidentiality of the information is crucial for reliable data transmission across the millions of smart applications as the Internet of Things increases. In this paper, I have focused on the MQTT application protocol for secure data transport. A user may segregate the specific data anyway he wants using the many big data analysis techniques. Because it primarily focuses on industrial IoT applications, big data analysis, and potential research prospects for future industrial researchers, this study differs from previous IoT review studies.

REFERENCES

[1] M. Díaz, C. Martín, and B. Rubio, “State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing,” *Journal of Network and Computer Applications*. 2016. doi: 10.1016/j.jnca.2016.01.010.

[2] I. Khan and P. S. D. Sawant, “A review on integration of cloud computing and Internet of Things,” *Int. J. Adv. Res. Comput. Commun. Eng.*, 2016.

[3] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, "Internet of Things and Edge Cloud Computing Roadmap for Manufacturing," *IEEE Cloud Comput.*, 2016, doi: 10.1109/MCC.2016.91.

[4] N. Feng, "Research on the modern intelligent healthcare platform from the perspectives of grid based cloud computing and information management system assisted internet of things technology," *Int. J. Grid Distrib. Comput.*, 2016, doi: 10.14257/ijgdc.2016.9.11.03.

[5] A. Khanna, "An architectural design for cloud of things," *Facta Univ. - Ser. Electron. Energ.*, 2016, doi: 10.2298/fuee1603357k.

[6] E. Cavalcante *et al.*, "On the interplay of Internet of Things and Cloud Computing: A systematic mapping study," *Comput. Commun.*, 2016, doi: 10.1016/j.comcom.2016.03.012.

[7] Y. Singh, P. Assistant, and T. Parmar, "Cloud of Things: A State-of-the-art Review on Integration of Internet of Things with Cloud Computing," *Int. J. Comput. Appl.*, 2016.

[8] G. Blair, D. Schmidt, and C. Taconet, "Middleware for Internet distribution in the context of cloud computing and the Internet of Things: Editorial Introduction," *Annales des Telecommunications/Annals of Telecommunications*. 2016. doi: 10.1007/s12243-016-0493-z.

[9] Q. Lele and K. Lihua, "Technical framework design of safety production information management platform for chemical industrial parks based on cloud computing and the internet of things," *Int. J. Grid Distrib. Comput.*, 2016, doi: 10.14257/ijgdc.2016.9.6.28.

[10] C. S. Nandyala and H. K. Kim, "Green IoT Agriculture and Healthcare Application (GAHA)," *Int. J. Smart Home*, 2016, doi: 10.14257/ijsh.2016.10.4.26.

CHAPTER 18

AN ANALYSIS OF MONITORING SYSTEM WITH IOT AND CLOUD COMPUTING

Dr. Ravendra Pratap Rana, Professor/Dean
Department of SOMFT, IIMT University, Meerut Uttar Pradesh, India
Email id- ravindra.rana777@gmail.com

ABSTRACT

The merging of IOT and cloud computing in the context of health care assistance is particularly needed given the rapid growth of cloud computing related computer science equipment. Prior study has focused predominantly on the individual advancement of a specific technology; very little studies have been conducted in the areas of medical management and surveillance support processes. Finally, the hospital healthcare data service cloud system monitoring as well as management application was provided by the final efficient PSOSAA algorithm. The recommended result of the analysis shows the other cutting-edge algorithms, according to laboratory simulation. We explore additional interesting study areas.

KEYWORDS

Cloud Computing, Cloud Service, Internet of Things, IoT Devices, Sensor Network.

INTRODUCTION

The Internet of Things (IoT) paradigm is built on nodes (things) that are intelligent and capable of consciousness that are linked together in a dynamic, global network architecture. It stands for one of the most line with the technological developments in the field of ubiquitous and pervasive computing. The term "internet of things" often refers to small, limited-capacity physical objects as well as significant issues with reliability, performance, security, and privacy. However, cloud computing, a more advanced technology that may at least partially address the issue with the majority of the Internet of Things, offers nearly limitless storage and processing power . Thus, a unique IT paradigm that combines IoT and Cloud as two complimentary platforms is anticipated to upend both the present and the future. It is known as the new Cloud-IoT paradigm[1]–[3].

This paper looks into the literature on the potential fields of cloud computing and the Internet of Things. To suggest an integrated more use cloud and IoT, we have completed a review. Figure 1 shows how each issue has grown in popularity over the last several years as well as the overall number of publications that have dealt with it. The generation of digital technologies is the Internet of Things . This represents a significant advancement in the information and conversion possibility fields. The panel is of the opinion that the development of Internet of Things applications will significantly aid in the future solution of societal issues. In order to teach current logistics management, modern information technology is used. Good service, affordable prices, and higher performance are the three fundamental needs. Modern uses of health information technology serve a broad range of goals.

The nation's well-being and the livelihood of the people are intimately tied to medical digital technologies and healthcare services. A great breakthrough would be the introduction of cloud computing and Internet of Things to current medicine. Because large-scale cloud computing provides benefits like high reliability, virtualization, efficiency, and scalability, building a public cloud for a hospital and its patients can encourage data exchange, cost savings, and the improvement of highly effective medical monitoring and management systems. The main technology of RFID, photos, and some other acoustic electromagnetic sensors can achieve major breakthrough in medical transmission of information, intelligent health monitoring, and precise location. Internet is a crucial support to realize the safe, effective, and high quality of medical surveillance and management[4], [5].

Hospitals benefit greatly from IoT, particularly in terms of managing patient monitoring and tracking. Due to the Internet's aggressive expansion, the hospital will have new prospects in the social spheres thanks to cloud computing and World Wide Web integration of medical monitoring and administration platforms. This research paper provides an overview of health information technology in the cloud computing and Internet of Everything disciplines, with a focus on application areas for health monitoring and management in the context of the present research situation. In this research, we present and investigate a cloud-based remote monitoring and management platform for health information (RMCPHI) paradigm. The administration of applications for cloud computing for medical monitoring is then suggested using the effective PSOSAA algorithm. The efficiency of our suggested strategy is shown by the quantitative analysis and simulation.

IoT and Cloud Computing

The Necessaries of the Integration

IoT and the cloud have had independent evolutions. However, many shared benefits of their combination have been noted in literature and are used to forecast the future. On the one hand, the cloud's almost inexhaustible capacity and resources may help the Internet of things overcome its technological limitations. In particular, cloud computing may provide a practical way to administer Internet services as well as construct and utilize programmer that utilize items or data. On the other side, cloud computing may benefit from the Internet of things by extending its ability to deal with real-world situations in a more dispersed and dynamic fashion and by offering new services across a wide range of real-life situations. The Cloud essentially serves as a transitional layer between objects and applications, hiding all the sophistication and functionality required to construct the latter. The issue is outlined here, as is the benefit of the Cloud-IoT paradigm[6]–[8].

By definition, IoT incorporates a huge number of relevant sources. It generates a significant quantity of semi or unstructured data with regard to that same three key aspects of data: volume, velocity, and diversity. This necessitates that collecting, acquiring, manipulating, visualizing, archiving, transmitting, and searching vast volumes of data. The cloud is the most practical and economical method to deal with the information produced by the Internet of Things since it

offers practically infinite and an on storage capacity at minimal cost. New potential for query processing, integration, and exchange with those other parties are made possible by this integration, generating a new convergence scenario. Once in the cloud, information is accessible directly from anywhere, shielded by the best security measures, and shown in a consistent manner using a common API. Processing resources for IoT equipment are not permitted to interpret data in the field.

The the majority of the time, collected data are combined and delivered to a more capable node for processing; however, this does not always provide the infrastructure with the necessary scalability. The Internet of Things can now handle enormous demand according to the cloud's on-demand approach and limitless capacity, which also enables suitable content and advanced analysis. Algorithms for data-driven decision-making and projection would be affordable, and they would increase profits while lowering risks. Making IP access devices communicate via specialized hardware is one of the needs of something like the Internet of Things, and supporting the connection may be highly costly. A bespoke portal and built-in apps could be used to monitor and manage anything at any anytime from anywhere with the help of a cloud connection. Most of these issues are resolved by integrating with the cloud, which even offers other benefits include simple access, simple usage, and affordable deployment. Making educated services and applications for some changed surroundings based on the proliferation of the cloud by objects using the Cloud-IoT paradigm:

i. Sensing as a Service,

ii. Sensing and Actuation as a Service,

iii. Sensor Event as a Service,

iv. Database as a Service,

v. Ethernet as a Service,

vi. Identity and Policy Management as a Service,

vii. Video Surveillance.

Ambient-assisted living and telemedicine have paved the way for IoT and multimedia technologies in the healthcare sector. In this case, the use of the cloud results in the abstraction of technical specifics, removing the need for knowledge of or command over the technological infrastructure. In order to solve the issue, it also implements security multimedia health services on a device that runs a lot of multimedia and security algorithms but has a low processing power and a tiny battery. Interoperability, system security, the quality of service (QoS) for streaming video, and dynamically increasing storage are often seen as barriers in this field because to their shared issues with management, technology, safety, and legal inquiry. One of the most prevalent cardiovascular illnesses is hypertension. It is estimated that 160 million individuals worldwide experience it. Heart disease and high blood pressure are becoming more common[9], [10].

This guarantees early detection. It may alert the emergency mechanism when users are in an emergency or hazardous situation. As a result, advancements in medical care are recorded.

Additionally, it is simple to set up national health records, which may be used to compare and analyses medical data to give a decision-making foundation for regional sickness. Body sensors, sensor networks, communication modules, family gateways, platforms for the analysis and processing of medical information, medical personnel, and more are all included in the remote monitoring cloud platform for medical information.

A distinct kind of sensor network is used in medicine to gather data. Data from personal health records is vast and expanding quickly. As an information service provider, a vast volume of data must be automatically classified, analyzed, and processed. Examples include a security service center that offers security services, a disease detection and control emergency organization run by the Centers for Disease Control, emergency services based on the extraction of emergency first aid information, a hospital that offers remote medical diagnosis, a rehabilitation center that offers remote rehabilitation guidance based on a variety of recovery information, and a health service center that offers health instruction. As a result, they should need a way to share network resources and an efficient way to retrieve information. The sections that follow provide examples of our suggested work.

New technology called "mobile cloud computing" describes an architecture where data computation and storage take place outside of mobile devices. Internet of Things is a modern technology as well. The Internet of Things is a new technology that is emerging quickly in the telecoms industry. IoT is more particularly connected to wireless telecommunications. The basic purpose of entities and objects communicating and working together across wireless networks is to achieve the goal specified to them as a whole. Additionally, both Cloud Computing and indeed the Internet of Things are growing strongly in terms of wireless communications. In this paper, we provide an overview of IoT and Cloud Computing with a concentrate on their respective security challenges. We specifically utilize the two aforementioned technologies Cloud Computing and Cloud computing investigate their commonalities and to learn about the advantages of their combination. Finally, we demonstrate how cloud computing contributes to the Internet of Things technology. Thus, it demonstrates how cloud computing technology increases IoT functionality. We conclude by examining the security issues raised by the combination of IoT and cloud computing .

Industrial Internet of Things (IIoT) is rapidly expanding, and the several sources are continuously creating massive amounts of information. Since the energy and storage capacities of the end devices are seriously limited, it is not a good idea to locally store all the raw data in the IIoT devices. Independent of the unique qualities of resource limit, self-organization and short-range Internet of Things (IoT) networking provide cloud computing and outsourced data. There is a series of unexpected precautions for IoT and cloud components in the remaining results. The delivery of cloud computing is very effective, storage is constantly evolving, and several organizations are already transferring their information from their internal databases to cloud computing vendor hubs. While employing cloud computing resources, intensive IoT applications for processes and data are prone to difficulties. In order to help the secure migration of IoT applications to the cloud, we investigate IoT and cognitive hosting in this paper and address cloud-compatible issues and computing methodologies .

Flexible architecture that cloud computing offers, data and resources may be distributed across many different places and accessed from a variety of industrial settings. Utilizing, storing, and sharing resources including data, services, and applications for industrial applications have all altered as a result of cloud computing. In the last ten years, companies have quickly shifted to cloud computing in order to benefit from superior productivity, lower costs, and more extensive access. Additionally, the internet of things (IoT) has significantly improved when cloud computing is included in the. The following are some of the research's findings: We present a thorough analysis of the supporting cloud-based IoT architecture, services, combinations, and security models; the classification of cloud security problems in IoT into four major categories, which are discussed in detail; we identify and examine the most latest developments in cloud-based IoT attacks; we identify, communicate, and analyses significant security issues in each category and preemptive assessments; and finally, we present a comprehensive study of the cloud security considerations .

The most recent information technology that is fundamentally altering business paradigms is the Internet of Things, which came after the technologies of integrated circuits, home computers, and the Internet. The impact of IoT in the industrial industry has not yet been extensively examined. On the other hand, the complexity, dynamism, and uncertainties that contemporary companies face are becoming a bottleneck for the computer-aided software solutions that are now available. It is believed that the bottleneck would be removed if IoT and cloud computing were used in company networks. This study discusses the difficulties of producing assembly plans for sophisticated goods. It is suggested that IoT and cloud computing may assist a moving assembly modelling system in developing into an advanced system that can handle complexity and adjustments automatically. The automated retrieval of relational assembly matrices for assembly planning is actually achieved by an assembly modelling system that incorporates the following innovations: a flexible modular architecture that makes the system robust, reputable, flexible, and expandable; integrated object-oriented templates that make it easier to interchange with and reuse system components; and automated retrieval algorithms. Examples of assembly modelling for aircraft engines are used to show how efficiently the system works.

The integration between the Internet of Things (IoT) and cloud computing can potentially leverage the utilization of both sides. As the IoT based system is mostly composed by the interconnection of pervasive and constrained devices, it can take a benefit of virtually unlimited resources of cloud entity i.e storage and computation services to store and process its sensed data. On the other hand, the cloud computing system may get benefit from IoT by broadening its reach to real world environment applications. In order to incarnate this idea, a cloud software platform is needed to provide an integration layer between the IoT and cloud computing taking into account the heterogeneity of network communication protocols as well as the security and data management issues. In this study, an architectural design of IoT-cloud platform for IoT and cloud computing integration is presented. The proposed software platform can be decomposed into five main components namely cloud-to-device interface, authentication, data management, and cloud-to-user interface component. In general, the cloud-to-device interface acts as a data transmission endpoint between the whole cloud platform system and its IoT devices counterpart. Before a session of data transmission established, the communication interface contact the

authentication component to make sure that the corresponding IoT device is legitimate before it allowed for sending the sensor data to cloud environment. The received sensor data are then collected in data storage component. Any stored data can be further analyzed by data processing component. User or any developed applications can then retrieve collected data, either raw or processed data, through API data access and web console .

Internet of things (IoT) and cloud computing technology has made our life more convenient in recent years. Cooperating with cloud computing, Internet of things can provide more efficient and practical services. People can accept IoT services via cloud servers anytime and anywhere in the IoT-based cloud computing environment. However, plenty of possible network attacks threaten the security of users and cloud servers. To implement effective access control and secure communication in the IoT-based cloud computing environment, identity authentication is essential. In 2016, He et al. put forward an anonymous authentication scheme, which is based on asymmetric cryptography. It is claimed that their scheme is capable of withstanding all kinds of known attacks and has good performance. However, their scheme has serious security weaknesses according to our cryptanalysis. The results show that our proposed scheme is secure and can effectively resist all kinds of known attacks. Furthermore, compared with the original scheme in terms of security features and performance, our proposed scheme is feasible .

The development of new technologies in our day and age has led to the downsizing of sensors, and efforts to use them in a variety of applications are succeeding. They are also moving towards a concept of "Smart" like Smart Health Care systems, Smart Cities, Smart Mobility, Smart Grid, Smart Home and Smart Metering, etc. as a result of the adoption of Internet of Things (IoT) and Cloud Computing in all areas. Agriculture is one such field of study that has also benefited from this adoption, making it a Smart Agriculture. Any nation with a big population, like China, India, etc., relies heavily on agriculture to support its economy and way of life. By reducing costs, observing performance, and maintaining equipment, IoT and cloud computing in agriculture will improve crop output, which would be advantageous for both farmers and the country as a whole. The introduction of a smart drone for crop management is the main topic of this paper, and how IoT and cloud computing technologies, together with real-time drone data, may assist create a sustainable smart agriculture .

Internet of Things (IoT) and cloud computing-based customized healthcare solutions, this paper suggests a revolutionary identity management paradigm. The suggested architecture performs authentication using multimodal encrypted biometric features. It combines biometric-based continuous authentication with centralized and federated identity access mechanisms. When conducting authentication, the framework combines electrocardiogram and photoplethysmogram readings. The security of the framework is strengthened by the use of Holomorphic Encryption in addition to depending on the distinctive identifying qualities of the users' biometric attributes. This prevents several conventional security threats in addition to offering a quick and trustworthy authentication process. A machine learning model that tested the framework using a dataset of 25 users in sitting postures was used to assess and verify the framework's performance. The results of employing the suggested fused-based biometric framework shown that it was effective in identifying and authenticating all 25 users with 100% accuracy, as opposed to using

just ECG or PPG signals. Consequently, providing some notable enhancements to the general security and privacy of systems for providing tailored healthcare .

Internet of Things (IoT) is rapidly changing our society to a world where every “thing” is connected to the Internet, making computing pervasive like never before. This tsunami of connectivity and data collection relies more and more on the Cloud, where data analytics and intelligence actually reside. Cloud computing has indeed revolutionized the way computational resources and services can be used and accessed, implementing the concept of utility computing whose advantages are undeniable for every business. However, despite the benefits in terms of flexibility, economic savings, and support of new services, its widespread adoption is hindered by the security issues arising with its usage. From a security perspective, the technological revolution introduced by IoT and Cloud computing can represent a disaster, as each object might become inherently remotely hackable and, as a consequence, controllable by malicious actors. While the literature mostly focuses on the security of IoT and Cloud computing as separate entities, in this paper we provide an up-to-date and well-structured survey of the security issues of cloud computing in the IoT era. We give a clear picture of where security issues occur and what their potential impact is. As a result, we claim that it is not enough to secure IoT devices, as cyber-storms come from Clouds .

The integrated information systems are crucial defenses against misuse and overuse of land resources. The Internet of Things (IoT) and cloud computing are only two examples of information technologies that are unavoidably necessary for the effectiveness and calibre of duties related to managing land resources. A innovative online and off-line integrated system with synchronize internal and field data that incorporates the complete process of "discovering breaches, evaluating issues, authenticating fieldwork, and investigating cases" was created in this research. It is based on IoT and cloud computing innovations. The system incorporates key technologies, including the automatic extraction of high-precision information based on remote sensing, semantic ontology-based technology to excavate and distinguish public sentiment mostly on Internet that is related to illegal incidents, header computing based on MapReduce, consistent storing and compressing (bitwise) technology, global positioning system data communication and data asynchronous mode, intelligent recognition and classification, and machine learning. The Department of Land and Resource Management of Guizhou Province in China has officially deployed an integrated system built on the "One Map" platform that has been discovered to considerably improve the effectiveness and standard of land resource monitoring. The framework empowers the general growth of digital technologies in areas connected to management of land resources .

A technological transition that will revolutionize how we program and interface with the outside world. Two well-known research topics who have already had such an effect are cloud computing and mobile applications. Another interesting field of study is the Internet of Things (IoT), which focuses on creating a network of World Wide Web objects to support a smart environment. There are several new machine paradigms in use today that are associated to those study fields and/or their intersections. These include mobile IoT computing, IoT cloud technology, fog computing, mobile edge computing (MEC), edge computing, the Web of Things

(WoT), the Semantic WoT (SWoT), the Wisdom WoT (W2T), opportunistic sensing, participatory sensing, mobile crowd sensing, and mobile crowdsourcing. Nevertheless, such paradigms lack standardized definitions, therefore we often come across words that refer to several paradigms by the same name or even several terms that relate to the same paradigm. In order to avoid a significant issue, this work aims to explicate those paradigms and explain how and why they belong in the previous three research domains and/or their intersections. As much as conceivable, they are traced back toward its genesis. In addition, each area's research directions are discussed. In addition, the paper describes IoT-related technologies including ubiquitous and widespread computation, the Internet of Nano-Things (IoNT), and the World Wide Web of Underwater Things (IoUT) .

Precision agriculture (PA), which includes the information, communication, and control technology in farming, is becoming more popular every day. New developments in cloud computing and the Internet of Things (IoT) may improve PA connection. But since they aren't designed for semi-arid conditions or do not adequately address comprehensive PA management, they are often only used in a few high-cost, specialized settings. In order to address the requirements of soilless cultivation in full-recirculation greenhouses utilizing moderately saline water, we suggest a modular platform. It is backed by a three-tier open source software infrastructure at the local, edge, and cloud planes and is predicated on swappable low-cost hardware. Cyber-Physical Systems (CPS) connect with agricultural equipment on the electromagnetic plane to collect information and carrying out atomic control activities in real time. In order to boost adaptive capacity against network access failures, the edge plane of the platform is in charge of controlling and monitoring the primary PA tasks close to the access network. In a FIWARE application, the cloud platform also includes data analytics modules and gathers both recent and old information. While Next Generation Service Interface (NGSI) is utilized for southward and northbound access to the cloud, IoT protocols like Message Queue Telemetry Transport (MQTT) or Constrained Application Protocol (CoAP) are used to interface with CPS .

DISCUSSION

More distant devices are now able to wirelessly gather, store, and transfer data across very large networks across long distances to many businesses thanks to the growth of IoT applications. Because of this evolution, hackers now have a broader playing field with more targets, consequently remote IoT solutions must be created with personalized device security, well-thought-out IoT hardware, and understanding of risk aversion. Due to their accessibility through both wired and wireless networks, remote IoT linked devices are exposed to the following common forms of attacks: IoT Device Authentication By modifying the manufacturing code, hackers may deceive distant network components and sow discord. Modern security techniques Hackers may target technologies that are out of date or incompatible in order to fix problems with the large number of dispersed IoT devices.

Security Network Encryption to decompress IoT data, hackers may quickly acquire and acquire the encryption keys. Protection for mechanical port access Remote IoT devices may be violently threatened by hackers who get access through the JTAG port, network interfaces, or Ethernet

ports. The creation and implementation of a cutting-edge IoT security framework is the IoT answer to help with the prevention of these cyber-attacks. A specialized IoT solution will be the focus of the security solution, which will also include cutting-edge features like security mechanisms via the use of a remote computer that will keep track on and patch up on devices. Additionally, remote services will aid in the storage of IoT data and the verification that it came from the right device. It will have a hardened coprocessor that enables security functions apart from the main processor in a hardened security environment, adding additional levels of IoT security.

CONCLUSION

Knowledge has both a theoretical and a practical aspect, both of which are beneficial. The real masters of just about any trade or subject matter comprehend both extremes. They invest the time to appreciate how those tactics fit into a bigger context and tradition as well as the reasons behind why they are effective. They put in the hours to learn the practical skills. As the "Internet of Things" expands, IT and rotary encoder makers are using the occasion to have new innovative hardware devices. More automation will be needed for both the industrial and the consumer contexts as the number of devices keeps growing. Vulnerabilities in software and hardware will rise and including automation in IoT control systems. Since current end devices and wearable have little to no built-in security, data from IoT hardware equipment and sensors will be handled by proxy network servers in the near future. The IoT client device, which is put in the field, uses MQTT to transmit interior system data such host name, MAC address, current core temperature, the system uptime. In this instance, the MQTT Broker receives the information and transfers it to the server, which then refreshes the database and dynamically displays the data on the homepage. As a result, we have successfully tested the remote management of on-field instruments in practice. The planned concept for a remote OTA (over-the-air) download is an active campaign.

REFERENCES

[1] M. Díaz, C. Martín, and B. Rubio, “State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing,” *Journal of Network and Computer Applications*. 2016. doi: 10.1016/j.jnca.2016.01.010.

[2] A. Sajid, H. Abbas, and K. Saleem, “Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges,” *IEEE Access*. 2016. doi: 10.1109/ACCESS.2016.2549047.

[3] C. S. Nandyala and H. K. Kim, “From cloud to fog and IoT-based real-time U-healthcare monitoring for smart homes and hospitals,” *Int. J. Smart Home*, 2016, doi: 10.14257/ijsh.2016.10.2.18.

[4] P. Divya Vani and K. Raghavendra Rao, “Measurement and monitoring of soil moisture using Cloud IoT and android system,” *Indian J. Sci. Technol.*, 2016, doi: 10.17485/ijst/2016/v9i31/95340.

[5] R. Al-Shaqi, M. Mourshed, and Y. Rezgui, “Progress in ambient assisted systems for independent living by the elderly,” *Springerplus*, 2016, doi: 10.1186/s40064-016-2272-8.

[6] U. Dhanaliya and A. Devani, "Implementation of E-health care system using web services and cloud computing," in *International Conference on Communication and Signal Processing, ICCSP 2016*, 2016. doi: 10.1109/ICCSP.2016.7754306.

[7] H.-J. Yoon, "Development of Contents on the Marine Meteorology Service by Meteorology and Climate Big Data," *J. Korea Inst. Electron. Commun. Sci.*, 2016, doi: 10.13067/jkiecs.2016.11.2.125.

[8] N. Chen, Y. Chen, S. Song, C. T. Huang, and X. Ye, "Poster abstract: Smart urban surveillance using fog computing," in *Proceedings - 1st IEEE/ACM Symposium on Edge Computing, SEC 2016*, 2016. doi: 10.1109/SEC.2016.25.

[9] K. Kaur, "The Agriculture Internet of Things: A review of the concepts and implications of implementation," *Agric. IoT Int. J. Recent Trends Eng. Res. Issue*, 2016.

[10] S. Tyagi, A. Agarwal, and P. Maheshwari, "A conceptual framework for IoT-based healthcare system using cloud computing," in *Proceedings of the 2016 6th International Conference - Cloud System and Big Data Engineering, Confluence 2016*, 2016. doi: 10.1109/CONFLUENCE.2016.7508172.

CHAPTER 19

AN INTRODUCE TO DIFFERENT COMPONENT AND PROTOCOLS OF THE IOT AND ITS USES

Dr. Pooja Sagar, Assistant Professor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id-pooja@sanskriti.edu.in

ABSTRACT

The Internet of Things (IoT) is a framework in which things possessing sensors, actuators, and computing interact with each other order to achieve a useful task. We review the most recent techniques, procedures, and implementations in this newly developing domain in this study. In besides highlighting some of the most significant technologies and highlighting certain applications that possess the potential to substantially enhance human life, primarily for the elderly and others with special needs, these survey report suggests new unique categorization for IoT technologies. When comparison to other survey surveys conducted in the field, this one is far more thorough and covers all of the key technologies, from sensors to implementations.

KEYWORDS: Cloud Computing, Cloud Service, Internet of Things, IoT Devices, Sensor Network.

INTRODUCTION

Dynamic Characteristics of Internet of Things

IoT is a dynamic global distribution infrastructure of physical and virtual objects with distinct identities that are integrated with software, sensors, electronic controls, electronic components, and network connectivity to support intelligent applications by gathering and transmitting data. The important factors in understanding are listed below:

A. Zero-order System:

The output displays a quick response to that same input signal. Energy-storing components are not provided. Potentiometer assessments, for instance, or linear and spinning displacements.

B. First-order System:

The output steadily approaching its ultimate value comprised of a mechanism for storing and transferring energy.

C. Second-order System:

Intricate output reaction while reaching steady state, the projector's predicted optimal oscillates.

Sensor Classification:

1. Passive & Active
2. Analog & digital

3. Scalar & vector

i. **Passive Sensor:**

Unable to perceive the input on its own. Examples include sensors for temperature, water level, soil moisture, and acceleration.

ii. **Active Sensor:**

Recognize the input on their own. Radar, sounder, and laser altimeter sensors are a few examples.

iii. **Analog Sensor:**

A continuous function of the sensor's input parameter determines its response or output. For instance, a temperature sensor, an LDR, an analogue pressure sensor, and an analogue Hall Effect.

iv. **Digital Sensor:**

Binary character of response. Designing for the shortcomings of analogue sensors additionally, it has additional circuitry for bit conversion in addition to the analogue sensor. For instance, a digital temperature sensor and a passive infrared (PIR) sensor (DS1620).

v. **Scalar Sensor:**

Only determines the input parameter's magnitude. The sensor's response depends on the size of some input parameter not impacted by how the input parameters are oriented. example: sensors for temperature, gas, strain, colour, and smoke.

vi. **Vector Sensor:**

The sensor's response is influenced by the size, direction, and orientation of the input parameter. For instance, sensors with an accelerometer, gyroscope, magnetic field, and motion detector.

Now, some of these elements will indeed be present in a smart city:

i. Smart Homes:

Smart parking lots must also include occupancy sensors in each parking space to identify the presence or absence of a vehicle in that location. The person who wants to park may choose a free spot by simply using such a mobile application that displays the location of the parking spot. Smart retail, industrial automation, smart highways, among other topics. These are only two of the Internet of Things' most actively used implementations[1]–[3].

ii. Exactly what does the Internet of Things entail?

It refers to giving ubiquitous sensors and items network services and processing capabilities to enable them to share and consume data even without human interaction or a minimal amount of human interference. As a result, the Internet of things is a dynamic global distribution infrastructure with personality capabilities based on numerical and interoperable communication channels, where physical and virtual objects have individuality, physical characteristics, but instead virtual personalities, use open protocols that are easily incorporated into the information network, and more often communicate information associated to users and their eco system.

iii. The requirements of building an IoT system are as follows:

- **Dynamic:** IoT systems and devices should be be able to quickly adjust to changes in the environment.
- **Self-Configuring:** This should make it possible for so many devices to cooperate in order to carry out certain functionalities.

Should work on interoperability communication protocols to make it easier for different gadgets to interact with one another. Each IoT device should have a distinct identity that supports Internet-based control of it. As a result, everything we mentioned will have sensors installed into it some titles reflect this by having the term "smart" added to them, such as "smart city" or "smart house".

Some of the ground-breaking technologies that we might assume from the Internet of things technologies involve Smart City and Smart Home. This year, well-known firms are about to bring some of the previously mentioned products to the market. A new smart refrigerators from LG will be available which thus uses digital tags and expiration stamps to warn us when the food is indeed ready to spoil. Many of the above-mentioned smart city components will be implemented as part of a plan for smart cities that even the Indian government has presented [4], [5].

Voice over Internet Protocol

i. Voice over Internet Protocol (VoIP):

By using a broadband Internet connection as opposed to an analogue (normal) phone line, Voice over Internet Protocol (VoIP) technology enables voice calls to be placed. While some VoIP services only let you connect other subscribers, others could let you call anyone at all. They have the option of possessing or not having a phone number that normally includes, long-distance, mobile, and internationally numbers. While some VoIP programs can only be used with a workstation or specialized VoIP phone, everyone else let you use a regular phone that has been linked to a VoIP adaptor as mention in Figure 1.

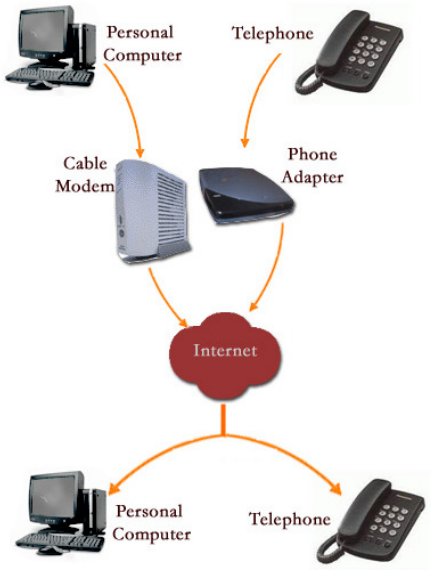


Figure 1: Illustrated that the Working Process of VoIP.

VoIP services turn your voice into a digital signal for Internet transmission. The signal is changed into a normal telephone signal before it reaches the intended destination if you are dialing a traditional phone number. VoIP makes it possible to make calls from a computer, a dedicated VoIP phone, or a traditional phone that is linked to an adaptor. Meanwhile, wireless "hot spots" in common areas like parks, airports, and cafés let you use the web and maybe operate VoIP services wirelessly.

ii. Working of VoIP:

VoIP services that use the Internet transmit voice as a digital stream. The signal is transformed to a standard telephone signal, or an analogue signal, before it reaches the intended destination if the conventional telephone number is dialed. With VoIP, you may be able to place a call right from your computer using a dedicated VoIP phone or from a regular phone using an adaptor. In places like airports, hospitals, cafés, etc., there are wireless hot spots that let you establish an Internet connection and use VoIP services wirelessly.

iii. Equipment's Required:

It is necessary to have a high-speed Internet connection, which may be achieved via a cable modem as well as other high-speed options such a local area network. It is necessary that you use a computer, adapter, or special phone. Some VoIP services may only be used with some of these VoIP computers or smartphones. You may connect a conventional phone coupled with something like a VoIP adaptor with a few other services. A cheap microphone and perhaps some software are required if you use a computer. VoIP phones function basically the same as regular handsets and plug right into your internet service. You can dial using a VoIP adapter-equipped smartphone exactly as you normally would, and the phone carrier could even provide a landline phone.

iv. Advantages of VoIP:

- Some VoIP services include apps and functionalities that are either not offered by conventional phones or are offered but at a premium price.
- It is possible to avoid having to pay for both a wired network and a landline.
- A connection may be made more smoothly than with an analogue transmission.

v. Disadvantages of VoIP:

- Some VoIP providers may not supply backup power, and some VoIP services may not function during power outages.
- Not all VoIP providers use emergency service numbers to communicate directly to emergency services.
- Directory help could or could not be provided by VoIP companies.

Revolution of Internet of Things- Internet of Everything (IoE)

Nobody can likely envisage life without the internet having had the influence it has. Since its beginnings, the internet has evolved significantly, leaving all the complexity behind. By conforming to societal dynamics, it has grown more user-friendly. Even while the society has progressed into a "network society" and is no longer merely a society, we cannot conclude that this was the outcome that people have been striving for several thousand years. Humans now

have such a strong need for connectedness that the sole causes of separation are changes in bandwidth and cost.

Internet of Everything (IoE):

Although the idea of IoE has been in existence for a while, the majority of people are unaware of it. Have you investigated tying your internet-enabled products, such as laptops, smart watches, and smartphones, to your moderate equipment, such as doorknobs, coffee machine, fans, and coffee makers? Possibly not by developing an ecosystem of characterized by various and allowing them to connect, gather, and share the information, either using or without wires, IoE has made it possible to simplify our lives. We may now dim the kitchen light from the bedroom or regulate the bedroom fan from the kitchen. IoE, to put it more simply, is the fusion of people, data, institutions, and objects.

Change is the only constant in life so is the case with technology. Technology is rapidly changing every day and is changing the social fabric around it.

IoT vs. IoE

Is there a distinction between the Internet of Everything (IoE) and the Internet of Things (IoT)? If the answers is "no," you are most likely in error. It's really crucial to understand the distinctions since the IoE is already becoming into a vital instrument in everyone's life:

i. When juxtaposed to the Internet of Things, the Internet of Everything is a novel idea. IoE is often referred to as the intense level of IoT by technology professionals. But it spans so this whole IoT space and even a little something beyond.

ii. The Internet of Everything (IoE) incorporates more than just machine-to-machine (M2M) connectivity. It enables intuitive conversation between humans and machines, fusing the two very potent knowledge sources to produce a superhero source. In scientific terms, it is put forward as:

    1. Machine to people (M2P)
    2. People to Machine(P2M)
    3. People to people communication(P2P)

IoE is a place where all the routes, among them those between people, machines, and technology, converge. To simplify the process, the Internet of Everything (IoE) is a network of sensors as well as detectors that are used to record, analyses, and maintain tabs on every movement performed by either humans or technology.

Application:

i. Saving Lives By Connecting Roads and Hospitals:

Around 857 cyclists died in the US in 2018 as a result of traffic accidents, according to the US Department of Transportation. Some experts have hypothesised that these lives may have been spared by using the IoE. Medical care may be delivered, that could save many lives, by connecting a rider's visor to essential services like traffic lights, hospitals, and neighborhood police stations via sensing. So that the ambulance arrives at the scene in a timely manner, the ambulance is able to interact with the street lighting to show green lights the entire journey, the victim can be transported to the hospital without any barriers blocking the way, and the doctor

is able to be prepared only with necessary supplies when the patient arrives. This way, information about just the patient's criticality can be immediately received by the doctor by observing a hospital around the area right away[6], [7].

ii. Supply Chain Management:

As a result of globalization, supply chain management has grown in importance and faced intense rivalry. The timing of transportation may be coordinated earlier with the supermarkets if there is a system in place to notify the trucks of the early harvest. This will allow the groceries to keep an eye on their supply and prevent overstocking sales. By doing this, markets may avoid enduring financial losses, and customers will always have access to fresh products. Through a shared network, even harvesters may engage with merchants directly and sell their goods at a profit without suffering losses by forsaking middlemen. Customers may engage with retailers through their cellphones to check alerts for new goods arrivals and take advantage of early bird promotions, which will increase customers' satisfaction even further. All parties interested in the game stand to gain from it.

iii. Elderly Care:

Senior citizens today make up a significant proportion of the population, and they have very distinct demands. Many academics and manufacturers have made countless attempts to satisfy these demands and lessen their daily struggles. The role of IoE may assist older adults remain active and stay in contact through their loved ones, which can be a response to these common issues. The elderly may be cared for by a variety of machines that are available on the market. These robots can provide timely medicine, monitoring their health, and even help someone with any difficulties with mental health they may be having by speaking with them. These robots enable emotional simulation, helping people uses cellphones to communicate with their near and dear ones or providing company to those dealing with mental illness.

iv. Agriculture is No More a Hectic Human Task:

With a growing population comes an ever-increasing need for food, yet despite supply growth, demand has always been completely dwarfed by supply. To discover methods to boost food production, governments all through globe are implementing new regulations, offering farmers incentives to use cutting-edge technology, and raising their R&D expenditures. Although there have been a few small-scale experiments, smart farming has never been used extensively. Precision farming is the solution to go in order to eliminate hunger, improve returns on investments for farmers, and close the demand-supply gaps. The Internet of Everything (IoE) has the potential to enable changes in the agricultural industry by helping farmers monitor soil moisture, nutritional composition, and water use, as well as by linking them directly to markets.

v. Smart city technology as a solution to urban mobility:

A Californian city called Santa Clara makes use of cloud-based data to improve traffic. To monitor the recordings, highway cameras being consolidated in a cloud-based command center. More dynamic traffic projections are offered, decreasing road congestion and giving employees access to less crowded routes, lowering the likelihood of accidents. Another northern Californian city, San Jose, has started a traffic planning project to better understand peak hour traffic and lessen the accidents it causes. IoE has been tested and demonstrated in a

few of these situations, but there are more applications for this game-changing technology that may be used as examples throughout the development of technology.

Internet of Everything (IoE) in Business:

Since the dawn of time, the supply chain has existed and continued to expand. What is the root of the growth? The feedback system, which introduced "target marketing" into the equation and made customer pleasure a key aspect impacting the whole organization, was the first element that helped form an exceptional business model. This business has been significantly impacted by IoE by the introduction of several technologies that comprehend the demands of its clients. Micromarketing is mostly related to the various websites that enable clients to contact company owners with their needs. Additionally, IoE has also been utilized in the development of platforms for ERP-software, such as SAP-Cloud-Platform. This serves as an integration and extension platform for a variety of applications. Applications built using SAP help the customer electronics organization and improve the sales process. To redesign the company, all the multiple service lines must be interconnected and engaged [8], [9].

Pros: Let's look at some advantages that the Internet of Everything in this part:

1. **Information Access:**

Accessing evidence will now be simple and convenient no matter where you are. It is simple for you to gather intelligence from anywhere on the universe thanks to the network of connected devices.

2. **Communication:**

Decreased inefficiencies and broadband connections with linked devices.

3. **Affordability:**

The same data which used to take hours to transport will now be delivered in a matter of seconds, dramatically tumbling the suspension and, therefore, the expenses involved.

4. **Automation:**

The term "automation" has gained in popularity and has long drawn the interest of people. This lowers the need for personal communication and improves service quality.

Cons: In this section, let us have a look at all the cons of the Internet of everything:

- **Privacy and security:**

In terms of data security and privacy, there are many "what ifs" and "buts." Data leaks have long been quite a cause for worry. Technology's rewards come at the expense of cybersecurity. This is a major downside, but it may be addressed with the right precautions appropriate safety procedures. The "deep web" and data breaches have subsequently become significant challenges for law enforcement, and Facebook has just been accused of data leaks in evidence in the trial.

- **Dependability:**

Technology has compelled us rely on it for even the easiest chores, which has made people complacent and killed their imagination. The influence of technology on how we live with us daily lives is tremendous.

The Future Work:

Future possibilities for IoE seem to be almost limitless and the ability to deploy, automate, and protect technologies has the possibility of changing industrial processes. Networking gadgets has the potential to ease daily activities, but it also has the ability to diversify corporate operations via the use of data. To meet these concerns, new service providers are developing on the market, establishing new income streams. Academics and academics have staked a significant amount of cash on IoE because they think it will one day satisfy the market's high standards. A social contact ecosystems will provide the technology-driven world new experiences and prospects for distant learning. Li-Fi and 5G broadband communication advancements provide the World Wide Web of Everything (IoE) more traction.

LITERATURE REVIEW

The key challenges facing the Internet of Things are security and confidentiality (IoT). IoT is encountering a number of difficulties, namely incorrect device updates, an absence of effective and reliable cryptographic protocols, user ignorance, and well-known active device monitoring. We are examining the history of IoT systems and safeguarding measures in this work, as well as different security and privacy concerns, methodology for securing IoT-based environments and systems, current security quick fixes, and the best privacy product lines required and appropriate for various layers of IoT-driven applications. In this study, we suggested a novel IoT layered model that is stretched and general with layers identification and privacy and safety components. Installation and evaluation of the suggested IoT system with cloud and edge support. The top layer was implemented using the cloud-enabled appropriate atmosphere in AWS. Between each of these levels, there would have been security measures and crucial management sessions to guarantee the confidentiality of the users' information. To facilitate data flow out across levels of the suggested cloud enabled IoT paradigm, we built security features. The suggested developed system not only eliminates potential security flaws, but it can also be utilized in conjunction with the best security measures available to reduce the cybersecurity risks that every one of the three layers cloud, edge, and IoT faces.

Internet of Things (IoT) is still ambiguous. IoT may enable variety of communication patterns, such as human-to-object, object-to-object, and object-to-object, while going to employ traditional network infrastructure. This is how it is usually understood. However, as the majority of network technologies and communication protocols have been forms and spaces for unrestrained items, integrating IoT gadgets through into normal Internet has uncovered a number of security issues. Additionally, IoT items have their own limitation in terms of memory, bandwidth, and faster processors. Consequently, IoT vision has been impacted by previously unheard-of assaults that target both persons and businesses. Some samples of these attacks include invasion of rights, criminal gangs, mental anguish, and the propensity to endanger human lives. Therefore, it is essential to offer a thorough taxonomy of IoT cyber-attacks and the various responses against them. In this research, we present a unique four-layered IoT reference model based on the basic elements approach, in which we establish a thorough IoT assault model that consists of four important stages. Finally, we demonstrate the correlation between each assault and indeed the security objectives it has disobeyed, as well as a number of responses to safeguard each asset. To the of our knowledge, this is the first study that puts forth the effort to present an extensive IoT vulnerabilities model based on a prototype that is blocked by skyscrapers.

Internet of Things (IoT) has become an important technology that enables various machines and equipment to communicate among themselves across heterogeneous networks. The combination of various methods is anticipated to significantly increase the promise of IoT applications both now and in the future. Today, the secure communication amongst coupled IoT components is a major source of worry. Therefore, the establishment of an authentication system that enables safe communications between IoT components has already become essential. In order to provide secure communication between multiple IoT entities, we presented an identity-based authorization and key agreement protocol for the IoT environment in this research. The designed protocol makes use of the physically unlovable functionality, which improves to the IoT components' strong resistance to physical assault. We provide a thorough analysis of the proposed protocol that establishes its perfect forward secrecy, equipment anonymity, and intractability. It also exhibits its resistance to needs considerable, IoT node impersonation, and server impersonation assaults. Using the well-known Random Oracle Model, the proposal protocol's security properties are retrieving information as well (ROM). Additionally, telecommunication and computational overhead have been thought about while evaluating the performance of the developed protocol. The assessment of the designed protocol's security and efficiency demonstrates its advantages to other comparable protocols .

DISCUSSION

The design of the instruments is the first thing to be taken into consideration. Although there may not be much of a selection when it comes to the sensors themselves, there is absolutely a wide range of options that are available when it to the processing and communications capabilities that are provided with the sensors. We have a variety of options, from tiny sub-mW boards designed for sensor specks to Arduino or Atom boards that need 300–500 mW. The decision we make here is based upon the amount of analytics and data preparation we want to undertake at the sensor level. Second, there is the logistical challenge. We require board design skills, which may not be easily accessible, to produce a sub-mW board. Therefore, it would be wise to include a sensor in a kit with an integrated CPU that is widely available from vendors.

Communication is the next crucial aspect to think about. The main problem with IoT nodes is electricity. The choice of networking technology is crucial since a significant portion of the entire power is used for sending and receiving messages. The distance in between receiver and the transmitter and the kind of obstructions, signal distortion, background noise, and regulatory rules are the crucial elements that we need to think about. We must choose a certain wireless networking protocol based on these important factors. For instance, Zigbee may be used to communicate just inside a separate building, but Sigfox or LoraWAN should be used to communicate through a smart city. The frequency and wattage that may be used for transmission are sometimes subject to substantial limitations as well. Government entities primarily impose these restrictions. All of these considerations must go into the decision-making process.

Next, let's discuss middleware. The first consideration to be taken is whether to use a proprietary solution or an open source middleware like FiWare. Both have pluses and minuses. Although open source middleware is, in principle, more versatile, they could not have full compatibility for Internet of Things (IoT) devices. Even though it would be ideal, not all internet protocols and hardware may be compatible with middleware solutions. Therefore, a proprietary solution is preferable if we want precise compatibility with certain technologies

and protocols. Open source solutions, however, often have lower costs and are simpler to implement. Additionally, we have decide on the reference implementation and confirm that it is interoperable with the firewalls employed by the participating businesses. In general, from this perspective, using a protocol based on HTTP is the best option. Furthermore, we must decide between TCP and UDP. When it comes to power usage, UDP is always cheaper. We also need to take into account querying languages, facilities for creating dynamic warnings, including alternatives for storing sensor data streams.

IoT devices have internal sensors, actuators, CPUs, and communication devices for this intelligence and connectivity. IoT is a collection of several technologies that operate in concert even though opposed to being a single technology. Devices that aid in interfacing with the physical world include actuators and sensing devices. In order to draw conclusions that are relevant, the sensor data must be intelligently processed and retrieved. Remember because we interpret the word "sensor" widely; a cell phone or even a toaster oven might qualify as a sensor if it make a concerted effort about its present condition. A device known as an actuator is one that alters the surrounding, such the thermostat controller in an air conditioner[8].

Data processing and storage might take place on the network's edge or at a distant server. If data preparation is feasible, it is usually carried out at the sensor or another nearby device. The data that has been processed is then often transferred to a distant server. The resources available, which are often severely limited owing to restrictions on size, energy, power, and computing capacity, also limit the storage and processing capabilities of an IoT item. As a consequence, the key problem in doing research is ensuring that we get the appropriate data at the acceptable degree of precision. There are difficulties in communicating in addition to issues with data processing and gathering. Because IoT devices are often located at geographically scattered sites, wireless communication is the primary method of communication between them. The wireless channels are unstable and often exhibit significant rates of distortion. Communication methods are crucial to the research of IoT devices since in this context successfully transmitting data without too many retransmissions is a significant concern.

CONCLUSION

The Internet has stretched to practically every region of the world today and is having an immeasurable impact on the way people live their lives. The voyage is still far from done, however. A very broad range of appliances will soon be online as we move into an epoch of increasingly more comprehensive connection. The "Internet of Things" era is going to begin. Many various writers have defined this phrase in various ways. Let's examine two among the most often used definitions. Numerous sensors and actuators are used to interface between the physical and digital worlds. These abilities are used to inspect the object's status and, if possible, alter it. The name "Internet of Things" describes a brand-new kind of environment where essentially all of the appliances and products we use are linked to a network. They may be used in harmony to complete difficult challenges that call for high intellect.

Now that the data has been processed, some action must be performed based on the conclusions that have been drawn. There are many different types of actions. Actuators allow us to directly alter the physical environment. Or we might work remotely. For instance, we might

communicate with other intelligent objects. The process of bringing about a change in the physical world often depends on its current condition. Context awareness is what we refer to as. Because an application might react differently in various settings, each action is executed while taking context into account. For instance, a person could dislike being interrupted while on vacation by messages from his workplace.

REFERENCES

[1] A. Laya, C. Kalalas, F. Vazquez-Gallego, L. Alonso, and J. Alonso-Zarate, "Goodbye, ALOHA!," *IEEE Access*, 2016, doi: 10.1109/ACCESS.2016.2557758.

[2] M. Stočes, J. Vaněk, J. Masner, and J. Pavlík, "Internet of things (IoT) in agriculture - Selected aspects," *Agris On-line Pap. Econ. Informatics*, 2016, doi: 10.7160/aol.2016.080108.

[3] C. A. Trasviña-Moreno, R. Blasco, R. Casas, and A. Marco, "Autonomous WiFi Sensor for Heating Systems in the Internet of Things," *J. Sensors*, 2016, doi: 10.1155/2016/7235984.

[4] S. H. Lee, D. H. Kim, and H. Y. Lee, "Smart IoT hardware control system using secure mobile messenger," *Trans. Korean Inst. Electr. Eng.*, 2016, doi: 10.5370/KIEE.2016.65.12.2232.

[5] M. Stočes, J. Vaněk, J. Masner, and J. Pavlík, "Agris on-line Papers in Economics and Informatics Internet of Things (IoT) in Agriculture -Selected Aspects," *AGRIS on-line Pap. Econ. Informatics*, 2016, doi: 10.7160/aol.2016.080108.

[6] H. Hamadeh, S. Chaudhuri, and A. Tyagi, "Area, Energy, and Time Assessment for a Distributed TPM for Distributed Trust in IoT Clusters," in *Proceedings - 2015 IEEE International Symposium on Nanoelectronic and Information Systems, iNIS 2015*, 2016. doi: 10.1109/iNIS.2015.17.

[7] M. Brachmann, O. Landsiedel, and S. Santini, "Concurrent Transmissions for Communication Protocols in the Internet of Things," in *Proceedings - Conference on Local Computer Networks, LCN*, 2016. doi: 10.1109/LCN.2016.69.

[8] M. Riecken, K. Lessmann, and D. Schillero, "Internet of Things: a possible change in the distributed modeling and simulation architecture paradigm," in *Modeling and Simulation for Defense Systems and Applications XI*, 2016. doi: 10.1117/12.2223979.

[9] R. Petrolo, A. Roukounaki, V. Loscrí, N. Mitton, and J. Soldatos, "Connecting Physical Things to a SmartCity-OS," in *2016 IEEE International Conference on Sensing, Communication and Networking, SECON Workshops 2016*, 2016. doi: 10.1109/SECONW.2016.7746805.

CHAPTER 20

AN ANALYSIS TO ADDRESSING CLOUD-RELATED THREATS TO THE IOT

Dr. Lokesh Kumar, Assistant Professor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id-lokesh@sanskriti.edu.in

ABSTRACT

These risks include unsecure data flows between the cloud and the edge computing environments, lack of IT expertise in configuring the cloud for maximum security and data breaches that compromise data integrity and customer and client data privacy. The main objective of this paper is to create the information about addressing cloud related threats. In future this paper will be helps to another students and author for their work.

KEYWORDS: Cloud Computing, Cloud Service, Internet of Things, IoT Devices, Sensor Network.

INTRODUCTION

The Internet of Things (IoT) permits consumers to link billions of intelligent machines and disseminate information, monitoring, but instead control for services like connected home automation systems, connected agricultural systems, connected surveillance cameras, connected power grids, and associated critical infrastructure control and control. The Internet of Things (IoT) is the most recent modern strategy that consistently blurs the lines distinguishing artificial and natural settings by continually digitalizing physical systems geared to provide value-added services to handheld devices. This life-saving introduction must become a collection of interconnected devices in an increasingly connected world, enabling surgeons to conduct remote operations and people and evaluate their homes and power service provider. The Internet of Things is run by primary function software, which might do so by Feeling, trying to control, and changing the state of things.

Organize the infrastructures with a framework for vital national situational security and appropriate efficiency. The proliferation of smart devices linked to the Internet of Things (IoT) has massively increased due to the variety of IoT application technologies and is predicted to surpass 20.4 billion by the end of 2020. It will be very challenging for the decentralized Internet of Things to apply electricity and bandwidth for activities effectively because of the increasing number of heterogeneous connected systems to the IoT and data creation. According to this approach, the idea of combining cloud computing with both the IoT emerged.

Multimedia material is produced when the IoT and the Cloud are connected. It will be crucial to handle entertainment well and carry out effective cloud strategic planning since it requires more computational power, storage, and resource scheduling. Otherwise, very rapid processing is necessitated for IoT services with important responsibilities. In this situation, your user is unable to converse over the Internet over the Cloud range. Large-scale IoT deployments have many conveniences, but they also increase security risks first from edge to the cloud as there are more IoT devices and a more complicated IoT infrastructure as a result. Most firms see that the

devices themselves as potential attack vectors when endeavouring to analyse risks rather than the services that the cloud provides.

However, enterprises increasingly turning to cloud services to lessen the burden on their own IT architecture as a result of all the data being gathered via the edge, which adds a whole new level of cloud security problems. Due of this, many businesses unhappily wait until it is too late to realise how bad it is to develop an IoT cybersecurity program. A measured strategy may assist security professionals reduce risks immediately while threats grow and able to adapt in the future. In this case, prevention is much stronger than treatment. When it comes to maintaining, monitoring, and safeguarding all connected IoT settings, corporations who have just begun to use the IoT or those trying to grow their existing IoT networks are practically in the same circumstance. The IoT depends on cloud computing to interconnect servers, analyse sensor data, enhance computational power, and expand storage capacity. The vulnerabilities to IoT security described here are peculiar to the cloud.

Major cloud-related challenges facing the IoT

i. API gateway misconfigurations

Application programming interfaces (APIs) make fast and efficient communication with IoT cloud servers possible for device manufacturers and developers. An IoT device can request specific actions from the cloud server using an API gateway and vice versa. The gateway serves as a doorway to the cloud as it limits IoT device traffic. It also facilitates specific commands such as turning the device on or off, checking the device's status, upgrading the firmware, downloading or uploading screenshots or videos, and accessing data. Threat actors can use a misconfigured device or a cloud service for malicious activities such as faking a command sequence by changing the logic between the APIs, thus causing more vulnerabilities. Other possible activities include user spoofing, man-in-the-middle (MiTM) attacks, denial of service (DoS) attacks, and session replays. Our report on cloud-based IoT solutions also provides an insightful context on this and other related threats.

ii. Identity and Access Management (IAM) misconfigurations

IAM is a framework of processes, policies, and technologies that enables the management of digital devices and identities. An IAM framework allows information technology (IT) managers to control user access to critical information within their organizations. Developers, on the other hand, configure specific rules and policies for IoT devices connected to cloud servers through the IAM. As this is done, every IoT device is expected to process a huge workload equivalent to the corresponding limitations for data access and streams. Some cloud-based IoT devices utilize the same design, logic, and trust chain as some cloud-based servers and services used for alignment and ease of configuration. Threat actors can exploit IAM misconfigurations in many ways. They can breach the server, block data traffic and access, launch more complex attacks, control the cloud service, or spoof a guest or device user.

iii. Cloud misconfigurations

Misconfiguration is a common problem in cloud computing, as it can provide a path for attacks like data exfiltration. Misconfigurations and similar security flaws in the cloud can cause serious damage to the IoT ecosystem to which it belongs.

iv. Unsecure communication and data flow between the edge and the cloud

Access controls and the integrity of the data sent between the endpoints is endangered if the cloud lacks security features such as authentication and encryption. Weaknesses in the security of data traffic or path exposes the device or the cloud server.

v. Misuse of cloud services

Threat actors can wilfully violate their contracts with the cloud platform by launching attacks on the networks such as brute force attacks, Trojans, SQL injections, botnets, phishing, and denial of service (DoS) attacks. Some cloud service providers may not always have the ability to detect the attacks on their networks because they can neither generate nor block the attacks.

Security Recommendations

Here are a few pointers to consider for minimizing cloud-related risks in your IoT infrastructure:

i. Have a system for device identification, visibility, and inventory in place.

One of the first steps to establishing a good security foundation is to assess your organization's various assets and business processes. Establishing an accurate inventory that is regularly updated can be challenging because of the fast proliferation of devices with varying life cycles and functionalities. More often than not, there is a discrepancy between what enterprises think they have versus what they actually have. Also, knowing what normal device behavior looks like can help determine a potential breach should traffic deviate from the norm. These steps are crucial to identifying what your organization needs to protect.

ii. Perform a comprehensive risk assessment.

A thorough asset inventory can help an organization analyze its attack surface. This helps determine the various entry points that threat actors may use. One needs to consider the entire IoT-cloud infrastructure in order to fully understand cloud-related threats. The process is multifaceted: from analysing device communication, administration, and the software and hardware used to documenting physical assets, IoT endpoints, networking hardware, digital assets such as cloud capabilities and databases, and access controls. While the task of risk assessment may seem overwhelming, it is necessary for identifying and prioritizing vulnerabilities.

Adopting a risk-based security strategy requires a definitive overview of the assets to determine the risks they pose. The goal is to establish a baseline so the attack surface they create can be sufficiently defined.

iii. Evaluate current security practices from the edge to the cloud and adopt best practices.

Once current security practices and gaps are assessed, organizations can plan how to implement best practices in all aspects of the IoT-cloud infrastructure.

iv. Towards a More Secure IoT-Cloud Infrastructure

The following pointers can help improve the cyber-hygiene practices in your teams:

v. Implement monitoring and filtering tools at the start

Enterprises need to implement tools to monitor and filter traffic flow from the IoT endpoints to the cloud at the outset. This enables the security team to detect suspicious activity, determine

anomalies, and ensure visibility for all connected devices. Define a clear, effective, and detailed access control plan. Develop a complete access control plan that covers the entire environment from the cloud to the edge. Identify all users, groups, or roles and define detailed authentication and authorization policies that apply throughout the IoT-cloud ecosystem. Consider the principle of least privilege, which refers to giving users only the access or permissions needed to perform their tasks.

vi. Perform vulnerability checks regularly

To minimize the threats arising from cloud, API, and IAM misconfigurations, enterprises can conduct vulnerability testing to these components, along with the rest that comprise the entire IoT-cloud ecosystem. Consistency is key.

vii. Use secure passwords for both IoT devices and linked cloud services

Successful data breaches still happen because of weak credentials. Since passwords are still the primary means of authentication, enterprises should enforce strict password policies to prevent breaches.

viii. Inspect cloud infrastructure for control features before use

Organizations that use the cloud to manage their IoT devices need to check the cloud infrastructure for vulnerabilities and see if proper controls are in place. Companies seeking to migrate operations to the cloud should read the Service Level Agreements (SLA) carefully to be clear about which security controls the cloud provider will maintain and which ones they will have to implement on their own.

ix. Consistently implement cloud security procedures

Efforts to establish security protocols will all be for naught if they're not maintained, monitored, and acted on in a timely manner. While cloud providers carry much of the security burden, it is incumbent upon enterprises to take charge of access control, traffic segregation and filtering, security configurations, data protection, virus protection, and other incident monitoring, including prompt response and prevention.

IoT security risks that are frequently observed include

i. **Breach of in-vehicle security:** According to a recent studies, more than 50% of US drivers are exposed to hacking, and many of these assaults actually happen without the victim's knowledge.

ii. **Hacking IoT devices:** One of the most popular techniques to take advantage of IoT devices seems to be to tamper with its software, which might also lead to damaged or deleted data.

iii. **Data theft:** Data theft seems to be a typical IoT security risk that is frequently utilized to obtain personal or financial information data.

iv. **Insecure internet connections:** Devices connected with IoT networks may be vulnerable to hacker’s assaults due to a lack appropriate security standards.

v. **Open-source IoT firmware flaws:** A lot of IoT devices use transparent firmware, which is sensitive to assaults.

IoT Security Solutions

Although there is no one technique that will shield all IoT devices from each and every danger, there are a few standard operating procedures that may assist to lessen the hazards that some of these devices bring. As a single perspective, ensure that all Sensor networks are configured and managed properly. Setting up user logins and passwords, configuring firewalls and antivirus software, and applying software updates all often belong to this category.

Another method is to link IoT devices to company networks or governmental systems via secure wireless networks. In addition to safeguarding against assaults, this prevents the movement of sensitive data across untrusted networks. Finally, it's critical to be knowledgeable about the security dangers posed by IoT devices and to put the right safety measures in place to shield them from assaults. This guarantees that the units are correctly set up, secure from intrusions, and not compromised in terms of personally identifiable information.

Some Examples of End-To-End Security Systems Include

i. Development of Secure IoT products:

We incorporate various layers of security measures throughout the lifecycle of product development to ensure the security of IoT products. To safeguard products from the root, we have been using a secure by design strategy. We incorporate security by design and VAPT testing into your product development lifecycle as part of our security workflow. This approach ultimately helps customers to deploy secure products in the open world that helps protect products from IoT Security related threats.

ii. **Data security solutions:**

These solutions can help to protect data by encrypting it and securing it in a manner that prevents unauthorized access.

iii. Data Loss Prevention (DLP):

DLP solutions can help in preventing data loss by identifying and blocking unauthorized access, copying, and transmission.

iv. Data governance solutions:

These solutions can help organizations in managing their data securely by ensuring that it is accessed only by authorized personnel, stored in a secure location, and protected from unauthorized changes.

Proven Methods for Ensuring Fool-proof IoT Security

i. Expert collaboration simplifies IoT deployments:

Ensuring security from the very beginning of the design process is one of the fundamental ideas. Using expert knowledge should happen as early in the product design process as feasible. It makes sense to work with professionals with extensive knowledge of IoT and cloud technologies, like CloudThat. Due to their strategic alliances with key cloud providers like AWS, Azure, Google, and VMware, these companies can provide tailored IoT security solutions that are in line with an organization's business goals and have demonstrable expertise handling Cloud DevOps and DevSecOps concerns.

ii. IoT cybersecurity from the ground up

Assessing the dangers in the networks and devices is the first step in developing a company's security. DevSecOps strategies should be used by businesses to guarantee IoT cybersecurity from the ground up. Security is included into the software/product development process via the use of DevSecOps practises, and each team member is responsible for enforcing security protocols, making security a fundamental component of the final product.

iii. PKI and digital certificates

The term "public key infrastructure" (PKI) is used. It is an encryption technique that employs digital certificates to verify the identification of persons, devices, or programmer that possess private keys and the associated public keys, as well as an asymmetric method of encryption and decryption (via a public key and private key pair). Man-in-the-middle attacks are prevented because to this.

iv. Network security

Threat actors may always seize ownership of IoT equipment owned by somebody else. Therefore, enterprises need stop port forwarding, maintain authentication methods, and avoid leaving ports open needlessly in order to secure IoT security. They should also make use of firewalls, intrusion detection systems, and anti-malware software.

v. Application Programming Interface (API) security

There is always a chance that hackers would break into the API channels and access IoT devices. Strong API cryptographic protocols are very important to ensure the integrity of data transferred from IoT devices to back-end organizations and to limit access to only infrastructure technologies and developers.

Internet of Things (IoT) is a revolutionary technology that offers effective and dependable answers for the transformation of several fields. Solutions built on the Internet of Things are being designed to autonomously control and monitor agricultural fields with the least quantity of human participation. The paper covers a wide range of technological factors linked to IoT in agriculture. The key elements of IoT-based smart farming are discussed. Network architecture and layers, network topologies, and communications have all been comprehensively discussed in relation to network technologies used in IoT-based agriculture. Additionally, it has also been demonstrated how IoT-based farm systems would work with pertinent techniques like cloud computing, big data storage, and analytics. Safety issues in IoT agriculture have also been talked forward. A list of programmed created for very many facets of farm management leveraging sensors and smart phones has also been presented. In addition to a few success examples, the guidelines and policies developed by several jurisdictions to standardize IoT-based agriculture have been described. Finally, several unresolved problems and difficulties inside this realm of IoT agriculture have now been discussed [1].

Blockchain technology has a diverse range of applications, including online micropayments, supply management monitoring, forensic investigations, sharing of medical records, and insurance payments. By applying the technology to the Internet of Things (IoT), we may establish an IoT network that is verifiable and traceable. Cryptographic protocols is being used in new IoT research to record transaction data, enhance the effectiveness of existing systems, or

build next-generation systems that can offer more security, instantaneous transaction management, highly centralized platforms, offline-to-online collection and evaluation, and other benefits. In this post, we properly investigate some well-known blockchain network as well as the important aspects of IoT blockchain.

"Internet of things" (IoT) refers to the collection of heterogeneous devices, which would include sensors, RFID, and actuators, that work together to build a vast network and enable non-internet network components to create better services, such as connected devices, smart cities, smart transportation, and smart industries. The IoT network, which comprises registration, authorization, data protection, network monitoring, and access control, on the other hand, places a premium on privacy and confidentiality. In addition, the processing and data storage capacity of standard network security prevent its direct use in IoT networks. Additionally, certification is the foundation of the IoT network since it is a need for all components to initiate communications. As a result, authentication security is crucial. We have concentrated mainly on the authentication procedures used by IoT devices in this study whenever discussing security. Therefore, we concentrated significant assaults and technology approaches against the IoT authentication system. We also covered cybersecurity verification methods and IoT authentication assessment methods. Analysis of specifications and design has also been covered in all sections and some recommendations were made. Finally, the goal of our work is to aid research community by presenting security risks, unresolved problems, and new potential applications of IoT authenticating [2].

C. Stolojescu-Crisan et al. illustrated that in recent years, smart home devices have become increasingly popular as daily living has been smoother as a result of quick technology advancements. Almost everything has been automated and digitalized. To facilitate numerous house automation, a system for interconnecting sensors, actuators, and some other data sources is presented in this dissertation. The system, designated as q-Toggle, relies on the robustness of an Application Programming Interface (API), the backbone of a straightforward and widely used communication scheme. Q-Toggle often embedded sensors or actuators that have upstream internet connectivity and perform the Q-Toggle API. The majority of Q-Toggle's devices are designed on Raspberry Pi boards and/or ESP8266/ESP8285 chips. A smartphone application has been developed that allows users to control a series of home appliances and sensors. The q-Toggle system is user-friendly, flexible, and can be further developed by using different devices and add-ons.

Industry sources, corporate executives, and business executives all agree that the next industrial revolution, which is about to begin, has been one of the most disruptive and consequential in human history. Without a doubt, one of the foundations of this industrialization is automation. Customers generally prefer automatic versus manual systems. The Internet has become seamlessly integrated into modern life. Life alone cannot be imagined without the Internet. In this paper, we will show you an automated system that uses the Internet of Things, a rapidly expanding new Internet technology, in the real world (IoT). An IoT-based automation system improves the efficiency, speed, and security of the consumer's life. By employing a web browser and a connection to the internet, this state-of-the-art technology enables the user to fully control all of the house items and appliances from anywhere on the globe. The simulation we constructed for this study is a crude representation of a much bigger real-world system, but the concept, technique, and methodology are the same [3].

The automation of smart buildings and housing has greatly benefited from the Internet of Things (IoT). IoT, cloud computing, and rules-based data are additionally used in the management of smart buildings and residences to guarantee the safety, accessibility, and comfort of just about everyone who uses the space. This research showed that once radio band interference affected the commands and control signals communicated through electrical wiring, the use of IoT for intelligent home automation was more fully adopted in the twenty-first millennium. IoT is determined to improve smart home governance by trying to ensure that home electronics and appliances can be truly controlled remotely and in a practical, secure, and comfortable fashion. IoT, cloud computing, and rules-based real-time evaluation were combined by the author to investigate the case of various devices and devices for command and control purposes. Fire protection connections, security cameras, smart TVs, lighting controls, home automation, air conditioners, doors, fans, and moisture control and gas management systems are among the devices that are taken into account for this evaluation. When it comes to smart home automation without the use of IoT the above tools and equipment operate incorrectly. The use of IoT has optimized the functionality and automation of home and construction equipment and systems to ensure that they efficiently and effectively provide the security, comfort, and access needed for a smart campus, as this study concludes by telling. [4].

The everyday performance of industrial and commodity operations is being redefined by the Internet of Things (IoT). The incorporation of sensors, efficient processing, and widespread use of various wireless technologies on the IoT platform makes it possible for people to connect with their physical environment in great detail. To make it easier for authors and developers to monitor and operate diverse IoT devices, many different IoT platforms have been established in response to the rapid development of IoT. By offering APIs, IoT platforms serve as a link between consumers and basic IoT functionality in general. IoT platforms have a wide range of applications, thus they differ greatly in their topology and design. Therefore the correct design, deployment, and security of IoT systems are complicated by significant configuration discrepancies, which provide a challenge for IoT administration, developers, and researchers.

Smart grids are increasingly integrating gadgets and technologies from the Internet of Things (IoT). There are many exploitable vulnerabilities in these gadgets. The IoT protocol has been improved with security features to fight this. However, these processes require additional processing, which can lead to further delays. The reliable performance of a smart electrical network, which depends on the exchange of information, can be affected by this additional delay. This research examines the real-time characteristics of device-to-device security protocols. We assess how IoT protocols affect the need for real-time operation of smart grid operations i.e. security, control, and monitoring. We assess the scalability and volume of new telecommunications traffic size and latency. The author sets the criteria that the enhanced security procedures must meet.

The devices that connect to the Internet of Things (IoT) want a secure communication protocol with communication channels that are compatible with the network capacity on public networks. As network bandwidth increases, such as wireless technology via 5G, the limited computational power of IoT devices can become a performance bottleneck for encryption and decryption throughput. As a result, IoT devices struggle to achieve the required degree of communication and security performance. In this paper, we use the Unblock Lightweight Cyber method to enhance encryption and decryption performance for IoT devices. Better nanostructures from hardware suppliers should result in more than two-fold performance gains for the author. With

low power consumption, our suggested approach can provide the required degree of communication and security performance[5], [6].

The pace of technological improvement is accelerating with time. People and everyday activities rely significantly on the internet. Of the development and quick development of smart homes, precision agriculture, smart cities, and smart everything, the Internet of Things (IoT) is a field with profound impact, growth, and promise. The Internet of Things (IoT) establishes an environment where everything is connected and computerized. People rely on their smartphones and want to perform their everyday duties quickly and easily. Multiple digital appliances found in typical houses are managed or regulated by separate remote systems. Using many distinct games consoles to operate different kitchen appliances is highly annoying. Nowadays, essentially all types of integrated component are accessible in digital form rather than as appliances. In the literature, several home automation technologies with various standards and executions were suggested. The goal of this study is to develop a Internet of Things-based strategy for a productive system for home automation utilising Arduino and ThingSpeak. The majority of the key components of consumer devices have been automated. The suggested method is successful in that it uses less electricity, stimulates green construction, and lengthens the life of electronic devices. The home's components are integrated, the data has been analysed, and processed using the ThingSpeak cloud platform. Modern MQTT protocol has been put into effect for LAN communication. This paper will provide a technique for IoT researchers and developers to detect, digitalize, and govern dwellings in light of IoT in the future. Additionally, this project serves as a demonstration of how IOT apps will make life simpler [7].

G. Gardašević et al. illustrated that the difficulty posed by the deployment of the Internet of Things (IoT) idea will profoundly affect mankind by permanently changing existing networking and communications infrastructure. The current IoT research efforts are focused on the creation and design of open infrastructures and standards, but before the ultimate installation, there are still many challenges that require to be resolved by a worldwide agreement. The paper discusses design issues for IoT hardware and software components, as well as IoT application context representatives, including smart cities, healthcare, agriculture, and nano-scale applications. It also presents and discusses IoT architectural frameworks proposed under the ongoing standardization efforts (addressed within the concept of Internet of Nano-Things). The early findings for the Time-Slotted Channel Surfing and Message Queuing Telemetry Communication protocol are presented in order to understand the performances relevant to newly suggested protocols for developing Industrial Internet of Things application. The OpenMote computer system and Contiki and OpenWSN, two IoT operating systems, were employed in the testing [8].

DISCUSSION

The goal of this review is to explore the viability of deploying the unstaffed offline retail style. We do this by proposing any smart unstaffed retail store plan based on AI and the IoT. An end-to-end classifications model trained by the MASK-RCNN approach is built for SKU counting and classification based on the data set of 11, 000 photos in multiple configurations that comprise 10 distinct kinds of stock keeping unit (SKU). The approach we recommended does away with character segmentation, which eliminates the inaccuracy that character segmentation produces. This technique provides exceptional counting precision and good recognition accuracy on the test dataset, according to the experiment findings throughout this paper. We will concentrate on strengthening algorithm effectiveness and recognizing rate, lowering number of false positives, and setting up a greater picture data set for more SKU in our forthcoming work.

There are frequent attacks against IoT systems since of their multiple attack surfaces, and as IoT has become more and more widespread, more has been found. Systems must always be shielded from these attackers as effectively as feasible. Experts are looking to AI as a method of defending these systems rationally and in real-time as the quantity and frequency of threats increase. Naturally, hackers additionally utilized to defeat these AI and might employ AI to attack systems. This paper describes common methods was using to try to infiltrate or disrupt IoT and provides a high-level description of how these attacks are executed. Illustrations are also given when required to further explain these arguments. The applications of a range of AI algorithms in cyber security are then investigated. These models are quite often in the process of being developed or are still challenging to execute, making them unique since they are not yet widely used in commercial products. Furthermore, the models shown motivated to participate and might rapidly spread to other threat detection systems. In the context of IoT systems, methods of countering AI threat and countering AI attacker are also considered. As IoT systems expand, these cyber-attack will become an emerging concern, especially as humongous networks like smart cities laboratory activity with them. Not only are humongous networks more difficult to guarantee due to the sheer number of attack surfaces they have, but daily life and safety depend on AI, which should be more or less fault-tolerant. The concerns discussed in this paper are then replicated in a chart, along with conventional or suggested countermeasures against another assault.

CONCLUSION

By laying a solid cybersecurity foundation, a corporation may successfully manage cloud-related IoT risks. This requires using a comprehensive strategy that includes determining what property and data to safeguard, doing a comprehensive risk analysis across all aspects of the IoT-cloud ecosystem, and going to make sure that security protocols are not just in place but are constantly followed. As long as businesses implement a proactive security posture and employ as many best practices as they can, they can prosper from the IoT-cloud converging. The management of information in especial will undergo major transformation as a result of computing and the internet of Things. Depending on the deployment strategy, the cloud is the sole software that can analyses, store, and acquire IoT data. Because of the characteristics of on-demand knowledge, cloud computing is accessible anywhere and anytime there is a Network connection. Many businesses are becoming conscious of the advantages of hybrid cloud computing adoption and the need to embrace it. For a very lengthy time to come, cloud computing will continue making new possibilities for IoT.

REFERENCES

[1] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, “A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming,” *IEEE Access*, vol. 7, pp. 156237–156271, 2019, doi: 10.1109/ACCESS.2019.2949703.

[2] T. Nandy *et al.*, “Review on Security of Internet of Things Authentication Mechanism,” *IEEE Access*, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.

[3] S. Paul, V. Indragandhi, N. K. Kumar, R. Raja Singh, and V. Subramaniyaswamy, “An IoT Based Home Automation System,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 623, no. 1, p. 012014, Oct. 2019, doi: 10.1088/1757-899X/623/1/012014.

[4] A. S. Abdulraheem *et al.*, "Home Automation System based on IoT," *Technol. Reports Kansai Univ.*, 2020.

[5] M. Stočes, J. Vaněk, J. Masner, and J. Pavlík, "Agris on-line Papers in Economics and Informatics Internet of Things (IoT) in Agriculture -Selected Aspects," *AGRIS on-line Pap. Econ. Informatics*, 2016, doi: 10.7160/aol.2016.080108.

[6] S. Rao, D. Chendanda, C. Deshpande, and V. Lakkundi, "Implementing LWM2M in constrained IoT devices," in *2015 IEEE Conference on Wireless Sensors, ICWiSE 2015*, 2016. doi: 10.1109/ICWISE.2015.7380353.

[7] M. Ali *et al.*, "An IoT based Approach for Efficient Home Automation with ThingSpeak," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, 2020, doi: 10.14569/IJACSA.2020.0110615.

[8] G. Gardašević *et al.*, "The IoT Architectural Framework, Design Issues and Application Domains," *Wirel. Pers. Commun.*, vol. 92, no. 1, pp. 127–148, Jan. 2017, doi: 10.1007/s11277-016-3842-3.

CHAPTER 21

AN ANALYSIS TO THE RELATIONSHIP BETWEEN CLOUD COMPUTING AND INTERNET OF THINGS

Dr. Himanshu Singh, Assistant Professor
Department of Computer Science Engineering, Sanskriti University, Mathura, Uttar Pradesh, India
Email Id-himanshu.singh@sanskriti.edu.in

ABSTRACT

IoT cloud computing is used to manage IoT information and acts as a team effort. A centralized server with computational resources that can be downloaded whenever needed is nicknamed the Cloud. Home automation big data packages may easily flow via the Internet using cloud computing. They will just be significant elements of the Digital Revolution when their usage and acceptance become more widespread. It is envisaged that a unique framework combining cloud computing with the internet of objects would be disruptive and enables a wide variety of application scenarios. In future this paper will be separate the proper information about the relation between cloud computing and IoT.

KEYWORDS: Cloud Computing, Cloud Service, Internet of Things, IoT Devices, Sensor Network.

INTRODUCTION

The Internet of Things (IoT) and cloud computing have a symbiotic interaction since one technology supports and complement the other. IoT integrates a multitude of devices and sensors with the capacity of Big Data and real-time analytics. In addition, the scalable infrastructures and processing power required to store and manage this information are offered by cloud computing. These innovations work together to help firms boost productivity, streamline processes, improve enhance decision-making. As a result, the interaction between cloud computing and the internet of things (IoT) is essential for enable companies to expand their operations and operate in the modern digital economy.

Due of this, the usage of computing and the internet of Things has increased dramatically (IoT). But how do IoT and cloud computing relate to each other? And which technology is most effective for your technical specifications? In order to assist you choose which innovation is best for you, we'll investigate the parallels and discrepancies amongst IoT and cloud computing throughout this blog paper.

Relationship between Cloud Computing and IoT

As the globe grows more connected, there has never been an greater demand for dependable and scalable Cloud Computing solutions. As organization's try to take advantage of data to get insights into their operation, the Internet of Things (IoT) is a major driver of just this need.

When it comes to IoT applications, cloud computing delivers the scalability and flexibility required to accommodate a large number of users and equipment, making it the ideal platform. The follow are some crucial ways whereby IoT and cloud computing may interact to help organizations to grow:

i. Increased Data Storage Capacity

Traditional on-premise storage arrays may be rapidly overwhelmed by that of the sheer amount of data supplied by IoT cloud devices. Businesses have practically limitless capability to store and analyse the data thanks to cloud storage.

ii. Improved Data Processing Power

To make sense of the plethora of information being created by IoT devices, organisations need much more storage space as well as enhanced data processing skills. Cloud-based technologies may provide the computational power required to complete demanding analytics jobs.

iii. Greater Scalability

IoT cloud computing's capability to scale up or down as appropriate is one of its primary advantages. This is critical for businesses whose network is continually expanding with incoming IoT devices. With on-premise alternatives, adding more capacity or processing capacity may be both costly and time-consuming. These resources may be added or deleted as required with cloud-based technologies, offering enterprises unprecedented flexibility.

iv. Reduced Infrastructure Costs

By switching to a cloud-based alternative, businesses may severely reduce their infrastructure expenditures. Everything can be operated from either the cloud, so there is no need to investment in pricey on-premise gear or software licencing.

v. Quicker Deployment Period

New on-premise continuity management its initiatives may sometimes take months or even years to conclude. IoT cloud computing gives companies a competitive advantage by making it easier to roll out new apps.

vi. Improved Security

Despite worries about IoT security, installing apps in the cloud frequently proves to be safe than doing it on-premise. This is caused by the fact that cloud providers have made significant advances in security technology and seem to have teams of specialists entrusted with safeguarding data.

IoT built on Cloud Computing

Businesses now have access with never levels of visibility into their operations because to IoT and cloud computing. The economic world is adapting in the following ways courtesy to IoT and cloud computing.

i. Collecting Data from More Sources

IoT enables a company to gather data from a greater number of different sources than ever before. This intelligence may be utilized to automate business processes, make wiser choices, and boost customer satisfaction.

ii. Identifying Trends Faster

Businesses currently have a lot greater ability to see movements than they used to in the past because to the accumulation of information from different sources. Any product or service may be altered to improve its efficiency and efficacy by using this data.

iii. Making Real-time Decisions

Businesses can harness the data they are obtaining to make the decisions in real-time thanks to the convergence of IoT and cloud computing. This supports enterprises in making quick choices overall and respond to shifts in their surroundings.

iv. Automating Processes

The ability to automate operations is one advantage of information gathering. Through the eliminating of redundant stages from their workflows, mechanization may help businesses save dollars and time.

v. Improving Customer Experience

Businesses may implement IoT to gather information about consumer behavior and use it to improve their customer experience. Personalized offerings, improved customer service, and the expansion of incentive systems all are included in this category.

vi. Reducing Costs

Reducing expenses for companies is one of the major benefits of IoT. By automating methods and making wiser judgments, organizations may reduce their spending on employees, supplies, and some other costs.

IoT and Cloud Computing integration

Additionally, in recent years, a younger generation of services built on the idea of "cloud computing" have emerged with the aim of enabling data and information to be accessed from any location at any time, therefore reducing or completely removing the need for hardware resources. The use of computers logistical resources and software at the software level via the utilization of services delivered over the Internet sometimes referred to as "cloud computation." These days, the battle between the top software and IT businesses inside this world is centered on cloud computing services. One technologies that may be used as the foundation for IoT is cloud computing.

Mobile cloud computing is described more accurately as the integration of cloud computing technologies with mobile devices to enhance the mobile devices' computing, memory, storage, energy, and meta - learning capabilities. The result of multidisciplinary methods that combine cloud computing with mobile computing is mobile cloud computing. Additionally, cloud computing offers applications, communications, storage, and computation through to the Internet. The technology behind mobile cloud computing is the result of multidisciplinary research that integrates cloud and mobile computing. As a result, this academic field is also known as mobile cloud applications. The following are some of the key aspects of the cloud computing technology that correlate to both Internet of Things traits:

1. Storage over Internet,
2. Service over Internet,
3. Applications over internet,
4. Energy efficiency,
5. Computationally capable.

When paired with the characteristics of IoT, the advantages of mobile cloud computing in regards to the convenience it provides. It enumerates the advantages of cloud computing

technology in terms of the convenience it supplies. It also lists the key characteristics of innovation related to the Internet of Things. The major goal of the unique Cloud Computing technology features seems to be to enhance and further relate here to capabilities of Internet of Things technology. "Service over Internet" and "computationally competent" are the aspects of cloud computing that have the most impact. In general, it is evident that these two technologies support each other better in terms of many of their aspects. We have the chance to utilize the technology that is given in cloud surroundings more widely thanks to the convergence of IoT and cloud. Through this connection, it is possible to employ data and applications that use Internet of Things technologies. Figure 1 depicts the fusion of IoT and cloud technologies. The cloud enables access to all the data and applications required for IoT connection for mobile and wireless users.

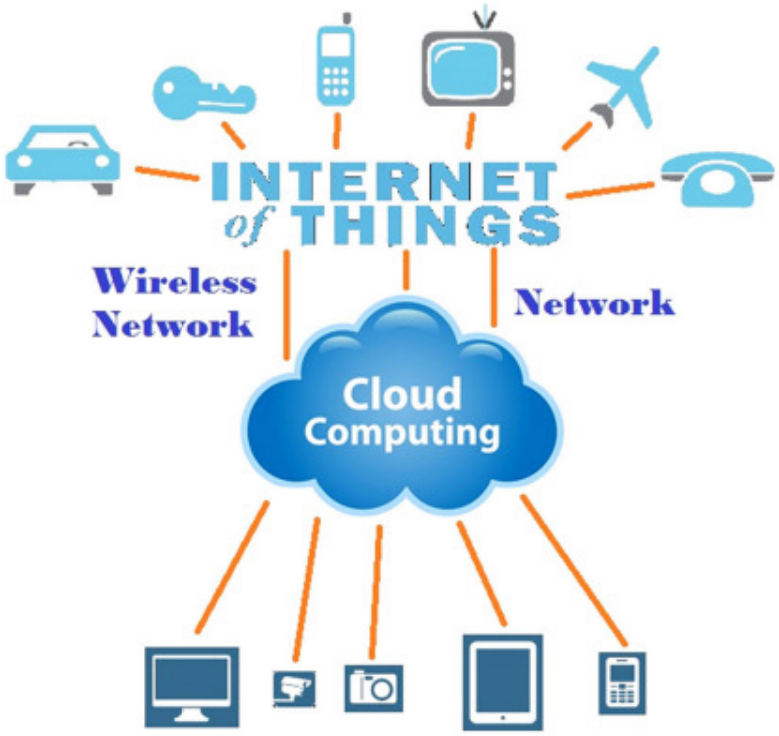


Figure 1: Represented that the IoT & Cloud Computing integration.

Security issues in IoT and Cloud Computing integration

When you combine the keywords Internet of Things with cloud computing, you see a quick and separate growth. First off, the Internet of Things technology may benefit from the almost boundless capabilities and resources of cloud - based solutions, which may help it surmount its technical constraints in terms of processing, storage, and communication. Further, IoT technology broadens its application to connect with objects in the real world in a more widespread and dynamic way, and by providing additional services in several real-world situations, it may be favorable for the usage of Cloud Computing technology. Many times, the cloud might act as a transitional layer, concealing all the sophistication and features required to implement the apps.

When IoT and cloud computing are joined, it can be shown that cloud computing can address several of the holes left by IoT, such as the constrained storage and internet-based applications.

IoT may also cover some of the holes left by cloud computing, such as the major problem of a narrow spectrum. We may think of some drivers for the integration based on incentives like those previously mentioned and the fundamental concern of security in both systems. This integration's security concern is a major one. Difficulties occur when crucial IoT applications switch to cloud computing owing to a lack of confidence in the service provider, understanding of service level agreements (SLAs), and awareness of the physical whereabouts of data. According to polls, important developments therefore need particular attention. Additionally, multi-tenancy may jeopardize security and cause accidental disclosure of private data. Additionally, because of the limitations on computational capacity imposed by the objects, public key cryptography cannot be employed at all levels. These are a few illustrations of the subjects that are now being researched in order to address the major problem of security and confidentiality in the integration of cloud computers and IoT.

The difficulties in blending different technologies in terms of security are instead highlighted.

i. Heterogeneity:

The enormous array of devices, operating systems, frameworks, various services accessible and theoretically leveraged for new or enhanced programs is a massive obstacle for cloud computing and IoT connection.

ii. Performance:

Applications for Cloud Based and Device on a network often bring unique and quality of service (QoS) needs at several levels i.e. for connection, compute, and storage elements, while in some specific cases, these expectations may not be simple to achieve.

iii. Reliability:

Reliability issues typically develop when Cloud Computing and IoT connection is chosen for mission-critical applications, for example, in the context of smart mobility, where cars are continually in motion and vehicular communication and network connectivity is frequently intermittent or unreliable. Frequently sporadic or unreliable. There are several challenges with device failure or equipment that aren't always available when systems are deployed in source of energy situations.

iv. Big Data:

By 2020, it's predicted that there's going to be 50 billion networked devices, which means that the transit, storage, access, and handling of the vast amounts of data they will generate need to be provided special consideration. Cloud infrastructure platforms are in fact necessitated due to the widespread on use mobile devices and sensors.

v. Monitoring:

Monitoring is a critical phase in Cloud environment for production scheduling, for utilizing its resources, SLAs, security, and performance and for diagnostics, as is well documented throughout the literature.

LITERATURE REVIEW

We encounter several new CloudIoT applications in daily life, including smart phones, smart TVs, smart cities, industrial automation, smart agriculture, etc. The combination of cloud computing combined internet of things technologies is known as cloudIoT. Despite the fact that

IoT and cloud have opposing qualities, their partnership helps to partly solve their problems and gives birth to new services. The goal of this research is to create a model using structural equation modelling to determine the factors that influence the adoption of cloud IoT technologies by Indian MSMEs, which contribute greatly to the development of the country. Cloud computing, perceived IT security risk, social impact, internet of things, facilitating conditions of use, perceived utility, trust, and intention to use were the criteria taken into consideration for the investigation. 500 Indian MSMEs that responded to the survey provided the responses. The investigation's findings showed that perceived ease of use, trust, and perceived IT security risk all had a favorable influence on the desire to use cloud computing, social influence, the internet of things, and perceived ease of use. The updating the information aims to assist organizational managers, decision-makers, and policy-makers in comprehending the link between the multiple parameters and intent to employ CloudIoT technologies [1].

S. Villamil et al. illustrated that most processes and devices today use the internet of things, an emerging technology that has the potential to improve people's quality of life by making it easier to access certain information and services. The main goal of this paper is to provide a broad overview of the internet of things employing data from recently published papers. The analysis of the most important recent publications and the variety of internet of things technology applications that's what gives this paper its added value. The internet of things technology stands out as a facilitator in commercial and industrial performance, but more pressingly in improving the quality of life, as a result of the analysis of the current literature. The internet of things is a tool that can solve the difficulties associated with security, computing power, and data mobility, provided that the development of other technologies proceeds as predicted [2].

L. Atzori et al. discussed the Internet of Things in this paper and the integration of various technologies and communications solutions is the primary enabling factor of this encouraging paradigm. The most pertinent applications are distributed intelligence for smart things, wired and wireless sensors, actuator networks, upgraded modulation schemes shared with the Next Generation Internet, and identification and tracking technologies. Any significant advancements in the Internet of Things, as one can easily imagine, must necessarily be the result of synergistic efforts made in a wide range of disciplines, including telecommunications, informatics, electronics, and social science. This questionnaire is designed for people who want to learn more about this complicated discipline and help shape it in light of the current complicated topic. A variety of Internet of Things paradigms are reported, and supporting technologies are reviewed. What becomes clear is that the scientific community will continue to confront pressing concerns. Those that are the most important are discussed in greater depth [3].

S. Li. et al. stated that the Internet of Things (IoT) has received a lot of research attention recently. IoT is viewed as a component of the future Internet and will include billions of intelligent, talkative "things." A heterogeneously connected network of devices will make up the Internet of the future, further extending the boundary lines of the globe with both real and virtual elements. The connected things will gain new capabilities thanks to the Internet of Things (IoT). The concepts, architecture, underlying technology, and applications of IoT are methodically examined in this study. First, several definitions of IoT are introduced. Next, emerging techniques for IoT implementation are discussed. Third, some open aspects associated with IoT applications are explored. Finally, the principal challenges that the research community needs to address are researched, along with potential solutions [4].

R. Ande et al. stated that the IoT has expanded to various areas of life in recent years, including smart homes, smart cities, agriculture, offices, and businesses. Lighting, locks, and industrial machinery are examples of common physical objects that may now be part of the IoT ecosystem. To improve the security, effectiveness and comfort of our lives, the Internet of Things has revolutionized how critical and non-critical systems are managed. As a result IoT technology has a great impact on our lives. IoT systems have attracted unwanted attention from criminal users who, apart from these good aspects, want to exploit the vulnerabilities of IoT systems for their own benefit, which are known as cyber security attacks. The purpose of this study is to highlight IoT cyber security vulnerabilities and mitigation approaches for the reader by providing an introduction to IoT. The paper is suitable for developers, practitioners and scholars, especially those from industries such as computer networking, information technology or electronics. The first section of the paper introduces IoT as the result of 200 years of advances in communications technology. This evolutionary introduction is followed by a comparison of IoT designs and an introduction to some of the technologies that make up each architectural layer. Finally, the paper wraps up with possible future advances. Security vulnerabilities are investigated inside each architectural layer, along with various mitigation measures [5].

A. Shivanathan et al. illustrated that the Internet of Things (IoT) devices that are purchased from a variety of suppliers and deployed in significant numbers are subject to increasing cyber security vulnerabilities. Therefore, it is becoming more and more important for network operators to control these devices. Existing network monitoring systems analyze traffic using special acceleration on network switches or thorough packet inspection in software, but these methods can be difficult, expensive, rigid, and unprofitable. In this study, we use the SDN paradigm with machine learning to leverage programmable flow-based telemetry and customizable data-driven models to control IoT devices according to their network activities. Our three contributions are as follows. The first one is the author has been examine traffic traces of 17 real consumer IoT devices, which were collected in our lab over a period of six months, and we find a set of traffic flows (per-device) are time-series characteristics of the network behavior of various IoT device types and their operating states (i.e., booting, actively interacting with the user, or idle) calculated over multiple timescales (from one minute to one hour) describes the characteristics of and the second is the author develop a multi-stage and at last the third one is We quantify the trade-off between performance and cost of our system and show how our monitoring scheme can be used to identify behavioral changes. Could be, such as a firmware upgrade or a cyber-attack. We train our models and test their effectiveness using real traffic traces [6].

P. Radanliev et al. stated that the new kinds of cyber dangers are sparked by the Internet of Things (IoT). Therefore, a self-assessment of IoT cyber security posture is necessary before integrating new IoT devices and services. This paper uses the term "security posture" to refer to an organization's capacity to identify, stop, and react to cybersecurity attacks. Because there are currently no self-assessment techniques for calculating IoT cyber risk posture, there is a gap in the state of the art. An empirical examination of 12 techniques to cyber risk assessment is carried out to fill this gap. Following conclusions and suggestions on a transformation pathway that describe how IoT systems might attain the target state with a new goal-oriented dependency model, the results and key findings from the study are provided as the current and a target risk state for IoT systems. The cyber security target that satisfies the general security needs of an organization is referred to as the target state. Goal-oriented dependency modelling is identified as the leading method among the risk assessment models explored in the study paper, which

examines and adapts four options for IoT risk assessment. The novel goal-oriented dependency model described in this paper allows for the quantitative self-evaluation of the IoT cyber risk posture and the assessment of unmanageable risk situations in complex IoT systems.

R. Sardar and T. Hanees illustrated that the Web of Things is a more advanced and promising architecture for Internet of Things that enables smart objects to interface not only with the Web but also with the Internet. To be included in the World Wide Web, it enables users to exchange and produce information as well as provide capabilities for data aggregation and analysis over a network. Despite these developments, it has revealed a number of security issues that must be resolved for WOT to be successfully deployed on a wide and diverse commercial scale. Through a review of previously published empirical investigations, the authors of this work study the most prominent security concerns associated with WOT, such as unauthorized access, eavesdropping, denial of service attacks, tampering and impersonation. We have also talked about some of the methods that can be used to solve security related problems keeping in mind the size and dynamics of the network. To educate users about protective measures and prevent security threats from exploiting system flaws, the authors attack threat analysis and modeling techniques. An essential understanding of how some existing processes and algorithms can be used to enhance security is provided by the authors. According to the study's findings, WoT security methodology is still in its infancy, and further research is needed to address these problems.

J. Provoost et al. illustrated that the use of open web standards and semantic technologies, the Web of Things (WoT) allows for the open sharing of information collected by sensors placed in urban settings, allowing for better integration with other web-based data. Convenience is available and knowledge is progressed. As with WoT, artificial intelligence is important for understanding dynamic urban systems (AI). AI allows the analysis and transformation of data generated by WOT-enabled sensory observations to characterize and predict current and future conditions in space and time. This study analyzes the effects of WoT and AI in smart cities by taking into account a practical issue: forecasting parking availability. Weather forecasting web services as well as traffic cameras have been deployed as WOT sensors. AI analytics uses machine learning (ML), which builds predictive models using neural networks and random forests [7].

F. Antoniazzi et al. stated that the Web of Things (WoT) is the most recent iteration of the Internet of Things and, as the name implies, demands the use of Web protocols and protocols for device interoperability across the Internet. Only a few speculative strategies to combat the segmentation of the IoT world via the use of semantics have now been offered by scholars and industry. This new development, called Semantic WoT, is based on a WoT implementations created using the Semantic Web stack's capabilities. Through the use of a common ontology for representing devices, this paper demonstrates a workable realization of the WoT in its Semantic flavour. We characterize the ontology as a dynamic ontology since it also incorporates patterns for interrelations between devices. The proposed dynamic setup can promote interoperability at the required times by allowing on the one hand smart discovery and on the other hand instrumentation and automatic engagement through the semantic information available. A real example will provide a demonstration of idea and overall evaluation [8].

The more physical items may now connect to the Internet and provide their services as resources on the Web courtesy to technological advancements. In order to effectively exploit the coming Web of Things, search engines are essential because they connect users and apps with the

resources they require to execute. Due to the variety of Web of Things resources most systems use, developing them is a difficult and varied task. A separate kind of search engine is required for each resource combinations in the query grievance procedure, each with its own set of technological difficulties and application circumstances. The creation of new systems and the examination of the state of the art are both challenged by this variability. We give a systematic analysis of Web of Things search engines in this paper, highlighting the variety of settings that these systems might take. On the basis of this model, we provide an analytical framework for investigating the growth and state of the field as shown by 30 exemplary works. We explore unresolved difficulties in our research's conclusion in an effort to close the gap between current advancements and the ideal Web of Things Search Engines [9].

DISCUSSION

The Future Internet (FI) may be used for a multitude of cutting-edge purposes, including linking all material things together. In order to supply a comprehensive variety of services for everyone, improve and monitor our lives, and give access to many tools across various disciplines, these devices and applications may cooperate and communicate. The phrase "Future Internet" refers to a group of upcoming technologies for transmitting data networks. The Internet of Devices, which offers a common international information technology platform for fusing networked things and seamless networks, is the most widely accepted and potent notion of the future internet. People will be linked to anything, anybody, anytime, and anywhere on the network infrastructure while appropriately using whatever service and any network. The Internet of Things also examines at the connection, collections, content, convergence, technology, and communication between people and things[10].

On the other hand, the Cloud Computing is seen as the backend solutions for processing massive data streams and operations while addressing the issues with everything being linked with seamless communications in the future. Context-aware computing including online services for supporting the Internet of Things may be allowed by cloud technologies, which provide a flexible, effective, scalable, and virtual computer system. Most of the time, an abundance of Internet of Things smart sensors will receive data from the environment and environment and send it to a cloud service for judgment call. The intelligent and self-configuring connections that are casemated and integrated in a live, global network architecture are what the Internet of Things concept is based on. The most reoccurring themes of Internet of Things (IoT) products are tiny, with concomitant difficulties related to privacy, security, productivity, and dependability. Nevertheless, in regards of processing and storage capacity the possibilities of cloud computing is near unlimited. Additionally, it is a considerably evolved technology, and it has a resolution for most or perhaps all of the IoT's difficulties. As a result, it is plausible to see cloud computing and indeed the Internet of Things as two basic technologies that have been incorporated into a new IT architecture that will incorporate both the present and the future Internet. Clouds and IoT are referred to here as vital components of something like the Future Internet, which provides a live, global network infrastructure that we use every day for a variety of reasons. The self-configuring possibilities and practical transmission media for implied and physical Things are the most prominent characteristics of this technology.

CONCLUSION

Although the cloud computing technology presents countless opportunities, it also has a number of restrictions. In an environment known as the "cloud," data processing and storage take place

outside of mobile devices. In this paper, we provide an overview concerning IoT technology in addition to an explanation on how to utilize it. We also highlight the primary advantages and drawbacks of cloud computing. The term "cloud computing" refers to an infrastructure where data computation and storage take place off of mobile devices. In the communications industry, and particularly in the contemporary sector of wireless telecommunications, the Internet of Things is a new technology that would be expanding quickly. Fulfilling the mission entrusted to them as a united entity is the primary goal of the interaction and communication between things as well as objects delivered over wireless networks. Additionally, the technologies of the cloud computing and the internet of things both advance significantly since they are reliant on wireless network technology. In this chapter, we therefore provide overview of IoT and Cloud Computing with a concentration on their respective security challenges. We specifically integrate the two aforementioned technologies Cloud Computing and IoT to investigate their common features and to learn about the advantages of their integration. In concluding, the contribution of cloud computing to IoT technology was described, along with examples of how this technology enhances IoT performance. The suggested algorithm model was applied to evaluate the security issues associated with the integration of IoT and Cloud Computing, and there is also a presentation of how the two encryption algorithms that were used contributed to the integration of IoT and Cloud Computing. Future studies on the fusion of the different systems may focus on this area. In order to have a better analysis framework given the fast growth of both technologies, the security problem has to be resolved or mitigated. The security issues that were addressed in this chapter might be the subject of further investigation as a practical example with the goal of lowering them.

REFERENCES

[1] V. S. Narwane, B. E. Narkhede, R. D. Raut, B. B. Gardas, P. Priyadarshinee, and M. S. Kavre, “To identify the determinants of the CloudIoT technologies adoption in the Indian MSMEs: structural equation modelling approach,” *Int. J. Bus. Inf. Syst.*, vol. 31, no. 3, p. 322, 2019, doi: 10.1504/IJBIS.2019.101110.

[2] S. Villamil, C. Hernández, and G. Tarazona, “An overview of internet of things,” *Telkomnika (Telecommunication Comput. Electron. Control.*, 2020, doi: 10.12928/TELKOMNIKA.v18i5.15911.

[3] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[4] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Inf. Syst. Front.*, 2015, doi: 10.1007/s10796-014-9492-7.

[5] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, “Internet of Things: Evolution and technologies from a security perspective,” *Sustain. Cities Soc.*, vol. 54, p. 101728, Mar. 2020, doi: 10.1016/j.scs.2019.101728.

[6] A. Sivanathan, H. Habibi Gharakheili, and V. Sivaraman, “Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning,” *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 60–74, Mar. 2020, doi: 10.1109/TNSM.2020.2971213.

[7] J. C. Provoost, A. Kamilaris, L. J. J. Wismans, S. J. van der Drift, and M. van Keulen, “Predicting parking occupancy via machine learning in the web of things,” *Internet of Things*, vol. 12, p. 100301, Dec. 2020, doi: 10.1016/j.iot.2020.100301.

[8] F. Antoniazzi and F. Viola, "Building the Semantic Web of Things Through a Dynamic Ontology," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10560–10579, Dec. 2019, doi: 10.1109/JIOT.2019.2939882.

[9] N. K. Tran, Q. Z. Sheng, M. A. Babar, and L. Yao, "Searching the Web of Things," *ACM Comput. Surv.*, vol. 50, no. 4, pp. 1–34, Jul. 2018, doi: 10.1145/3092695.

[10] S. Rao, D. Chendanda, C. Deshpande, and V. Lakkundi, "Implementing LWM2M in constrained IoT devices," in *2015 IEEE Conference on Wireless Sensors, ICWiSE 2015*, 2016. doi: 10.1109/ICWISE.2015.7380353.