ESSENTIALS OF MANAGEMENT INFORMATION SYSTEMS

Neha Saxena
Dr. Akhila Udupa

ALEXIS PRESS
JERSEY CITY, USA

ESSENTIALS OF
MANAGEMENT INFORMATION SYSTEMS

ESSENTIALS OF MANAGEMENT INFORMATION SYSTEMS

Neha Saxena

Dr. Akhila Udupa

ALEXIS PRESS

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.

Essentials of Management Information Systems by *Neha Saxena, Dr. Akhila Udupa*

ISBN 978-1-64532-961-9

CONTENTS

CHAPTER 1

AN ANALYSIS OF INFORMATION TECHNOLOGY INFRASTRUCTURE

Ms. Neha Saxena
Assistant Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id: nehasinha@presidencyuniversity.in

ABSTRACT:

Information technology infrastructure plays a vital role in enabling and supporting organizational operations in the digital age. This abstract provides an overview of information technology infrastructure, its components, and its significance in facilitating efficient and effective use of technology within organizations.Information technology infrastructure refers to the underlying framework of hardware, software, networks, and data centers that supports the storage, processing, and transmission of information within an organization. It provides the foundation for various IT services and applications, enabling seamless connectivity, data management, and resource allocation.The web-based system can manage project-related paperwork for the duration of a project, including processing building plans and paperwork for obtaining development planning approvals, building plans approvals, structural plans approvals, temporary occupation permits, fire safety certificates, and certificates of statutory completion.

KEYWORDS:

Cloud Computing, Disaster Recovery, Hardware, IT Infrastructure, Network Infrastructure, Operating Systems.

INTRODUCTION

Part Two examines hardware, software, database, and networking technologies, as well as tools and approaches for security and control, to give the technological underpinnings for understanding information systems. This section provides solutions to inquiries like: What technologies are required by modern firms to carry out their operations? What do I need to know about these technologies in order to ensure that they improve the company's performance? What future changes are these technologies most likely to undergo? What methods and technologies are necessary to guarantee the security and dependability of systems.

Reforming the construction permit regulatory system the Construction 21 Blueprint and a strategic ambition to become a "World Class Builder in the Knowledge Age" are how the Singaporean government sees the need to improve the building and construction sector.

Because of the symbiotic link between technology and knowledge, more IT utilization is essential for this administration to achieve its objectives.

It goes without saying that firms in knowledge-based industries must use technology to increase production, cut costs, and improve the caliber of their goods and services. Government efforts must concentrate on creating a set of IT infrastructure initiatives that will provide companies and other organizations the tools they need to optimize information utilization, improve business activity, and achieve and maintain a competitive edge[1]–[3].

Since its inception in 1995, the CORENET project has advanced significantly to become a significant IT venture. Re-engineering the business processes of the building and construction sector is being led by the Ministry of National Development and pushed by the Building and Construction Authority with the goal of achieving significant improvements in turnaround time, productivity, and quality. Design, procurement, construction, and maintenance are the four core activities of a building project life cycle, and CORENET is focused on establishing IT systems and crucial infrastructure to combine them. Implementing a suitable IT infrastructure to enable construction project participants, including the planning authorities, to share information easily and quickly is one of CORENET's main objectives. In essence, setting up a government-to-business infrastructure allows companies to submit electronic construction plans to the 16 government agencies spread over eight ministries that control industrial operations in order to get clearances and licenses.

The whole building process typically consists of four different, consecutive phases. Design, tender paperwork, selection, construction, handover, and maintenance comprise these steps. The main design tasks at the initial stage are creating concept and schematic designs and getting planning permissions. The building owner must submit the building plans via the designated design consultant to these agencies individually in order to seek for the permissions since the different regulatory bodies give planning approvals. Numerous parties are involved in the intricate process of submitting the application, comparing it to planning regulations, evaluating the project, re-submitting it for conformity, and awarding permission. The "Qualified Person" must submit numerous plans, documents, and applications to various authorities using the conventional process, which results in the production of a large number of paper documents, inefficient manual processing of submissions by regulatory agencies, a lack of storage space for all the paper documents, and an unorganized exchange of project information among project team members.

How may this situation's submissions process be made better using an IT infrastructure? The CORENET e-submission system offers a virtual one-stop 24/7 counter to make it easier to electronically submit building plans and documents to various regulatory agencies, check the status of those submissions online, submit an application while also collecting fees, process applications more quickly, and do away with printing plans, documents, and application forms. In other words, by enabling business participants to submit their applications online, they may do so without printing paper copies of their plans and documentation or making the trip to the offices of the relevant government bodies. All stakeholders may track the status and development of submitted planning applications online, which further increases the aspect of openness.

According to the Singaporean government, each sub-mission will save around S$450 thanks to the implementation of the e-submission method. Estimates of the amount are based on the quantity of hardcopy printouts of plans and papers that have been reduced, as well as the removal of manual distribution of documents to the different agencies involved. Additional findings from a 754 company industry-wide poll indicate that most of them have found it to be helpful to their job.

The high percentage attained contributes to the new system's relatively widespread acceptance and the implementation's overall success. Bee Hua Goh, a student at the National University of Singapore, contributed this example. The CORENET project serves as an example of a government's strategic plan and attempts to transform the conventional building and construction sector into one that is more knowledge-based. To enable enterprises and other organizations to work together in order to share and exchange common construction project information, an IT infrastructure is put into place.

More precisely, it demonstrates how creating a G2B infrastructure may assist the industry at large in streamlining its procedures and practices for submitting construction designs. There has been a noticeable reduction in turnaround time for each application, which translates into quantifiable cost reductions. In other words, without the IT infrastructure, different commercial and public organizations would have to operate independently, which would lead to duplication of effort, resource waste (time, money, etc.), a lack of integration, and an opaque application process.

Everyone involved in the process of acquiring and awarding planning permissions and licenses for building work is aware of the advantages, both tangible and intangible. However, businesses in the building sector also have a benefit. The collection of project data that is digitally recorded may be quickly accessed for use in the future. Construction projects are the most advantageous for knowledge reuse since each one provides relevant best practices that may be applied to other projects to improve their chances of success. Here are some issues to consider: How does CORENET's e-submission technology help corporations and other organizations simplify their work flows and business processes? What are the advantages of CORENET's G2B infrastructure for construction plan submission to enterprises and other organizations?

The common technological assets that serve as the foundation for the unique information system applications of the company are what we referred to as information technology infrastructure. A firm's whole business divisions or the entire company may invest in hardware, software, and services including consulting, training, and education as part of its IT infrastructure. The IT infrastructure of a company serves as the cornerstone for managing internal firm business activities as well as engaging with suppliers and servicing customers.When telecommunications, networking hardware, and telecommunications services are taken into account, it is anticipated that the market for providing IT infrastructure to businesses globally in 2012 will be worth $3.6 trillion. This excludes the $400 billion in additional IT and associated business process consulting services. In major businesses, infrastructure investments make up between 25 and 50 percent of information technology spending, with financial services companies leading the pack with well over half of all capital investment in IT.

DISCUSSION

Defining It Infrastructure

An IT infrastructure is made up of a collection of hardware and software programs needed to run the complete business. However, an IT infrastructure is also a collection of corporate-wide services that management budgets for and that include both technical and human resources. The following are some of these services: Large mainframes, midrange computers, desktop and laptop computers, mobile handheld devices, and distant cloud computing services are some examples of the computing platforms that are used to deliver computing services that integrate workers, clients, and suppliers into a cohesive digital ecosystem.

Telecommunications services that link workers, clients, and suppliers through data, phone, and video The services that a company may provide to its clients, partners, and staff directly depend on the state of its IT infrastructure.

The business and information systems strategy of the company should ideally be supported by this architecture. The business and IT strategies, as well as the services that may be offered to clients, are all significantly impacted by new information technology. services for managing and storing company data as well as providing tools for analysis

Application software services, including online software services, that provide company-wide features such shared knowledge management systems, customer relationship management, supply chain management, and enterprise resource planning systems Services for managing physical facilities that create and maintain the infrastructure needed for computer, telecommunications, and data management services IT management services that coordinate with the business units for IT services, plan and build the infrastructure, manage accounting for the IT spending, and provide project management services. IT standards services that provide the company and its business divisions guidelines on how, when, and what information technology to utilize IT education services that teach personnel in system usage and managers in the planning and management of IT investments IT research and development services that provide the business information about possible IT investments and initiatives for the future that might help it stand out in the market.

This "service platform" approach makes it simpler to comprehend the commercial value delivered by infrastructure investments. For instance, it might be difficult to comprehend the true commercial value of a fully loaded personal computer running at 3 gigahertz that costs around $1,000 and a high-speed Internet connection without knowing who would use it and how. However, it becomes apparent how valuable these technologies are when we consider the services they offer: A high-cost employee earning $100,000 a year may access to all of the company's key systems and the open Internet thanks to the new PC. This employee spends less time waiting for information online thanks to the high-speed Internet connectivity, saving them around an hour per day. Without this computer and Internet access, this one employee's worth to the company may be halved.

Change in It Infrastructure

Today's IT infrastructure in businesses is the result of more than 50 years of advancements in computer platforms. There have been five phases in this history, each corresponding to a particular arrangement of infrastructure and computational resources. The five periods include client/server networks, cloud and mobile computing, general-purpose mainframe and minicomputer computing, and personal computers.

Technologies that are typical of one age could also be employed for other reasons in a different era. For instance, several businesses continue to employ mainframe computers as powerful servers for corporate enterprise applications and legacy mainframe systems. Era of the General-Purpose Mainframe and the Minicomputer

The mainstream commercial usage of mainframe computers began in 1959 with the release of the IBM 1401 and 7090 transistorized machines. With the release of the IBM 360 series in 1965, the mainframe computer fully came of age. The 360 was the first commercial computer to come with a robust operating system capable of time sharing, multitasking, and virtual memory in more sophisticated variants. Since then, IBM has dominated mainframe computing. Many online remote terminals linked to the centralized mainframe utilizing proprietary data lines and communication protocols as mainframe computers grew in power.

The mainframe era was a time when computing was heavily centralized and managed by skilled programmers and systems operators. The majority of the infrastructure components were supplied by a single vendor, the company that made the hardware and software[4]–[6]. With the arrival of minicomputers manufactured by Digital Equipment Corporation in 1965, this trend started to alter. Decentralized computing, tailored to the unique demands of each departments or business units rather than time sharing on a single enormous mainframe, was made feasible by DEC minicomputers, which delivered powerful machines at costs far cheaper than IBM mainframes. The minicomputer has developed into a midrange computer

or midrange server in recent years and is now a component of a network. Despite the fact that the first genuinely personal computers were introduced in the 1970s, only a small number of computer hobbyists could afford them. Because the IBM PC was the first to be extensively embraced by American corporations, its introduction in 1981 is often seen as the start of the PC era. The Wintel PC machine, which at first ran on the text-based DOS operating system, then switched to the Microsoft Windows operating system, became the de facto desktop personal computer. There are thought to be 1.2 billion PCs in use worldwide as of 2012, and 300 million new PCs are sold annually. It is believed that 90% of them run a Windows OS and 10% run a Mac OS. The dominance of the Wintel computer platform is waning as more people choose iPhones and Android phones. Around the globe, about a billion individuals use cellphones, and the majority of these users utilize their portable devices to access the Internet.

Word processors, spreadsheets, electronic presentation software, and tiny data management systems were among the personal desktop productivity software tools that exploded with the rise of PCs in the 1980s and early 1990s. These tools were very beneficial to both home and business users. Before 1990s PC operating system software made it feasible to connect these PCs to networks, they were standalone systems.

Era of Client/Server

In client/server computing, desktop or laptop computers, referred to as clients, are connected through a network to robust server machines, which provide the clients a range of services and functionalities. These two different devices each handle a different aspect of computer processing. The client is the user's point of entry, while the server often handles network administration, processes and saves shared data, and serves up Web sites. The word "server" is used to describe both the computer's physical hardware and the network software that runs on it. The server might be a mainframe, but in modern times, server computers are usually more powerful versions of personal computers that are built on cheap chips and often use numerous processors in a single computer box or in server racks.

A client computer connected to a server computer splits processing between the two kinds of computers in the simplest client/server network. A two-tier client/server architecture is what this is. Small companies often have straightforward client/server networks, but most corporations have more intricate, multitier client/server designs where the workload of the whole network is distributed among a number of servers, depending on the kind of service being sought.

For instance, at the first level, a client that requests a service will be given a Web page by a Web server. The search for and administration of saved Web pages is handled by web server software. The request is sent to an application server if the client seeks access to a corporate system. All application actions between a user and a company's back-end business processes are handled by application server software.

The application server may be installed on a separate computer from the web server or on the same machine. More information on other pieces of software used in multitier client/server architectures for e-business and e-commerce.

Business organizations may split computing tasks over a number of more affordable, smaller computers that are far less costly than centralized mainframe systems thanks to client/server computing. The company as a whole experiences an explosion of computer power and applications as a consequence. At the start of the client/server era, Novell NetWare was the dominant client/server networking technology. Microsoft now dominates the industry with its Windows operating systems.

Era of Enterprise Computing

Early in the 1990s, businesses looked to networking standards and software tools to unite various networks and applications throughout the company into a corporate infrastructure. After 1995, corporate enterprises started taking seriously adopting the Transmission Control Protocol/Internet Protocol networking standard to connect their dispersed networks as the Internet matured into a trusted communications environment. The resultant IT infrastructure connects various computer hardware and smaller networks into a company-wide network to enable unfettered information flow inside the company and between the company and other businesses. It includes public infrastructures like the telephone system, the Internet, and public network services. It may connect various kinds of computer hardware, such as mainframes, servers, PCs, and mobile devices. Additionally, the corporate infrastructure needs software to connect various applications and allow data to move freely across various divisions of the company, such as enterprise apps and Web services.

Era of Mobile and Cloud Computing the client/server approach has been advanced by the Internet's expanding bandwidth capacity, moving it closer to the "Cloud Computing Model." A computer approach known as "cloud computing" allows users to access a shared pool of computing resources over a network, often the Internet. Any linked device and location may access these "clouds" of computing resources as required. Cloud computing is now the area of computing that is expanding the quickest, with businesses spending an anticipated $207 billion by the end of 2016 on public cloud services, up from $109 billion in 2012.

As personal and business computing increasingly shift to mobile platforms, thousands or even hundreds of thousands of computers are housed in cloud data centers where they can be accessed by desktop, laptop, tablet, TV, entertainment center, smartphone, and other client machines connected to the Internet. Large-scale cloud computing facilities are run by IBM, HP, Dell, and Amazon.

These facilities provide high-speed Internet connections, processing capacity, and data storage to businesses that wish to manage their IT systems remotely. Applications for software are sold as services that are offered through the Internet by software companies like Google, Microsoft, SAP, Oracle, and Salesforce.com[7]–[10].

The Technology Inspiring the Evolution Of The Structure

The modifications to IT infrastructure we've just discussed are the result of advances in computer processing, memory chips, storage devices, telecommunications and networking hardware and software, as well as software design, which have exponentially increased computing power while exponentially lowered costs. Let's examine the most significant changes.

Microprocessor Power and Moore's Law

The number of components on a chip with the lowest manufacturing costs per component had doubled every year since the first microprocessor chip was introduced in 1959, according to a 1965 article by Gordon Moore, the director of Fairchild Semiconductor's Research and Development Laboratories, an early producer of integrated circuits.

This claim served as the basis for Moore's Law. Later, Moore lowered the growth rate to a doubling every two years. Later, several interpretations of this statute would be used. Moore never said any of the following three versions of the law: computing power doubles every 18 months, microprocessor power doubles every 18 months, and computing costs halve every 18 months.

Processing power has risen dramatically as a result of fitting more than 2 billion transistors onto a small computer. Over 128,000 MIPS worth of processing power is now available.The exponential rise in transistor density and processing power, together with the exponential fall in computing costs, are anticipated to continue.

Miniaturization of chip components is ongoing. The size of a virus rather than a human hair should be used to compare the size of modern transistors. Manufacturers of chips may even make transistors that are just a few atoms wide by using nanotechnology. Individual atoms and molecules are used in nanotechnology to make computer chips and other objects hundreds of times smaller than what is now possible. Chip makers are working to create a manufacturing method that may efficiently build nanotube processors. IBM has just recently begun employing this technique to produce microprocessors.

CONCLUSION

In conclusion, the foundation of an organization's information technology capabilities is its infrastructure. In order to provide effective data management, communication, collaboration, and security, it includes hardware, software, networks, and data centers. An infrastructure that is well-designed and maintained boosts operational effectiveness, encourages innovation, and gives enterprises a competitive edge in the digital environment.

To adapt to changing technological trends and satisfy the increasing needs of the digital world, organizations must continuously evaluate and invest in their information technology infrastructure. With its scalable, on-demand resources and services, cloud computing has completely changed how information technology infrastructure operates. Cloud-based infrastructure enables businesses to outsource certain IT tasks and use affordable, adaptable solutions without having to make substantial upfront hardware and software expenditures.

REFERENCES

[1] C. Fernández-Baladrón, “ITIL: Information Technology Infrastructure Library,” *Renata*, 2014.

[2] N. B. Duncan, “Capturing flexibility of information technology infrastructure: A study of resource characteristics and their measure,” *J. Manag. Inf. Syst.*, 1995, doi: 10.1080/07421222.1995.11518080.

[3] B. R. Lewis and T. A. Byrd, “Development of a measure for the information technology infrastructure construct,” *Eur. J. Inf. Syst.*, 2003, doi: 10.1057/palgrave.ejis.3000449.

[4] N. Pouti and M. R. Taghva, “Determining Organizational Maturity of Information Technology with Information Technology and Business Alignment Approach by Capability Maturity Model Integration and Best Practices of Information Technology Infrastructure Library; Case Study: Kermanshah Electric Power Distribution Company,” *Iran. J. Inf. Process. Manag.*, 2020.

[5] J. Benitez, G. Ray, and J. Henseler, “Impact of information technology infrastructure flexibility on mergers and acquisitions,” *MIS Q. Manag. Inf. Syst.*, 2018, doi: 10.25300/MISQ/2018/13245.

[6] A. Cardoso, F. Moreira, and D. F. Escudero, “Information Technology Infrastructure Library and the migration to cloud computing,” *Univers. Access Inf. Soc.*, 2018, doi: 10.1007/s10209-017-0559-3.

[7] T. A. Byrd and D. E. Turner, "Measuring the flexibility of information technology infrastructure: Exploratory analysis of a construct," *J. Manag. Inf. Syst.*, 2000, doi: 10.1080/07421222.2000.11045632.

[8] D. Chatterjee, C. Pacini, and V. Sambamurthy, "The shareholder-wealth and trading-volume effects of information-technology infrastructure investments," *Journal of Management Information Systems*. 2002. doi: 10.1080/07421222.2002.11045723.

[9] T. R. Soomro and H. Y. Wahba, "Role of Information Technology Infrastructure Library in data warehouses," *Am. J. Appl. Sci.*, 2011, doi: 10.3844/ajassp.2011.1384.1387.

[10] D. Handoko and A. S. Girsang, "Service Desk Implementation with Information Technology Infrastructure Library Framework (Study Case Financial Company)," in *Journal of Physics: Conference Series*, 2018. doi: 10.1088/1742-6596/1090/1/012059.

CHAPTER 2

AN ASSESSMENT OF MASS DIGITAL STORAGE

Dr. Vijayarengam Gajapathy
Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: vgajapathy@presidencyuniversity.in

ABSTRACT:

The rapid advancement of digital technology and the exponential growth in data generation have led to the emergence of mass digital storage systems. This abstract explores the legal implications and challenges associated with the law of mass digital storage. It highlights the key legal considerations and frameworks that govern the storage, access, and protection of digital information.Mass digital storage refers to the capacity to store vast amounts of data in digital form, facilitated by technologies such as cloud computing, data centers, and storage devices. These systems enable individuals, organizations, and governments to collect, store, and access a wide range of digital information, including personal data, intellectual property, financial records, and government records.

KEYWORDS:

Cloud Storage, Data Protection, Digital Preservation, Intellectual Property Rights, Legal Hold, Privacy Laws.

INTRODUCTION

The Law of Mass Digital Storage is a second technological factor that is changing IT infrastructure. Every year, the volume of digital information nearly doubles. Fortunately, the price of digital data storage is decreasing at an exponential rate of 100% annually. 5.7 demonstrates that from 1950 to the present, the amount of gigabytes that could be stored on magnetic media for $1 nearly quadrupled every 15 months. A 500 GB hard drive costs around $60 at retail in 2012. Nanotubes are very thin tubes, 10,000 times as thin as a human hair. They are made of sheets of carbon hexagons that have been rolled up, and they have the capacity to be used as miniscule wires or in very small electronic devices. They are also highly effective electrical current conductors. Tyler Boys from Shutterstock.

Law of Metcalfe and Network Economics

We can better comprehend why computer resources are now so easily accessible thanks to Moore's Law and the Law of Mass Storage. Why, therefore, do individuals seek out more computing and storage capacity? Some solutions are offered by the economics of networks and the expansion of the Internet. The Ethernet local area network's creator, Robert Metcalfe, said in 1970 that a network's worth or power increases exponentially with the increase in the number of network users.

As more and more individuals join the network, Metcalfe and others highlight the rising returns to scale that network member’s experience. The value of the whole system increases exponentially as the number of participants in a network increases linearly, and this growth lasts indefinitely. The social and commercial benefits of digital networks, which quickly increase the number of real and prospective linkages among network members, has been a major driver of the demand for information technology[1]–[3].

Internet use and declining communication costs

The significant decrease in communication costs and the exponential increase in Internet size are the fourth technological factor reshaping IT infrastructure. Globally, an estimated 2.3 billion individuals have access to the Internet. The steadily decreasing cost of communication across telephone and Internet networks.

Utilization of communication and computing capabilities explodes when communication costs decline toward a very small number and close to zero. Businesses must considerably increase their Internet connections, including wireless connectivity, as well as the computational capacity of their desktop clients, client/server networks, and mobile computing devices if they want to benefit from the commercial value that the Internet offers. There is every indication that these trends will persist.

DISCUSSION

Standards and Network Effects

Without agreements between manufacturers and broad customer adoption of technological standards, today's business infrastructure and Internet computing would be impossible—both now and in the future. Technology standards are guidelines that determine a product's interoperability and network communication capabilities.

As producers concentrate on the items made to a single standard, technology standards release strong economies of scale and cause price decreases. Any kind of computer would be far more costly than it is right now without these economies of scale. Important standards that have influenced IT infrastructure are described in 5.1.

Businesses began transitioning to standardized computing and communication platforms in the 1990s. The most popular desktop and mobile client computing platform is a Wintel PC running Windows and Microsoft Office desktop productivity software.

The replacement of exclusive and expensive mainframe infrastructures was made feasible by the widespread acceptance of Unix-Linux as the preferred corporate server operating system. The Ethernet standard in telecommunications made it possible for PCs to form tiny local area networks (LANs), and the TCP/IP standard made it possible for these LANs to connect to companywide networks and, eventually, to the Internet.

Frequently Used Business Language

facilitated data transmission between computers made by various manufacturers; subsequently used as the common language connecting input and output devices like keyboards and mouse to computers. The American National Standards Institute adopted it in 1963. A simple programming language that significantly increased programmers' capacity to create business-related applications while lowering software costs. Sponsored in 1959 by the Defense Department.

Internet Protocol and Transmission Control Protocol

Millions of computers may link to one another in a massive global network thanks to a set of communication protocols and a shared addressing system. Later, it served as the standard set of networking protocols for intranets and local area networks. Designed for the United States in the early 1970s. Defense Department. Computer with Intel, Microsoft, and IBM Standard Intel CPUs, other standard hardware, Microsoft DOS, and eventually Windows software make up the Wintel architecture for personal desktop computers. This commonplace,

inexpensive product's introduction established the groundwork for a 25-year era of tremendous expansion in computing across all enterprises in the world. Today, more than 1 billion PCs fuel daily operations in industry and government.

Components of The Structure

The modern IT infrastructure is made up of seven main parts. These infrastructure parts are shown in 5.9, along with the top suppliers for each component group. To provide the company a cohesive infrastructure, these elements -- which are investments -- must be integrated with one another. Technology providers that provided these components in the past were often in rivalry with one another and offered buying companies a variety of proprietary, incompatible, incomplete solutions.

But huge clients have increasingly compelled the vendor companies to work together in strategic alliances. A hardware and services company like IBM, for instance, collaborates with all of the main enterprise software vendors, has strategic relationships with system integrators, and guarantees compatibility with any database solutions that its client companies want to employ. To provide the company a cogent IT infrastructure, seven key elements need to be harmonized. Major technologies and suppliers for each component are listed below.

Hardware Platforms for Computers

In 2013, businesses throughout the globe are anticipated to spend $448 billion on hardware, including servers and client devices. In blade servers in racks, Intel or AMD processors predominate, while Sun SPARC microprocessors and IBM chips made specifically for servers are also used in the server industry. Blade servers are computers made up of a circuit board with processors, memory, and network connections that are kept in racks, as we mentioned in the opening example. In comparison to conventional box-based servers, they occupy less space. Each blade server's hard disk or external mass-storage devices may provide secondary storage.

The market for computer hardware is gradually being dominated by three chip manufacturersIntel, AMD, and IBMas well as leading companies like IBM, HP, Dell, and Sun Microsystems. The server market for UNIX and Linux computers, which may employ Sun or IBM CPUs, is the biggest exception to the industry's decision to make Intel the standard processor for business computing. Mainframes are still around. In cloud computing centers, mainframes are still utilized to manage heavy workloads, analyze enormous amounts of data, and safely and securely handle high volumes of transactions.

For banking and communications networks, the mainframe remains the digital workhorse. However, there is now just one supplier left: IBM. Additionally, IBM has repurposed its mainframe computers to make them enormous servers for huge enterprise networks and business websites. A single IBM mainframe is capable of replacing hundreds of smaller blade servers and can run up to 17,000 instances of Linux or Windows Server software.

Platforms For Operating Systems

On the server operating system market, Linux, a reliable and affordable open source relative of UNIX, makes up around 65 percent of corporate servers, with Microsoft Windows Server accounting for roughly 35 percent. Microsoft Windows Server appeals to businesses looking for Windows-based IT infrastructures because it can provide enterprise-wide operating system and network services. In comparison to mainframe operating systems, UNIX and Linux are far more affordable, scalable, and dependable. They can also function on a wide range of CPU types. IBM, HP, and Sun are the three main producers of UNIX operating

systems, and each has somewhat distinct and largely incompatible versions.90% of PCs utilize some variation of the Microsoft Windows operating system at the client level to control the machine's resources and operations. However, there is now a far wider selection of operating systems than there was in the past, with new operating systems for computers linked to the cloud or portable mobile digital devices. Netbooks may use Google's Chrome OS, a minimal operating system for cloud computing. The Chrome Web browser is used to access programs that are not kept on the user's computer but rather are utilized through the Internet. On servers scattered over the Internet are user data. Android is an open source operating system created by the Open Handset Alliance, which is headed by Google, for mobile devices such smartphones and tablet computers.

It has overtaken iOS, Apple's mobile operating system for the iPhone, iPad, and iPod Touch, to become the most widely used smartphone platform globally. Traditional client operating systems are built on the mouse and keyboard, but touch technology is making them seem more natural and intuitive. With a multitouch interface, iOS, the operating system for the wildly popular Apple iPad, iPhone, and iPod Touch, allows users to interact with items on a screen using one or more fingers rather than a mouse or keyboard.

Microsoft's Windows 8 includes a user interface that is built for touch but also functions with a mouse and keyboard and operates on both tablets and PCs.

Computer Business Applications

About $301 billion is anticipated to be spent by businesses globally in 2013 on corporate application software, which is seen as a part of IT infrastructure. SAP and Oracle are the two biggest suppliers of corporate application software. Middleware software provided by vendors like IBM and Oracle is also included in this category since it links the company's current application platforms to achieve firmwide integration. By concentrating on small and medium-sized enterprises that have not yet adopted enterprise software, Microsoft is seeking to access the lower ends of this market.

Storage And Management of Data

Enterprise database management software is in charge of maintaining and arranging the company's data so that it can be accessed and utilized effectively. This program is described in full in 6. More than 90% of the U.S. database software industry is supplied by the top four database software vendors, IBM, Oracle, Microsoft, and Sybase. Apache Hadoop is an open source software framework for handling enormous data volumes, and MySQL is a Linux open source relational database system that is now owned by Oracle Corporation[4]–[6].

For large-scale systems, EMC Corporation and a select group of PC hard disk manufacturers lead by Seagate and Western Digital dominate the physical data storage industry. Every two years, the amount of digital data doubles, with 1.8 zettabytes of data being produced in 2011 alone. Thousands of Libraries of Congress may be created by combining typical business data with tweets, blogs, videos, emails, and Facebook posts.

The market for digital data storage devices has been expanding at a rate of more than 15% per year over the last five years due to the world's rising need for fresh digital information. The use of network-based storage solutions by major companies is increasing in addition to the conventional disk arrays and tape libraries.

Multiple storage devices are connected by storage area networks, which are their own high-speed storage-specific networks. A large central storage pool that can be quickly accessed and shared by several servers is created by the SAN.

Telecommunications/Networking Platforms

In 2013, businesses throughout the globe are projected to spend $408 billion on telecoms equipment and an additional $1.7 billion on services. It is committed to providing a thorough understanding of the Internet and the business networking environment. As a local area network operating system, Windows Server is most often used, followed by Linux and UNIX. Some kind of UNIX is used by large, enterprise wide area networks. The TCP/IP protocol suite is used as a standard by most wide area corporate networks and local area networks. The top manufacturers of networking gear are Juniper Networks, Cisco, Alcatel-Lucent, Nortel, and Cisco. Telecommunications/telephone service providers that provide voice and data connection, wide area networking, wireless services, and Internet access generally provide telecommunications platforms. Leading providers of telecom services include AT&T and Verizon. New suppliers of wireless cellular, high-speed Internet, and Internet telephone services are flooding this market.

Network Platforms

The basic networking infrastructure, hardware, and software platforms of the company intersect with and must be related to Internet platforms. They include the hardware, software, and administration services needed to operate a company's website, such as routers, cabling, and wireless or web hosting services.

A web hosting business manages a large web server, or group of servers, and offers space to subscribers who pay a monthly subscription to host their websites.As a result of the Internet revolution, hundreds of modest servers were purchased by several companies to power their online businesses. Since then, there has been a constant drive toward server consolidation, which involves decreasing the number of server computers by increasing each one's size and power and by using software technologies that enable multiple applications to be run on a single server. The market for Internet hardware servers has grown more dominated by IBM, Dell, Sun, and HP as a result of sharp price reductions.

Services For Consulting and System Integration

Even a major company nowadays lacks the personnel, the expertise, the financial resources, and the relevant experience to implement and manage their whole IT infrastructure. Significant adjustments in corporate practices and procedures, training and education, and software integration are necessary for the implementation of a new infrastructure. Accenture, IBM Global Services, HP, Infosys, and Wipro Technologies are renowned consulting organizations that provide this knowledge.Software integration entails making sure the new infrastructure is compatible with the company's older, so-called legacy systems as well as that the new infrastructure's components are compatible with one another. To avoid the expensive expense of revamping or replacing them, legacy systems are often older transaction processing systems designed for mainframe computers that are still in use. If these older technologies can be incorporated into a modern infrastructure, replacing them would be both expensive and unnecessary.

Trends In Modern Hardware Platforms

More computing power is now being distributed across networks and portable handheld devices as a result of the explosive growth in computing hardware and networking technologies. The consumerization of IT, grid computing, virtualization, cloud computing, green computing, high-performance/power-efficient CPUs, and autonomous computing are the eight hardware developments we examine.

Portal For Mobile Digital

It was noted that as alternatives to PCs and bigger computers, new mobile digital computing platforms have arisen. Smartphones like the iPhone, Android, and BlackBerry have largely replaced PCs in terms of functionality, including data transfer, web browsing, e-mail and instant messaging transmission, presenting digital material, and data exchange with internal business systems. The new mobile platform also includes compact, lightweight netbooks designed for Internet access and wireless communication, tablet computers like the iPad, and digital e-book readers with Web access capabilities like Amazon's Kindle.Computers and smartphones are increasingly being used to access the Internet. Both consumer and commercial apps are rapidly being utilized on these devices. Senior executives at General Motors, for instance, use smartphone apps to dig down into data on car sales, financial performance, production KPIs, and project management status.

Commercialization

There is growing interest in enabling workers to use their own mobile devices at work, or "bring your own device" because of how commonplace they are, how simple they are to use, and how many valuable apps they have available. BYOD is one example of how new information technology that initially appears in the consumer sector seeps into commercial organizations as a result of the consumerization of IT. The consumerization of IT extends beyond only mobile personal devices to corporate applications of software services like Gmail, Google Apps, Dropbox, Facebook, and Twitter as well as Google and Yahoo search.

Businesses, particularly major corporations, are being forced to reconsider how they acquire and handle information technology services and equipment as a result of the consumerization of IT. The choice and management of the information technology and applications utilized by the company and its workers, at least in big organizations, historically fell within the purview of the central IT department. It provided workers with PCs or laptops that allowed secure access to company systems. In order to defend the company and make sure that information systems worked for the needs of the company and its management, the IT department retained control over the hardware and software used by the company. Employees and business departments are now much more involved in technology decisions and often demand that workers be allowed to access the corporate network using their own personal computers, cellphones, and tablets. Making ensuring these consumer technologies meet the demands of the company while managing and controlling them is more challenging for the company. The BYOD and IT consumerization management concerns are explored in the interactive management session.

Grid Country

Grid computing involves joining geographically dispersed computers into a single network in order to combine the processing capability of all computers on the grid to create a virtual supercomputer. Grid computing makes use of the fact that most computers in the US only utilize their central processing units for their assigned duties on average 25% of the time, freeing up these idle resources for other processing activities. Before high-speed Internet connections made it feasible for businesses to link faraway equipment affordably and transmit massive amounts of data, grid computing was not conceivable. In order to manage and distribute resources on the grid, grid computing needs software tools.Grid computing's business case includes cost savings, computation speed, and adaptability. To locate the best oil reserves, for instance, Royal Dutch/Shell Group uses a scalable grid computing platform. This platform increases the precision and speed of its scientific modeling applications. One of the biggest commercial Linux supercomputers in the world is effectively created by this

platform, which connects 1,024 IBM servers running Linux. The grid can adapt to the varying data quantities that are common in this seasonal industry. The Royal Dutch/Shell Group believes that the grid has allowed it to speed up seismic data processing, enhance output quality, and assist its scientists in identifying issues while looking for new oil sources.

Virtualization

A group of computer resources are presented via the technique of virtualization, allowing users to access them all regardless of their actual location or configuration. A single physical resource may be made to appear to the user as many logical resources thanks to virtualization. One way to make a server or mainframe act like many separate computers is to configure it to run several instances of an operating system. The use of grid computing or storage area networks, for example, allows numerous physical resources to appear as a single logical resource thanks to virtualization. A corporation may manage its computer processing and storage utilizing computing resources stored in distant places thanks to virtualization. For servers running Linux and Windows, VMware is the top virtualization software provider.

By enabling the hosting of numerous systems on a single physical computer, virtualization assists businesses in increasing equipment utilization rates, saving both space and energy in the data center. The majority of servers only operate at 15–25% of their potential, whereas virtualization may increase server utilization rates to 70–80%. A lower number of computers are needed to perform the same amount of work when utilization rates are higher. Additionally, virtualization makes it easier to centralize and combine hardware management. With the advent of cloud computing, it is now feasible for businesses and people to do all of their computing tasks utilizing a virtualized IT infrastructure.

Search the area. Many individuals are using their cellphones on the street, at businesses, restaurants, and sporting events. Additionally, a lot of individuals are beginning to utilize these gadgets at work. By 2014, 350 million workers will be using personal gadgets at work, according to a Juniper Research estimate. Today, almost 150 million individuals use their personal smartphones and tablets at work.Why not use a personal smartphone for work since practically everyone has one? Companies may benefit from all of the advantages of a mobile workforce by allowing employees to use their own smartphones, but IT departments must overcome a number of practical challenges to make that vision a reality. Companies face challenging challenges when employees use their own devices for work. These challenges include security, inventory management, support, integrating mobile devices into current IT systems and functions, and calculating return on investment. To put it another way, it's not that easy[7]–[10].

Managing and maintaining a high number of devices inside a company takes up a substantial percentage of corporate IT resources. Companies have previously attempted to restrict the usage of corporate smartphones to a single platform. Because all workers were using the same devices, or at the very least, the same operating system, it was easy to maintain track of each mobile device and to push out software updates or patches. Due to its reputation as the "most secure" mobile platform available, Research in Motion's BlackBerry used to be the most common smartphone that employers provided. The mobile digital world is significantly more challenging now since there are many different devices and operating systems available, many of which lack sophisticated administration and security features.

Companies need a reliable method to keep track of all the devices their workers are using if they are permitted to use many types of mobile devices and operating systems. The firm's networks must be set up to accept connections from that device in order to access corporate information. Companies will need to act swiftly and flexibly to make sure that their workers

can continue to be productive when they make changes to their personal phones, such as moving cellular providers, changing their phone number, or purchasing a whole new mobile device. Businesses need an effective inventory management system that tracks the devices that workers are using, where they are situated, whether they are in use, and what software they are running. Keeping track of who has access to what data might be a headache for firms that are unprepared.It may be challenging to provide each employee with enough technical assistance given the range of phones and operating systems available. Employees will need help from the information systems division if they are unable to access crucial data or have other issues with their mobile devices. Businesses that use desktop computers often have a large number of the same machines with the same specifications and operating systems, which makes tech support considerably simpler. Companies must be equipped to manage the added complexity and diversity that mobility brings to tech support.

A company's software development teams may benefit from having a dedicated individual working to ensure that future apps will be simple to use and beneficial on smartphones. These "mobility experts" are being integrated by many businesses into fundamental IT operations and software development. A business smartphone is just a phone if it can't be used to connect to the company's current IT platform and its enterprise resource planning, supply chain management, and customer relationship management systems. Mobility experts can assist a company in maximizing mobility.

The security of corporate data accessible through mobile devices is a serious problem. Companies require strategies to make sure that private or confidential information isn't made publicly accessible in the event that a device is lost or corrupted. Assets and data are more at danger when they are mobile than if they were just present within the firm's walls and on corporate computers. Businesses often use technologies that enable them to remotely erase data from devices or encrypt data so that it cannot be utilized in the event of theft.

For remotely setting devices, enforcing various sets of rules for various people and devices, and controlling programs running on all of them, Sybase Ajaria, Trellis, Microsoft Systems Center Device Manager, and Odyssey Software Athena provide these features. The Danish company Novo Nordisk manufactures and sells pharmaceutical goods and services all over the globe. Its 2,000-person sales team utilizes a variety of mobile phones, smartphones, and portable devices while working in 25 different countries. Sybase Ajaria was put in place by Novo Nordisk to centrally handle all of these devices. The company's internal IT division can swiftly and with little end-user involvement deliver new apps on mobile devices using Ajaria. Novo Nordisk's setup method just requires a "yes" response from a new mobile phone user to begin the installation process. The fact that every Novo Nordisk market has its own data connections, rules, and needs necessitates the inclusion of elements in Ajaria that allow different nations or areas to provide their own local assistance.

The virtualization of mobile device management is another method. No of the operating system of the device, businesses may install software like Citrix Systems XenDesktop to run Windows desktops and individual apps. Employees are then able to utilize the same applications on the go as they use at work by using that software to access their whole desktop on cellphones and mobile handhelds. Due to security measures built into the virtualization software, businesses may forbid workers from storing data to local devices, encrypt all corporate data without affecting the programs or data they use personally, and remotely delete data in the case of a security breach. Citrix XenDesktop was adopted by India's Anthem Group, a prominent supplier of pharmaceutical and biotechnology services, so that staff members could access data from anywhere. This virtualization solution uses less bandwidth and works on all devices.

Companies must thoroughly assess their business processes to decide whether or not mobility makes sense for them before effectively deploying mobile devices. Mobility won't be as advantageous to every company in the same way. Companies will wind up squandering their money on pointless gadgets and programs if they don't have a clear understanding of how precisely mobile devices fit into their long-term ambitions.The challenge of calculating return on investment is one of the main concerns managers have concerning mobility. Although many employees vouch for their mobile devices and the advantages are too great to ignore, it may be challenging to put a dollar figure on how much money is made or saved by becoming mobile.

CONCLUSION

In conclusion, the law of mass digital storage covers a variety of legal issues including cybersecurity, data protection, privacy, and intellectual property. Organizations and people using mass digital storage systems to store, manage, and access digital information must adhere to legal frameworks and best practices. In order to handle the changing difficulties and advance a balanced and responsible approach to mass digital storage, continual legislative advancements and coordination among stakeholders are required as the amount of digital data keeps increasing. The rule of mass digital storage must change as technology progresses in order to take into account new problems like cloud computing, international data transfers, and upcoming storage technologies. To guarantee uniform and effective regulation of mass digital storage systems, international collaboration and judicial harmonization of legislation are essential.

REFERENCES

[1] T. D. Oganesian, “The right to privacy and data protection in the information age,” *J. Sib. Fed. Univ. - Humanit. Soc. Sci.*, 2020, doi: 10.17516/1997-1370-0664.

[2] D. J. Grimm, “The Dark Data Quandary.,” *Am. Univ. Law Rev.*, 2019.

[3] E. S. Slater, “Copyright and Mass Digitization,” *Learn. Publ.*, 2014, doi: 10.1087/20140210.

[4] R. S. Bucy and K. D. Senne, “Digital synthesis of non-linear filters,” *Automatica*, 1971, doi: 10.1016/0005-1098(71)90121-X.

[5] A. P. Sukhodolov and A. M. Bychkova, “Digital technologies and drug-related crime: Problems of counteracting the use of «telegram» messenger for trafficking drugs,” *Russ. J. Criminol.*, 2019, doi: 10.17150/2500-4255.2019.13(1).5-17.

[6] H. B. Havenith *et al.*, “Tien Shan Geohazards Database: Earthquakes and landslides,” *Geomorphology*, 2015, doi: 10.1016/j.geomorph.2015.01.037.

[7] D. Massie, “Interlending trending: A look ahead from atop the data pile,” *Interlend. Doc. Supply*, 2012, doi: 10.1108/02641611211239623.

[8] J. L. Drury and S. D. Scott, “Awareness in Unmanned Aerial Vehice Operations,” *Int. C2 J.*, 2008.

[9] C. P. Nandini, “Criminalization of copyrights infringements in the digital era with special reference to India,” in *Copyright Law in the Digital World: Challenges and Opportunities*, 2017. doi: 10.1007/978-981-10-3984-3_14.

[10] M. C. Dash, M. Prakash, and C. Behera, “E-Governance in India and Comparative Study of its Various Policies,” *IJRAR19VP023 Int. J. Res. Anal. Rev.*, 2019.

CHAPTER 3

APPLICATION OF THE CLOUD COMPUTING

Mr. Venkatesh Ashokababu
Assistant Professor, Masters in Business Administration,
Presidency University, Bangalore, India.
Email Id: ashokababu@presidencyuniversity.in

ABSTRACT:

Cloud computing has revolutionized the way individuals and organizations access and utilize computing resources. This abstract explores the concept of cloud computing, its key characteristics, and its implications for businesses and society as a whole.Cloud computing is a model for delivering on-demand access to a shared pool of computing resources, including networks, servers, storage, applications, and services. It enables users to access these resources over the internet on a pay-as-you-go basis, without the need for upfront investments in hardware or infrastructure.One of the fundamental characteristics of cloud computing is scalability. Cloud providers offer virtually unlimited computing resources, allowing users to easily scale up or down based on their needs. This scalability provides organizations with the flexibility to handle variable workloads, accommodate growth, and optimize resource allocation.

KEYWORDS:

Big Data, Cloud Deployment Models, Cloud Infrastructure, Cost Savings, Data Security, Elasticity, Hybrid Cloud.

INTRODUCTION

A computing architecture known as "cloud computing" makes use of a pool of virtualized resources to provide computer processing, storage, software, and other services through a network, typically the Internet. Any linked device and location may access these "clouds" of computing resources as required. A pool of virtualized resources are made available across a network, often the Internet, in cloud computing, where hardware and software capabilities are concerned. Applications and IT infrastructure are accessible to businesses and workers at any time, from any location, using any device.

According to the American National Institute of Standards and Technology, cloud computing must include the following key qualities: On-demand self-service: Customers may automatically and independently get computer resources such as server time or network storage as required.Access to cloud resources is possible through any normal network or Internet device, including mobile ones. Pooling of resources without regard to location: Computing resources are gathered to serve a number of users, with various virtual resources being dynamically allotted in accordance with user demand. In most cases, the user is unaware of the location of the computer resources. Rapid elasticity: To adapt to changing user demand, computing resources may be quickly provided, raised, or reduced[1]–[3].

Measured service: The cost of cloud resources is determined by the actual quantity of usage. Three major service categories make up cloud computing.

Infrastructure as a service in the cloud: Customers employ cloud service providers' processing, storage, networking, and other computer capabilities to power their information systems. For instance, Amazon offers a widely based cloud environment where it sells

services related to IT infrastructure by using the extra capacity of its IT infrastructure. These include its Elastic Compute Cloud offering for executing clients' apps and its Simple Storage offering for storing their data. Users only pay for the storage and computational power they really utilize.

Customers that utilize cloud platform as a service may create their own applications using the infrastructure and programming tools supplied by the cloud service provider. For software development and testing on the IBM Cloud, for instance, IBM provides a service called Smart Business Application Development & Test. Another example is Force.com by Salesforce.com, which enables programmers to create apps that are hosted as a service on its servers.Software as a service in the cloud Customers utilize software that is distributed via a network and hosted by the vendor on their cloud infrastructure. Leading examples include Salesforce.com, which also rents out customer relationship management and associated software services online, and Google Apps, which offers basic business applications online. Both have an annual membership price, however Google Apps also offers a condensed version for free. The data and software for these apps are kept on the distant servers of the providers, and users access them using a Web browser.

A cloud may be either public or private. A public cloud is one that a cloud service provider, like Amazon Web Services, owns, maintains, and makes accessible to the general public or a particular sector. An organization is the only one using a private cloud. It might exist on or off premises and be controlled by the company or a third party. Similar to public clouds, private clouds may smoothly distribute storage, processing power, or other resources to provide computing resources as required. These private clouds are becoming more popular among businesses that want adaptable IT resources and a cloud service model while yet maintaining ownership of their own IT infrastructure.

Organizations adopting public clouds might avoid making significant expenditures in their own hardware and software since they do not control the infrastructure. As an alternative, they buy their computing services from distant suppliers and only pay for the processing power they really use, or they are charged on a monthly or yearly subscription basis. Such services have also been referred to as on-demand computing.

The cloud computing model has several flaws. The supplier is in charge of data storage and control unless consumers make preparations for keeping their data locally. Some businesses are concerned about the security concerns associated with handing over their vital information and systems to a third party provider. Businesses want their systems to be operational around-the-clock and do not want to lose any business capabilities due to faulty cloud infrastructures. Users' dependence on the cloud computing provider is another drawback of the technology, and as was mentioned in the case study at the conclusion, this dependence may not always be desired. In spite of this, businesses are increasingly moving more of their computer processing and storage to a cloud infrastructure.

Small and medium-sized firms, who lack the means to buy and operate their own gear and software, find cloud computing to be more instantly attractive. Large firms, however, make significant expenditures in sophisticated proprietary systems that support special business procedures, some of which provide them competitive advantages. For big businesses with existing IT infrastructures, it may be difficult to estimate the cost savings from migrating to cloud services. Corporate data centers often operate on an IT budget that includes a combination of construction and operations costs. Pricing for cloud services is sometimes determined by an hourly rate or other per-use fee. It is still necessary to determine how much of the company's network management, storage management, system administration,

electricity, and real estate costs should be allocated to a single on-premises IT service, even if a company can approximate the costs of hardware and software to run a particular computing task on-premises. It's possible that an information systems department lacks the data necessary to analyze such issues on a service-by-service basis.Large businesses are more likely to employ a hybrid cloud computing strategy where they use their own infrastructure for their core operations that need the most vital systems while using public cloud computing for non-critical systems or to enhance processing capacity during busy business seasons. With the rise of cloud computing, businesses will gradually transition from having a fixed infrastructure capacity to a more flexible one that is partially owned by the company and partially leased from massive data centers run by computer hardware manufacturers.

DISCUSSION

Green Computing

Green computing, also known as green IT, refers to practices and technologies for designing, manufacturing, using, and disposing of computers, servers, and associated devices like monitors, printers, storage devices, networking and communications systems to minimize the impact on the environment.

Virtualization has become one of the main technologies for promoting green computing by reducing hardware proliferation and power consumption. A top "green" goal has been to lower computer power use. About 2% of the total is attributable to information technology. According to estimates, the United States contributes roughly 2% of the global greenhouse gas emissions. Data center power reduction has emerged as a significant commercial and environmental problem. This issue is looked at in the interactive session on organizations.

Power-Saving and High-Performance Processors

Using more effective and power-saving CPUs is another technique to minimize power consumption and hardware sprawl. Multiple processing cores are now included on a single chip in modern microprocessors. A multicore processor is an integrated circuit with two or more processor cores for improved speed, lower power use, and more effective handling of numerous activities at once. With less power consumption and heat generation, this technology allows two or more processing engines to work together to complete tasks more quickly than a chip with a single processing core. PCs with twin, quad, six, and eight core CPUs are common nowadays.

Microprocessors with low power consumption have been created by Intel and other chip makers, which is crucial for extending the battery life of tiny mobile digital devices. Netbooks, digital media players, and cellphones use very power-efficient microprocessors from ARM, Apple's A4 and A5 CPUs, Intel's Atom, and others. A laptop dual-core CPU uses around 1/50 to 1/30 the power of the dual-core A5 processor found in the iPhone 4S and iPad 2[4]–[6].While reading the most recent studies on global warming one early morning in the autumn of 2007, Dennis Jonson felt that something needed to be done.

Then he understood that he and his Nordea colleagues, who all had airline gold cards and access to airport lounges, were contributing to the issue, particularly given that majority of the seats on the daily 7:10 flight between Copenhagen and Helsinki were taken up by Nordea employees.The biggest bank group in the Baltic and Nordic countries is called Nordea. It has almost 10 million clients, 1,400 branch locations, and 6.1 million e-customers, which puts it in the top spot for internet banking. Approximately 34,000 people work with the bank across 23 nations. The company that is currently Nordea has integrated over 250 banks since its

founding in 1820, including Danish Unibank, Finnish Marita, Swedish Nordbanken, and Norwegian Christiania Kreditkasse. Due to torical mergers, the organization is geographically dispersed and needs significant travel between its national divisions.

One person's carbon dioxide emissions from flying between two Nordic capitals are in the neighborhood of 200 kg, which is double what a vehicle carrying four people would generate over the same trip. A third of Nordea's overall carbon dioxide emissions come from short- and long-haul air travel combined. Reduced travel is beneficial from a cost-savings standpoint as well as from an environmental one. A considerable sum of money is spent on air travel each year. Additionally, fewer travel days would allow many Nordea employeeswho often travelto spend more time at home with their loved ones. Dennis Jonsson was one of the Nordea workers on the 7:10 flight to Helsinki at the beginning of 2008. The IT management team had asked him to talk on "Nordea and Global Warming," with an emphasis on what steps Nordea should take. The presentation's central issue was whether Nordea could utilize technology more effectively to save expenses and lessen its impact on the environment at the same time. Two areas that the IT department was accountable for were the focus of the presentation. Air travel between several Nordic branches was the first.

The second category was power use by computers, which makes up a significant portion of all power usage in IT-intensive businesses like banks. Jonsson was hired by Nordea as the green IT manager in the spring of 2008. There were two components to the technology-based effort to cut down on air travel. First, Nordea branches received specialized, top-notch videoconferencing technology for their conference rooms. In order to facilitate two-party video chats, desktop and laptop PCs with Web cameras, headphones, and software were also made available. It was thought that video conferencing and video conferences would lessen the need for travel while also raising the standard of teamwork at Nordea. Nordea's efforts in the area of computer power consumption include finding creative methods to cool down operating computers as well as minimizing the amount of electricity required to operate the computer park. Nordea noticed that electricity use was shockingly high at night after deploying a new component in its property management system that could record power use in the Nordea offices. It was straightforward:

Many PCs were left on all the time. In order to force a shutdown at night if the computers weren't in use, power management software was installed on 23,100 PCs at Nordea as part of the Power- Off initiative. Additionally, settings for putting computers into sleep or standby mode and shutting off displays were adjusted. This prevented the emission of 3.5 million kKh yearly, or 647 tons of carbon dioxide.On the server side, the IT division used server virtualization to cut down on the number of physically powered-up computers. The expense of computer cooling is important for a company that relies heavily on IT, like Nordea. In addition to paying to heat other places, the company also has to pay to cool its computer rooms. The answer was to install its computer halls in locations where the surplus heat could be utilized to heat the space instead of losing it to the atmosphere, or to adopt a cooling system with less of an environmental effect. Today, a significant computer hall for Nordea is situated close to the sea. The hall is cooled by frigid Nordic saltwater. Nordea decreases its environmental effect and saves money by cutting the electricity needed for cooling.

Nordea has seen that decreasing prices and minimizing its environmental effect typically go hand in hand since doing so frequently entails using fewer resources, and resources are expensive. To put it another way, it is challenging to identify a drawback to the business case for green IT. Changing people's behavior and ingrained habits is the largest barrier to green IT.Low environmental impact is a component of corporate social responsibility, which is now a key component of Nordea's strategy to draw in and keep talented workers and consumers.

Nordea has set out to cut energy usage by 15%, travel by 30%, and paper consumption by 50%, all in accordance with the European Union's energy use regulation. Although the directive proposes a realistic timeframe of 2020 for accomplishing these targets, Nordea has set a deadline of 2016. If the organize- IT in its many forms will undoubtedly play a crucial role—both as part of the issue and as part of the solution—if the organization is to be successful in this.

Analogous Computing

Computer systems have become so vast, containing thousands of networked devices, that some experts fear they may become unmanageable in the future. The use of autonomous computing is one solution to this issue. An industry-wide initiative called autonomous computing aims to create systems that can deceive themselves, adjust and optimize themselves, repair damaged parts of themselves, and defend themselves against intruders and self-destruction Some of these features are seen in desktop computing platforms. For instance, virus and firewall protection software may identify and automatically remove infections from PCs while also warning operators. By connecting to an online virus protection provider like McAfee, these apps may be updated automatically as needed. IBM and other manufacturers are beginning to include autonomic characteristics into their large-systems-focused solutions.

Open Source Software and Linux

A community of several hundred thousand programmers from all over the globe creates open source software. Open source software is free and open to user modification, according to the major open source professional group, OpenSource.org. The program may be transferred by the user without further license, and any works developed from the original source must be free as well. Although the majority of open-source software is now based on a Linux or Unix operating system, open-source software is by definition not limited to any particular operating system or hardware technology.

The open source movement has been developing for more than 30 years and has shown that it is capable of producing high-quality, commercially viable software. The Linux operating system, the Apache HTTP Web server, the Mozilla Firefox web browser, and the Apache OpenOffice desktop office suite are all examples of well-known open source software applications.

On netbooks, open source programs are employed as less costly Microsoft Office substitutes. Leading manufacturers of hardware and software, such as IBM, HP, Dell, Oracle, and SAP, now provide Linux-compatible versions of their goods. The Open Source Initiative and the Learning Tracks for this include further information on the Open Source Definition and the background of open source software.

Linux

Linux, a Unix-related operating system, is perhaps the most well-known piece of open source software. Linus Torvalds, a Finnish programmer, developed Linux, which was originally made available online in August 1991. Cell phones, smartphones, netbooks, and other consumer gadgets all have Linux software. Free versions of Linux may be downloaded via the Internet, and low-cost commercial versions with tools and support from companies like Red Hat are also offered. Linux is not often seen on desktop computers, but it is a prominent player in LANs, Web servers, and high-performance computing. Linux has become a key component of IBM's, HP's, Intel's, Dell's, and Oracle's offerings to businesses. Because Linux

runs on all the major hardware platforms, including mainframes, servers, clients, and servers, it has significant implications for corporate software platforms in terms of cost savings, reliability and resilience, and integration.

Awesome Web Software: Java, Html, and Html

The most popular interactive environment for the Web is Java, an object-oriented programming language that is independent of operating systems, processors, and browsers. In 1992, James Gosling and the Green Team of Sun Microsystems developed Java. Sun began the process of making a large portion of Java available as open source software on November 13, 2006, and it was finished on May 8, 2007.

Cell phones, smartphones, cars, music players, gaming consoles, and eventually set-top cable television systems that provide interactive content and pay-per-view services all use the Java platform. No matter what kind of CPU or operating system a computer or computing device employs, Java software is designed to work on all of them. Java is the most widely used development platform for mobile devices running the Android operating system, according to Oracle Corporation, which estimates that 3 billion devices are running Java.

Sun developed a Java Virtual Machine that translates Java programming code for each of the computer environments in which Java is utilized. By doing this, the code only has to be written once and can then be used on any system that supports the Java Virtual system. Java programmers can design tiny applet applications that can be downloaded to run on a web browser and embedded in Web sites. A Web browser is a simple-to-use software application having a graphical user interface for accessing the Internet and for viewing Web sites. Examples include the web browsers Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer. For increasingly complicated e-commerce and e-business applications that need to communicate with an organization's back-end transaction processing systems, Java is being employed at the enterprise level.

HTML is a page description language used to create dynamic linkages to other Web sites and objects as well as to indicate where text, pictures, video, and sound should be displayed on a Web page. By clicking on one of these links, a user is instantly sent to another page after only pointing at a highlighted phrase or image[7]–[10]. HTML was first intended to be used to produce and connect to text-heavy static publications. Today's web, however, is considerably more social and interactive, and a lot of web sites include multimedia content, including photos, audio, and video.

These rich media needs to be integrated with Web sites using third-party plug-in programs like Flash, Silverlight, and Java. These additions, however, need for more programming and tax computer processing. One reason Apple stopped supporting Flash on its mobile devices was due of this.

This issue is resolved by HTML5, the latest iteration of HTML, which enables the direct embedding of components like as photos, audio, and video into documents without the need for processor-intensive add-ons.HTML5 will also allow the offline storing of data for applications that operate over the Web, making it simpler for Web sites to work across a variety of display devices, including mobile and desktop computers. Web pages will run more rapidly and resemble mobile applications. Although HTML5 is still under development, a number of Internet products, such as Google Chrome and more recent iterations of the Firefox Web browser, already make use of its aspects. Parts of the HTML5 standard have also been included into Google's Gmail and Google Reader. Websites deemed "iPad ready" such as CNN, The New York Times, and CBS heavily use HTML5.

Web Services And Architecture That Focuses On Services

A group of loosely linked software components known as web services communicate with one another utilizing common Web communication protocols and languages. Regardless of the operating systems or programming languages on which the systems are built, they may transmit information between two different systems. They may be used to develop applications that connect several systems inside a single firm as well as open standard Web-based applications linking systems of two separate enterprises. Web services allow diverse programs to connect with one another in a standard manner without the need for time-consuming bespoke coding since they are independent of any particular operating system or programming language.

Extensible Markup Language, often known as XML, is the core technology underlying Web services. The World Wide Web Consortium created this language in 1996 as a more potent and adaptable markup language for Web pages than hypertext markup language. HTML can only specify how information should be shown on Web pages, but XML can handle data presentation, communication, and storage.

A number in XML is not just a number; an XML tag identifies the number's representation as a price, a date, or a ZIP code. 5.2 provides examples of XML statements.XML enables computers to automatically process and analyze data and conduct operations on the data without human intervention by tagging certain pieces of document content for their meanings. Web browsers and computer applications, such order processing or business resource planning software, may apply and display the data according to predefined criteria. Web services may transmit data across processes using the standard format provided by XML.

Through common Web protocols, XML messages are used by web services to communicate. Similar to how they would find services in a phone book's Yellow Pages, businesses find and locate Web services using a directory. A software program may effortlessly connect to other programs using Web protocols without having to write unique bespoke code for each program it wishes to speak with. The criteria are the same for everyone.A service-oriented architecture is made up of the Web services that are used to create a company's software systems.

A service-oriented architecture is made up of a collection of independent services that interact with one another to provide a functional software program. These services are used to carry out various business operations. Software engineers combine these services to create different applications as required. For the development and integration of software applications employing Web services, almost all significant software suppliers provide tools and complete platforms. Microsoft has integrated Web services capabilities into its Microsoft.NET platform, while IBM has included Web service tools in its WebSphere e-business software platform.

For its online reservation system with Southwest Airlines' website, Dollar Rent A Car's systems leverage Web services. Although the systems of the two businesses have separate technological foundations, a customer making a ticket reservation on Southwest.com may make a vehicle reservation through Dollar without leaving the airline's website. Dollar employed Microsoft.NET Web services technology as a middleman rather than battling to get its reservation system to communicate data with Southwest's information systems. Southwest reservations are converted into Web services protocols, which are subsequently converted into forms that Dollar's computers can comprehend. Previously, several automobile rental firms connected their information systems to the websites of airline companies.

However, these connections had to be created one at a time in the absence of Web services. Web services provide a standardized method for Dollar's computers to "talk" to the information systems of other businesses without the need to create unique linkages for each one. In order to connect directly to the systems of a small tour operator, a major travel reservation system, as well as a wireless Web site for mobile phones and smartphones, Dollar is now extending its usage of Web services. It does not need to create new software for every new wireless device or every new partner's information system.

CONCLUSION

In conclusion, the way computer resources are accessed, provided, and used has changed as a result of cloud computing. Businesses looking for agility, flexibility, and cost savings will find it to be an appealing alternative because to its scalability, resource pooling, self-service provisioning, and cost-efficiency. To maximize the advantages of cloud computing while minimizing possible hazards, security, privacy, and vendor selection must be carefully taken into account. Even while cloud computing has many benefits, there are also difficulties. Interoperability across cloud platforms, vendor lock-in, data sovereignty issues, vendor lock-out, and the need for strong service-level agreements (SLAs) to assure quality of service and performance are a few of these.

REFERENCES

[1] S. Shilpashree, R. R. Patil, and C. Parvathi, "'Cloud computing an overview,'" *Int. J. Eng. Technol.*, 2018, doi: 10.14419/ijet.v7i4.10904.

[2] N. Taleb and E. A. Mohamed, "Cloud computing trends: A literature review," *Academic Journal of Interdisciplinary Studies*. 2020. doi: 10.36941/ajis-2020-0008.

[3] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *J. Internet Serv. Appl.*, 2010, doi: 10.1007/s13174-010-0007-6.

[4] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2016.11.031.

[5] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - The business perspective," *Decis. Support Syst.*, 2011, doi: 10.1016/j.dss.2010.12.006.

[6] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electron.*, 2019, doi: 10.3390/electronics8070768.

[7] J. Lee, "A view of cloud computing," *Int. J. Networked Distrib. Comput.*, 2013, doi: 10.2991/ijndc.2013.1.1.2.

[8] M. Armbrust, A. Fox, and R. Griffith, "Above the clouds: A Berkeley view of cloud computing," *Univ. California, Berkeley, Tech. Rep. UCB*, 2009, doi: 10.1145/1721654.1721672.

[9] B. de Bruin and L. Floridi, "The Ethics of Cloud Computing," *Sci. Eng. Ethics*, 2017, doi: 10.1007/s11948-016-9759-0.

[10] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, 2013, doi: 10.1186/1869-0238-4-5.

CHAPTER 4

EXPLORING THE SOFTWARE OUTSOURCING AND CLOUD SERVICES

Dr. Bipasha Maity
Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: bipasha@presidencyuniversity.in

ABSTRACT:

Software outsourcing and cloud services have become increasingly popular strategies for organizations to leverage external expertise and access scalable computing resources. This abstract explores the concepts of software outsourcing and cloud services, their benefits and challenges, and their impact on businesses.Software outsourcing involves contracting third-party vendors or service providers to develop, maintain, and support software applications. Organizations outsource software development to gain access to specialized skills, reduce costs, and accelerate time-to-market. It allows organizations to focus on their core competencies while relying on external expertise for software development and maintenance.Many businesses still use legacy systems today since replacing them would be very expensive and they still serve a purpose. However, the majority of their new software applications will be acquired or rented from other sources. There are three outside sources for software: commercial software vendors' software packages, outside vendors' bespoke application development, and cloud-based software services and tools.

KEYWORDS:

Cloud Computing, Cost Savings, Data Security, Hybrid Cloud, Infrastructure as a Service (IA as), Offshore Outsourcing.

INTRODUCTION

One of the main categories of software components in modern IT infrastructures, corporate software packages have previously been mentioned. A software package is a collection of prewritten, commercially accessible software packages that take the place of a company's requirement to build custom software for tasks like order processing or payroll processing. Enterprise application software providers like SAP and Oracle-PeopleSoft have created potent software packages that can support a company's core business operations globally, including finance and human resources, supply chain management, customer relationship management, and warehousing. These massive corporate software systems provide businesses access to a single, integrated, global software system for a fraction of the price they would spend if they created it themselves. Enterprise systems are thoroughly covered. Over $279 billion will be spent on software by American businesses in 2012. A third of it will come from outside the company, either from independent application service providers renting or selling software modules, or from enterprise software vendors offering firmwide solutions. SaaS suppliers will offer an additional 4% of services online in the cloud[1]–[3].

Outsourcing of software

Software outsourcing allows a business to hire outside companies, many of which are based abroad in low-wage countries, to build bespoke software or maintain existing legacy systems. Industry researchers estimate that in 2012, $251 billion was spent on offshore IT outsourcing

services. The majority of outsourcing expenses go to domestic American businesses that provide middleware, integration services, and other software support, all of which are often necessary to run bigger corporate systems. For instance, IBM and Cemex, the biggest cement producer in Mexico, agreed to an outsourcing agreement worth $1 billion over ten years in July 2012. In accordance with the agreement, IBM is responsible for managing the IT infrastructure at the Cemex corporate headquarters in Monterrey, Mexico, as well as globally. Cemex's financial, accounting, and human resources systems will be taken over and managed by IBM. Although increasingly sophisticated and experienced offshore businesses, notably those in India, have been recruited for new-program development, offshore software outsourcing companies have historically focused on lower-level maintenance, data entry, and contact center operations. However, some work that would have been moved overseas is returning to local firms as offshore salaries increase and the expenses of administering offshore projects are taken into account.

DISCUSSION

Cloud-Based Software Services and Tools

In the past, programs like Microsoft Word or Adobe Illustrator were packaged in boxes and made to run on a single computer. Nowadays, you're more likely to utilize the program as a cloud service supplied over the Internet or to download it from the vendor's website. A standard Web browser and an Internet connection are required to access cloud-based software, which is housed on strong servers in sizable data centers. In addition to the free or inexpensive tools offered by Google or Yahoo for people and small organizations, the big commercial software providers also offer enterprise software and other complicated business activities as services. Subscribing companies rent the same features from these services rather than purchasing and installing software applications, with users paying either on a subscription basis or per transaction basis. Software as a service is the current term for Web-based services that offer and enable remote access to software. Salesforce.com, which offers on-demand software services for customer relationship management, is a prime example.

Firms need a contract that contains a service level agreement in order to manage their relationship with an outsourcer or technology service provider. The SLA is a legal agreement between consumers and their service providers that specifies the particular duties of the latter and the caliber of service that the former is to give. SLAs often include the types and levels of services offered, performance measurement standards, support choices, security and disaster recovery guidelines, ownership and upgrade rights for hardware and software, customer assistance, pricing information, and termination terms. On this subject, we give a Learning Track.

Apps and mashups

The software you use for both personal and professional duties may be made up of substantial standalone programs or it may be made up of interchangeable components that are easily integrated with other online apps. These software components may be mixed and matched by both individual users and large businesses to build their own personalized apps and exchange information with others. Mashups are the name given to the resultant software applications. The goal is to combine several sources to create something "greater than" the sum of its parts. If you've ever added a feature that allows you to display movies or slide presentations to your blog or Facebook page, you've done a mashup. Web mashups generate a kind of hybrid that offers customers greater value than the original sources alone by combining the capabilities of two or more online apps. For instance, ZipRealtydisplays a comprehensive list of multiple listing service real estate listings for any zip code chosen by the user using Google Maps and

data from the online real estate database Zillow.com. To combine user profiles and partner websites' product descriptions, Amazon leverages mashup technology. Apps are brief bits of software that are often downloaded from the Internet and operate on a computer, a mobile device, or both. The Google Apps suite of desktop productivity tools is included in Google's list of internet services that are referred to as apps. But when we discuss applications nowadays, the majority of the focus is on those that were created for the mobile digital platform. These applications are what transform smartphones and other portable computing devices into all-purpose computing tools.

Around 200 million individuals in the United States were among the projected 1 billion users of apps in 2012. More than 32 billion applications have been downloaded by 2012 alone. Many cost significantly less than traditional software and may be downloaded for free or for a low price. Over 700,000 applications are now available for the Apple iPhone and iPad, and a comparable amount are available for devices running Google's Android operating system.

The variety and caliber of the applications offered by these mobile platforms play a significant role in determining their success. Apps bind the user to a particular hardware platform, increasing the barrier to switching to a rival mobile platform as more and more apps are downloaded to the user's phone.

While some downloadable applications may not access the Web, many do, offering conventional Web browsers a quicker way to access web information. Games, news and weather, maps and navigation, social networking, music, and video/movies are now the most downloaded applications. The ability to produce and modify documents, connect to corporate systems, organize and take part in meetings, manage shipments, and transcribe voice communications are all made possible by serious applications for business users. In addition, there are a ton of e-commerce applications available for online product and service research and purchase.

Management Concerns

Dealing with platform and technological change, management and governance, and making smart infrastructure expenditures are just a few of the difficulties involved in developing and maintaining a cohesive IT infrastructure.

Platform And Infrastructure Change Management

Businesses often rapidly overrun their infrastructure as they expand. Businesses that experience a decline may be burdened by surplus infrastructure that was acquired during a boom. When the majority of expenditures in IT infrastructure are made as fixed-cost purchases and licenses, how can a company maintain flexibility? How scalable is the infrastructure? A computer, product, or system is said to be scalable if it can grow to accommodate many people without malfunctioning. When designing hardware capacity, it is important to take new applications, mergers and acquisitions, and changes in business volume into account since they all affect computer workload.

For administering these platforms, businesses adopting mobile and cloud computing platforms will need new rules and processes. They will need to make a list of all the mobile devices they use for work and create rules and methods for monitoring, maintaining, and protecting them as well as for managing the information and software that they run. In order to ensure that the hardware and software for important applications are always accessible when required and that they fulfill corporate requirements for information security, businesses employing cloud computing and SaaS will need to create new contractual

agreements with distant vendors. To sustain the level of business performance they anticipate, management of the company must decide on the accept levels of computer reaction time and availability for the firm's mission-critical systems.

Management and Administration

The subject of who will be in charge of and manage the company's IT infrastructure has long been a source of contention among CEOs and information system managers. 2 explained the idea of IT governance and discussed some of the problems it attempts to solve. Other crucial considerations concerning IT governance include: Should IT infrastructure be centrally controlled and managed or should departments and divisions be responsible for making their own information technology decisions? What connection exists between business unit information systems management and the administration of the central information systems? How will business units split up the expense of infrastructure? Each firm will have to come up with solutions based on its own requirements.

Investing wisely in infrastructure

The company has made a large investment in IT infrastructure. If too much money is spent on infrastructure, it sits unused and hinders the company's financial performance. Important business services cannot be provided if spending is too low, and the company's rivals will beat the underinvesting firm. What much should the business invest in infrastructure? The solution to this question is not simple. Whether a business should build and maintain its own IT infrastructure or lease it from outside vendors, particularly those providing cloud services, is a related subject. The rent-versus-buy option is the choice between owning your own IT assets and renting them from third parties.Although using the cloud may be a low-cost approach to boost scalability and flexibility, businesses should carefully consider the option's implications for business operations and security requirements. In certain cases, renting software is more expensive overall than buying and maintaining a program in-house. However, if employing cloud services enables the organization to concentrate on fundamental business concerns rather than technological difficulties, there may be advantages[4]–[6].

Technology Assets' Total Cost of Ownership

The actual cost of owning technology resources includes the upfront price of purchasing and installing hardware and software, as well as ongoing administrative costs for hardware and software upgrades, maintenance, technical support, training, and even utility and real estate costs for operating and housing the technology. These direct and indirect expenses may be analyzed using the total cost of ownership model to assist businesses calculate the true cost of a particular technology adoption. The total cost of ownership (TCO) for a PC may be up to three times the equipment's initial purchase price when all these cost factors are taken into account. While a wireless portable computer may cost a few hundred dollars to acquire for a corporate employee, the total cost of ownership (TCO) for each device is substantially higher, ranging from $1,000 to $3,000, according to different consultant estimates.

Gains in efficiency and productivity from supplying workers with mobile computing devices must be weighed against the higher expenses associated with integrating these devices into the company's IT infrastructure and with providing technical assistance. Fees for wireless airtime, end-user instruction, help desk assistance, and software for specialized applications are additional cost elements. If the mobile devices need to be connected with back-end systems, such as corporate apps, or run a variety of applications, the costs will be greater.

In order to understand the complete cost of the company's hardware and software, managers must pay special attention to administrative expenses, which make up just around 20% of TCO. Through improved management, some of these administrative expenses may be decreased. Because their departments and divisions have been permitted to buy their own technology, many huge businesses are burdened with redundant, incompatible gear and software. These businesses might lower their TCO in addition to using cloud services by centralizing and standardizing their hardware and software resources. If a company limits the variety of computers and software that its workers are permitted to use, it may be able to lower the amount of the information systems workforce necessary to maintain its infrastructure. System administration and troubleshooting may both be done from one single place in a centralized architecture Model of Competitive

Forces for Investment in IT Infrastructure Services offered by your business are in demand. Make a list of the services you now provide to clients, partners, and staff. To determine if the services you now provide are fulfilling the requirements of each group, conduct surveys or focus groups. Are clients, for instance, voicing complaints about receiving delayed replies to their availability and pricing inquiries? Do workers voice complaints about getting the information they need for their jobs? Are your suppliers expressing frustration about their inability to learn about your manufacturing needs?

Your company's business plan. Try to determine what new services and skills will be needed to fulfill strategic objectives by analyzing the five-year business plan of your company. The cost, infrastructure, and IT strategy of your company. Analyze the alignment of your company's information technology strategies for the next five years with its business plans. Calculate the overall cost of the IT infrastructure. You should do a TCO analysis. If your company doesn't already have an IT strategy, you'll need to create one that takes into consideration the five-year strategic plan of the company. You may use six variables to determine how much money your company should allocate on IT infrastructure." evaluation of information technology. Is your business at the cutting edge of information technology, or is it lagging behind? You should stay away from both scenarios. Spending money on cutting-edge technologies that are still under development, often pricey, and sometimes unstable is typically not a good idea. You wish to invest in technologies for which there are a variety of providers, IT vendors compete on price rather than design, and standards have been developed. You don't want to delay investing in new technology, however, or let rivals build new capabilities and business models based on them.

competing business services. Analyze the technological services that rival companies provide to clients, partners, and staff. Establish qualitative and quantitative benchmarks to contrast their performance with that of your company. If your company's service standards are subpar, it will have a competitive disadvantage. Look for ways that your company can provide exceptional service. IT infrastructure investments made by rival companies.

Compare your IT infrastructure spending to those of your rivals. Many businesses make their creative IT spending extremely public. You may be able to uncover information on IT investments in public businesses' SEC Form 10-K annual filings to the federal government if rival firms attempt to keep their IT expenditures a secret when such expenditures have an influence on a firm's financial outcomes. It's not necessary for your business to spend equal to or more than its rivals. It could have found much less costly methods to provide services, which might give it a cost edge. Alternately, your company can be spending far less than rivals yet still doing poorly and losing market share. Information management and databases are the cornerstones of business intelligence.

The largest manufacturing business in the UK is AE Systems, which is also one of the biggest commercial aerospace and defense companies in Europe. One of the most powerful multi-role combat aircraft in the world, the Eurofighter Typhoon, is only one of its high-tech, information-driven products and services, along with the Jetstream. family of commercial aircraft, to the delivery of information technology and information systems for e-business to create and put into practice logistics, IT, and e-capability services. With 88,000 employees and more over US$30 billion in annual revenue, BAE has production, sales, and support facilities located all over the globe, including the UK, Europe, the US, and Australia.

Although BAE continues to expand into new markets in the Middle East and Asia and has solidified its competitive position in established markets, the performance of its aircraft division was being hampered by outdated information systems that support the computer-aided design and computer-aided manufacturing of its aircraft. The distributed nature of BAE's design and manufacturing facilities made it more difficult and resource-intensive to store and analyze precise operational data sets describing the intricate parts of the various aircraft types to produce aircraft assembly reports for the production lines. When there are different part naming standards and codes, data representing the same aircraft component components may need to be resolved.

The process of gaining access to the data from the various systems was one that required several technological difficulties. The probability of delays in delivering the aircraft assembly reports and other operations data sets required for aircraft production management decision making increased as BAE's aviation business developed. In the worst situation, the assembly line would cease producing airplanes until proper information was available, which would have an impact on the schedule and cost. In order to develop assembly reports and other operations data, BAE's CAD/CAM team stored and analyzed data sets obtained from five significant aircraft design and manufacturing facilities dispersed around the United Kingdom. Each of these facilities is home to thousands of workers participating in the design and manufacture process. Despite the fact that the majority of the data that the legacy systems processed was stored in computer files, there were countless situations when paper drawings with com-

Uncertainties and contradictions in the assembled reports were resolved using information on component design and manufacturing. The assembly reports were created with a feeling of uncertainty when these data ambiguities and inconsistencies occurred. A single source for CAD/CAM data that would also make it easier to integrate data from previous systems was what BAE required. The company made the decision to replace its old systems with an enterprise-wide knowledge management system that would combine design and manufacturing data into a single database that the design and manufacturing engineers could access simultaneously. Siemens' Teamcenter product lifecycle management software and Dassault Systems' CATIA CAD/CAM software were both adopted by BAE. Using Microsoft Azure, IBM Smart Cloud Enterprise+, and Amazon Web Services, Teamcenter may be configured to benefit from current advancements in cloud computing.

BAE Systems now has access to robust integrated data management solutions thanks to the combination of Siemens' Teamcenter and Dassault Systems' CATIA. Users may see the impact of component design modifications and configuration choices in real-time by using the component markup and rollup tools included in the Teamcenter database. In terms of its design and manufacturing data management and storage, the new system has significantly reduced BAE's costs while enhancing performance. By being able to develop comprehensive and precise aircraft component definitions and configurations, BAE has been able to satisfy quality, schedule, and cost requirements with fewer legacy systems and data files to handle.

By synchronizing upstream CAD and downstream CAM component definitions, BAE's new design and manufacturing database system has increased speed-to-market and enabled greater cross-discipline cooperation. The organization has been able to devote additional resources to enhancing data management throughout the whole operation thanks to these savings.

The introductory graphic highlights crucial issues brought up by this case and this. The management of BAE Systems determined that the company needed to enhance its data management. It was exceedingly difficult to access, accurately assemble, and utilize data on design components, produced components, and their final assembly that had been stored in several massive legacy systems for use in the assembly of airplane components on a manufacturing line. The data's utility was limited by frequent repetition and inconsistency. It was impossible for management to have an enterprise-view of the business.

In the past, BAE Systems has relied on manual paper methods to compile data for management reporting and to reconcile its redundant and inconsistent data. The company's information technology staff was unable to do higher-value tasks since this solution was so time-consuming and expensive. Installing new technology and software to provide an enterprise-wide repository for business data that would support a more simplified set of business applications was a more suitable approach. The updated database management system was coupled with corporate software that could provide data for reporting throughout the whole company. Redundancies had to be removed from the data, and rules, roles, and procedures had to be established for updating and utilizing the data. The data also needed to be reorganized into a consistent company-wide structure[7]–[10].

In order to conduct daily CAD/CAM transactions for the final assembly of aircraft components and to identify and compile data for management reporting, BAE Systems uses a state-of-the-art database management system suite of software. This software helps BAE Systems increase efficiency. The cost of handling and keeping the data has been decreased, and the data are now more accurate and trustworthy.

Consider the following: In its legacy database infrastructure, what kind of data management issues did BAE Systems encounter? What tasks needed to be completed before the business could fully benefit from the new data management technology?Users get reliable, timely, and relevant information via an efficient information system. Information that is accurate is error-free. When information is accessible to decision-makers at the appropriate moment, it is timely. When information is applicable and suitable for the tasks and choices that call for it, it is said to be relevant. It may come as a shock to you to find that a lot of firms lack timely, accurate, or relevant information because their information systems' data has not been properly managed and maintained. Data management is crucial because of this. Let's examine the issue by examining how information systems organize data in computer files and conventional file management techniques.

CONCLUSION

In conclusion, Organizations may gain a lot from software outsourcing and cloud services, including access to specialized talents, cost savings, scalability, and flexibility. To reduce risks and guarantee good results, however, cautious vendor selection, transparent communication, security measures, and regulatory compliance are necessary. Organizations may promote innovation, increase efficiency, and maintain competitiveness in the digital world by strategically using software outsourcing and cloud services. Another issue that businesses may have when significantly using outsourced software or cloud services is vendor lock-in. To retain flexibility and prevent reliance on one vendor, it is crucial to carefully analyze contract terms, service-level agreements (SLAs), and exit alternatives.

REFERENCES

[1] M. I. Malik, "Cloud Computing-Technologies," *Int. J. Adv. Res. Comput. Sci.*, 2018, doi: 10.26483/ijarcs.v9i2.5760.

[2] S. Schneider and A. Sunyaev, "Determinant factors of cloud-sourcing decisions: Reflecting on the IT outsourcing literature in the era of cloud computing," *J. Inf. Technol.*, 2016, doi: 10.1057/jit.2014.25.

[3] E. M. Bodero, M. P. Lopez, A. E. Congacha, E. E. Cajamarca, And C. H. Morales, "Google Colaboratory como alternativa para el procesamiento de una red neuronal convolucional," *Rev. Espac.*, 2020.

[4] L. Wang, "Architecture-Based Reliability-Sensitive Criticality Measure for Fault-Tolerance Cloud Applications," *IEEE Trans. Parallel Distrib. Syst.*, 2019, doi: 10.1109/TPDS.2019.2917900.

[5] M. Lewis, "Outsourcing, new technologies and new technology risks: Current and trending UK regulatory themes, concerns and focuses.," *J. Secur. Oper. Custody*, 2018.

[6] G. A. Vazquez-Martinez, J. L. Gonzalez-Compean, V. J. Sosa-Sosa, M. Morales-Sandoval, and J. C. Perez, "CloudChain: A novel distribution model for digital products based on supply chain principles," *Int. J. Inf. Manage.*, 2018, doi: 10.1016/j.ijinfomgt.2017.12.006.

[7] O. M. Yigitbasioglu, K. Mackenzie, and R. Low, "Cloud computing: How does it differ from IT outsourcing and what are the implications for practice and research?," *Int. J. Digit. Account. Res.*, 2013, doi: 10.4192/1577-8517-v13_4.

[8] O. M. Yigitbasioglu, "External auditors' perceptions of cloud computing adoption in Australia," *Int. J. Account. Inf. Syst.*, 2015, doi: 10.1016/j.accinf.2015.09.001.

[9] M. Walterbusch, B. Martens, and F. Teuteberg, "Evaluating cloud computing services from a total cost of ownership perspective," *Manag. Res. Rev.*, 2013, doi: 10.1108/01409171311325769.

[10] M. Sebesta, "On ICT Services Outsourcing in the Context of Small and Medium Enterprises," *Procedia - Soc. Behav. Sci.*, 2013, doi: 10.1016/j.sbspro.2013.06.467.

CHAPTER 5

FEATURES OF THE DATABASE APPROACH TO DATA MANAGEMENT

Dr. Vankadari Gupta
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: chithambargupta@presidencyuniversity.in

ABSTRACT:

The database approach to data management revolutionized the way organizations store, organize, and access their data. This abstract explores the concept of the database approach, its fundamental principles, and its significance in effective data management.The database approach involves using a centralized repository, known as a database, to store and manage structured data. It offers a structured and systematic approach to organizing data, enabling efficient data retrieval, manipulation, and analysis.\

The database approach relies on database management systems (DBMS) to facilitate data storage, retrieval, and maintenance.The smallest piece of data that a computer can process is called a bit. A byte, which is made up of a collection of bits, stands in for a single character, which might be a letter, a number, or another symbol. A field is a collection of characters that form a word, a collection of words, or a whole number. A record is made up of a number of linked fields, such as the student's name, the course they took, the date, and their grade; a file is made up of a number of records of the same kind.

KEYWORDS:

Data security, Data warehousing, Database management system (DBMS), Indexing, Query optimization, Relational database, Schema design.

INTRODUCTION

Data is arranged by a computer system in a hierarchy that moves from bits and bytes through fields, records, files, and databases. The smallest piece of data that a computer can process is called a bit. A byte, which is made up of a collection of bits, stands in for a single character, which might be a letter, a number, or another symbol. A field is a collection of characters that form a word, a collection of words, or a whole number. A record is made up of a number of linked fields, such as the student's name, the course they took, the date, and their grade; a file is made up of a number of records of the same kind.

An entity is described in a record. An entity is a person, place, object, or event that is the subject of information that we keep and preserve. An attribute is a feature or characteristic that describes a certain thing. For instance, the entity COURSE has the properties Student, Course, Date, and Grade.

The fields of the record representing the entity COURSE include the particular values that these characteristics may have. Data is arranged by a computer system in a hierarchy that begins with the bit, which may represent either a 0 or a 1. One letter, integer, or symbol may be represented by a byte, which is made up of many bits. A field may be made up of bits, and a record can be made up of linked fields. A file may be created from a group of connected records, and a database can be created from a group of related files.

Traditional File Environment Controversies

Without a corporate strategy, systems tended to develop on their own in the majority of firms. Each industry created its own systems and data files, including those for accounting, finance, manufacturing, human resources, and sales and marketing[1]–[3]. Of course, each application needed its own set of files and software to function. For instance, the functional area of human resources may contain a personnel master file, payroll file, medical insurance file, pension file, mailing list file, and so on, until tens or even hundreds of files and programs existed. This procedure resulted in several master files being produced, kept up with, and used across the organization by various departments or divisions. After five or ten years of this procedure, the company is left with hundreds of cumbersome programs and applications that are exceedingly challenging to administer.

Data redundancy and consistency issues are the results.Each functional area in a business is encouraged to create specialized applications when a conventional method to file processing is used. Every program needs its own data file, which is most likely a subset of the master file. These master file subsets result in redundant and inconsistent data, rigid processing, and a waste of storage space. Dependency on program data, rigidity, inadequate data security, and an inability for apps to exchange data.

Data Redundancy and Inconsistency

Data redundancy is the existence of identical data in numerous data files, resulting in the storage of the same data in various locations. When many groups within an organization independently acquire the same piece of data and store it in separate locations from one another, data redundancy arises. Data redundancy consumes store space and may result in inconsistent data, where several values may exist for the same property.

Using several coding schemes to represent values for an attribute might cause more confusion. For instance, multiple codes may be used to describe garment size across the sales, inventory, and production systems of a clothes shop. One system could refer to a garment's size as "extra-large," while another would use the designation "XL" instead. Companies would find it challenging to develop enterprise systems that combine data from many sources for customer relationship management, supply chain management, and other purposes due to the ensuing confusion.

Data Dependence on Programs

Program-data dependency describes the relationship between the data kept in files and the particular programs needed to update and maintain those files, such that changes to the programs need modifications to the data. Every conventional computer program is required to specify the location and type of the data it uses. Any modification to a software program in a conventional file system could need a change in the data the program accesses.

A five-digit zip code might be changed to a nine-digit zip code with one application. Other applications that needed the five-digit zip code would no longer function correctly if the original data file were altered from five to nine digits. Millions of dollars may be required to effectively execute such modifications.

DISCUSSION

Not Being Flexible

After substantial programming, a typical file system can provide regular scheduled reports, but it is unable to produce ad hoc reports or quickly address sudden requests for information.

Ad hoc queries need information that is somewhere in the system, but it can be too costly to get it. To compile the necessary data elements in a new file, many programmers may need to labor for weeks.

Lack of Security

Access to and dissemination of information may be out of control because there is little management or control over data. It's possible that management has no means of knowing who is accessing or even changing the data of the firm.

Data availability and sharing issues

It is almost hard to communicate or access information quickly because bits of information in various files and areas of the organization cannot be coupled to one another. It is impossible for information to easily move across various functional areas or portions of the organization. Users may decide not to utilize these systems if they discover different values for the same piece of information in two distinct systems because they cannot trust the accuracy of their data.Data management using a database approach Many of the issues with conventional file organizing are solved by database technology.

A more precise definition of a database is a collection of data that has been centrally located and controlled to effectively support several applications. Data appears to users as being kept in only one area, as opposed to being separated into files for each program. Multiple applications may be supported by a single database. A company may, for instance, construct a single common human resources database rather than holding employee data in several information systems and different files for people, payroll, and benefits.

Systems for managing databases

A database management system is a piece of software that enables an organization to consolidate data, manage it effectively, and provide application programs access to the data that is stored. The database management system serves as a link between application applications and the actual data files. When an application software requests a data item, such gross pay, the database management system (DBMS) locates the requested item and displays it to the application program.

When using conventional data files, the programmer would have to tell the computer where each data piece was placed after describing its size and format. By separating the logical and physical representations of the data, the DBMS frees the programmer or end user from having to understand where and how the data are really kept. The physical view demonstrates how data are really arranged and structured on physical storage media, as opposed to the logical view, which depicts data as they would be seen by end users or business professionals.

The physical database is made accessible by the database management software for the various logical views needed by users. An employee's name, social security number, and health insurance coverage could be needed by a benefits expert for the human resources database. Data like the employee's name, social security number, gross salary, and net pay could be required by a member of the payroll department.

All of these views' data are kept in a single database, making it easier for the company to manage them. How a DBMS Addresses Issues with the Conventional File Environment By decreasing isolated files where the same data are duplicated, a DBMS lowers data redundancy and consistency. Although the corporation may not be able to completely eradicate data redundancy, the DBMS can assist reduce redundancy. Using a DBMS may

assist an organization verify that every instance of redundant data has the same values, even if the business keeps some duplicate data. This prevents data inconsistency. Programs and data are separated by the DBMS, allowing data to stand alone.

Several alternative data views are available from a single human resources database, depending on the user's information needs. Two potential viewpoints are shown, one of which would be of interest to a benefits expert and the other of which would be of interest to a worker in the company's payroll division. by themselves. Because users and programmers may run ad hoc queries on the database's data, information access and availability will rise, and program development and maintenance costs will decrease. The company is able to centrally manage data, their usage, and their security thanks to the DBMS.

Relations DBMS

Different database models are used by modern DBMS to maintain track of entities, properties, and relationships. The relational DBMS is now the most common form of DBMS for PCs, as well as for bigger systems and mainframes. Two-dimensional s are how relational databases display data. s may be thought of as files. Each one has information about an entity and its characteristics. While DB2, Oracle Database, and Microsoft SQL Server are relational DBMS for big mainframes and midrange computers, Microsoft Access is a relational DBMS for desktop systems. A well-liked open source DBMS is MySQL, while a DBMS designed for mobile computing devices is Oracle Database Lite. The actual data on a particular provider that is included in an is referred to as a row. Informally known as records or, in more technical terminology, tuples, rows are rows. Data for the PART entity are kept separate.

Each entry in the SUPPLIER table is uniquely identified by the Supplier Number column so that it may be accessed, modified, or sorted. It's known as a critical field. In a relational database, each object has a single field that serves as its main key.

This key field serves as the single, unchangeable identifier for all the data in any row of the database. The main key for the SUPPLIER is Supplier_ Number, while the primary key for the PART is Part_ Number. Keep in mind that Supplier Number may be found in the PART and SUPPLIER s. Supplier Number serves as the SUPPLIER's main key. It is referred to be a foreign key when the field Supplier Number exists in the component because it serves as a field for looking up information about the supplier of a certain component.

Relational DBMS operations

If any two relational databases have a similar data piece, it is simple to combine them to offer the data that consumers need. Consider searching for the names of vendors who may provide us part numbers 137 or 150 in this database. Two people would have to provide us with information: the SUPPLIER and the PART. Keep in mind that Supplier_Number is a common data element between these two files.

Select, join, and project are the three steps to creating useable data sets. All of the file's entries that satisfy the specified criteria are created as a subset by the select procedure. Select, in other words, generates a subset of rows that satisfy certain requirements. For the sake of this example, we wish to pick out entries from the PART where the Part_Number is either 137 or 150. In order to provide the user more information than is accessible in individual s, the join operation joins relational s. In our example, we wish to combine the SUPPLIER and the now-shortened PART into a single item[4]–[6].

The project action generates a subset of columns in a, allowing the user to build new s that only include the necessary data. In our case, we only want to extract the Part_Number, Part_Name, Supplier_Number, and Supplier_Name columns from the new.

Non-Relational Databases and Cloud-Based Databases Relational database technology has been the industry standard for more than 30 years. Database alternatives to the conventional relational model of data organization in the form of s, columns, and rows are needed because of cloud computing, enormous data volumes, heavy workloads for Web services, and the requirement to store novel forms of data. For this aim, businesses are turning to "NoSQL" non-relational database technology.

A more adaptable data architecture is used by non-relational database management systems, which are built for handling big data sets across several dispersed servers and for simple scaling up and down. They can speed up basic queries against huge amounts of structured and unstructured data, such as Web, social media, graphics, and other types of data that are challenging to examine with conventional SQL-based tools.

NoSQL databases come in a variety of forms, each with unique technological characteristics and behavior. One such is the Oracle NoSQL Database, as well as Amazon's SimpleDB, a cloud-based Amazon Web Service. In order to build and store several data sets, simply query data, and return the results, SimpleDB offers a straightforward Web services interface. A formal database structure does not need to be pre-defined, nor does it need to be altered if new data are subsequently added.

Relational database services are also offered by Amazon and other cloud computing providers. Oracle Database, MySQL, and SQL Server are available as database engines via Amazon Relational Database Service. The cost is determined by consumption. Cloud-based data management services are particularly attractive to Web-focused start-ups or small to medium-sized businesses looking for database capabilities at a lower cost than in-house database products. Oracle has its own Database Cloud Service using its relational Oracle Database 11g, and Microsoft SQL Azure Database is a cloud-based relational database service based on Microsoft's SQL Server DBMS.

In order to better handle peak system loads during significant ticket sales, TicketDirect, which sells tickets for concerts, sports events, theater productions, and movies in Australia and New Zealand, selected the SQL Azure Database cloud platform. Data was sent to the SQL Azure database. TicketDirect is able to increase its processing capabilities in response to real-time demand while keeping prices down by switching to a cloud-based solution.

Companies now have the option of employing databases in private clouds in addition to public cloud-based data management services. For instance, Sabre Holdings, the leading global supplier of software as a service to the aviation sector, has a private database cloud that serves 700 users and more than 100 projects. Multiple applications may access database services using a consolidated database that spans a pool of standardized servers running Oracle Database 11g. Even when the workload fluctuates, workload management solutions make sure there are enough resources available to fulfill application demands. These projects, which include customized airline travel apps as well as rail, hotel, and other travel sector applications, need less servers, DBMS, and storage devices thanks to the common hardware and software platform. Servers, storage, operating systems, databases, and a variety of workloads are consolidated into private clouds using a common hardware and software architecture. IT organizations may increase service levels and save operational and capital expenses by deploying databases on a consolidated private cloud. The return on investment increases with increasing consolidation density.

Database Management Systems' Capabilities

The ability to manage, access, and organize data in a database is provided by a DBMS. The data definition language, data dictionary, and data manipulation language are the most crucial. The structure of the database's content may be specified using the data definition feature of DBMSs. It would be used to build databases and specify the properties of each field's contents. A data dictionary would be used to record this database information. A data dictionary is a human or automated file that contains descriptions of various data components and their properties.

Microsoft Access offers a basic data dictionary feature that shows details about each field's name, description, size, type, format, and other characteristics. Large corporate databases' data dictionaries may also include use, ownership, authorisation, security, and details about the people, business processes, software applications, and reports that utilize each data piece.

Reporting and Querying

Tools for navigating and modifying data in databases are part of DBMS. To add, modify, remove, and retrieve data from a database, most DBMS contain a specific language called a data manipulation language. This language has commands that let programmers and end users get data out of the database to create applications and fulfill information requests. SQL, also known as structured query language, is now the most well-known language for data manipulation. To get the data they need from the database, users using DBMS for large and midrange systems, such as DB2, Oracle, or SQL Server, would use SQL. While using SQL as well, Microsoft Access offers a unique set of user-friendly tools for searching databases and assembling data from databases into polished reports.

Users may make queries using features in Microsoft Access by specifying the results, fields, and s they want, then choosing the rows from the database that satisfy certain requirements. These subsequent actions are converted into SQL instructions. 6.8 is an example of how the SQL query to choose suppliers and components may be created using the Microsoft query-building tools. Microsoft Access and other DBMS have the ability to generate reports, making it possible to show the relevant data in a more organized and professional manner than would be feasible with a simple query. Although it may also be used with Access, Crystal Reports is a well-known report generator for big corporate DBMSs. Access provides the ability to create desktop system apps as well. Tools for building data input displays, reports, and the logic necessary to conduct transactions are among them.

Database Design

Understanding the links between the data, the types of data that will be kept in the database, how the data will be utilized, and how the organization will need to alter to handle data from a company-wide perspective are all necessary before you can develop a database. Both a conceptual and a physical design are necessary for the database. The physical design of a database depicts how the database is really set up on direct-access storage devices, as opposed to the conceptual, or logical, design of a database, which is an abstract representation of the database from a business viewpoint.

Diagrams of Entity-Relationships And Normalization

The conceptual database design outlines the classification of the database's data items. In order to satisfy corporate information needs, the design process determines linkages between data pieces and the most effective approach to organize data items together. Additionally, the procedure locates redundant data items and the collections of data elements needed for

certain application programs. Until an overall logical perspective of the connections among all the data in the database develops, groups of data are arranged, improved, and simplified.

Complex data groupings must be simplified to reduce duplicate data pieces and uncomfortable many-to-many links in order to utilize a relational database architecture efficiently. Normalization is the process of extracting simple, adaptable data structures from large, complicated collections of data. S 6.9 and 6.10 provide examples of this approach. In the specific company being represented here, an order may include many parts, but only one supplier will provide each element. Even if the order is for components from a single supplier, the name and address of the supplier would need to be repeated if we built a relation named ORDER with all the data given above. Because several components may be ordered from the same source, this connection includes repeated data groups. Breaking down ORDER into smaller relations, each of which describes a single object, is a more effective approach to organize the data. The original connection ORDER has been divided into four more manageable relations after normalization. Entity-relationship modeling and database design are used in the Learning Tracks to achieve this. The relation ORDER is left with only two characteristics, and the relation LINE_ITEM has a combined, or concatenated, key consisting of Order_Number and Part_Number.

Relational database systems make an effort to uphold referential integrity principles in order to maintain the consistency of connections between connected s. You cannot add a record to a foreign key-pointing database unless the connected database already has a record with the same name. The foreign key Supplier_Number connects the PART to the SUPPLIER in the database we previously looked at. If there isn't a comparable record in the SUPPLIER for Supplier_Number 8266, we can't add a new record to the component for the component with Supplier_ Number 8266. If we remove the entry for Supplier_ Number 8266 in the SUPPLIER, we must also delete the matching item in the PART. In other words, we shouldn't be using components from providers that don't exist! It cannot be underlined enough:

The system will not be able to effectively support the company if the data model is not correct. Systems for the corporation won't operate as efficiently as they might since they'll have to deal with data that may be incorrect, lacking, or challenging to locate. Undoubtedly, the most significant thing you can take away from this course is how to understand an organization's data and how it should be stored in a database.

For instance, Famous Footwear, a network of shoe stores with over 800 locations in 49 states, was unable to fulfill its promise to customers to always have "the right style of shoe in the right store for sale at the right price" because its database was not correctly configured for quick inventory adjustments.

The corporation used an Oracle relational database, but it was largely intended for creating conventional reports for management rather than responding to market changes. It was operating on a midrange machine. The management was unable to get exact information on the inventory of certain goods in each of its outlets.

The business required to create a new database in order to better arrange the sales and inventory data for analysis and inventory management[7]–[10]. Databases are used by businesses to record routine operations like paying suppliers, fulfilling orders, monitoring consumers, and paying staff. Databases are also necessary to give data that will improve decision-making by managers and staff and help the organization function more smoothly. The data holds the solution whether a business wants to discover which of its products is the most popular or who its most lucrative client is.

The Big Data Difficulty

The majority of data gathered by corporations up until around five years ago consisted of transaction data, which was simple to fit into the rows and columns of relational database management systems. Since then, there has been an increase in the amount of data created by machines, including data from sensors or electronic trading systems, as well as data from Web traffic, e-mails, and social media posts. These data may not be suitable for relational database solutions that arrange data in the form of columns and rows since they may be unstructured or semi-structured. These datasets with quantities so large that traditional DBMS cannot collect, store, or analyze them are now referred to as big data. Although there is no set definition of big data, it often refers to data in the petabyte and exabyte range, or billions to trillions of records from several sources. Compared to conventional data, big data are created far more quickly and in much higher volumes. For instance, there are more than 25,000 airline flights every day, and a single jet engine may produce 10 terabytes of data in only 30 minutes. Twitter produces more than 8 terabytes of data per day, despite "tweets" having a character restriction of only 140. The quantity of data that is accessible to enterprises is exploding, according to the technology research company International Data Center, which estimates that data are more than doubling every two years.

Businesses are interested in big data because it has the potential to provide new insights into consumer behavior, weather patterns, financial market activity, and other phenomena. Big data may also show more patterns and intriguing anomalies than smaller data sets. However, enterprises require new technologies and tools capable of handling and analyzing non-traditional data in addition to their standard corporate data if they are to generate economic value from this data.

CONCLUSION

In conclusion, Data may be stored, arranged, and accessed in an organized and effective manner using the database method to data management. Data independence, integrity, sharing, and security are just a few advantages it provides.The majority of data gathered by corporations up until around five years ago consisted of transaction data, which was simple to fit into the rows and columns of relational database management systems.

Since then, there has been an increase in the amount of data created by machines, including data from sensors or electronic trading systems, as well as data from Web traffic, e-mails, and social media posts. The database strategy helps firms to efficiently manage and exploit their data for informed decision-making and competitive advantage with the right design, implementation, and governance. The database strategy must take into account data governance and data management. Organizations must define roles, methods, and policies for data management in order to guarantee data security, accuracy, and legal compliance.

REFERENCES

[1] D. G. D. Funcion, “Predictive analysis on student competency in database management system: A data mining approach,” *Int. J. Sci. Technol. Res.*, 2020.

[2] W. S. Campbell, J. Pedersen, J. C. McClay, P. Rao, D. Bastola, and J. R. Campbell, “An alternative database approach for management of SNOMED CT and improved patient data queries,” *J. Biomed. Inform.*, 2015, doi: 10.1016/j.jbi.2015.08.016.

[3] R. Angles, H. Thakkar, and D. Tomaszuk, “Mapping RDF Databases to Property Graph Databases,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2993117.

[4] W. J. Pate and A. S. Brocard, "Lessons Learned from Implementation of a Web-Based Environmental Health and Safety Management Database in an Academic Medical Center," *ACS Chem. Heal. Saf.*, 2020, doi: 10.1021/acs.chas.9b00001.

[5] M. T. Bazelier *et al.*, "Data management and data analysis techniques in pharmacoepidemiological studies using a pre-planned multi-database approach: A systematic literature review," *Pharmacoepidemiol. Drug Saf.*, 2015, doi: 10.1002/pds.3828.

[6] C. Balantic and T. Donovan, "AMMonitor: Remote monitoring of biodiversity in an adaptive framework with r," *Methods Ecol. Evol.*, 2020, doi: 10.1111/2041-210X.13397.

[7] S. Berrouiguet *et al.*, "An approach for data mining of electronic health record data for suicide risk management: Database analysis for clinical decision support," *JMIR Ment. Heal.*, 2019, doi: 10.2196/mental.9766.

[8] K. Munir and M. Sheraz Anjum, "The use of ontologies for effective knowledge modelling and information retrieval," *Applied Computing and Informatics*. 2018. doi: 10.1016/j.aci.2017.07.003.

[9] S. Tang, D. R. Shelden, C. M. Eastman, P. Pishdad-Bozorgi, and X. Gao, "A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends," *Automation in Construction*. 2019. doi: 10.1016/j.autcon.2019.01.020.

[10] R. Rialti, G. Marzi, C. Ciappei, and D. Busso, "Big data and dynamic capabilities: a bibliometric analysis and systematic literature review," *Manag. Decis.*, 2019, doi: 10.1108/MD-07-2018-0821.

CHAPTER 6

APPLICATION OF THE BUSINESS INTELLIGENCE INFRASTRUCTURE

Dr. Jayakrishna Herur
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: jayakrishna.udupa@presidencyuniversity.in

ABSTRACT:

Business intelligence (BI) infrastructure plays a critical role in enabling organizations to transform raw data into valuable insights and actionable information. This abstract explores the concept of BI infrastructure, its key components, and its significance in supporting effective decision-making and strategic planning.as well as from external sources, like competition or demographic data. You may need to utilize big data more often. A modern infrastructure for business intelligence comprises a wide range of tools for extracting information from the many data types utilized by organizations today, including enormous amounts of semi-structured and unstructured big data. Data marts and warehouses, Hadoop, in-memory computing, and analytical platforms infrastructure refers to the technology, tools, and processes that organizations employ to collect, store, analyze, and present data in a meaningful way. It encompasses various components, including data sources, data warehouses, data integration, data modeling, analytics tools, and reporting capabilities.

KEYWORDS:

Data Modeling, Data Visualization, In-Memory Computing, Metadata Management, OLAP (Online Analytical Processing), Predictive Analytics.

INTRODUCTION

Imagine you needed succinct, accurate information on the business's present operations, trends, and changes. If you worked for a major firm, you could have to piece together the data you need from many systems, including sales, production, and accounting, as well as from external sources, like competition or demographic data.

You may need to utilize big data more often. A modern infrastructure for business intelligence comprises a wide range of tools for extracting information from the many data types utilized by organizations today, including enormous amounts of semi-structured and unstructured big data. Data marts and warehouses, Hadoop, in-memory computing, and analytical platforms are some of these capabilities.

Data Marts and Data Warehouses

The data warehouse has been the conventional instrument for evaluating company data for the last 20 years. A data warehouse is a database that houses both recent and old data that may be useful to decision-makers throughout the whole business. The data may also contain information from transactions made on websites. The data originate in several fundamental operational transaction systems, including those for sales, customer accounts, and production. From many internal operating systems, the data warehouse collects both recent and old data. Before being imported into the data warehouse, these data are merged with data from other sources, corrected for accuracy and completeness, and restructured for management reporting and analysis.

Anyone may access the data via the data warehouse as required, but it cannot be changed. A data warehouse system also offers various analytical tools, ad hoc and predefined query tools, and graphical reporting features[1]–[3].Enterprise-wide data warehouses, where one central data warehouse services the whole company, or smaller, decentralized warehouses known as data marts, are often built by businesses. A data mart is a subset of a data warehouse in which an organization's data is housed in a separate database for a particular user demographic and is summarized or highly focused. To manage customer information, a business may create marketing and sales data marts. Bookseller Barnes & Noble formerly kept track of sales data from retail point-of-sale systems, sales data from college bookstores, and sales data from internet channels.

Big data or data that cannot readily fit into the columns and rows utilized in their data models are not well-suited for organization and analysis by Hadoop Relational DBMS and data warehouse technologies. Organizations use Hadoop to handle massive amounts of structured and unstructured data, as well as semi-structured data. The Apache Software Foundation oversees Hadoop, an open source software architecture that allows distributed parallel processing of massive volumes of data across low-cost machines. It divides a massive data challenge into smaller problems, spreads them among thousands of inexpensive computer processing nodes, and then aggregates the solutions into a more manageable data set. You've undoubtedly used Hadoop to look for the lowest priced flights online, discover a restaurant's location, conduct a Google search, or get in touch with a buddy on Facebook.

Hadoop is made up of a number of essential services, including MapReduce for fast parallel data processing and the Hadoop Distributed File System for data storage. In order to create a single, large file system, HDFS connects the file systems on all of the nodes in a Hadoop cluster. Google's MapReduce method for decomposing processing of large datasets and allocating work to the many nodes in a cluster served as a model for Hadoop's MapReduce. The non-relational database used by Hadoop, HBase, offers quick access to the data kept in HDFS as well as a transactional framework for executing large-scale real-time applications.

Hadoop is capable of processing huge amounts of any kind of data, including unstructured audio and video data, loosely organized data like that found in Facebook and Twitter feeds, and complicated data like that found in Web server log files. It is possible to add or subtract processors from the Hadoop cluster of low-cost computers as required. Hadoop is used by businesses for both the analysis of extremely large data volumes and as a staging place for unstructured and semi-structured data before it is fed into a data warehouse. A large portion of Facebook's data is kept on its enormous Hadoop cluster, which has a capacity of 100 petabytes, or nearly 10,000 times as much data as the Library of Congress. Yahoo tracks user activity using Hadoop so that it may tailor its home page to their interests. The genomic research being done by pharmaceutical corporations is processed by the life sciences research company NextBio using Hadoop and HBase. Leading database providers including Microsoft, Oracle, Hewlett-Packard, and IBM all offer their own Hadoop software releases. Other companies provide tools for studying data inside Hadoop or for transferring data into and out of it.

DISCUSSION

In-Memory Computing

Utilizing in-memory computing, which stores data mostly in a computer's main memory, is another method for aiding big data analysis. Users have access to data that is kept in the system's main memory, which eliminates the bottlenecks associated with reading and retrieving data from a conventional, disk-based database and significantly speeds up query

response times. Large data sets the size of a data mart or small data warehouse may be processed fully in memory thanks to in-memory processing. Complex commercial computations that formerly took hours or days may now be finished in a matter of seconds, and they can even be done on mobile devices. In-memory processing is made feasible by advancements in modern computer hardware technology, including multicore processing, strong high-speed processors, and declining computer memory costs, which are all described in the preceding. These innovations aid businesses in maximizing memory use, enhancing processing speed, and cutting expenses.

Oracle Exalytics and SAP's High Performance Analytics Appliance are two of the top commercial in-memory computing systems. Each offers a collection of integrated software elements that operate on hardware designed for in-memory computing tasks, such as in-memory database software and specialized analytics software. Using HANA, Centrica, a gas and electric company, can swiftly collect and examine the enormous volumes of data produced by smart meters. Every 15 minutes, the firm may assess utilization, providing them a far better view of usage by area, home size, business type serviced, or building type. HANA enables Centrica to use web and mobile applications to display its consumers their energy use habits in real-time.

Analytical Frameworks

In order to analyze enormous datasets, commercial database manufacturers have created specialized, high-speed analytical platforms that use both relational and non-relational technologies. The preconfigured hardware-software systems used by these analytic platforms, including IBM Netezza and Oracle Exadata, are created expressly for query processing and analytics. In contrast to conventional systems, IBM Netezza's closely integrated database, server, and storage components can process sophisticated analytical queries 10 to 100 times quicker. In-memory systems and NoSQL non-relational database management systems are further examples of analytical platforms. the technological framework for modern business intelligence that we just discussed. In addition to Web data, machine-generated data, unstructured audio/visual data, and data from external sources that have been restructured and reorganized for reporting and analysis, current and historical data are also taken from numerous operational systems. For usage in the data warehouse, data marts, an analytical platform, or for direct querying by power users, Hadoop clusters preprocess massive data. Reports, dashboards, and query results are all examples of outputs.

Tools for Analysis

Data may be further analyzed using software for database querying and reporting, multidimensional data analysis, and data mining after it has been collected and arranged using the business intelligence tools we have just discussed.

Processing Analytical Data Online

In the East, West, and Central areas, let's say your business offers four separate products: nuts, bolts, washers, and screws. How many washers were sold over the previous quarter, for example, is a reasonably simple question that can be answered by accessing your sales information.

But what if you wanted to compare actual results with predicted sales and find out how many washers were sold in each of your sales regions? You would need online analytical processing to find the solution. Because OLAP provides multidimensional data analysis, users may use many dimensions to see the same data in various ways. Product, price, cost, area, or time

period all reflect distinct dimensions of information. In order to find out how many washers were sold in the East in June, how it compares with Junes past and present, as well as how it relates to the sales estimate, a product manager may utilize a multidimensional data analysis tool. Even when the data are housed in extremely big databases, such as sales over numerous years, OLAP allows users to access online responses to ad hoc inquiries like these in a reasonably quick length of time.

A multidimensional model that may be developed to represent goods, areas, existing sales, and future sales. A cube with six sides may be created by stacking a matrix of actual sales on top of a matrix of predicted sales. The face that will be seen will be product vs actual and expected sales if you rotate the cube 90 degrees in one direction. You may view region vs actual and expected sales by rotating the cube a second time by 90 degrees. The anticipated sales and product versus region are visible if you turn your screen 180 degrees from the initial view. To create sophisticated representations of data, cubes may be layered inside of one another. A business might employ a technology that produces multidimensional views of data in relational databases or a customized multidimensional database.

Data Analysis

The answers to inquiries like "How many units of product number 403 were shipped in February 2013?" may be found via traditional database searches. With OLAP and query-oriented data analysis, users need to have a good idea about the information they are looking for. For example, "Compare sales of product 403 relative to plan by quarter and sales region for the past two years" is a much more complex request for information supported by OLAP, or multidi- mensional analysis. Data mining is more focused on discovery. Data mining uncovers hidden patterns and correlations in huge datasets, and by deducing rules from them, it may reveal insights into business data that OLAP cannot. Decision-making and forecasting are guided by the patterns and norms.

This perspective contrasts product and area. The face that displays is product vs actual and expected sales if you rotate the cube 90 degrees. You may view region vs actual and expected sales by rotating the cube a second time by 90 degrees. Other perspectives could exist. the results of their choices. Data mining may provide relationships, sequences, classifications, clusters, and predictions among other sorts of information. Associations are instances connected to one specific event. For instance, a survey of supermarket shopping habits could show that, when corn chips are bought, cola drinks are bought 65 percent of the time, but 85 percent of the time when there is a promotion. Managers may now better understand the financial viability of a promotion thanks to this information.

Events are connected across time in sequences. For instance, we may discover that when a house is acquired, a new refrigerator is bought 65 percent of the time within two weeks and an oven is bought 45 percent of the time within a month[4]–[6].By looking at previously categorized things and deducing a set of criteria, classification finds patterns that characterize the group to which an item belongs.

Businesses like credit card or phone providers, for instance, are concerned about losing their loyal consumers. In order for managers to create specific efforts to retain these consumers, classification may assist identify the traits of customers that are most likely to quit and can develop a model to help managers forecast who those customers are. When no groups have been established, clustering functions similarly to categorization. When using a data mining tool, you may locate various categories within the data, such as affinity groups for bank cards or customer segments based on demographics and kinds of personal assets.

Predictions are used in various applications, but forecasting employs them in a different manner. It makes predictions about future values based on a set of current values. Using patterns in the data, forecasting may, for instance, assist managers in determining the future value of continuous variables like sales s.These systems analyze patterns or trends at a high level, but they may also dig deeper to deliver more specific information as required. Applications of data mining exist for employment in the government, academia, and all functional sectors of business. Data mining is often used to discover profi consumers or to give in-depth analysis of trends in customer data for one-to-one marketing efforts.

The biggest gambling business in the world is Caesars Entertainment, previously Harrah's Entertainment. It continuously examines consumer information obtained from those who utilize its casinos, hotels, or slot machines. Based on a specific customer's continuous worth to the business, the corporate marketing department utilizes this data to create a thorough gaming profile. For instance, data mining enables Caesars to learn a frequent patron's preferred gaming experience at one of its riverboat casinos, as well as that patron's preferences for lodging, dining, and entertainment. This data helps management make judgments on how to develop the most profitable customers, persuade them to spend more, and draw in new clients with a high potential for revenue generation. Business intelligence significantly increased Caesars' profitability, making it the focal point of the company's business strategy.

Internet and textual data mining

Unstructured data, the majority of which is in the form of text files, is one of the main sources of big data that businesses desire to examine and is thought to include more than 80% of important organizational information. Email, memoranda, contact center transcripts, survey results, court documents, patent descriptions, and service reports are all useful sources for identifying patterns and trends that may guide staff members in making more informed business choices. Businesses may now study this data using text mining techniques. These techniques may extract important information from massive data collections that are unstructured, find patterns and relationships, and summarize the data. To discover significant service and repair problems or to gauge customer satisfaction, businesses may use text mining to examine call transcripts from customer care centers. Sentiment analysis software may identify positive and negative attitudes about certain topics by mining text comments in an email, blog, social media chat, or survey form.

For instance, the discount broker Charles Schwab analyzes hundreds of thousands of its client contacts each month using the Attensity Analyze program. To find indications of dissatisfaction that might lead a client to discontinue using the company's services, the program examines Schwab's customer service notes, emails, survey results, and online comments. Attensity may detect a person's intent to purchase, intent to leave, or response to a particular product or marketing message by automatically identifying the different "voices" consumers employ to communicate their opinion. This information is used by Schwab to take remedial action, such as increasing up direct broker engagement with the consumer and working promptly to address any issues that are upsetting the customer.

Unstructured big data from the Web is another abundant source for identifying patterns, trends, and insights into consumer behavior. Web mining is the process of finding and analyzing valuable patterns and data from the Internet. Businesses may use web mining to analyze a certain Web site's efficacy, study client behavior, or determine the degree of a marketing campaign's success. For instance, marketers may find out what consumers are interested in and what they want to purchase by using the Google Trends and Google Insights

for Search services, which monitor the popularity of different terms and phrases used in Google search queries. Web mining uses content, structure, and use mining to seek for patterns in data. Web content mining is the process of obtaining information from the text, picture, audio, and video data that makes up Web sites. Web structure mining looks at information about a certain Web site's structure. For instance, links going to a document indicate its popularity, but links emanating from a document indicate its richness or maybe the range of subjects it covers. Web use mining looks at user interaction data that a web server records each time a request for a web site's resources is made. When a person browses or performs an action on a website, usage data captures that activity and stores it in a server log. By analyzing such data, businesses may learn more about the worth of specific consumers, develop cross-product marketing strategies, and evaluate the success of advertising campaigns. The Interactive Session on Technology explores how firms employ the business intelligence and analytical tools we've discussed to address "big data" problems.

Large Data, Large Rewards

Companies now must cope with a deluge of data from conventional sources as well as social media, search, and sensors. Digital information production is predicted to reach 988 exabytes in 2012, which is the same as a stack of books stretching from the sun to Pluto and back. For businesses of all sizes, understanding "big data" has emerged as one of their top difficulties, but it also presents new possibilities. How are businesses now using big data opportunities? To manage massive data, the British Library has to change.

Over 6 billion searches are made on the British Library website each year, and the library is also in charge of keeping old British Web sites like the sites of former MPs alive even if they no longer exist. Millions of these Web pages couldn't be archived using conventional data management techniques, and conventional analytics tools couldn't make sense of such massive amounts of data. As a result, the British Library and IBM collaborated to build a big data solution to these problems. Large volumes of unstructured Web data may be extracted, annotated, and graphically analyzed with the aid of IBM BigSheets, an insight engine that provides the findings via a Web browser. Users may see search results, for instance, as a pie chart. Because it is based on the Hadoop architecture, IBM BigSheets is able to handle massive volumes of data rapidly and effectively.

Big data analysis is being used by state and federal law enforcement organizations to find patterns in criminal behavior that would be difficult to find in smaller data sets, such as connections between time, opportunity, and organizations, or less obvious connections between individuals and criminal organizations. Criminals and criminal gangs are increasingly coordinating and carrying out their crimes online. With the use of new technologies, authorities may now examine data from a variety of sources and use analytics to forecast potential crime trends. As a result, law enforcement may be more proactive in its attempts to combat crime and prevent it from happening. Millions of data points about city crime and criminals are available in New York City's Real Time Crime Center data database. The warehouse, which houses information on over 120 million criminal complaints, 31 million national crime records, and 33 billion public documents, was developed in collaboration between IBM and the New York City Police Department.

The NYPD can easily get information from any of these data sources because to the system's search capabilities. A suspect's picture and information about previous crimes, as well as addresses and maps, may be shown on a video wall in a matter of seconds or immediately sent to responding cops at a crime scene.

In the instance of Vestas, the data is being used by other firms to become more environmentally friendly. Vestas, with its headquarters in Denmark, is the biggest wind energy firm in the world, with more than 43,000 wind turbines spread throughout 66 nations. For Vestas to precisely position its turbines for the best wind power output, location data are crucial. A lack of wind will prevent places from producing the required electricity, while an abundance of wind might harm the turbines. To choose the optimal locations for its turbine installations, Vestas uses location-based data.

Vestas' wind library integrates data from current turbines with data from worldwide meteorological systems to compile information on potential turbine sites. Each grid in the company's prior wind library was 27 by 27 kilometers in size and presented data in a grid arrangement. Engineers from Vestas were able to establish the precise wind flow pattern at a certain location by reducing the resolution to around 10 x 10 meters.

Vestas sought to reduce the grid area even further in order to boost the accuracy of their turbine placement models, which required 10 times as much data as the prior system and a more potent data management platform.

A high-performance IBM System x iDataPlex server running IBM InfoSphereBigInsights software was used in the company's implementation of the solution. Vestas increased the size of its wind library thanks to these technologies and is now able to handle and analyze location and meteorological data using models that are stronger and more accurate. A total of 178 factors, including barometric pressure, humidity, wind direction, temperature, wind velocity, and other historical business data, are stored in the 2.8 petabyte-sized Vestas wind library. Global deforestation measurements, satellite photos, geographical data, and information on moon phases and tides are all planned additions by Vestas.

The business can now scale down the resolution of their wind data grids to a 3 x 3 kilometer region, a reduction of approximately 90%. With this skill, Vestas can anticipate the best location for a turbine in 15 minutes as opposed to three weeks, saving a month of turbine site construction and allowing Vestas customers to see a return on investment considerably faster. Big data solutions are also being used by businesses to study customer sentiment.

For instance, the world's largest vehicle rental company Hertz collects information from online surveys, emails, texts, Web site traffic patterns, and data produced at all of its 8,300 sites across 146 different countries. Now that all of that data is stored centrally rather than at each location, the organization can analyze data more quickly and react to client input and adjustments more quickly.

in feeling. Hertz was able to identify, for instance, that waits for returns in Philadelphia occurred at certain times of the day by evaluating data collected from various sources. After looking into this oddity, the business was able to promptly change the number of employees working during certain busy hours at its Philadelphia office, ensuring a manager was on hand to handle any problems.

This improved Hertz's efficiency and raised client happiness[7]–[10]. The use of big data has its limitations. A large number of people does not guarantee that the proper data is being gathered or that individuals will make wiser judgments.

A McKinsey Global Institute research from the previous year issued a warning that there is a dearth of experts who can make sense of all the information being produced. The trend toward big data, however, doesn't seem to be slowing down; in fact, it's far more probable that big data will continue to grow.

The Web and Databases

Have you ever attempted to purchase anything online or browse a product catalog? If so, you were presumably utilizing a website that was connected to a corporate database that was only accessible internally. Today, a lot of businesses make information from their internal systems accessible to clients and business partners over the Web. Consider a scenario where a consumer using a web browser wishes to look up price data in a database of an online shop.

The Web server sends these data requests to software that converts HTML instructions into SQL so the commands can be handled by the DBMS working with the database since many back-end databases are unable to understand commands provided in HTML. The DBMS is located on a specific machine called a database server in a client/server setup. The needed data is provided in response to the SQL queries by the DBMS.

Middleware transfers data from the company's internal database back to the web server so that the user may access it as a Web page. An application server operating on a separate dedicated machine serves as the middleware between the Web server and the database management system (DBMS). Between browser-based PCs and the back-end business applications or databases of an organization, the application server software manages all application processes, including transaction processing and data access. The application server receives requests from the Web server, executes the business logic to process transactions determined by those requests, and offers access to the company's back-end databases or systems. As an alternative, a CGI script or a bespoke application might be used as the software to handle these processes. A CGI script is a brief program that processes data on a web server according to the Common Gateway Interface standard.

Using the Web to access an organization's internal databases has a variety of benefits. First off, compared to proprietary query tools, Web browser software is significantly simpler to use. Second, the internal database has to be altered very little, if at all. In order to increase user access, it is significantly less expensive to add a Web interface than to rethink and replace the existing system. Web-based corporate database access is generating new possibilities, efficiency, and business models. A current online list of over 650,000 providers of industrial goods including chemicals, metals, plastics, rubber, and automotive equipment is available at ThomasNet.com. The business, once known as Thomas Register, used to distribute massive paper catalogs containing this information. Now, it makes this data available to people online through its And is now a more compact, leaner business. Other firms have started brand-new ventures based on using the Web to access big databases.

One is Facebook, a social networking site that enables users to communicate with one another and make new friends. More than 950 million active users have "profiles" on Facebook that include details about them, such as hobbies, friends, images, and groups to which they belong. For the purpose of storing and managing all of this material, Facebook keeps a sizable database. To make it easier for residents and customers to access useful information, the public sector also has a large number of Web-enabled databases. One of these databases, which has caused controversy over its techniques for giving information on consumer product safety, is described in the Interactive Session on Organizations.

CONCLUSION

In conclusion, Effective data-driven decision-making and strategic planning are built on a solid BI infrastructure. Organizations may turn data into useful insights by combining data from diverse sources, using analytics tools, and offering easy reporting options. Organizations that have the proper infrastructure in place may increase operational

effectiveness, acquire a competitive advantage, and foster innovation by building on a strong basis of business information. But putting in place a BI infrastructure also has its difficulties. Organizations must guarantee data quality, create frameworks for data governance, and handle issues with data security and privacy.

Critical factors to take into account include scalability and performance improvement, especially as data quantities increase. To realize the advantages of the BI infrastructure, firms must also promote a data-driven culture and provide training and support to users.

REFERENCES

[1] X. Chen and K. Siau, "Business Analytics/Business Intelligence and IT Infrastructure," *J. Organ. End User Comput.*, 2020, doi: 10.4018/joeuc.2020100107.

[2] J. Zucca, "Business intelligence infrastructure for academic libraries," *Evid. Based Libr. Inf. Pract.*, 2013, doi: 10.18438/b83g75.

[3] X. Chen and K. Siau, "Business Analytics/Business Intelligence and IT Infrastructure: Impact on Organizational Agility," *doi.10.4018/JOEUC.2020100107*, 2020.

[4] O. Moscoso-Zea, J. Castro, J. Paredes-Gualtor, and S. Lujan-Mora, "A Hybrid Infrastructure of Enterprise Architecture and Business Intelligence Analytics for Knowledge Management in Education," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2906343.

[5] H. Baars and H. G. Kemper, "Management support with structured and unstructured data - An integrated business intelligence framework," *Inf. Syst. Manag.*, 2008, doi: 10.1080/10580530801941058.

[6] C. M. Olszak and E. Ziemba, "Business Intelligence Systems in the holistic infrastructure development supporting decision-making in organisations," *Interdiscip. J. Information, Knowledge, Manag.*, 2006, doi: 10.28945/3011.

[7] R. Wickramasuriya, J. Ma, M. Berryman, and P. Perez, "Using geospatial business intelligence to support regional infrastructure governance," *Knowledge-Based Syst.*, 2013, doi: 10.1016/j.knosys.2013.08.024.

[8] Z. Sun, "Introduction to Business Intelligence and Database," *Bus. Intell. A Mod. Approach*, 2019.

[9] X. Chen and K. L. Siau, "Effect of business intelligence and IT infrastructure flexibility on organizational agility," in *International Conference on Information Systems, ICIS 2012*, 2012.

[10] X. Chen and K. Siaus, "Impact of business intelligence and IT infrastructure flexibility on competitive performance: An organizational agility perspective," in *International Conference on Information Systems 2011, ICIS 2011*, 2011.

CHAPTER 7

A REVIEW STUDY OF CONSUMER PRODUCT SAFETY DATABASE

Dr. Lakshmi Prasanna Pagadala
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: lakshmi.prasanna@presidencyuniversity.in

ABSTRACT:

The Consumer Product Safety Database (CPSC) is a comprehensive repository of information related to consumer product safety incidents, recalls, and hazards. This abstract explores the purpose and significance of the CPSC database, its key features, and its impact on ensuring consumer safety.The CPSC database serves as a central hub for collecting and disseminating information about product-related incidents, injuries, and potential hazards. It is managed by the U.S. Consumer Product Safety Commission (CPSC), an independent federal agency tasked with protecting consumers from unsafe products.Numerous parents have lost their infants as a result of the drop-side cribs' flawed design, including Michele Witte. The drop-side rail of Tyler Witte's crib broke loose, partly detached, and crushed his neck between the rail and the headboard in 1997, resulting in Tyler's death at the age of 10 months. Cribs are no longer permitted. Before her kid died, Witte wished there had been a public information source for consumer concerns. She could have decided against getting a drop-side crib after reading the horror experiences of other parents.

KEYWORDS:

Consumer Product Safety, Hazard Identification, Incident Reporting, Product Recalls, Product Safety Standards, Public Database, Safety Investigations.

INTRODUCTION

The U.S. Consumer Product Safety Commission launched an online data repository in March 2011 at www.saferproducts.gov in an effort to serve the needs of parents like Witte. The public will have access to the database's whole archive of received product safety concerns. These complaints may be filed online and are immediately added to the database. Users of the database will be able to do product searches, browse through related complaints, and examine safety alerts published by the CPSC. A complaint's details in the database will contain the product's description, any risks or damage it poses, the manufacturer's name, contact details, and a confirmation that the submitter is speaking the truth. Although it won't be included in the database, the submitter's name could be sent to manufacturers with their consent.

Consumer groups like the Consumer Federation of America and other advocates for consumers hail the database as a ground-breaking tool that will fundamentally alter how people shop for goods. Manufacturing firms and a sizable portion of Congress, however, are opposed. They contend that because every user has the ability to file a complaint, the database will be filled with false and deceptive information"fictitious slams" against goods. It will also be vulnerable to misuse by disgruntled clients or litigators looking to damage a product's or manufacturer's image for their own advantage[1]–[3].The database indicates an improvement in the CPSC's visibility and power since it was established in 1972 by the Consumer Product Safety Act. The CPSC's mandate is to regulate a vast array of items, with a specific emphasis on those that are not already subject to regulation by other branches of the government, such as food, weapons, and vehicles.

The CPSC gathers complaints of faulty goods from customers, medical professionals, death certificates, news reports, and other sources. However, until recently, very little of such information was available to the general public. It utilizes that information to make choices on product recalls and bans. Manufacturers were previously compelled by federal law to provide their consent before disclosing such information, and they weren't keen to do so due to their defective goods. Additionally, in order to decide the conditions of product recalls, the CPSC had to engage in direct negotiations with manufacturers. In the meanwhile, people continue to purchase subpar and potentially harmful items like drop-side cribs since this procedure often takes a year or more.

Consumer complaints will be placed online and made accessible to the public within 15 days under the new procedure. When a company receives a complaint about one of its goods, the CPSC will notify it within five days. The company will then have ten days to react publicly and have their remarks included to the database alongside the complaint. Users will have the option to keep their comments private if they so want. Manufacturers will be able to appeal to the CPSC to get rid of complaints that are untrue or deceptive, and complaints will only be allowed for flaws that might endanger human life, not for the dependability or quality of the device.Programs like the CPSC database have become targets for cost-cutting at a time when the federal budget is coming under heightened scrutiny, and manufacturers have grabbed the chance to halt the database in its tracks. Businesses claim that the increased jurisdiction given to CPSC by the statute to regulate dangerous items is too onerous. Draft legislation to limit who may submit reports to the database, enhance how goods are recognized, and address accusations that reports are false is being considered by a House Energy and Commerce subcommittee.

The site was launched in March 2011 to mostly favorable reviews, despite fierce resistance from manufacturers and others. Additional capabilities, such as the ability to attach photographs to comments, were made available by the CPSC. The requirement that commenters provide their name, mailing address, phone number, and email address is likely to reduce the anonymous remarks that manufacturers worry about. Even yet, it's possible that the CPSC staff won't have enough time to devote to maintaining the database without any incorrect reports.According to the Consumer Product Safety Commission, there have been hundreds of thousands of visits to the website and millions of product searches since the database went online. It may not withstand congressional efforts to cut off financing, despite its rising popularity, as a result of pressure to lower the government budget and opposition from the business sector. If saferproducts.gov becomes as a crucial consumer resource, only time will tell.

DISCUSSION

Managing Data Resources

Creating a database is only the beginning. Your company will need unique rules and processes for data management in order to guarantee that the data for your business remains accurate, trustworthy, and easily accessible to those who need it.

Formulating A Policy for Information

Any company, regardless of size, requires an information policy. Data from your company are a valuable resource, and you don't want anyone to use them anyway they like. Rules must be established on who may access the data, how it should be preserved, and how it should be changed. An organization's standards for sharing, distributing, obtaining, standardizing, categorizing, and inventorying information are laid forth in an information policy.

Information policy outlines certain processes and accounting- capacities, specifying who may share information with whom and within what organizational units, where information can be delivered, and who is in charge of preserving and updating the information. A typical information policy might state, for instance, that only specific personnel in the payroll and human resources departments are permitted to view or alter sensitive employee data, such as a worker's salary or social security number, and that it is their responsibility to ensure the accuracy of such data.

The owners or management of a small firm would develop and carry out the information policy. It is common in big organizations to need a formal data administration role to manage and prepare for information as a corporate resource. The exact rules and processes that allow data to be handled as a resource for an organization are the responsibility of data administration. These duties include creating an information policy, organizing data, supervising the creation of logical databases and data dictionaries, and keeping an eye on how information systems professionals and end-user groups utilize data.

Many of these operations may be referred to as data governance. Data governance is a concept supported by IBM that focuses on fostering privacy, security, data quality, and compliance with governmental standards while also controlling the rules and procedures for managing the availability, usability, integrity, and security of the data used in a business. The corporate information systems section of a major company will also have a database design and administration department that is in charge of establishing and managing the database's structure and content as well as its upkeep. The design team creates the physical database, the logical relationships between components, the access rules, and the security protocols in close collaboration with users. Its activities are referred to as database administration.

Guaranteed Data Quality

The firm will have the information it needs if the database and information policy are well-designed. To make sure that the information in organizational databases is correct and continues to be dependable, extra measures must be implemented. What would happen if a customer's account balance or phone number were wrong? What would happen if the database held the incorrect price for the goods you sold or if the prices shown by your sales system and inventory system were different? Decisions that are made incorrectly, cause product recalls, and result in financial losses are caused by data that is faulty, delayed, or conflicting with information from other sources. According to Gartner Inc., more than 25% of the critical data in the databases of large Fortune 1000 companies is inaccurate or incomplete. This includes incorrect product codes and descriptions, inaccurate inventory descriptions, incorrect financial data, inaccurate supplier information, and inaccurate employee information. Critical data inaccuracies are present in 10 to 25% of customer and prospect records, according to a Sirius Decisions research on "The Impact of Bad Data on Demand Creation." The sales process was more productive and led to a 66 percent increase in revenue when these mistakes were fixed at the source and best practices for data quality were followed[4]–[6].

Some of these issues with data quality are brought about by redundant and inaccurate data that comes from many systems feeding a data warehouse. For instance, information about the items of the company may be kept in both the sales ordering system and the inventory management system. However, the inventory system may refer to the same property as Product Number while the sales ordering system may use the phrase Item Number. Different codes may be used by a clothes retailer's production, inventory, or sales systems to indicate values for various attributes. One system could refer to a certain size of clothes as "extra-

large," while another would use the designation "XL" instead. Data representing entities, such as a customer, product, or order, should be identified and described similarly for all business areas utilizing the database throughout the warehouse database design phase.

Consider all the times you have gotten many direct mail advertisements on the same day. This is most likely the outcome of your name being kept in a database more than once. It's possible that your name was spelt incorrectly, you used your middle initial on one time but not the next, or the data was first submitted on a paper form and improperly scanned into the system. The database would treat you differently because of these discrepancies! Mail addressed to Laudon, Lavdon, Lauden, or Landon often arrives in duplicate.

Duplicate or inconsistent data components ought to be limited in a database that has been appropriately constructed and where enterprise-wide data standards have been established. However, the majority of data quality issues, such as misspelled names, transposed numbers, inaccurate or missing codes, originate during data entry. As organizations expand online and enable data entry from clients and suppliers into internal systems through their websites, the prevalence of these mistakes is increasing.

Organizations must locate and fix inaccurate data before implementing a new database and develop improved procedures for amending data once the database is operational. A data quality audit, which is a methodical examination of the correctness and degree of completeness of the data in an information system, is often the first step in the analysis of data quality. Complete data files, sampling from data files, or end users' impressions of data quality may all be surveyed as part of a data quality audit.Data scrubbing, sometimes referred to as data cleaning, is the process of identifying and repairing redundant, inaccurate, incomplete, or poorly structured data inside a database. In addition to erasing mistakes, data cleaning maintains uniformity across several sets of data that were originally collected by various information systems. There is specialized data-cleansing software available to automatically review data files, fix data problems, and integrate the data in a manner that is uniform throughout the whole organization.

Problems with data quality extend beyond corporate concerns. They also present major issues for people, impacting their employment and possibly their financial situation. For instance, erroneous or out-of-date information about customers' credit histories kept by credit agencies may make it more difficult for creditworthy people to get loans or decrease their chances of landing a job. Internet, wireless technology, and telecommunications With 164,000 people in 46 countries, Continental AG, with its headquarters in Hanover, Germany, is a multinational car and truck components manufacturer. It is also one of the top five automotive suppliers globally and the fourth-largest tire maker in the world.

Sarreguemines, France, is home to one of Continental's tire division's plants. This plant, which spans roughly 1.5 million square feet, manufactures 1,000 different types of tires. Large wheeled carts holding sheets of rubber or other components must be moved from storage to workstations when tires are constructed as part of the manufacturing process. Until recently, if a carrier was not where it was supposed to be, a worker had to actively search for it. The facility often lost track of individual tire components due to manual tracking, which was time-consuming and imprecise.

When the business was expanding and the firm sought to increase production capacity, missing materials led to bottlenecks and delays in the manufacturing process. A new real-time locating system based on a Wi-Fi wireless network, combining radio frequency identification tags, AeroScoutMobileView software, mobile PCs, and the material inventory tracking system software from Global Data Sciences, provided Continental with the answer. On the

sides of 1,100 of its carriers, the Sarreguemines facility affixed AeroScout T2-EB Industrial RFID tags. The carriers broadcast position data about the cart to close-by nodes of a Cisco Wi-Fi wireless network as they travel from one production or storage station to another. The carrier is represented as a symbol on a map of the area that is shown on computer displays by AeroScout'sMobileView program, which locates the location. For the purpose of verifying if a carrier has been delivered to a certain workstation or has been filled with components, fifteen Honeywell Dolphin 6500 and Motorola Solutions MC9190 portable computers are employed.

DLOG mobile vehicle-mounted computers are installed on seven of the tuggers at the factory, which are tiny vehicles used to transport carriers throughout the facility. A tugger driver may use the mobile device to access the MobileView system, bring up a map of the facility, and view an icon showing where the carrier of a certain component is situated. The factory's whole inventory of parts is visible in real time thanks to the location tracking system.Each component and carrier has a bar code label attached, and the system begins tracking that component as soon as it is put into a carrier. Plant workers scan the bar code labels on the component and its carrier using a Motorola or Honeywell handheld and the MobileView software, which is linked to the ID number provided by an RFID tag put on the carrier. The information from the bar code scans is kept in a system for monitoring material inventories. The carrier's position is tracked by the MobileView software both during transportation to and after placement in storage.

A tugger driver utilizes the DLOG mobile computer to locate the carrier that has the specific components required for manufacture, and then travels there as necessary. The carrier's bar code is read by a worker at that station using one of the portable computers once it has been recovered and brought to a workstation. This updates the system to reflect the receipt of the necessary components. The new approach has enhanced production and ensured that supplies are not neglected or lost by making it easy for tugger drivers to find components. Because they were no longer useful and were thrown away, less stuff is wasted. Materials that have remained stationary for an excessive amount of time might trigger alarms from the system.

In September 2011, when AeroScout and the new material inventory monitoring system were introduced, Continental made sure that all production workers, including truck drivers, tire manufacturers, and management, got training on how to use the new systems. Additionally, the business sent employees reference cards with instruction cards that included thorough explanations of system functionalities. The Sarreguemines tire plant has raised output from 33,000 to 38,000 tires per day as a result of the new technology. The amount of tire parts wasted has been cut by 20%.To automate tracking of components as they go through the manufacturing process, the business employs wireless networking, radio frequency identification technology, portable computers, and materials inventory management software.

The introductory graphic highlights crucial issues brought up by this case and this. To ensure that components are accessible when and where they are required in the manufacturing process, Continental Tires' production environment, which spans across a very vast region, needs intense control and coordination. Components were more likely to be forgotten about or lost while tracking them manually since it was so tedious and laborious.Management organized for the installation of a wireless RFID network across the whole Sarreguemines manufacturing plant after deciding that wireless technology and RFID tagging offered a solution. Tracking components and streamlining tugger truck movements became considerably simpler thanks to the network. To take use of the new technology, Continental Tires had to reorganize its manufacturing and other work processes and educate staff on the new system.

The business world of today

You cannot function without networks if you own or operate in a company. You must to quickly interact with your staff, vendors, and clients. Businesses utilized voice or fax communications through the phone or the postal service up until around 1990. Today, however, you and your staff do this using computers, e-mail, instant messaging, the Internet, mobile computers linked to wireless networks, and cell phones. Nowadays, networking and conducting business online go hand in hand.

Trends in networking and communication

Telephone networks and computer networks were the two primary kinds of networks utilized by businesses in the past. In the past, voice communication was handled by telephone networks, while data traffic was managed by computer networks. Voice transmission technology were used by telephone companies to build telephone networks during the 20th century, and these businesses nearly invariably functioned as globally controlled monopolies. To send data between computers in various places, computer firms first established computer networks. Telephone and computer networks are merging into a unified digital network utilizing common Internet-based protocols and technology as a result of ongoing telecommunications deregulation and information technology innovation. Today's telecommunications companies, like AT&T and Verizon, provide voice service as well as data transfer, Internet access, cellular telephone service, and television programming. Voice and Internet services are provided by cable providers like Cablevision and Comcast. Internet telephone and video services are becoming a part of computer networks. These audio, video, and data connections are increasingly all dependent on Internet technologies[7]–[10].

Networks for voice and data communications have both improved in strength, efficiency, and cost. The average Internet connection speed, for instance, was 56 kilobits per second in 2000, but now, more than 68 percent of the 239 million U.S. Internet users have access to high-speed broadband connections that operate at 1 to 15 million bits per second thanks to telephone and cable TV providers. It now only costs a minuscule fraction of a penny to use this service, down from 25 cents per kilobit in 2000. Broadband wireless platforms including cell phones, portable handheld devices, and PCs in wireless networks are increasingly being used for voice and data transmission as well as Internet access. In a few years, mobile devices like smartphones and netbooks will be used by more than half of American Internet users. 122 million Americans used mobile devices to access the Internet in 2012, and 135 million are predicted to do so by 2015.

A Computer Network Is What

A computer network would be required if the computers for two or more workers needed to be connected in the same office. What exactly is a network? A network, in its most basic form, is made up of two or more connected computers, as well as the following hardware, software, and transmission elements: client and server computers, network interfaces, a connection medium, network operating system software, and either a hub or switch. To connect to the network, each computer on the network has a network interface device. In the case of wireless local area networks and mobile phone networks, the connection medium for connecting network components might be a radio signal, coaxial cable, or telephone line.

The network operating system organizes network resources as well as directs and maintains communications on the network. It may be located on each computer in the network or it can be mainly located on a computer that serves as the server for all network applications. A server computer is a device connected to a network that serves up Web pages, stores data, and

houses the network operating system on behalf of client computers. The most popular network operating systems are server programs like Microsoft Windows Server, Linux, and Novell Open Enterprise Server. A switch or hub that serves as a connecting point between the computers is also present in most networks. Hubs are relatively basic network connectors that deliver a packet of data to every other connected device. A switch is more intelligent than a hub and has the ability to filter and route data to a specific network location.

What happens if you need to connect to a different network, like the Internet? A router would be necessary. A router is a communications processor that routes data packets via several networks in order to deliver the provided data to the intended recipient. To control the flow of data on the network, network switches and routers contain proprietary software incorporated into their hardware.

As a result, network bottlenecks may develop, and network configuration may become more challenging and time-consuming. With software-defined networking, many of these control tasks are managed by a single central application that may operate on low-cost, generic servers that are independent of the network devices themselves. In a cloud computing environment with a variety of hardware, this is particularly beneficial since it enables a network administrator to handle traffic loads more adaptably and effectively.

CONCLUSION

In conclusion, protecting consumers from dangerous items is made possible in large part by the Consumer Product Safety Database (CPSC). It fosters openness, advances product safety standards, and empowers stakeholders to take well-informed choices by gathering and publishing information on events, injuries, and dangers. The CPSC database promotes a safer marketplace for consumer goods by acting as a useful resource for producers, regulators, researchers, and consumers.

Effectively maintaining and using the CPSC database is difficult, however. Critical factors include ensuring fast and correct data input, preserving data privacy and security, and constantly enhancing data quality. The database's functionality, usability, and accessibility must all be improved by the CPSC in order for it to continue serving as a useful tool for stakeholders.

REFERENCES

[1] C. W. Babbitt, H. Madaka, S. Althaf, B. Kasulaitis, and E. G. Ryen, “Disassembly-based bill of materials data for consumer electronic products,” *Sci. Data*, 2020, doi: 10.1038/s41597-020-0573-9.

[2] S. J. Frisbee and H. Hennes, “Adult-worn child carriers: A potential risk for injury,” *Inj. Prev.*, 2000, doi: 10.1136/ip.6.1.56.

[3] K. L. Dionisio *et al.*, “Data Descriptor: The Chemical and Products Database, a resource for exposure-relevant data on chemicals in consumer products,” *Sci. Data*, 2018, doi: 10.1038/sdata.2018.125.

[4] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, C. H. Y. Lam, and P. S. Koo, “An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks,” *Ind. Manag. Data Syst.*, 2018, doi: 10.1108/IMDS-09-2017-0384.

[5] E. Sumarliah, T. Li, and B. Wang, “Hijab fashion supply chain: a theoretical framework traversing consumers’ knowledge and purchase intention,” *MATEC Web Conf.*, 2020, doi: 10.1051/matecconf/202030804004.

[6] M. R. Goldsmith *et al.*, "Development of a consumer product ingredient database for chemical exposure screening and prioritization," *Food Chem. Toxicol.*, 2014, doi: 10.1016/j.fct.2013.12.029.

[7] A. Falkovskaya and A. Gowen, "Literature review: spectral imaging applied to poultry products," *Poultry Science*. 2020. doi: 10.1016/j.psj.2020.04.013.

[8] Y. Liao and K. Xu, "Traceability System of Agricultural Product Based on Block-chain and Application in Tea Quality Safety Management," in *Journal of Physics: Conference Series*, 2019. doi: 10.1088/1742-6596/1288/1/012062.

[9] D. P. Trofa *et al.*, "Increasing Burden of Youth Baseball Elbow Injuries in US Emergency Departments," *Orthop. J. Sport. Med.*, 2019, doi: 10.1177/2325967119845636.

[10] R. Ismail, W. A. A. Wan Haniff, S. M. Isa, R. M. Fadzil, S. S. AlSagoff, and K. A. Talib Khalid, "The approach to safety of children's toys in United States and European Union: A comparative study," *Acad. J. Interdiscip. Stud.*, 2020, doi: 10.36941/ajis-2020-0011.

CHAPTER 8

ROLES OF THE NETWORKS IN LARGE COMPANIES OPERATIONS

Dr. Akhila Udupa
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: akhila.udupa@presidencyuniversity.in

ABSTRACT:

Networks play a crucial role in the operations of large companies, enabling efficient communication, collaboration, and information sharing across various departments, locations, and business units. This abstract explores the significance of networks in large companies, their key components, and their impact on organizational productivity and effectiveness.In large companies, networks provide the infrastructure that connects computers, servers, and other devices, allowing seamless communication and data exchange. They support a wide range of functions, including email, file sharing, video conferencing, enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, and other business-critical applications.

KEYWORDS:

Bandwidth Management, Cloud Networking, Data Centers, Firewall, Intranet, Network Infrastructure.

INTRODUCTION

The network we just discussed may be ideal for a small company. But what about big businesses with thousands of employees across several locations? As a company expands, hundreds of tiny local area networks may be gathered together, and these networks can be connected to create a corporate-wide networking infrastructure.

These many tiny local area networks are connected to other local area networks and company-wide corporate networks to form the network infrastructure for a major enterprise. A corporate Web site, corporate intranet, and maybe an extranet are supported by a number of strong servers. Some of these servers connect to other powerful computers that power back-end systems.

It gives an example of these more intricate, corporate-wide networks of a higher size. Here, you can see how the corporate network infrastructure supports a mobile sales force that uses smartphones and cell phones, mobile workers who connect to the company website, internal company networks that use mobile wireless local area networks, and a videoconferencing system to support managers around the world.

The company's infrastructure often also comprises a separate telephone network that manages the majority of voice data in addition to these computer networks. Using Internet telephones that connect to their existing data networks, many businesses are doing away with their old telephone networks. As you can see from this, a major business network architecture employs a broad range of technologies, including wired and wireless Internet, mobile phones, corporate data networks, and regular telephone service. One of the main issues that organizations nowadays are dealing with is how to integrate all[1]–[3]. The corporate local area networks that connect workgroups, departments, or office floors are only a few of the networks that make up the corporate network architecture of today.

Other networks include the Internet and public switched telephone network. the many communication networks and channels into a cohesive system that allows data to go from one system to another and from one area of the company to another. It will be simpler to interconnect communication networks as more switch to being digital and based on Internet technology.

Key Digital Networking Technologies

Three fundamental technologiesclient/server computing, packet switching, and the creation of generally accepted communications standardsare the foundation of modern digital networks, including the Internet.

Computing using client/server

Introduced, client/server computing is a distributed computing approach in which part of the processing capacity is housed in tiny, affordable client computers and is figuratively present on desktops, laptops, or portable devices. A network that is run by a network server computer connects these strong clients to one another. Every client receives an address from the server so that other clients can locate it on the network, and the server establishes the network's communication protocols.

Centralized mainframe computing, in which virtually all of the processing occurs on a single, huge mainframe computer, has been substantially superseded by client/server computing. Departments, workgroups, manufacturing floors, and other areas of the organization that could not be handled by a centralized design now have access to computers thanks to client/server technology. The biggest client/server computer deployment is on the Internet.

Network switching

With packet switching, digital communications are divided into packages called packets, sent through various communication channels as they become available, and then reassembled once they reach their destinations.

Computer networks utilized leased, dedicated telephone lines to connect with other computers in distant places before packet switching technology was developed. A full point-to-point connection must first be built in circuit-switched networks, like the telephone system, before communication can start. These costly dedicated circuit-switching methods squandered the communications bandwidth since they kept the circuit open whether or not any data were being delivered.

Using packet switching, a network's communication capacity is used significantly more effectively. Messages in packet-switched networks are first divided into manageable fixed data bundles known as packets. Along with the contents, the packets also include information for addressing the packet to the appropriate address and checking for transmission problems. Using routers, the packets are sent through numerous communication channels, with each packet going on its own. When traveling to their destinations, data packets that started from one source will have traveled via several networks and pathways before being reassembled into the original message.

The connectivity of TCP/IP

To transport data in a typical telecommunications network, several hardware and software components must cooperate. A network's many components can only interact with one another by abiding by a set of rules known as protocols. A protocol is a collection of guidelines that regulate how information is sent between two places on a network.

Business enterprises were often required to buy computer and communications equipment from a single vendor in the past due to the prevalence of several proprietary and incompatible protocols. However, business networks are becoming more often adopting Transmission Control Protocol/Internet Protocol, a single, universal standard. Early in the 1970s, TCP/IP was created to assist

U.S. initiatives made by the Department of Defense Advanced Research Projects Agency to assist scientists with long-distance data transmission between various kinds of computers. The two most important protocols used by TCP/IP are TCP and IP. The Transmission Control Protocol (TCP), which manages the transfer of data between computers, is referred to as TCP.

TCP creates a connection between the computers, orders the packet transfersand acknowledges each packet that is transmitted. The term "IP" stands for the Internet Protocol, which is in charge of packet delivery and involves packet deconstructing and reassembling during transmission. the four tiers of the Department of Defense's TCP/IP reference model are as follows:

1. layer of applications. The application layer establishes the protocols that applications utilize to communicate data and gives client application programs access to the other levels. The Hypertext transport Protocol, which is used to transport Web page files, is one of these application protocols.

2. Layer of transport. Communication and packet services for the Application layer are the responsibility of the Transport layer. TCP and other protocols are included at this layer.

3. network layer. Data packets known as IP datagrams are addressed, routed, and packaged by the Internet layer. One of the protocols used on this tier is the Internet Protocol.

4. Internet Protocol layer. The Network Interface layer, which is at the base of the reference model, is in charge of sending packets to and receiving them from the network medium, which might be any networking technology.

Even if two computers have different hardware and software platforms, they can still interact via TCP/IP. All four levels, beginning with the application layer of the sending computer and finishing with the network interface layer, are traversed by data transmitted from one computer to another.

The data move up the layers until they reach the target host computer, where they are then put back together in a format that the recipient computer can utilize. When a broken packet is discovered, the receiving computer requests a retransmission from the transmitting computer. When the receiving computer replies, this procedure is turned around.

Networks for communications

Let's take a closer look at some of the different networking technologies that are accessible to companies.

Signals: analog vs. Digital

A message may be sent through a network using either a digital signal or an analog signal. An analog signal, which has been utilized for voice communication, is represented by a continuous waveform that travels over a communications channel.

The telephone handset, computer speakers, and iPod earphones are the most popular analog gadgets since they all produce waveforms that can be heard by your ear.

DISCUSSION

Instead of being a continuous waveform, a digital signal is a discrete, binary waveform. One bit and zero bits, which are represented as on-off electrical pulses, make up the strings of two distinct states that make up digital signals, which transmit information. Computers provide digital signals, which a modem must convert into analog signals that may be transferred via analog mediums including telephone lines, cable lines, and wireless networks. Modulator-demodulator is referred to as a modem.

Your computer and the Internet are connected over a cable network by cable modems. DSL modems use the landline network of a telephone provider to connect your computer to the Internet. The same as standard modems, wireless modems link your computer to a wireless network, which might be a Wi-Fi or cellular network. Analog networks cannot be used by computers to communicate without modems.

In order for computers to communicate data across analog networks like telephone and cable networks, a modem converts digital signals into analog form.

A Range Of Networks

There are several network types and classification schemes. Networks may be analyzed in terms of their geographic reach.

Regional Networks

If your company employs networking, you presumably use a local area network to communicate with other staff members and organizations. Personal computers and other digital devices within a half-mile or 500-meter radius are connected through local area networks. LANs often link a few computers in a small office, every computer in a single building, or every computer in a cluster of buildings. LANs are also used to connect to larger global networks that utilize the Internet, such as long-distance wide area networks.

Who has access to what and in what order is decided by the server. The router links the LAN to other networks so that it may communicate with networks outside of it, such as the Internet or another business network. Windows, Linux, and Novell are the three most widely used LAN operating systems. As the standard networking protocol, TCP/IP is supported by all of these network operating systems. At the physical network level, Ethernet is the most used LAN standard, defining the physical media to convey signals between computers, access control policies, and a common set of bits used to transmit data across the network. Ethernet's initial data transport rate limit was 10 megabits per second. Newer variants, including Gigabit Ethernet, are utilized in network backbones and offer data transmission rates of 1 gigabit per second, respectively.

It employs a client/server design, where most of the network's management and resources are provided by a single file server, which also serves as the primary location for the network's operating system. LANs may also use a peer-to-peer design. Peer-to-peer networks are often utilized in small networks with 10 users or less and treat all processors equally.

Without using a separate server, the numerous computers connected to the network may share peripheral devices and exchange data directly[4]–[6]. The workgroup network model is the peer-to-peer architecture used in LANs running the Windows Server family of operating systems. It enables a small group of computers to share resources like files, directories, and printers via the network without the need for a dedicated server. In contrast, the Windows domain network approach employs a dedicated server to control the network's PCs. Larger

LANs contain a lot of clients and a lot of servers, with different servers for different functions like controlling printers, storing and managing e-mail, or storing and managing Web sites.

Wide-Area and Metropolitan Networks

Wide area networks connect vast geographic areas, including whole states, continents, and even the entire world. The Internet is the most pervasive and powerful WAN. Computers may connect to a WAN through leased lines, satellites, or open networks like the telephone network or private cable networks. A network that covers a metropolitan region, often a metropolis and its important suburbs, is called a metropolitan area network. Its geographic range is in the middle between a WAN and a LAN.

Media For Transmission and Transmission Speed

Various physical transmission media, such as twisted pair wire, coaxial cable, fiber optics, and medium for wireless transmission, are used by networks. Each has benefits and drawbacks. Depending on the software and hardware setup, every given media may operate at a broad variety of speeds.

Bandwidth: Transfer Rate

Bits per second are units used to quantify the entire quantity of digital data that may be conveyed across any kind of telecommunications media. One signal shift, or cycle, is needed to transfer one or more bits, hence the frequency of each kind of telecommunications media affects how much data can be sent across it.

Hertz units are used to express how many cycles per second may be transmitted across a certain medium; one hertz is equivalent to one cycle of the medium. Thickly insulated copper wire that can transmit data at high speeds and is less susceptible to interference than twisted wire is known as coaxial cable. Currently used for cable TV and longer-running networks. medium for wireless transmission based on radio transmissions of different frequencies and comprises cellular networks and microwave systems that are both terrestrial and satellite-based. used for wireless, long-distance, and internet connectivity.

The bandwidth of a given telecom- munications channel refers to the range of frequencies that may be carried there. The difference between the highest and lowest frequencies that may coexist on a single channel is known as the bandwidth. The bandwidth and transmission capacity of a channel increase as the frequency spectrum does.

The Internet At Large

All of us use the Internet, and many of us depend on it heavily. It has evolved into a vital tool for both individuals and businesses. What is the Internet, however, exactly? What benefits does Internet technology provide for businesses, and how does it operate? Let's examine the key components of the Internet.

The internet: what is it

The Internet has developed into the largest public communication network in the world, rivaling the worldwide telephone network in size and scope. Additionally, it links millions of separate networks throughout the globe and is the biggest client/server computer and internet-working system in the world. Early in the 1970s, a U.S. network gave birth to this worldwide network of networks. Department of Defense network to connect researchers and academics globally. The majority of families and small businesses use an Internet service provider to connect to the Internet. An Internet service provider (ISP) is a for-profit business with a

constant Internet connection that offers short-term access to retail customers. ISPs include EarthLink, NetZero, AT&T, and Time Warner. People may also access the Internet through the specified Internet domains of their employers, educational institutions, or research facilities.

For ISP Internet connections, there are many different options available. Broadband connections have essentially supplanted the once-dominant method of connection, which used to be a standard telephone line and modem operating at a speed of 56.6 kilobits per second. These broadband services are offered through digital subscriber lines, cable, satellite Internet connections, and T lines. Depending on use patterns and distance, digital subscriber line technologies use existing telephone lines to transmit speech, data, and video at transmission speeds ranging from 385 Kbps to 40 Mbps. Digital cable coaxial lines are used to supply high-speed Internet access to households and businesses via the cable Internet connections offered by cable television providers. Although the majority of carriers provide service ranging from 1 Mbps to 6 Mbps, they may give high-speed access to the Internet of up to 50 Mbps. Although some satellite Internet connections offer slower upload speeds than other broadband services, it is still feasible to access the Internet in locations where DSL and cable services are not accessible. International telephone standards for digital transmission include T1 and T3. For organizations or governmental bodies needing high-speed assured service standards, these are leased, dedicated lines. T3 lines can transport data at 45 Mbps, whereas T1 lines can ensure transmission at 1.54 Mbps. Instead of offering equivalent guaranteed service standards, the Internet only offers "best effort."

Network Addressing And Structure

The TCP/IP networking protocol suite mentioned previously in this is the foundation of the Internet. A distinct Internet Protocol address, now a 32-bit number expressed by four strings of integers spanning from 0 to 255 and separated by periods, is given to any machine connected to the Internet. For instance, www.microsoft.com's IP address is 207.46.250.119. Using the TCP protocol, a message is first divided into packets before being sent across the Internet to another user. The destination address is included in each packet. In order to reach a particular computer with a known address, the packets are then transferred from the client to the network server, and then on to as many more servers as required. The packets are put back together to form the original message at the destination address.

Donut Name System

The Domain Name System translates domain names to IP addresses because it would be very difficult for Internet users to memorize strings of 12 digits. The English-sounding name that corresponds to each computer's own 32-bit IP address when it is linked to the Internet is called the domain name. DNS servers keep a database with a mapping between IP addresses and the related domain names. Users just need to provide a computer's domain name in order to access it through the Internet. DNS is organized in a hierarchy.

The root domain is located at the top of the DNS hierarchy. A top-level domain is the offspring of the root, while a second-level domain is the offspring of a top-level domain. Top-level domains are two- and three-letter names that you are likely already acquainted with from your Web browsing, such as.com,.edu,.gov, and the numerous country codes like.ca for Canada or.it for Italy. Such second-level domains like buy.com, nyu.edu, or amazon.ca contain two components, a top-level name and a second-level name. On the Internet or a private network, a host name at the bottom of the hierarchy identifies a particular computer.

The list below contains the most popular domain extensions that are presently legal and available. Additionally, there is a new class of "internationalized" top-level domains that employ non-English characters, as well as country-specific domain names like.uk,.au, and.fr.

Internet Governance and Architecture

Transcontinental high-speed backbone networks that typically run in the range of 45 Mbps to 2.5 Gbps carry internet data traffic. Usually, national governments or long-distance phone corporations own these trunk lines. Regional networks are connected to the Internet backbone via which Internet service providers, major corporations, and governmental organizations may access the network. The hubs where the backbone meets regional and local networks and where backbone owners interact with one another are known as network access points and metropolitan area exchanges.

Regional telephone and cable television providers in the US hold the local connection lines that link retail consumers in homes and businesses to the Internet. Access to the regional networks is leased to ISPs, commercial businesses, and governmental organizations.

Each organization is responsible for paying for its own networks and local Internet connection services, with a portion going to the owners of long-distance trunk lines. ISPs receive payment from individual Internet users for utilizing their service, and regardless of how much or how little they use the Internet, they typically pay a set monthly price.

There is now a heated discussion on whether this system should remain in place or whether heavy Internet users who download huge music and video files need to pay more for the bandwidth they use. This subject is explored in the Interactive Session on Organizations by weighing the benefits and drawbacks of network neutrality.

The Internet has no official control and no one "owns" it. The World Wide Web Consortium, which establishes Hypertext Markup Language and other programming standards for the Web, the Internet Architecture Board, which aids in defining the overall structure of the Internet, the Internet Corporation for Assigned Names and Numbers, which assigns IP addresses, and these organizations all work together to create global Internet policies.

With the goal of ensuring the Internet runs as smoothly as possible, these groups exert influence on governmental entities, network operators, ISPs, and software developers. The laws of the sovereign nation-states in which it works, as well as their technological infrastructures, must be followed by the Internet.

Although there was relatively little legislative or administrative involvement in the early years of the Internet and the Web, this is increasingly changing as the Internet plays a larger role in the dissemination of information and knowledge, including material that some find offensive.

IPv6 and Internet2: The Internet of the Future

The transfer of enormous amounts of data and the presence of billions of users were not initially intended uses of the Internet. The world is soon to run out of accessible IP addresses using the previous addressing system since many firms and governments have been awarded massive blocks of millions of IP addresses to accommodate present and future workforces. A new version of the IP addressing schema called IP is taking the place of the previous addressing scheme. It has 128-bit addresses, or more than a quadrillion potentially unique addresses. The switch to IPv6 will take years since it is incompatible with the current Internet addressing scheme[7]–[10].

Over 350 American colleges, commercial companies, and government organizations make up the sophisticated networking consortium known as Internet2, which collaborates with 66,000 institutions nationwide and overseas network partners from more than 50 different nations. In order to link these communities together, Internet2 created a high-capacity 100 Gbps network that acts as a testbed for cutting-edge technologies that could eventually be adopted by the general public Internet, such as telemedicine, distance education, and other cutting-edge applications not currently supported by consumer-grade Internet services. This network's fourth generation is being implemented to provide 8.8 terabits of capacity.

CONCLUSION

In conclusion, large organizations need networks because they provide the infrastructure for communication, teamwork, and information exchange. They promote productivity, offer seamless communication, and support mission-critical operations. Large businesses may promote a connected and effective environment that fosters organizational success by investing in reliable network infrastructure, security measures, and scalability. In big businesses, managing and sustaining networks presents difficulties. Networks must be able to handle the increasing volume of users, devices, and data traffic, hence scalability is a crucial factor. In order to guarantee continuous operations and customer satisfaction, network dependability, performance optimization, and bandwidth control are essential. To maintain networks robust and current, regular maintenance, upgrades, and adherence to industry standards are required.

REFERENCES

[1] J. O. Miranda, A. V. Valenzuela, and M. D. L. Á. N. Hinojosa, “Innovation for integration into supplier networks of multinational companies,” *Contaduria y Adm.*, 2017, doi: 10.22201/fca.24488410e.2018.1069.

[2] X. Qian, T. Lei, J. Xue, Z. Lei, and S. V. Ukkusuri, “Impact of transportation network companies on urban congestion: Evidence from large-scale trajectory data,” *Sustain. Cities Soc.*, 2020, doi: 10.1016/j.scs.2020.102053.

[3] M. N. Larasati, R. Indradewa, T. Y. R. Syah, and D. Fajarwati, “Application of Risk Management in Development Noor Halal Minimarket at Islamic Education Institutions,” *J. Multidiscip. Acad.*, 2020.

[4] P. Poonpakdee, J. Koiwanit, and C. Yuangyai, “Decentralized Network Building Change in Large Manufacturing Companies towards Industry 4.0,” in *Procedia Computer Science*, 2017. doi: 10.1016/j.procs.2017.06.113.

[5] M. Ferrary and M. Granovetter, “The role of venture capital firms in Silicon Valley’s complex innovation network,” *Econ. Soc.*, 2009, doi: 10.1080/03085140902786827.

[6] E. Sundin, G. Ölundh Sandström, A. Öhrwall Rönnbäck, T. Sakao, and T. Larsson, “Challenges for industrial product/service systems - Experiences from a learning network of large companies,” in *CIRP IPS2 Conference 2009 - Industrial product-service systems (IPS^2)*, 2009.

[7] F. J. Martínez López, M. García Ordaz, R. Arteaga Sánchez, and A. Infante Moro, “The presence of large Spanish companies in online social networks,” *J. Mark. Anal.*, 2015, doi: 10.1057/jma.2015.15.

[8] T. Hakala, T. Lahdeaho, and P. Jarventausta, “Low-Voltage DC Distribution-Utilization Potential in a Large Distribution Network Company,” *IEEE Trans. Power Deliv.*, 2015, doi: 10.1109/TPWRD.2015.2398199.

[9] S. A. Einwiller and S. Steilen, “Handling complaints on social network sites - An analysis of complaints and complaint responses on Facebook and Twitter pages of large US companies,” *Public Relat. Rev.*, 2015, doi: 10.1016/j.pubrev.2014.11.012.

[10] A. Brintrup, A. Ledwoch, and J. Barros, “Topological robustness of the global automotive industry,” *Logist. Res.*, 2016, doi: 10.1007/s12159-015-0128-1.

CHAPTER 9

AN ASSESSMENT OF BATTLE OVER NET NEUTRALITY

Dr. Nalin Chirakkara
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: nalinkumar@presidencyuniversity.in

ABSTRACT:

The battle over net neutrality has emerged as a significant and contentious issue in the realm of internet governance. This abstract delves into the concept of net neutrality, its implications, and the ongoing debate surrounding its preservation or repeal.While Netflix, Spotify, YouTube, and other data-intensive services would not completely stop working if consumer demand for the Internet exceeds network capacity, users would experience very poor download rates. Service on the AT&T cellular network has already suffered due to the widespread usage of iPhones in crowded cities like New York and San Francisco. According to AT&T, 3 percent of its customer base is responsible for 40% of their data trafficNet neutrality refers to the principle that all internet traffic should be treated equally, without any discrimination or preferential treatment by internet service providers (ISPs). It advocates for an open internet where users have unrestricted access to content, applications, and services of their choice, without interference from ISPs.

KEYWORDS:

Broadband providers, Content discrimination, Data throttling, Digital divide, Internet Service Providers (ISPs), Net neutrality regulations, Open internet.

INTRODUCTION

Who are you as a user of the Internet? Do you mostly use the Internet to seek up phone numbers and send a little e-mail? Or do you spend the whole day playing online games, downloading music, and watching YouTube videos? Do you often stream TV episodes and movies on your smartphone, or do you just use it sometimes to make calls and browse the web? If you use your smartphone or the Internet extensively, the hundreds of millions of other people who do the same thing might start to slow down the Internet. In the year 2000, the whole Internet used as much bandwidth as YouTube used in 2007, and in the first two months of 2015, AT&T's mobile network will transmit more data than it carried in all of 2010. While Netflix, Spotify, YouTube, and other data-intensive services would not completely stop working if consumer demand for the Internet exceeds network capacity, users would experience very poor download rates. Service on the AT&T cellular network has already suffered due to the widespread usage of iPhones in crowded cities like New York and San Francisco. According to AT&T, 3 percent of its customer base is responsible for 40% of their data traffic.

Some observers contend that as the amount of digital traffic on the Internet increaseseven at a rate of 50% annuallythe technology needed to handle it all is developing at a same fast rate. However, expenses for Internet providers will continue to rise regardless of what happens with Internet infrastructure, and well-known media businesses are looking for new income sources to cover those costs. Making Internet users pay for the amount of bandwidth they consume is one idea. But due to the current network neutrality argument, metering Internet use is not generally supported[1]–[3].According to the principle of "network neutrality,"

Internet service providers must provide users equal access to all material and applications, regardless of the content's origin or kind. The Internet is now neutral, with Internet backbone owners treating all Internet traffic equally and on a first-come, first-served basis. However, because of this system, telecommunications and cable providers are unable to set varied charges in accordance with the amount of bandwidth used to serve Internet content. These businesses consider differential pricing to be "the fairest way" to fund necessary network infrastructure developments. Internet service providers mention the increase in online copyright infringement.

The second-largest U.S. Internet service provider, Comcast, revealed that unauthorized file sharing of content that is protected by a copyright was using 50% of their network bandwidth. In 2008, the business curtailed the transmission of BitTorrent files, which were often used for copyright infringement and illegitimate sharing of media, including video. Comcast was ordered by the Federal Communications Commission to cease blocking peer-to-peer traffic in the name of network management. After that, Comcast filed a lawsuit to contest the FCC's right to impose network neutrality. A federal appeals court decided in favor of Comcast in April 2010 and declared that the FCC lacked the jurisdiction to control how an Internet service provider operates its network. This dealt net neutrality a serious setback. Comcast apparently started charging Level 3 Communications, which facilitates the streaming of Netflix movies, an extra cost for ongoing regular service in late 2010. The FCC was contacted by Level 3 to look into the incident.

Net neutrality advocates are urging Congress to take action to regulate the sector and stop internet service providers from following Comcast's example. MoveOn.org, the Christian Coalition, the American Library Association, every major consumer organization, a plethora of bloggers and small companies, as well as streaming video firms like Netflix, are all part of the odd coalition of net neutrality proponents. Net neutrality proponents contend that when network operators have the ability to arbitrarily restrict or delay access to certain material, such as Netflix video streams, or access to rival low-cost services, such as Skype, the possibility of censorship grows. A neutral Internet, according to proponents of net neutrality, allows everyone to develop without seeking permission from phone and cable companies or other authorities, and this fair playing field has given rise to a vast number of new enterprises. As more and more business and social interactions take place online, allowing unrestricted information flow becomes crucial to free markets and democracy.

Network operators fear that regulations enforcing net neutrality would make the United States less competitive by impeding innovation, deterring capital investments for new networks, and restricting their networks' capacity to handle the explosive growth in Internet and cellphone traffic. This claim is supported by the fact that Internet access in the United States is less affordable, faster, and of higher quality than in many other countries. Furthermore, legislation would not be necessary to promote net neutrality if there were sufficient choices for Internet access. Customers who are dissatisfied may easily change providers to ones who support net neutrality and provide limitless Internet use.

The FCC adopted provisions in December 2010 that would let the federal government control Internet traffic. In addition to not being able to prohibit access to websites or goods that compete with their own, broadband providers would have to notify their customers about Internet speeds and services. However, the rules did not formally protect net neutrality, and cellular carriers may restrict the usage of programs that use excessive amounts of bandwidth. Online content companies have signed exclusive distribution agreements that put their rivals at a disadvantage, and wireless carriers have already started to establish tiered plans that charge heavy bandwidth users more service prices. For instance, in 2012, Comcast and

Microsoft reached an agreement to provide streaming video via the Xbox 360 as part of the company's Xfinity TV package, which is exempt from the 250 GB monthly internet data restriction. This offers Comcast's television programming an advantage over competing streaming programs that use subscribers' data caps. Netflix and other rivals are furious, claiming that this violates the idea of net neutrality and is an anti-competitive behavior.

Nearly all internet providers implemented data caps in 2011 and began charging consumers extra costs for exceeding those limits. Numerous experts have long advocated in favor of these limitations, but moving ahead, the FCC is likely to take issue with agreements like the ones between Comcast and Microsoft. The existing net neutrality regulations are now rife with flaws. For instance, they enable broadband providers to designate certain "managed" services to specific network segments. However, support for net neutrality among the general population is remains high[4]–[6].

DISCUSSION

Internet Services and Communication Tools

The client/server model underlies the Internet. Client programs, such as Web browser software, that are installed on users' PCs provide them control over what they do when accessing the Internet. The information is kept on servers, including email messages and web pages. A client requests information from a certain Web server located on a remote computer via the Internet, and the server responds by sending the requested information back to the client through the Internet. S 5 and S 6 explain how Web servers collaborate with application servers and database servers to obtain data from a company's internal information systems applications and their related databases. In addition to PCs and other computers, client platforms now also include smartphones, tiny portable digital devices, and other information appliances.

Website Services

The services available to client computers connected to the Internet are many. E-mail, chat and instant messaging, electronic discussion groups, Telnet, File Transfer Protocol, and the Web are some of the services that fall under this category.

Through the use of e-mail, messages may be sent from one computer to another and can be forwarded, routed to numerous recipients, or attached with text or multimedia assets. Today, the majority of email is sent through the Internet. Email costs far less than equivalent phone, postal, or overnight delivery fees, making the Internet a relatively affordable and quick form of communication. The majority of emails reach anywhere in the globe in only a few seconds. Employees engage with one another in over 90% of American companies using chat or instant messaging software. Chatting allows two or more individuals who are online at the same time to have real-time, interactive discussions. As well as supporting textual chats, chat systems today also offer audio and video chat. To attract customers, promote repeat business, and enhance customer service, many online retailers include chat facilities on their websites.

One form of chat service that lets users construct their own personal channels is instant messaging. When someone on the user's private list is online, the instant messaging system notifies the user so they may start a chat conversation with them. Consumer instant messaging platforms include Windows Messenger, Google Talk, and Yahoo! Messenger. Security-conscious businesses utilize specialized messaging and communication platforms like IBM Sametime. In newsgroups, individuals from all over the globe debate a certain subject, such as radiology or rock bands, on electronic bulletin boards on the Internet. On

these bulletin boards, anybody may write messages that other people can read. There are many organizations that cover practically every imaginable subject.

The use of email, instant messaging, and the Internet by employees is meant to boost productivity, but the interactive session that goes with it allows machines running Web browsers and other software to connect to servers that host a variety of services over the Internet. All of these services might be provided by a single server or by a number of specialized servers. Management demonstrates that this isn't always the case. Today, many business managers feel that they must keep an eye on and even control their workers' internet behavior. However, is this moral? What does it imply for employee privacy if firms need to keep an eye on their workers' email and web use, despite the fact that there are some compelling commercial reasons for doing so?

Call over IP

A common platform for voice transmission and business networking is now the Internet. Voice over IP technology uses packet switching to send voice data in digital form, eliminating the fees incurred by local and long-distance phone networks. Makes those During a VoIP phone connection, a spoken message is digitalized and divided into data packets that may take multiple paths before being put back together at the intended location. The packets are organized in the right sequence and sent to the receiver's phone number or the computer's IP address via a processor known as a gateway that is closest to the call's destination.

Employee Network Monitoring: Ethical or Profitable

How long did you spend on Facebook today while you were at work? Did you visit any sports websites or send any personal emails? If so, you are not alone yourself. A Nucleus Research research found that 77% of employees who have Facebook accounts utilize it while at work. According to a Ponemon Institute research, the typical employee spends around 30% of their workday on unrelated Web surfing, and according to other surveys, up to 90% of workers write or receive personal e-mail at work[7]–[9]. Serious business issues are caused by this practice. According to Basex, a New York City business research firm, these distractions cost $650 billion in lost productivity annually! Checking e-mail, responding to instant messages, or sneaking in a quick YouTube video creates a series of nonstop interruptions that divert employee attention from the job tasks they are supposed to be performing!

Many businesses have started keeping an eye on how their employees use the Internet and e-mail, often without their knowledge. More than one in three major American firms, according to a Proofpoint Plus survey from 2010, deploy workers to read or analyze employee e-mail. Two out of every three of the small, medium, and large businesses polled, according to a different recent study by the American Management Association and the ePolicy Institute, tracked Web use. Additionally growing are the use of instant chatting and text message monitoring. Although Is it immoral for American businesses to watch their employees' online and email behavior while they are at work, or is it just smart business?

Managers are concerned about the time lost and decreased productivity of staff members who are preoccupied with personal matters rather than work-related matters. Spending too much time on personal matters costs money. Some workers could even overcharge customers by paying them for the time they spend online engaging in personal hobbies. Additionally, excessive personal traffic on corporate networks might choke the network of the organization and prevent the conduct of necessary commercial operations. Procter & Gamble discovered that on a typical day, staff members watched 50,000 five-minute videos on YouTube and

listened to 4,000 hours of music on Pandora. videos on YouTube. Large amounts of data were being streamed during these events, which hindered P&G's Internet connection.Anything an employee does, including any criminal activity, while using email or the Internet at work or on corporate property represents the business.

As a result, the employer may be located and made accountable. Many businesses worry that racial, sexually explicit, or other potentially objectionable content that workers access or exchange might lead to bad press for the company and perhaps legal action. Even if the business is deemed not at fault, defending itself against claims may incur significant legal costs. According to Symantec's 2011 Social Media Protection Flash Poll, the average legal expense for businesses that had social media accidents was $650,000. Companies worry that trade secrets and private information may leak through social media or email. In a separate study by the American Management Association and the ePolicy Institute, 14% of the respondents confessed sending private or potentially embarrassing work emails to third parties.

Companies in the United States are permitted by law to keep an eye on what staff members are doing while using corporate property. The issue is whether electronic monitoring is a useful tool for preserving a productive and happy workplace. Some businesses want to outlaw all private online activitieszero tolerance. Others restrict personal Internet use or prevent access to certain Web pages or social networking sites for employees. P&G, for instance, has instructed staff members to restrict their usage of Pandora and prohibits Netflix. Some YouTube watching is still permitted, and access is not being restricted.

because employees utilize social networking sites for digital marketing initiatives. Software from SpectorSoft Corporation is used by Ajax Boiler in Santa Ana, California, to keep track of all the websites staff members visit, the time spent at each site, and all emails written. Wedbush Securities, a financial services and investment company, keeps an eye on the daily e-mails, instant messages, and social networking activities of its more than 1,000 workers. The company's email monitoring software marks certain message types and terms inside messages for further examination. Many businesses have let go of workers who crossed the line. According to a Proofpoint poll, one in five significant U.S. corporations dismissed a worker for breaking email rules in the previous year. The majority of managers who terminated workers for using the Internet improperly did so because the workers' e-mails included private, humiliating, or sensitive material.

No solution is devoid of issues, but a lot of advisors think businesses should create corporate guidelines on how employees should use email, social media, and the Internet. The guidelines should clearly outline when workers are permitted to use business resources for email, blogging, or web browsing, according to position or level. Employees should be informed in the policies as to whether these actions are being watched and why.

Currently, IBM has "social computing guidelines" that address employee use of Facebook and Twitter. The policies advise staff to avoid hiding their identities, keep in mind that they are personally liable for what they write, and avoid engaging in contentious conversations unrelated to their jobs at IBM.

The regulations must take into account the organizational cultures and particular company demands. For instance, investment companies must provide many of their staff members access to other investing websites. A business that depends on open information exchange, creativity, and independence can discover that monitoring causes more issues than it fixes. Communications in One System Previously, the company's networks for wired and wireless data, voice communications, and videoconferencing ran independently of one another and

required the information systems department to maintain them individually. However, businesses may now use unified communications technology to combine several communication channels into a single, accessible service. Users using unified communications may smoothly transition between various communication modes by integrating diverse channels for phone communications, data communications, instant messaging, email, and electronic conferences into a single user experience.

A person's availability to take a call is indicated through presence technology. To assess the value of new technology, businesses will need to look at how work flows and operational procedures will change.Unified communications technology was employed by CenterPoint Properties, a significant industrial real estate business in the Chicago region, to develop collaborative Web sites for each of its real estate transactions. A single point of access to both structured and unstructured data is offered by each Web page. Team members may email, instant chat, phone, or videoconference with just one click thanks to integrated presence technology.

Networks that are virtualized

What if your company had a marketing team with people all around the country tasked with creating new goods and services? Without any possibility of outsiders intercepting the conversations, you would want to be able to email each other and connect with the home office. Working with major private networking companies that provide consumers with secure, private, dedicated networks was one solution to this issue in the past. However, this was a pricey fix. Creating a virtual private network inside the public Internet is a considerably less costly approach.

A virtual private network is a safe, encrypted, private network that has been created inside of a larger public network to benefit from its economies of scale and administration tools. When compared to conventional non-Internet providers that utilize their private networks to protect communications, a VPN offers your company safe, encrypted communications at a far reduced cost. A network architecture for fusing voice and data networks is also made available by VPNs.Point-to-Point Tunneling Protocol is one of the competing protocols used to secure data sent over the open Internet. Data packets are encrypted and enclosed in IP packets in a technique known as tunneling. Business organizations establish a private connection over the open Internet by adding this wrapper to network messages to mask their contents.

A Website

About 239 million Americans of all ages—roughly 75 percent of the population—use the Internet. The most used Internet service is the Web. It is a system that uses a client/server architecture and universally recognized standards for information storage, retrieval, formatting, and presentation. Hypertext links are used to structure web pages so that they may link to other documents as well as external objects like sound, video, and animation files. You have clicked a hyperlink when you click a graphic and a video starts to play. A typical Web site is made up of a main page and a number of other Web pages.

Hypertext

Hypertext Markup Language, the foundation of web pages, is a standard for formatting texts and including dynamic connections to other papers and images held on the same or other computers. Because Web browser software on your computer may make requests for Web pages stored on an Internet host server using the Hypertext Transfer Protocol, Web pages are

available across the Internet. The Web page transfer protocol used for transmission is called HTTP. For instance, when you enter the Web URL http://www.sec.gov into your browser, your browser makes an HTTP request to the sec.gov server asking for the site's main page.

Every Web address begins with the letters HTTP, followed by the domain name, which identifies the company's server machine that is housing the content. Most businesses have a domain name that closely resembles or is identical to their actual company name. Two more bits of information in the Web address that aid the browser in finding the desired page are the directory path and document name.

The address is collectively referred to as a uniform resource locator. A URL instructs the browser software just where to search for the content when it is entered into a browser. In the URL http://www.megacorp.com/content/features/082610.html, for instance, content/features denotes the directory path that identifies where on the domain Web server the page is stored, while 082610.html denotes the document's name and the format it is in.

Online servers

A Web server is a piece of software used to find and control saved Web pages. It delivers the requested Web pages to the user's computer after finding the requested Web pages on the computer where they are kept. Even though they may all live on a single computer in small businesses, server applications typically operate on dedicated PCs. Apache HTTP Server, which has a market share of 65%, is the most widely used web server at the moment. Apache is a free open source program that may be downloaded from the Internet. With a 15% market share, Microsoft Internet Information Services is the second most popular Web server. Finding Information About the We B How many Web pages there really are is a mystery. The portion of the Web that search engines visit and record information on is known as the surface Web. For instance, Google accessed 400 billion pages in 2012, which represents a significant share of the population of publicly available Web sites. However, there is a "deep Web" that is thought to include an extra 1 trillion pages, many of which are private or are kept in secure corporate systems.

Search Engines It goes without saying that with so many Web pages available, it might be difficult to quickly locate certain Web sites that can benefit you or your company. Out of the billions of indexed Web pages, how can you locate the one or two that you actually want and need? Search engines are perhaps the "killer app" of the Internet age since they aim to quickly address the issue of discovering meaningful information on the Web. Search engines of today are capable of sifting through a variety of file types, including HTML, Microsoft Office, PDF, audio, video, and picture files. Despite the fact that there are thousands of other search engines available, Google, Yahoo!, Baidu, and the Bing search engine from Microsoft. Early on in the 1990s, very rudimentary software programs known as web search engines roamed the developing World Wide Web, visiting sites and learning about the information contained on each page. The original search engines were just keyword indexes of every website they visited, providing users with lists of sites that may not have been very relevant to their search.

David Filo and Jerry Yang, computer science students at Stanford University, compiled a list of their favorite Web sites in 1994 and dubbed it "Yet Another Hierarchical Officious Oracle," or Yahoo. Yahoo, which now uses Microsoft for search results, was originally not a search engine but rather a curated collection of Web sites arranged by categories the editors considered helpful. Two further Stanford computer science students, Larry Page and Sergey Brin, unveiled the first iteration of Google in 1998. This search engine was unique because it prioritized search results based on the relevancy of each page in addition to indexing the

words on each Web page. Page patented the concept of a page ranking system, which effectively gauges a Web page's popularity by counting both the sites that link to it and the pages that those sites link to.

Really well-liked Web sites are considered to be more "relevant" to visitors. Brin built a unique Web crawler software that indexes both word combinations and keywords on a page. The Google search engine was built on these two concepts.Due to its widespread usage, many individuals choose search engine Web sites as their default home page from which to browse the Internet. The fastest-growing kind of marketing and advertising, search engine marketing, is likewise built on search engines.In order to react promptly to user requests to see a website, the Google search engine continually crawls the Web, indexes each page's content, determines its popularity, and stores the pages. It takes the whole operation roughly 0.5 seconds. Mobile Search The nature of e-commerce and search is evolving as a result of the rise of mobile smartphones and tablet computers and the approximately 122 million Americans who access the Internet via mobile devices. About 20% of all searches were made on mobile devices in 2012, and Google predicts that this percentage will grow significantly over the next years. To improve the convenience of browsing and buying on smartphones, Google and Yahoo have each created new search interfaces. For instance, Amazon sold more than $1 billion worth of items in 2012 thanks to mobile shop searches.

Search Engine Marketing By providing what is now referred to as search engine marketing, search engines have evolved into significant ad platforms and shopping facilities. Users of Google, Bing, Yahoo, or any of the numerous websites these search engines serve up get two sorts of listings when they input a search term: sponsored links, for which advertisers have paid to be displayed, and unsponsored "organic" search results. Additionally, little text boxes on the side of search results pages may be purchased by advertising. The fastest-growing kind of Internet advertising is paid, sponsored content. These effective new marketing tools accurately match consumer interests with promotional messaging at the ideal time. The value of the search process is commercialized via search engine marketing. Over half of all internet advertising income ($19.5 billion) was earned by search engine marketing in 2012. In 2012, Google will control more than 40% of all internet advertising. 95% of the internet advertising income, which totaled $39 billion for Google in 2011, came from search engine marketing.

Companies strive to optimize their Web sites for search engine recognition due to search engine marketing's effectiveness. The page will rank higher in search engine result listings the more optimized it is. By using a number of strategies that help a website rank better with the main search engines when certain keywords and phrases are entered in the search box, search engine optimization is the process of enhancing the quality and amount of Web traffic to a website. Making ensuring that the keywords used in the Web site description align with those that potential buyers are likely to enter as search terms is one tactic.

It is advantageous to link your Web site to as many other Web sites as you can because search engines evaluate such links to determine the popularity of a Web page and how it is linked to other content on the Web. For instance, your Web site is more likely to be among the first ranked by search engines if it uses the keyword "lighting" rather than "lamps" if most prospective customers are searching for "lighting." It is also advantageous to use keywords that are relevant to your Web site's target audience. Scammers may manipulate search engines by creating hundreds of fake Web sites, linking them together, or linking them to a single retailer's website in an effort to trick Google's search engine. Assorted "link farms" may be paid by businesses to connect to their website. In 2012, Google modified their search algorithm. The new algorithm, code-named "Penguin," meticulously assesses link quality. It is assumed that a website must be more valuable if there are more links pointing to it.

Search engines have generally been highly beneficial to small firms who are unable to afford expensive marketing strategies. Search engine users are what marketers refer to as "hot prospects"—people who are seeking for information and often plan to buy—because they are searching for a particular item or service. Additionally, search engines only charge when a user clicks through to a website. Only for advertising that get a click do merchants have to pay; not for ads that don't. Search engine marketing helps customers since adverts for businesses only show up when people are seeking for a certain product. Pop-up windows, Flash animations, movies, interstitials, emails, and other pointless messages are not present. Thus, search engine marketing helps customers conserve their mental energy and lowers the cost of their searches. According to a recent research, search is worth over $800 billion to both consumers and businesses worldwide, with roughly 65 percent of the value coming to consumers in the form of cheaper pricing and search expenses.

Social Search One issue with Google and mechanical search engines is how comprehensive they are: type in "ultra computers" and you'll get over 300 million results in just.2 seconds! The discrimination of search engines is lacking. A person's network of social connections is used in social search to provide fewer, more relevant, and reliable search results. A social search Web site would examine your friends' suggestions, their previous Web visits, and their usage of "Like" buttons, as opposed to the top search engines, which employ a mathematical algorithm to discover results that meet your query.

One such example is Google's development of Google +1, a social layer built on top of the company's current search engine. Users may immediately notify their peers by adding a +1 next to websites that they found useful. The +1 sites that their friends had suggested would appear higher in subsequent searches made by their peers. A comparable social search feature is the Like button on Facebook. A social search engine has not yet been completely deployed by Google or Facebook. One issue with social search is that your close friends may not be intimately familiar with the subjects you are researching or they could have preferences you don't share. It's also likely that your close buddies are unaware of what you're looking for.

Semantic Search Creating search engines that can comprehend what we are really seeking for is another technique to make search engines more discriminating and beneficial. The term "semantic search" refers to the effort to create a search engine that can really comprehend human language and behavior. As an example, Google's search engine started producing millions of links in 2012. It began to provide consumers more concrete information and straightforward responses, as well as more relevant connections to websites based on the search engine's assessment of the user's intent and even the user's prior search history. The goal of Google's search engine is to comprehend what individuals are most likely considering when they do a search. Google aims to provide people a better result than merely millions of results by using its enormous collection of things and intelligent technologies. For instance, if you type "Lake Tahoe" into a search engine, the results will include a map, lodging options, and some basic information on the lake. .The proliferation of photographs and videos on the Internet generated a need for searching and categorizing these visual things, despite the fact that search engines were first developed to search text materials. A digital representation of a human face may be produced using facial recognition software. Tag Suggest, a new function created by combining Facebook's face recognition technology with tagging, was debuted in 2012. The program generates a digital fingerprint of the face that resembles a fingerprint. On their timelines and on the timelines of their friends, users may post their own tagged photos. When a person is tagged in a photo, Facebook may choose that individual from a group picture and let others know who else is there. Additionally, you may discover and recognize individuals on Facebook by searching for them using their digital photograph.

Intelligent Agent Shopping Bots are software agents with intelligence built-in that can collect or filter information and carry out various functions to help users. Shopping bots scan the Internet for shopping-related information using intelligent agent software. Shoppers interested in making a purchase may utilize shopping bots like MySimon or Google Product Search to filter and obtain information about relevant items, compare similar products based on user-defined criteria, and bargain with vendors over conditions of pricing and delivery. Several of these shopping assistants look up the cost and availability of items entered by the user on the Web and provide a list of stores selling the item along with price details and a link to make a purchase[10]–[12].

CONCLUSION

In conclusion, the concepts of fair access, competition, and freedom of speech online are at the center of the debate over net neutrality. There are significant repercussions for internet users, companies, and society as a whole depending on whether net neutrality restrictions are maintained or repealed. Finding a compromise between an open internet and the interests of ISPs and other stakeholders is a difficult task for policymakers and society at large as the debate rages on. The result of the fight for net neutrality will have a big impact on how the internet develops in the future. It affects not just the experiences and rights of internet users but also the dynamics of digital inclusion, competitiveness, and innovation online. In the constantly changing digital world, finding a balance between maintaining an open internet and allowing for innovation and investment is still a difficult task.

REFERENCES

[1] A. Lamparello, “The Internet is the New Marketplace of Ideas: Why <I>Riley v. California</I> Supports Net Neutrality,” *SSRN Electron. J.*, 2014, doi: 10.2139/ssrn.2514523.

[2] M. C. Leal, “The EU approach to net neutrality: Network operators and over-the-top players, friends or foes?,” *Comput. Law Secur. Rev.*, 2014, doi: 10.1016/j.clsr.2014.07.009.

[3] Alex, “A vote on ‘net neutrality’ has intensified a battle over the internet’s future,” *Econ. (United Kingdom)*, 2017.

[4] J. A. Pouwelse, P. Garbacki, D. Epema, and H. Sips, “Pirates and Samaritans: A decade of measurements on peer production and their implications for net neutrality and copyright,” *Telecomm. Policy*, 2008, doi: 10.1016/j.telpol.2008.09.004.

[5] A. Odlyzko, “Network Neutrality, Search Neutrality, and the Never-Ending Conflict between Efficiency and Fairness in Markets,” *SSRN Electron. J.*, 2011, doi: 10.2139/ssrn.1095350.

[6] G. H. Pike, “What the Future Holds for Net Neutrality,” *Inf. Today*, 2010.

[7] C. T. Marsden., *Network neutrality: From policy to law to regulation*. 2017.

[8] C. Marsden T., *Network neutrality: From policy to law to regulation*. 2017. doi: 10.26530/oapen_622853.

[9] D. A. Farber and A. J. O’Connell, “Agencies as adversaries,” *California Law Review*. 2017. doi: 10.15779/Z38H12V721.

[10] D. C. Nunziato, “The First Amendment Issue of Our Time,” *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.3000594.

[11] J. Meyrowitz, "Medium theory and cultural transformations," in *Routledge Handbook of Cultural Sociology: Second Edition*, 2018. doi: 10.4324/9781315267784-67.

[12] V. G. Cerf, "Who Rules the Net?," in *Who Rules the Net? Internet Governance and Jurisdiction*, 2003.

CHAPTER 10

A COMPREHENSIVE REVIEW OF WIRELESS REVOLUTION

Dr. Pramod Pandey
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: pramodkumar@presidencyuniversity.in

ABSTRACT:

The wireless revolution has transformed the way we communicate, access information, and interact with technology. This abstract explores the evolution of wireless technology, its impact on various sectors, and the implications of this revolution for individuals, businesses, and society as a whole.The wireless revolution refers to the rapid advancement and widespread adoption of wireless communication technologies, such as cellular networks, Wi-Fi, Bluetooth, and satellite communications. These technologies have liberated us from the constraints of wired connections, enabling seamless and ubiquitous connectivity.Software services called mashups allow users and system developers to combine different pieces of material or software to create something altogether new. For instance, Flickr, a service offered by Yahoo for the storing and sharing of pictures, mixes photos with additional image data contributed by users and tools to make it useable inside various programming environments.

KEYWORDS:

Connected Devices, Mobile Connectivity, Mobile Devices, Mobile Networks, Mobility, Smart Cities.

INTRODUCTION

Today's websites allow users to communicate, exchange knowledge, and develop new products and services online, not merely display static material. Web 2.0 describes these second-generation interactive Internet-based services. You've probably used some of these Web 2.0 services if you've uploaded photographs to Flickr or another photo sharing website, pinned a photo to Pinterest, uploaded a video to YouTube, started a blog, or added an app to your Facebook profile. Interactivity, real-time user control, social interaction, and user-generated content are the four distinguishing characteristics of Web 2.0. These elements are made possible by a variety of technologies and services, such as cloud computing, software mashups and applications, blogs, RSS, wikis, and social networks.Social networks and other online communities where individuals may engage with one another anyway they like have been made possible by Web 2.0 technologies and services[1]–[3].

Weblogs are often referred to as blogs. A blog is a personal website that generally includes links to linked Web sites as well as a chronology of postings by the author. A blogroll and trackbacks are possible on the website. The majority of blogs also let readers leave comments on the posts. It's common to refer to the process of writing a blog as "blogging." In addition to being hosted by third-party services like Blogger.com, TypePad.com, and Xanga.com, blogs may also be created using collaborative tools like Lotus Notes and social networks like Facebook. A popular content management system and blogging tool, WordPress is open source. Twitter uses a sort of blogging called microblogging, which consists of brief postings of 140 characters or fewer. The templates that the blogging software or service provides are often modified to create blog pages. Millions of individuals may publish their own Web sites

and share material with others even without any knowledge of HTML. The blogosphere is a term used to describe the whole of Web sites dedicated to blogs. Blogs have grown in popularity as tools for personal publication, but they also have advantages in business.

If you read blogs often, you may use RSS to follow your favorite blogs without having to check them frequently for updates. Really Simple Syndication (RSS), also known as Rich Site Summary, is a technology that automatically downloads certain material from websites to users' PCs. When you instruct RSS reader software to scan certain Web pages or blogs, it accumulates content from those pages and notifies you when there is new content available. The main web browsers and email applications all come with RSS readers built in, and they can be found on websites like Google and Yahoo.Blogs let readers remark on the original content but do not let readers edit the originally uploaded content. Wikis, on the other hand, are collaborative Web sites where users may add, remove, or change site material, including the contributions of earlier writers. The term "Wiki" is a Hawaiian word that means "quick." Wiki software often offers a template that specifies the design and components that are shared by all pages, displays user-edited software program code, and then generates the material into an HTML-based page for display in a Web browser. The inclusion of photos, videos, and even interactive components like polls and games is permitted by certain wiki software whereas just simple text formatting is permitted by others. The majority of wikis include tools for checking other users' work and fixing errors.

Wikis have numerous commercial applications since they make information sharing so simple. A wiki was implemented by the National Cyber Security Center of the U.S. Department of Homeland Security to promote cooperation on cybersecurity across government agencies. The wiki is used by NCSC and other agencies as a repository for technical and standards information as well as for real-time information exchange on threats, attacks, and responses. To promote the work of Pixar Animation Studios, a community-based collaborative website called Pixar website was created. Anyone may write or modify an entry on a Pixar movie using the wiki format.

Users of social networking sites may create networks of friends and professional associates. Typically, members build a "profile," a Web page where they may publish text, images, videos, and MP3 files, and then they share these profiles with other users on the site who are referred to as their "friends" or contacts. Social networking sites are heavily focused on social interaction, real-time user control, user-generated content, and the exchange of information and ideas. LinkedIn, Twitter, and Facebook are popular social networking platforms.

In the eyes of many, social networking sites are the essence of Web 2.0. They have fundamentally altered how people use the internet, how they communicate and with whom, how businesspeople stay in touch with clients, suppliers, and staff, how companies learn about their clients, and how advertisers reach prospective clients. The major social networking sites are also becoming into platforms for application development where users may produce and market software products to other community members. More than 1 million developers worked exclusively on Facebook to produce more than 550,000 games, video sharing, and messaging apps. We discuss social networking applications for businesses in greater detail. Social networking is also discussed. Web 2.0 is also covered in further depth in our learning tracks.

Web 3.0: The Future We b

Possibly less than half. All four major search enginesGoogle, Yahoo, Microsoft, and Amazonare working to make it more likely for users to get relevant results. However, with more than 400 billion Web pages indexed, the methods for locating the information you truly

need are fairly archaic and rely on the phrases used on the sites and their relative popularity among users of the same search terms. It's hit or miss, to put it another way.

The future of the Web mostly entails creating methods for making regular people's searches of the 400 billion public Web pages more efficient and worthwhile. Web 1.0 provided a solution to the issue of information access. Sharing the knowledge with others and creating fresh Web experiences were issues that Web 2.0 addressed. The promise of Web 3.0 is that in the future, all of this digital data and all of these interactions will be knitted together into a single, meaningful experience.

The Semantic Web is another name for this. The term "semantic" relates to meaning. The majority of material on the Web nowadays is created primarily for human consumption and computer display, rather than for computer programs to analyze and manipulate. The above-described Semantic Search is a part of a bigger effort to give the Web a more intelligent, human-like appearance. Although they can track when a certain phrase or keyword occurs in a Web publication, search engines do not fully comprehend what it means or how it links to other online information. By doing two searches on Google, you can verify this. Enter "Paris Hilton" first. Enter "Hilton in Paris" next. Google is unaware that you are interested in the Hilton Hotel in Paris in the second search since it cannot comprehend everyday English. Google's search engine returns the most popular results for those searches where "Hilton" and "Paris" occur on the sites since it cannot interpret the meaning of the pages it has indexed.

The Semantic Web, a collaborative initiative coordinated by the World Wide Web Consortium to add a layer of meaning on top of the current Web in order to decrease the amount of human participation in searching for and processing Web material, was first introduced in a 2001 Scientific American article. For instance, the New York Times launched Longitude in 2011, a semantic application that offers a graphical interface for accessing Times information.

For instance, to get all current news in the Times, you may search for stories published within the previous 24 hours concerning Germany or a certain American city. .Although opinions on the future of the Web differ, most of them center on how to make it more "intelligent," with machine-facilitated information comprehension fostering a more natural and efficient user experience. Let's imagine, for example, that you want to organize a party with your tennis friends at a nearby restaurant on Friday night after work. You already have plans to see a movie with another buddy, which is an issue. With a single set of instructions sent as text or speech to your mobile smartphone, you would be able to coordinate this change in plans with the schedules of your tennis partners and your movie buddy, as well as make a reservation at the restaurant, in a Semantic Web 3.0 context. This skill is currently out of our reach.

DISCUSSION

Because it is challenging to create devices, especially software programs, that are really intelligent like people, work on making the Web a more intelligent experience moves slowly. But there are alternative perspectives on the Web of the future. Some envision a 3-D web where users may navigate websites while within a 3-D world.

Others raise the possibility of a ubiquitous web that manages your schedule and appointments in addition to controlling everything from the lights in your living room to the rearview mirror of your automobile[4]–[6].

The widespread adoption of cloud computing and business models for software as a service, constant connectivity between mobile platforms and Internet access devices, and the evolution of the Web from a network of discrete, siloed applications and content into a more

seamless and interoperable whole are additional complementary trends that point toward a future Web 3.0. These more realistic expectations for Web 3.0's future are more likely to come true in the near future.

Electronic Revolution

The wireless revolution is here! A lot of the computing operations you used to do at your desk may now be completed on cell phones, smartphones, tablets, and wire-free personal PCs, in addition to a lot more. In discussions of the mobile digital platform, we presented smartphones. Smartphones like the iPhone, Android phone, and BlackBerry combine a mobile laptop computer with Wi-Fi capabilities with the functionality of a cell phone. This enables the integration of music, video, Internet access, and telephone service into a single gadget. The fastest-growing wireless devices for Internet access are smartphones. For the distribution of video, music, and Web search, a significant portion of the Internet is transitioning to a mobile, accessible from anywhere, broadband service.

Blood Cell Systems

Around the globe, 1.5 billion mobile phones are expected to be sold in 2012. In the US, 115 million people have smartphones, while 358 million people have mobile phone subscriptions. About 120 million individuals use their phones to access the Internet. In a few years, cellphones will overtake desktop computers as the primary search engine. Multiple competing standards are used by digital cellular services.

The Global System for Mobile Communications is the norm in Europe and a large portion of non-American countries. The capacity to travel internationally is a strength of GSM. In the US, GSM mobile phone networks exist, including T-Mobile and AT&T. Verizon and Sprint both employ the Code Division Multiple Access standard, which is a rival one in the US. The military created CDMA during World War II, and it is more effective than GSM because it communicates across several frequencies, uses the full spectrum, and randomly assigns users to a variety of frequencies over time.

Cellular networks from earlier generations were built mainly for voice communication and a little amount of data transfer in the form of text messages. 3G and 4G networks are now available from telecom operators. 3G networks provide adequate transmission speeds for e-mail, web surfing, and online shopping but are too sluggish for movies, with rates ranging from 144 Kbps for mobile users in, for example, a vehicle to more than 2 Mbps for stationary users. Long-term evolution networks, commonly known as 4G networks, operate at substantially faster rates of 100 Mbps download and 50 Mbps upload. LTE offers more than enough space for watching high definition video on your smartphone and is comparable to a home Wi-Fi connection.

WiMax, which employs Wi-Fi standards but has an expanded range of approximately 30 miles, enough to span a metropolitan region and maybe whole small nations, is a less well-developed high speed network standard.

Access To The Internet And Wireless Computer Networks

If you have a laptop, you may be allowed to use it at the university library or as you travel from room to room in your house or dorm to access the Internet. For PCs, various wireless portable devices, and mobile phones, high-speed wireless Internet connection is made possible through a variety of technologies. Numerous regions that were not accessible through regular wired Internet services now have access to the Internet thanks to these new high-speed offerings.

Bluetooth

The 802.15 wireless networking protocol, which is helpful for building tiny personal area networks, is more often referred to as Bluetooth. Using low-power radio-based communication to connect up to eight devices within a 10-meter radius, it can send data at up to 722 Kbps in the 2.4 GHz range. Bluetooth-enabled wireless phones, pagers, laptops, printers, and computing equipment may all interact with one another and even control one another without the need for a human operator.

One may instruct a laptop computer to wirelessly deliver a document file to a printer, for instance. Without using cables, Bluetooth links wireless keyboards and mouse to computers or mobile phones to earpieces. Bluetooth is suitable for battery-powered mobile computers or cell phones due of its low power consumption.

Although Bluetooth is well suited for personal networking, big businesses may also utilize it. For instance, FedEx drivers utilize Bluetooth to transfer the delivery information they have recorded on their portable PowerPad computers to cellular transmitters, which then relay the information to company computers. Bluetooth eliminates the need for drivers to spend time docking their portable devices, allowing a range of devices, including mobile phones, cellphones, wireless keyboards and mouse, PCs, and printers, to communicate wirelessly within a constrained 30-foot range. Bluetooth may be used to network related devices in addition to connections, such as sending data from one PC to another.

Wireless Internet Access and Wi-Fi

Wi-Fi is another name for the 802.11 family of wireless LAN and Internet access technologies. The first of these protocols to gain widespread acceptance was 802.11b, which has an effective range of 30 to 50 meters and can transmit data at up to 11 Mbps in the unlicensed 2.4-GHz band. Up to 54 Mbps may be sent using the 2.4-GHz band using the 802.11g standard. Over 100 Mbps may be sent with 802.11n. Wi-Fi is now supported natively by PCs, netbooks, the iPhone, iPad, and other devices. Access points are often used in Wi-Fi communication to connect wireless devices to a wired LAN. An access point is a device that connects to a wired network, router, or hub through antennas and a radio receiver/transmitter. The current cellular network is used by mobile access points, including Verizon's Mobile Hotspots, to establish Wi-Fi connections. a limited number of mobile devices are linked to the Internet and a larger wired LAN through an 802.11 wireless LAN. The majority of wireless devices are clients. The mobile client stations' required servers are located on the wired LAN. The primary wired LAN and the wireless LAN are connected by the access point, which also manages the wireless stations and serves as a bridge. The wireless stations are likewise controlled by the access point.

Network interface cards in portable laptop computers allow them to connect to the wired LAN by exchanging data with the access point. The client adapters transform the network signals from the wired network into data that the mobile device can interpret using radio waves, which are sent by the access point. The data is then returned from the mobile device via the client adapter to the access point, which sends it to the wired network. Wi-Fi is now mostly used for high-speed wireless Internet access. In this case, the access point is connected to a cable or DSL phone line that provides an Internet connection. The access point allows computers within its range to connect wirelessly to the Internet.

In a public setting, hotspots generally consist of one or more access points that provide wireless Internet access. Some hotspots are free to use or don't need any extra software, while others may need to be activated and a user account set up by giving a credit card information

online. Wi-Fi networks are being used by companies of all kinds to provide inexpensive wireless LANs and Internet connectivity. Hotels, airport lounges, libraries, cafés, and college campuses all have Wi-Fi hotspots to provide mobile Internet access. One of the numerous campuses where students increasingly utilize Wi-Fi for study, classwork, and pleasure is Dartmouth College.

The Wi-Fi technology does, however, present certain difficulties. The first is that Wi-Fi security mechanisms leave these wireless networks open to intrusion.

The vulnerability of Wi-Fi networks to interference from neighboring devices using the same spectrum, such as wireless phones, microwave ovens, or other wireless LANs, is another disadvantage. However, wireless networks based on the 802.11n standard are able to overcome this issue by using several wireless antennas simultaneously for data transmission and reception as well as MIMO technology to manage numerous simultaneous radio signals.

WiMAX

Surprisingly many places in the United States and throughout the globe lack access to fixed broadband internet or Wi-Fi. Since Wi-Fi systems have a 300-foot maximum range from the base station, it might be challenging for rural communities without cable or DSL connection to locate wireless Internet access. To address these issues, the IEEE created a new set of standards called as WiMax. The abbreviation for IEEE Standard 802.16 is WiMax, or Worldwide Interoperability for Microwave Access. It can transmit data at up to 75 Mbps and has a wireless access range of up to 31 miles. WiMax antennas have the strength to transmit high-speed Internet connections to rooftop antennas on distant residences and commercial buildings. WiMAX-capable mobile devices and laptops are starting to come on the market. One of the 4G network technologies we previously covered in this article is mobile WiMAX.

Networks of Rid and Wireless Sensor

Mobile technology are transforming how businesses operate and how employees collaborate. Radio frequency identification systems and wireless sensor networks are also having a significant influence in addition to the wireless systems we have just discussed. Identification Using Radio Frequency A potent technology is offered by radio frequency identification systems for tracing the flow of items throughout the supply chain. RFID systems send radio signals to RFID readers over a short distance using small tags with integrated microchips that hold information about an object and its position.

The data is subsequently sent to a computer for processing by the RFID readers across a network. Bar codes need line-of-sight contact to read, whereas RFID tags do not. An item's location, the place and time it was created, as well as other details about the item, such as its state throughout manufacturing, are all electronically encoded into the RFID tag. A microchip for storing the data is included within the tag. The tag's remaining portion is an antenna that sends information to the reader[7]–[10].

The reader unit is a permanent or portable device having an antenna, radio transmitter, and decoding capacity. Depending on its power output, the radio frequency used, and the surrounding environment, the reader emits radio waves at distances ranging from 1 inch to 100 feet.

An RFID tag is activated and begins transmitting data when it is in the reader's line of sight. These data are received by the reader, decoded, and then sent back to a host computer for further processing through a wired or wireless network. RFID tags and antennas are both available in a range of sizes and forms. Active RFID tags often allow for data rewriting and

modification and are powered by an internal battery. Active tags may cost several dollars per tag but may broadcast for hundreds of feet. Active RFID tags are used in automated toll collecting systems like New York's E-ZPass. Without an internal power source, passive RFID tags rely on the radio frequency energy that an RFID reader transmits to function. Compared to active tags, they are more compact, lighter, and less costly, but their range is just a few feet. RFID technologies gather and maintain more specific information about products in warehouses or during manufacturing than bar coding systems do in inventory control and supply chain management. When several things are sent together, RFID tracking devices keep tabs on every pallet, lot, or even individual item in the cargo. By making it easier for businesses like Walmart to "see" precisely what inventory is kept in warehouses or on store shelves, this technology may aid in enhancing receiving and storage processes. The first case explained how Continental Tires utilized RFID technology to accurately monitor the whereabouts of tire components as they were manufactured.

To keep track of the delivery of pallets and cases of merchandise sent with RFID tags, Walmart has placed RFID readers at store receiving docks. Just as the cases are being moved onto the sales floor from backroom storage rooms, the RFID scanner scans the tags once again. Software integrates RFID data about the number of cases transported out to the sales floor with sales data from Walmart's point-of-sale systems. at order to restock shop shelves before they run out, the algorithm predicts which things will soon be exhausted and automatically creates a list of items to select at the warehouse. This data enables Walmart to enhance sales, decrease out-of-stock products, and further cut expenses.

Once prohibitively expensive for general usage, RFID tags are now available in the US for as little as 7 cents per passive tag. RFID is becoming to be cost-effective for many applications as the price falls. Companies may need to improve their hardware and software in addition to installing RFID readers and tagging systems in order to manage the enormous volumes of data generated by RFID systemstransactions that may total tens or hundreds of gigabytes.RFID data is filtered, gathered, and kept from overwhelming corporate networks and system applications using software.

It is usually necessary to modify programs in order for them to accept significant amounts of constantly produced RFID data and communicate that data with other applications. Supply chain management tools from well-known business software providers like SAP and Oracle PeopleSoft are now available in RFID-ready versions.

Networks of Wireless Sensors

A wireless sensor network may be implemented if your business desired cutting-edge technology to monitor building security or identify dangerous compounds in the air. In order to give measurements of many sites over wide areas, wireless sensor networks are networks of linked wireless sensors that are implanted into the physical environment. These gadgets include processing, storage, and antennas and radio frequency sensors.

They are connected via a network, which sends the data they collect to a computer for processing. There are hundreds to thousands of nodes in these networks. Wireless sensor devices must have extremely low power consumption and long-lasting batteries since they are left in the field for extended periods of time without maintenance or human involvement.

In areas like monitoring environmental changes, traffic or military activity, protecting property, effectively operating and managing machinery and vehicles, setting up security perimeters, keeping an eye on supply chain management, or spotting chemical, biological, or radiological material, wireless sensor networks are useful.

CONCLUSION

In conclusion, the wireless revolution has changed how we interact with one other and with information and each other's businesses. Global connectivity, industry transformation, and the emergence of new opportunities for creativity and cooperation have all been made possible by it. A connected and inclusive future will be shaped by embracing the possibilities of this revolution and solving its limitations as wireless technologies continue to advance.

However, there are other difficulties and things to think about with the wireless revolution. Strong infrastructure and spectrum management are required due to the exponential increase in data consumption and the need for wireless access. Since wireless communication has weaknesses that may be exploited by hackers, security and privacy must always be guaranteed. Furthermore, closing the digital gap and guaranteeing fair access to wireless technology continue to be crucial social objectives.

REFERENCES

[1] A. Swindlehurst, E. Ayanoglu, P. Heydari, and F. Capolino, "Millimeter-wave massive MIMO: The next wireless revolution?," *IEEE Commun. Mag.*, 2014, doi: 10.1109/MCOM.2014.6894453.

[2] M. Bopp, "The wireless revolution," *Electronic Product Design*. 2005. doi: 10.4324/9781315701691-13.

[3] I. Vogiatzis, "The wireless revolution and cardiorespiratory system monitoring," *International Journal of Cardiology*. 2019. doi: 10.1016/j.ijcard.2018.09.036.

[4] G. Interdonato, E. Björnson, H. Quoc Ngo, P. Frenger, and E. G. Larsson, "Ubiquitous cell-free Massive MIMO communications," *Eurasip Journal on Wireless Communications and Networking*. 2019. doi: 10.1186/s13638-019-1507-0.

[5] A. Kumar, R. Shankar, K. Momaya, and S. Gupte, "The market for wireless electricity: The case of India," *Energy Policy*, 2010, doi: 10.1016/j.enpol.2009.11.037.

[6] A. A. Salih, S. R. M. Zeebaree, A. S. Abdulraheem, R. R. Zebari, M. A. M. Sadeeq, and O. M. Ahmed, "Evolution of mobile wireless communication to 5G revolution," *Technol. Reports Kansai Univ.*, 2020.

[7] P. Barpanda, G. Oyama, S. I. Nishimura, S. C. Chung, and A. Yamada, "A 3.8-V earth-abundant sodium battery electrode," *Nat. Commun.*, 2014, doi: 10.1038/ncomms5358.

[8] D. Y. C. Lie, J. C. Mayeda, Y. Li, and J. Lopez, "A Review of 5G Power Amplifier Design at cm-Wave and mm-Wave Frequencies," *Wireless Communications and Mobile Computing*. 2018. doi: 10.1155/2018/6793814.

[9] G. R. R. Patra and K. K. Sharma, "Overview of 5G Wireless Technology and its Revolution," *Int. J. Electr. Eng. Technol.*, 2020.

[10] S. Lam po Tang, "Recent developments in flexible wearable electronics for monitoring applications," *Trans. Inst. Meas. Control*, 2007, doi: 10.1177/0142331207070389.

CHAPTER 11

AN ANALYSIS OF INFORMATION SYSTEMS SECURITY

Mr. Ram Srinivas
Assistant Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: ramsrinivas@presidencyuniversity.in

ABSTRACT:

Securing information systems has become a paramount concern in today's interconnected and digital world. This abstract examines the importance of information system security, the evolving threat landscape, and the strategies and technologies used to protect sensitive data and ensure the integrity and availability of information systems.Information systems serve as the backbone of organizations, facilitating communication, data storage, and business operations. However, they are susceptible to a range of threats and vulnerabilities, including unauthorized access, data breaches, malware attacks, insider threats, and social engineering. These threats can result in significant financial losses, reputational damage, legal consequences, and compromised customer trust.

KEYWORDS:

Authentication, Cybersecurity, Data Encryption, Firewall, Intrusion Detection System (IDS), Malware Protection.

INTRODUCTION

One of the most well-known social networking services on the Internet is LinkedIn. With over 160 million users, LinkedIn mostly attracts white-collar professionals who are more interested in networking than socializing. Users update their online resumes, connect with coworkers and business acquaintances, and look for professionals who can help them with their regular business challenges. This service is highly valued by those seeking for employment or professional advancement. By any metric, LinkedIn has been among the biggest technological success stories of the last ten years. At this time, the corporation is worth more than $12 billion. However, the business had a shocking data breach in June 2012 that made millions of LinkedIn members' passwords public. LinkedIn's security was hacked by hackers, who then acquired 6.5 million user credentials and released them in the open on a Russian hacking website. Following the incident, both LinkedIn users and security professionals were astounded by how little a business that collects and manages consumer data had done to protect it. Especially for a very successful software firm with enough cash on hand, a solid customer base, and skilled staff, LinkedIn had appallingly poor computer security.

Security professionals berated LinkedIn for lacking a chief security officer whose main responsibility is to prevent security breaches. Even more unexpectedly, it was discovered that LinkedIn employed just a little amount of encryption to secure passwords and did not use numerous widely used encryption methods. The majority of businesses use a method called "salting," which involves appending a string of random numbers to the end of hashed passwords to make them more challenging to decipher. With just a few more lines of code, salting may be done for little to no money. Most businesses salt passwords using complex cryptographic methods, but extremely The security equivalent of leaving one's goods unattended in a crowded place is LinkedIn's failure to salt its users' passwords at all[1]–[3].

To make it more difficult for hackers to access data, most businesses keep hashed passwords on separate, secure Web servers. A solid password, Web server, and application security setup would cost a firm like LinkedIn somewhere in the low six figures, but the typical data breach costs businesses $5.5 million, according to a Ponemon Institute research sponsored by Symantec. LinkedIn's losses may really be substantially more than that, which is shocking given their near utter contempt for data security.

Some security professionals think that corporations like LinkedIn's lack of liability is a key factor contributing to their inadequate security procedures. Computer security and social network data security are not regulated and are often inadequately secured by businesses, in contrast to other industries where fundamental consumer safeguards are supervised and safeguarded. People also don't usually stop using social networks because of data breaches. For instance, many users wanted to quit LinkedIn after the hack but decided against it since it is the most well-known social network for business networking.

Following the password hack, LinkedIn promptly reassured its clients that their information was safe. The firm said that it has started a project to salt passwords to improve security and deactivated the 6.5 million disclosed passwords. However, a $5 million class-action complaint alleges that LinkedIn does not even adhere to the most basic industry standards for data safety, notably the more modern methods of salting hashed passwords.

Security experts said that although LinkedIn's security protocols would have been cutting edge a few years ago, they had not done much to stay up with and defend themselves against the recent spike in data leaks. In addition to bringing its security up to speed, LinkedIn must embrace the philosophy that safeguarding user data requires continuing work rather than a one-time repair.

The issues caused by the theft of 6.5 million LinkedIn credentials serve as an example of why firms should give information system security extra attention. LinkedIn offers significant advantages to both people and companies. However, from a security perspective, LinkedIn's website was not adequately guarded against hackers, who were able to obtain private user data. The introductory graphic highlights crucial issues brought up by this case and this.

Despite having some security technologies and processes in place, LinkedIn's administration has not taken sufficient steps to secure the data of its users. It didn't safeguard user credentials using common password encryption methods like "salting," for example.

This site is exceptionally appealing to thieves and hackers looking to steal vital personal and financial information and spread dangerous software because of its "social" aspect and big user base.

Given the volume of users on LinkedIn and the social aspect of the platform, management did not take sufficient precautions to secure the company's data. The dedicated user base of LinkedIn kept the damage from the breach from being substantially worse, and the majority of users thought they had to stay with the platform since it was so important to their professional development. However, the business risks a multimillion-dollar class action lawsuit as well as harm to its brand.

The message is obvious for all firms: the challenges of getting rid of dangerous software or fixing damage from identity theft raise operating expenses and reduce productivity for both people and enterprises. Here are some issues to consider: What organizational, technological, and managerial elements led to the LinkedIn data breach? What was the data breach's financial impact?

DISCUSSION

System Vulnerability

In a matter of seconds, your computer would become inoperable, and it would take you many days to get it back. If you relied on the computer to operate your company, a breakdown may prevent you from selling to clients or placing orders with suppliers. Additionally, you can discover that strangers broke into your computer system and stole or destroyed vital data, including sensitive payment information from your clients. Your company may never be able to function if too much data is lost or leaked! In other words, if you run a firm today, security and control must be your top priorities. Information systems are protected against illegal access, modification, theft, and physical damage by rules, procedures, and technology safeguards. To assure the security of the company's assets, the accuracy and dependability of its records, and operational conformity to management standards, controls are techniques, rules, and organizational processes.

Reasons For System Vulnerability

Large data sets that are kept in electronic form are far more open to dangers than those that are kept in manual form. Information systems at various places are interconnected through communications networks. Any access point in the network has the potential to allow unwanted access, misuse, or fraud; it is not only possible at certain locations. the most frequent dangers facing modern information systems. Poor management choices along with technological, organizational, and environmental variables may be the cause. Vulnerabilities exist at each stage and in communications between tiers in the multi-tier client/server computer infrastructure represented below. Client-layer users have the potential to destroy systems by making mistakes or gaining unauthorized access. Network data may be accessed, critical data can be stolen while being sent, and messages can be changed without permission. A network may experience multiple sites of disruption due to radiation. Malicious malware or denial-of-service attacks may be used by hackers to interfere with the functioning of websites. company data contained in databases or files may be destroyed or altered by someone skilled at breaking into company systems.

Systems fail if computer hardware malfunctions, is improperly maintained, is misused, or is harmed by illegal activity. Computer software may malfunction due to programming errors, incorrect installation, or illegal updates. Computer systems may potentially be affected by power outages, floods, fires, or other natural catastrophes.

If sensitive data is stored on networks and systems that are not within the organization's control, domestic or offshore collaboration with another business increases system susceptibility. Without adequate protection, crucial trade secrets or private information might be revealed, valuable data could be lost, destroyed, or even end up in the wrong hands. These problems are made worse by the growing use of portable mobile devices for commercial computing. Portable devices like mobile phones, smartphones, and laptops are simple to misplace or steal. Smartphones are susceptible to malicious malware and intrusion from outsiders and have the same security flaws as other Internet-connected devices.

Corporate personnel often use smartphones that carry sensitive information such sales figures, client names, phone numbers, and e-mail addresses. Through these gadgets, hackers could be able to access internal business networks.

Internet Security Flaws Because they are essentially accessible to everyone, large public networks like the Internet are more susceptible than internal networks. Because of how big

the Internet is, when abuses do happen, they may be very widely felt. The information systems of the company are even more open to outside interference when the Internet is integrated into the business network.the continual use of fixed Internet addresses, which make it easy to identify them, makes computers linked to the Internet through cable modems or digital subscriber lines more vulnerable to intrusion by outsiders. Hackers have a definite target when they have a set Internet address.

If a telephone service using Internet technology is not delivered through a secure private network, it is more susceptible than the switched voice network. Anyone with access to a network may listen in on talks since the majority of Voice over IP communication over the public Internet is not secured. By overloading VoIP systems with fake traffic, hackers may eavesdrop on conversations or stop phone service.

The prevalence of e-mail, instant messaging, and peer-to-peer file-sharing applications has further enhanced vulnerability. Email attachments might be gateways for harmful malware or unauthorized access to private business networks. Employees have the ability to send private customer information, financial information, and valuable trade secrets to unauthorized individuals through email.

Text messages sent over the open Internet may be intercepted and read by other parties because most consumer IM software do not employ a secure layer. In rare circumstances, online instant messaging may be used as a backdoor to a network that would otherwise be safe. Peer-to-peer file sharing, such as unauthorized music downloading, has the potential to spread harmful software and expose private or business computer information to the public. Wireless Security Challenges

Is it secure to connect to a wireless network in a public place like an airport, library, or other? Depending on how careful you are. Due to the ease with which radio frequency bands may be scanned, even your home's wireless network is at risk. Networks connected through Bluetooth and Wi-Fi may also be hacked by snoopers. The 802.11 standard's local area networks are readily breached by outsiders utilizing laptops, wireless adapters, external antennas, and hacking software. These tools are used by hackers to find vulnerable networks, keep track on network activity, and sometimes get into business or Internet networks.

Stations can easily locate and hear one another thanks to Wi-Fi transmission technology. The service set IDs used to identify the access points in a Wi-Fi network are broadcast repeatedly and are very easy for hackers to intercept using sniffer software.

Many places lack even the most basic defenses against war driving, a technique wherein eavesdroppers attempt to collect wireless network communications while passing by buildings or parking outside.

An attacker who has connected to an access point with the proper SSID is able to access additional network resources. The hacker might, for instance, access other users' computer hard disks, see who else is logged in to the network, and open or copy their data using the Windows operating system.

Many Wi-Fi networks are readily breached by hackers employing sniffer applications to collect an address and get unauthorized access to the network's services[4]–[6]. To compel a user's radio network interface controller to associate with the rogue access point, intruders also utilize the knowledge they have gained to set up rogue access points on a separate radio channel in physically close proximity to users. Once this connection is made, hackers may utilize the rogue access point to steal the usernames and passwords of unwary users.

Viruses, Worms, Trojan Horses, and Spyware Are All Malicious Software

Malware is the term for malicious software programs, which may contain a wide range of dangers including Trojan horses, worms, and computer viruses. A computer virus is a rogue software program that executes when attached to other software programs or data files, often without the knowledge or consent of the user. The "payload" that is delivered by most computer viruses may be quite innocent, such as instructions to show a message or picture, or it can be extremely destructive—destroying programs or data, clogging computer memory, reformatting a computer's hard drive, or causing applications to execute incorrectly—by cluttering computers with data or by deleting programs or data. Typically, viruses move from one computer to another when people do an action, such sending an email attachment or copying a file that is contaminated.

Worms, which are autonomous computer programs that replicate themselves from one computer to other computers through a network, have been the source of the majority of recent assaults. Worms may function independently of other computer program files, unlike viruses, and are less dependent on human activity to propagate from one machine to another. In light of this, it is clear why computer worms propagate considerably faster than computer viruses. Worms obliterate data and programs, impede or even stop computer networks from functioning, and destroy data and programs.

Worms and viruses are often transmitted via the Internet through downloaded software files, files attached to email communications, compromised email messages, online advertisements, and instant messaging. Computerized information systems have also been affected by viruses through "infected" disks or infected devices. Drive-by downloads, which include malware that is downloaded together with a file that a user either willingly or mistakenly requests, are very common nowadays. A hacker could potentially turn a smartphone into a robot in a botnet to send emails and text messages to anyone by installing programs running in the background to monitor user actions. Hackers could also request malicious files without the user's knowledge, delete files, transmit files, delete files, and transmit files. Smartphones are beginning to outsell PCs in sales, and they are being used more and more as payment devices, making them a big target for malware.

Though less prevalent than malware that targets bigger computers, malware that targets mobile devices is still spreading via e-mail, text messaging, Bluetooth, and file downloads from the Web over Wi-Fi or cellular networks. Almost all assaults targeted smartphones running Google's Android operating system, according to research by the security company McAfee, which detected roughly 13,000 distinct types of malware targeting mobile devices in 2012 as opposed to less than 2,000 in 2011. .Because there are so many wireless devices connected to corporate information systems nowadays, mobile device viruses pose substantial risks to workplace computing. Wikis, blogs, and social networking sites like Facebook have all become new distribution channels for malware and spyware.

These programs enable users to upload software code as acceptable content, and that code may run automatically the moment a user views a Web page. Hackers sent phony remarks regarding President Barack Obama on the "Fox News Politics" Twitter account on July 4, 2011. The hackers altered the account's password, making it impossible for Fox to update the messages for many hours.

Symantec, a company that provides internet security, said in 2012 that it had discovered 403 million new and distinct risks from malicious software in 2011, up from 286 million in 2010. According to Symantec, one out of every ten downloads from the Web contains malicious software, and the volume of bad software worldwide surpassed the amount of helpful

software in 2007. Small businesses are the target of 36% of malware today, according to Symantec, since it is more difficult for them to defend themselves against the wide variety of assaults.

A software application known as a "Trojan horse" gives the impression that it is harmless but really performs malicious actions. Due to its lack of replication, the Trojan horse is not a virus in and of itself, but is often used to deliver viruses or other harmful programs onto a computer system. The phrase "Trojan horse" refers to the enormous wooden horse that the Greeks tricked the Trojans into opening during the Trojan War. Greek warriors disguised as horses emerged through the city walls and seized control of the city. The Trojan for Android phones is an illustration of a contemporary Trojan horse. Numerous programs that seem to be legitimate, such as travel and weather apps, really contain this Trojan. Without the user's consent, it automatically puts orders for programs and movies, which might result in people receiving astonishment-inducing large phone bills. More than 100,000 smartphones have been infected by A, which has been found in many app marketplaces.

Attacks using SQL injection have grown to be a serious malware concern. SQL injection attacks use flaws in Web application software with poor coding to insert harmful code into a company's systems and networks. These flaws occur when a web program doesn't correctly check or filter user input on a web page, which might happen while making an online purchase. An attacker may access the database, insert malicious code, or gain access to other networked systems by using this input validation mistake to submit a malicious SQL query to the underlying database. Large Web applications include a large number of user data entry points, each of which presents a potential chance for a SQL injection attack.

There are tools available for hackers to examine Web apps for SQL injection vulnerabilities, which are thought to be present in a substantial proportion of web-facing programs. These programs can find an input field on a Web page form, enter data into it, and then evaluate the response to determine whether it reveals a vulnerability to a SQL injection. Some spyware varieties also function as harmful software. These little applications covertly install themselves on computers in order to track user Web browsing activities and provide advertisements. There are thousands of known types of spyware.

Such spyware is often considered to be unpleasant by users, and some critics are concerned that it may violate users' privacy. Spyware comes in a variety of very evil forms. Keyloggers keep track of each keystroke made on a computer in order to steal software serial numbers, initiate Internet assaults, access e-mail accounts, get passwords to secure computer systems, or gather private data like credit card numbers.

For instance, the Zeus Trojan secretly tracked users' keystrokes as they typed information onto their computers, stealing financial and personal data from online banking and social networking sites. Other spyware applications reset Web browser start pages, reroute search queries, or impede operation by using too much RAM.

Hacking and Data Crime

A hacker is someone who wants to use a computer system without authorization. Although the phrases "hacker" and "cracker" are sometimes used interchangeably in the media, among the hacking community, the term "cracker" generally refers to a hacker with criminal intent. By identifying gaps in the security measures used by websites and computer systems, hackers and crackers are able to obtain illegal access. They often use the Internet's many qualities that make it an accessible and open network.

Theft of commodities and information, as well as system damage and cybervandalism—the purposeful interruption, defacement, or even eradication of a Web site or corporate information system—have all been added to the list of hacker actions that have grown beyond simple system penetration. For instance, online vandals have transformed several MySpace "group" sites—dedicated to topics like animal welfare or home brewing—into online graffiti walls with derogatory text and images.

Fraud and Sniffing

In an effort to conceal their genuine identity, hackers often spoof, or misrepresent, themselves by using phony email accounts or posing as someone else. Using a site that seems to be the intended destination, spoofing may also include rerouting a Web link to a different address from the one that was intended.

For instance, if hackers trick users into visiting a phony website that nearly identically replicates the real one, they may then process orders, thereby stealing both business and private client data from the real site. In our topic on computer crime, we go into further depth on different types of spoofing.

An eavesdropping software known as a sniffer keeps track of information as it moves across a network. Sniffers may be useful in identifying possible network problem areas or criminal activity when used properly, but when used maliciously, they can cause damage and be difficult to catch. Sniffers provide hackers the ability to capture private data from any location on a network, including email messages, corporate files, and secret reports.

Attempted Denial-of-Service

A denial-of-service attack involves sending thousands of erroneous messages or service requests to a network server or Web server in an effort to bring down the whole network. The network gets so many requests that it is unable to handle them all, making it unable to fulfill valid requests. Multiple machines are used in a distributed denial-of-service assault to flood and overburden the network from many launch locations.

As an example, hours after the U.S. When the Department of Justice shut down the file-sharing website Megaupload on January 19, 2012, the hacker group Anonymous launched a massive DDoS assault in retaliation on government and entertainment Web sites. sites run by the FBI, the Department of Justice of the United States, For a significant portion of the day, the U.S. Copyright Office, Universal Music, the Recording Industry Association of America, and the Motion Picture Association of America were rendered inoperable. DoS assaults often result in a Web site being taken down, making it difficult for authorized users to access the site, despite the fact that they do not delete information or gain access to protected parts of a company's information systems. These assaults are expensive for busy e-commerce sites because they prevent users from making purchases while the site is offline. Small and medium enterprises are particularly at risk since their networks are often less secure than those of big organizations.

DDoS attackers often use tens of thousands of "zombie" PCs that have been gathered into a botnet and have been secretly infected with malicious software. By infecting other people's computers with bot software that unlocks a back door that allows an attacker to issue commands, hackers build these botnets. The infected computer then transforms into a slave, or zombie, working for another person's master computer. Once they have infected enough machines, hackers may conduct DDoS assaults, phishing campaigns, or unwanted "spam" email using the resources that the botnet has accumulated. 80 percent of malware and 90% of

spam are distributed worldwide by means of botnets. For instance, the Grum botnet, which was formerly the third-largest botnet in the world, was reputedly in charge of 18% of all spam traffic before it was disabled on July 19, 2012. Grum formerly held control over and infected between 560,000 and 840,00 computers.

Computer Theft

The majority of hacker operations are illegal, and the systems we just discussed are targets for various sorts of computer crime because of their vulnerabilities. George Castro, a citizen of New York, was accused of stealing over $4.5 million from Columbia University over the period of two months in November 2010. Castro had established a payee in the Columbia University Medical Center's accounts payable system that was his personal TD Bank account. The United States defines computer crime. Any criminal offenses that require the use of computer technology for their commission, investigation, or prosecution are defined by the Department of Justice as such. Nobody is aware of the scope of the issue with computer crime, including how many systems are compromised, how many individuals participate in the activity, or the overall monetary loss. The median yearly cost of cybercrime for the firms included in the survey was $5.9 million per year, according to the second annual Cost of Cyber Crime survey by the Ponemon Institute sponsored by ArcSight. Because workers may be involved in the crimes or because the firm worries that revealing its susceptibility would damage its brand, many businesses are hesitant to disclose computer crimes. The introduction of viruses, denial-of-service assaults, service theft, and interruption of computer systems are the types of computer crime that have the most economic impact.

Theft of Identity

Identity theft has increased in severity with the development of the Internet and electronic commerce. Identity theft is a crime when a fraudster steals vital pieces of personal data, including social security numbers, license numbers, or credit card numbers, in order to pose as someone else. The data might be used to provide the burglar fraudulent identification or to get credit, goods, or services in the victim's identity. On the Internet, identity theft is on the rise, and credit card information is a popular target for website hackers. Identity theft victims grew to 11.6 million individuals in 2011, up 13 percent from 2010, according to Javelin Strategy & Research's Identity Fraud Report. However, the overall cost of identity theft has been approximately the same at $18 billion.

E-commerce websites are also great resources for obtaining client contact details, such as name, address, and phone number. Criminals may assume new identities and generate new credit for their own objectives with the use of this information[7]–[10].

One strategy that is gaining popularity is phishing, a kind of spoofing. Phishing is the practice of asking people for private information through fraudulent websites or emails that seem to be from trustworthy companies.

The email asks recipients to update or confirm records by sending their social security numbers, bank account details, credit card numbers, and other private information by replying to the email, inputting the information on a fake website, or dialing a phone number. Several banks, eBay, PayPal, Amazon.com, Walmart, and Amazon.com are among the most popular targets for spoofing. Spear phishing is a highly specialized kind of phishing in which communications seem to be from a reliable source, such a friend or a member of the recipient's own firm. Pharming and the evil twins phishing scam are difficult to catch. Wireless networks, such as those in airport lounges, hotels, or coffee shops, that pose as offering dependable Wi-Fi connections to the Internet are known as evil twins. The fake

network has the exact same appearance as an actual public network. When users unknowingly join on to the network, fraudsters attempt to get their passwords or credit card details.

Even when a person puts the right Web page URL into their browser, phishing leads them to a fake Web page. This is feasible if cybercriminals who engage in pharming obtain access to the Internet address data that Internet service providers keep to facilitate Web surfing and the ISPs' servers are infected with faulty software that enables the hackers to alter the addresses.

According to the sixth annual U.S. According to the Cost of a Data Breach Study, in 2011, each exposed customer record cost U.S. businesses $194. In 2011, the average total cost per event was $5.5 million. Additionally, even though it's difficult to measure, brand harm may be quite serious. The Computer Fraud and Abuse Act, which makes it unlawful to enter a computer system without authorization, was passed by the US Congress in 1986 in response to the danger of computer crime. The laws of most states and of European countries are equivalent. In order to transform the propagation of malware and hacking assaults that render Web sites inoperable into federal offenses, Congress established the National Information Infrastructure Protection Act in 1996. Computer crimes involving intercepting electronic communication, using electronic communication to commit fraud, stealing trade secrets, gaining unauthorized access to stored electronic communications, using e-mail for threats or harassment, and transmitting or possessing child pornography are all covered by U.S. laws such as the Wiretap Act, Wire Fraud Act, Economic Espionage Act, Electronic Communications Privacy Act, and Child Pornography Act. Although it has not yet been passed, a proposed federal Data Security and Breach Notification Act would require firms that handle personal data to use "reasonable" security measures to protect the data and notify anybody impacted by a data breach.

Click Theft

The advertiser normally pays a charge for each click made on an ad shown by a search engine, with the goal of driving customers to their items. When a person or computer program fraudulently clicks on an internet advertisement without intending to find out more about the advertiser or make a purchase, this is known as click fraud. At Google and other websites that use pay-per-click internet advertising, click fraud has grown to be a significant issue. Some businesses pay third parties to click on rivals' advertising falsely in an effort to undermine them by raising their marketing expenses. In order to commit click fraud, software programs may also be deployed, and botnets are often used in this scenario. Search engines like Google make an effort to keep an eye on click fraud, but they have been hesitant to make their attempts to address the issue public.

CONCLUSION

In conclusion, A crucial component of organizational resilience and risk management is information system security. It requires a multi-layered strategy that includes technological controls, rules and regulations, user education and awareness, proactive monitoring, and incident response. Organizations may safeguard their information assets, preserve business continuity, and gain the confidence of stakeholders in an increasingly interconnected and digital world by adopting strong security measures and building a security-conscious culture. Artificial intelligence (AI), machine learning (ML), and behavioral analytics are among the technologies that are increasingly being utilized to improve threat detection, automate security procedures, and spot trends that might be signs of impending assaults. Staying ahead of new threats also benefits from the cybersecurity community's proactive threat intelligence and information sharing.

REFERENCES

[1] K. C. Laudon and J. P. Laudon, "Securing Information Systems," *Manag. Inf. Syst.*, 2016.

[2] B. O. I. Okike and 'Niran Adetoro, "Securing the information systems of libraries and the influence of tech-skills of librarians and users," *Educ. Inf. Technol.*, 2019, doi: 10.1007/s10639-018-9842-z.

[3] V. Jaganathan, P. Cherurveettil, and P. Muthu Sivashanmugam, "Using a prediction model to manage cyber security threats," *Sci. World J.*, 2015, doi: 10.1155/2015/703713.

[4] R. Bruzgiene and K. Jurgilas, "Securing remote access to information systems of critical infrastructure using two-factor authentication," *Electron.*, 2021, doi: 10.3390/electronics10151819.

[5] V. Kumar, R. Telang, and T. Mukhopadhyay, "Optimally Securing Interconnected Information Systems and Assets," *Work. Econ. Inf. Secur. 2007*, 2007.

[6] T. Khanh Dang and T. Tri Dang, "A survey on security visualization techniques for web information systems," *International Journal of Web Information Systems*. 2013. doi: 10.1108/17440081311316361.

[7] A. A.A, "Information Security Management System: Emerging Issues and Prospect," *IOSR J. Comput. Eng.*, 2013, doi: 10.9790/0661-12396102.

[8] K. A. Shcheglov and A. Y. Shcheglov, "New Approach to Data Securing in Information System," *Izv. vysših učebnyh Zaved. Priborostr.*, 2015, doi: 10.17586/0021-3454-2015-58-3-157-166.

[9] T. Coulson, J. Zhu, S. Miyuan, and T. Rohm, "The Price of Security: The Challenge of Measuring Business Value Investments in Securing Information Systems," *Commun. IIMA*, 2015, doi: 10.58729/1941-6687.1277.

[10] S. S. Bawaneh, "Securing Information Technology for Banks and Accounting Information Systems," *Int. J. Appl. Eng. Res.*, 2018.

CHAPTER 12

GLOBAL THREATS: CYBERTERRORISM AND CYBERWARFARE

Dr. Srinivasan Palamalai
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: srinivasanp@presidencyuniversity.in

ABSTRACT:

The rise of the digital age has brought with it unprecedented global threats in the form of cyberterrorism and cyberwarfare. This abstract examines the nature of these threats, their potential consequences, and the challenges faced in countering and mitigating them.Cyberterrorism and cyberwarfare are distinct yet interrelated phenomena that pose significant risks to individuals, organizations, and nations. Cyberterrorism refers to the use of cyber-attacks to instill fear, create chaos, and disrupt critical infrastructure or systems for ideological, political, or social reasons. Cyberwarfare, on the other hand, involves the use of cyber-attacks as a strategic weapon in military or geopolitical conflicts.Malware distribution, denial-of-service assaults, and phishing inquiries are just a few of the cybercriminal tactics we've discussed. Currently, the majority of malware in the globe is produced in China, the United States, South Korea, Russia, and Taiwan. Due to the Internet's worldwide reach, cybercriminals may operate and do havoc anywhere in the globe. Individuals and even whole nation states have become simple targets for politically motivated hacking to carry out sabotage and espionage due to internet vulnerabilities.

KEYWORDS:

Cyberterrorism, Data Breaches, Denial of Service (Dos), Espionage, Hacker Groups, Information Warfare, Malware, Nation-State Actors.

INTRODUCTION

A state-sponsored practice known as "cyberwarfare" involves infiltrating an adversary state or country's systems or networks with the intention of inflicting harm and disruption. Cyberwarfare assaults have generally increased in scope, sophistication, and potential devastation. Every hour, 250,000 probes attempt to enter the networks of the US Department of Defense, and since 2008, cyberattacks on US government agencies have surged by 150 percent. Hackers have taken designs for advanced jet fighters, satellite navigation systems, surveillance drones, and missile monitoring systems throughout the years.

Given how dependent contemporary societies are on the Internet for running their key financial, healthcare, governmental, and industrial institutions, cyberwarfare presents a substantial danger to their infrastructure. A component of cyberwarfare is defending against these kinds of assaults. In the Interactive Session on Organizations, it is discussed how sophisticated and severe recent cyberattacks have become[1]–[3]. EMPLOYEES We often assume that a company's security concerns come from outside the company. In reality, insiders at a firm may seriously compromise security. Employees often have unrestricted access to an organization's systems because they have access to sensitive data and because internal security controls are lax. According to studies, user ignorance is the main reason for network security breaches. Many workers let coworkers use their computer system passwords or forget their own, which undermines the system. Malicious users attempting to gain access to systems may sometimes coerce staff members into disclosing their passwords by posing as

essential customers of the business. This method is referred to as social engineering. A significant source of mistakes that are brought into information systems involves both end users and information systems professionals. End users cause mistakes by inputting inaccurate data or by failing to adhere to the correct procedures for processing data and using computer equipment. As they design, build, and manage new software or keep up with old programs, information systems professionals could make mistakes in their code.

Software Vulnerability

Information systems are always at risk from software faults, which result in enormous productivity losses. Software defects or vulnerabilities have grown in number as a result of the complexity and scale of software systems expanding, as well as market deadline expectations. For instance, between July and December 2011, Citibank doubled the fee for client payments due to a technical glitch in its iPad bill-paying app. Some clients who paid their cable bill or mortgage on their iPads, for instance, really paid twice.

Hidden faults or flaws in the computer code are a serious issue with software. According to studies, it is almost impossible to remove every flaw from complicated programs. The difficulty of the decision-making code is the major cause of errors. Tens of choices leading to hundreds or even thousands of possible routes may be found in a very simple program with few hundred lines. Tens of thousands or even millions of lines of code, each comprising many times the options and pathways of the smaller programs, are often found in important programs inside most organizations, which are typically far bigger.

Larger programs cannot reach zero faults. Simply said, it is impossible to test everything. Fully testing programs with hundreds of options, one of which was created to lie dormant for extended periods before being sped up to cause Iran's nuclear centrifuges to spin erratically out of control. In order to make it seem as if the centrifuges were running regularly while they were really ripping themselves apart, one person covertly recorded what typical operations at the nuclear facility looked like and then played those recordings back to plant personnel.

DISCUSSION

The intricacy of the worm required the expertise of experts. Michael Asante, the National Board's president and chief executive officer, Stunt is seen by Information Security Examiners as a weapon delivery mechanism similar to the B-2 Bomber.

The software program code was very modular, making it simple to alter it to target other systems. Only until it came across a particular set of controllers managing a set of operations exclusive to centrifuge facilities did subnet start to function. Iran accounts for more than 60% of Student-infected machines, and cyber security firm Kaspersky Labs theorizes that the worm was released with official cooperation with the goal of thwarting all or part of Iran's nuclear enrichment program. About one-fifth of Iran's nuclear centrifuges were destroyed by stunt. Iran's capacity to produce nuclear weapons may have been delayed by up to five years as a result of the irreversible damage. The stunted assaults may still be ongoing, according to no one. The stunted software code, according to several specialists who examined it, may contain the seeds for future versions and assaults.

stunted is possible to attack even well protected computer systems that adhere to industry best practices, according Tofino Security research. A well-designed, multi-pronged assault like stunted is practically hard to protect against due to businesses' requirement for connectivity amongst control systems.

Additionally, subnet is not the only cyber weapon active at the moment. Iran, Lebanon, Sudan, Saudi Arabia, Egypt, Syria, and Israel have all had computer infections due to the Flame virus, which was first discovered roughly five years ago. While experts are still examining the malware, information theft and espionage are the major objectives of the assault. Flame may remotely switch on users' microphones to record audio conversations, take screenshots of their computer displays, capture instant messaging chats, gather passwords, search drives for certain files, and record keystrokes and network traffic. Infected computers can become Bluetooth beacons that attempt to download contact information from nearby Bluetooth-enabled devices. The software can also record Skype conversations and send these recordings, along with locally stored documents, to one of several command and control servers that are dispersed throughout the globe. When further instructions are received from these servers, the software waits.

The September 2011 discovery of the Dudu worm also seeks to steal data via scanning computers. Dudu may use entirely distinct modules to infiltrate each of the very few, very particular systems that it attacks globally. One of Dudu's tasks is to grab digital certificates from targeted machines that are needed for authentication in order to make subsequent infections seem safe. It is mainly going unnoticed. Security experts think the same group of programmers that worked on stunted also produced Duruy An act of cyberwarfare against a vital resource, such as the power grid, banking networks, or communications infrastructure, is what security experts and government officials are most concerned about.

The U.S. lacks a clear plan for how the country would react to such a serious cyberattack, and the consequences would probably be catastrophic. Former director of national intelligence Mike McConnell said that the ability to threaten the U.S. money supply is the financial equivalent of a nuclear weapon and that, if even one major American bank were successfully attacked, it would have an order-of-magnitude greater impact on the world economy than the World Trade Center attacks. Numerous security professionals think that American cybersecurity is poorly coordinated. The Pentagon and the National Security Agency are only two of the organizations vying to be the leading organization in the continuing fight against cyberwarfare. In an attempt to clear up this administrative mess, Cybermob, the first government cybersecurity coordination center, was formed in May 2010. President Barack Obama issued executive orders in May 2011 integrating cyber capabilities into American military doctrine, however

Business Value of Control and Security Due to the fact that spending on security is not immediately correlated to sales income, many businesses are hesitant to do so. But safeguarding information systems is so vital to the running of the company that it merits further consideration. Businesses must safeguard their very valuable information assets. Systems often save private data on a person's finances, assets, health, and performance ratings at work. They may also include details on business operations, such as trade secrets, plans for developing new products, and marketing tactics.

Information regarding weaponry, intelligence activities, and military objectives may be stored in government systems. These information assets are very valuable, and their loss, destruction, or fall into the wrong hands might have disastrous repercussions. Systems that stop working as a result of security flaws, natural calamities, or broken technology may have a long-lasting negative effect on a company's finances. According to some experts, if application or data losses are not fixed within three days, 40% of all organizations would not recover.

Inadequate security and control might expose a company to significant legal risk. Businesses must safeguard all of their information assets, including those of their clients, staff members, and business partners. Failure to do so might expose the company to expensive legal action for data theft or disclosure. If a business doesn't take the proper preventive measures to avoid the loss of sensitive information, data corruption, or privacy breach, the organization may be held accountable for the unnecessary risk and damage generated. For instance, the BJ's Wholesale Club was

U.S. FTC for enabling hackers to access its networks and take control of credit and debit card information for unauthorized transactions. BJ's was asked for $13 million by the banks who provided the cards with the stolen data so they could be reimbursed for paying cardholders' fraudulent transactions. Thus, a strong security and control structure may provide a high return on investment by safeguarding firm information assets. Strong security and control can boost worker output and cut down on operating expenses.

Requirements for Electronic Records Management in Law and Regulation

Recent U.S. government requirements that require the protection of data from misuse, disclosure, and unauthorized access are compelling businesses to take security and control more seriously. The preservation and storage of electronic documents, as well as the protection of privacy, are now subject to new regulatory requirements for businesses. The Health Insurance Portability and Accountability Act of 1996 must be followed if you operate in the medical field. HIPAA specifies medical security and privacy policies and practices for streamlining the processing of medical bills and automating the exchange of patient information between payers, providers, and plans. Members of the healthcare sector are required to maintain the confidentiality of patient records for a period of six years. It lays forth requirements for health care providers managing patient information in terms of privacy, security, and electronic transactions. It also sets penalties for privacy violations involving medical information, email disclosure of patient details, or illegal network access[4]–[7].

You must comply with the Financial Services Modernization Act of 1999, sometimes known as the Gramm-Leach-Bliley Act after its legislative supporters, if you work for a company that offers financial services. Financial institutions are required by this law to protect the privacy and security of consumer information. Data must be sent securely and maintained on a secure medium. Additionally, extra security precautions must be taken to safeguard the data both during transmission and storage.

The Public business Accounting Reform and Investor Protection Act of 2002, often known as the Sarbanes-Oxley Act after its authors Senator Paul Sarbanes of Maryland and Representative Michael Oxley of Ohio, must be complied with if you work for a publicly listed business. After the financial crises at Enron, WorldCom, and other publicly traded firms, this Act was created to safeguard investors. Companies and their management are required to protect the truth and integrity of financial information that is utilized both internally and publicly. This has a learning track that goes into great depth on Sarbanes-Oxley.

Fundamentally, Sarbanes-Oxley aims to make sure that internal controls are in place to regulate the gathering and recording of data for financial statements. The Act compels businesses to take information systems security and other measures into account in order to protect the integrity, confidentiality, and accuracy of their data since information systems are used to create, store, and transmit such data. Controls are necessary for any system application that handles crucial financial reporting data to ensure the data are correct.

Controls that protect the company's network, stop unwanted access to systems and data, and guarantee data availability and integrity in the case of a catastrophe or other service interruption are also crucial.

Advanced Computer Forensics and Electronic Evidence

For responding to legal proceedings, security, control, and electronic records management have become crucial. Today, a large portion of the evidence in many civil cases, computer crimes, theft of firm trade secrets, stock fraud, and other crimes is in digital form. Legal proceedings nowadays increasingly depend on evidence that is presented as digital data held on CDs, hard drives, portable storage devices, e-mail, instant messaging, and online transactions, in addition to information from printed or typewritten pages. Currently, the most prevalent kind of electronic evidence is email.

In a court proceeding, an organization is compelled by law to respond to a discovery request for access to material that might be used as evidence. If the corporation is having problems gathering the necessary data or the data are damaged or deleted, the cost of responding to a discovery request might be quite high. For the wrongful deletion of electronic records, courts increasingly impose significant monetary and even criminal penalties.

Electronic documents, email, and other records are neatly structured, accessible, and neither kept for too long nor disposed of too soon when they are subject to a successful electronic document retention policy. Additionally, it demonstrates knowledge of evidence preservation techniques for computer forensics. Data kept on or recovered from computer storage media are collected, examined, authenticated, preserved, and scientifically analyzed in computer forensics in order to make the data admissible as evidence in a court of law. It addresses the following issues:

Data recovery from computers while maintaining the integrity of the evidence processing and safely storing recovered electronic data Invisible to the normal user, ambient data and computer files may be present on computer storage media as electronic evidence. A deleted file on a computer's hard disk might serve as an illustration. There are many ways to retrieve data from computer storage media that has been accidentally destroyed by the user. Experts in computer forensics work to locate such buried data so it may be presented as proof. A firm's procedure for contingency planning should include consideration of computer forensics. Working collaboratively, the CIO, security experts, IT personnel, and company legal counsel should have a strategy in place that can be carried out in the event of a legal necessity.

A Framework For Security And Control Is Being Established

Your information systems won't be dependable and secure even with the greatest security solutions unless you know how and where to install them. You'll need to be aware of the risks facing your business and the controls that are necessary to safeguard your information systems. Additionally, you must create a security strategy and contingency measures in case your information systems fail to function.

Controls Of Information Systems

Controls for information systems may be human or automated and include both general and application controls. The design, security, and usage of computer programs as well as the overall security of data files are governed by broad rules that apply to the whole organization's information technology infrastructure. Overall, general controls are applicable to all computerized applications and are made up of a combination of manual processes, software, and hardware that together form a control environment. Software controls,

hardware controls for physical devices, computer operations controls, data security controls, implementation controls for system processes, and administrative controls are all examples of general controls.

Application controls are specialized controls that are particular to each computerized application, such order processing or payroll. They consist of both automatic and manual steps that guarantee that only permitted data are fully and correctly handled by that application. Input controls, processing controls, and output controls are three categories for application controls. When data enters the system, input controls examine it for correctness and completeness. For input authorization, data conversion, data modification, and error handling, there are particular input controls. Processing safeguards ensure that updated data is correct and full. The accuracy, completeness, and correct distribution of computer processing outputs are ensured by output controls.

Device controls

Verify the physical security of the computer hardware and look for any device malfunctions. Businesses that rely heavily on computers must also plan for backup or continuous functioning in order to provide uninterrupted service. Data security measures make sure that sensitive corporate data files stored on disk or tape are protected from illegal access, modification, or destruction both during usage and storage.

Administration Of Sanctions

Establish formal standards, regulations, practices, and control disciplines to guarantee the effective implementation and enforcement of the organization's general and application controls. In our Learning Tracks, you may discover additional information regarding application and general controls.

Risk Analysis

Your organization has to know which assets need to be protected and how susceptible they are before devoting money to security and information system controls. These queries are addressed by a risk assessment, which also identifies the most economical combination of measures for asset protection. The degree of risk to the company from a particular activity or process that is not effectively regulated is determined by a risk assessment. Not all hazards can be predicted and quantified, but the majority of firms can get some understanding of the risks they are exposed to. Business managers should attempt to ascertain the worth of information assets, places of vulnerability, the likelihood of an issue occurring often, and the potential for harm while collaborating with information systems professionals. It would be foolish to spend $20,000 on the design and maintenance of a control to prevent an incident that is only likely to happen once a year and cause the organization to lose up to $1,000. However, $100,000 spent on a control could be totally fair if that identical occurrence might happen at least once every day, with a potential loss of more than $300,000 each year[8]–[10].

Privacy Policy

its business must create a security strategy to safeguard its assets after you've determined the primary threats to its systems. A security policy is made up of statements that list the information risks, specify the objectives for attaining compliance security, and specify the methods for doing so. What informational resources are the most crucial for the company? Who in the company creates and maintains this data? What security measures are currently in place to safeguard the data? For each of these assets, what amount of risk is management

ready to accept? For instance, is it willing to lose client credit information once every ten years? Or will it create a credit card data security system that can endure the catastrophe that occurs only once every hundred years? To attain this degree of accep risk, management must project the cost. Other rules governing the usage of the company's information resources and which employees have access to its information assets are driven by the security policy. A company's information resources and computing hardware, including desktop and laptop computers, wireless devices, phones, and the Internet, are subject to an accep usage policy that outlines acceptable uses. The policy should make clear the company's stance on user responsibility, privacy, and personal usage of its tools and networks. A good AUP outlines the acceptable and unacceptable behaviors for each user as well as the repercussions of disobedience. For instance, Unilever's security policy mandates that each employee use a device that the firm specifies and utilize a password or another form of identity while connecting into the corporate network.

Identity management requirements are included in security policies as well. Identity management is the process of recognizing legitimate users of a system and regulating their access to system resources using business procedures and technical tools. It covers the procedures and technology for authenticating users and safeguarding their identities, as well as rules for classifying and approving various types of system users. It also specifies which systems or sections of systems each user is permitted access to.

These two illustrations show two data security profiles or patterns that could be present in a personnel system. A user may be subject to limitations on access to certain systems, locations, or data inside an organization, depending on the security profile. The access guidelines presented here apply to two groups of users. All workers that carry out clerical duties, such entering personnel data into the system, make up one group of users. All users that have this kind of profile may update the system, but they are unable to access or alter sensitive areas like income, medical history, or earnings information. Another profile is for a divisional manager, who may see all personnel data fields for his or her division but cannot alter the system, including medical history and compensation.

CONCLUSION

In conclusion, Cyberterrorism and cyberwarfare are serious concerns that might have serious repercussions on a worldwide scale. A multifaceted strategy incorporating global cooperation, strong cybersecurity measures, improved information sharing, and the creation of cutting-edge technology is needed to combat these threats.

The international community can reduce the dangers and assure a more secure digital future by successfully tackling these concerns. Constant monitoring and adaptive protection systems are required due to the cyber terrorists' and cyber warriors' fast growth of technology and tactics. The ability to recognize threats and respond to them may be improved by embracing new technologies like artificial intelligence, machine learning, and behavior analytics. Additionally, continuing efforts in research and development are essential for keeping up with changing cyber threats.

REFERENCES

[1] I. J. Koralnik and K. L. Tyler, “COVID-19: A Global Threat to the Nervous System,” *Annals of Neurology*. 2020. doi: 10.1002/ana.25807.

[2] I. Roca *et al.*, “The global threat of antimicrobial resistance: Science for intervention,” *New Microbes and New Infections*. 2015. doi: 10.1016/j.nmni.2015.02.007.

[3] J. Lessler *et al.*, "Assessing the global threat from Zika virus," *Science*. 2016. doi: 10.1126/science.aaf8160.

[4] R. Kean and G. Ramage, "Combined Antifungal Resistance and Biofilm Tolerance: the Global Threat of Candida auris," *mSphere*, 2019, doi: 10.1128/msphere.00458-19.

[5] M. G. Guzman *et al.*, "Dengue: A continuing global threat," *Nat. Rev. Microbiol.*, 2010, doi: 10.1038/nrmicro2460.

[6] M. Ermann, "Dealing with 'new fears': Psychoanalysis facing global threats and terrorism," *Int. Forum Psychoanal.*, 2020, doi: 10.1080/0803706X.2020.1836398.

[7] J. Podgorski and M. Berg, "Global threat of arsenic in groundwater," *Science (80-.).*, 2020, doi: 10.1126/science.aba1510.

[8] J. Zheng, "SARS-coV-2: An emerging coronavirus that causes a global threat," *Int. J. Biol. Sci.*, 2020, doi: 10.7150/ijbs.45053.

[9] P. C. Saha and K. Phadke, "COVID-19: Global Threat," *Int. J. Recent Surg. Med. Sci.*, 2020, doi: 10.1055/s-0040-1713060.

[10] C. J. Vörösmarty *et al.*, "Global threats to human water security and river biodiversity," *Nature*, 2010, doi: 10.1038/nature09440.

CHAPTER 13

DISASTER RECOVERY PLANNING AND BUSINESS CONTINUITY PLANNING

Dr. Ranganathan Kumar
Associate Professor, Master in Business Administration (General Management),
Presidency University, Bangalore, India.
Email Id: drsenthilkumar@presidencyuniversity.in

ABSTRACT:

Disaster recovery planning (DRP) and business continuity planning (BCP) are critical components of organizational resilience in the face of unforeseen disruptions. This abstract explores the importance of DRP and BCP, their objectives, key considerations, and strategies employed to ensure the continuity of business operations during and after a disaster.Disasters, whether natural or man-made, can have devastating effects on organizations, resulting in financial losses, reputational damage, and operational disruptions. DRP and BCP aim to minimize the impact of such disruptions and facilitate the timely recovery of critical business functions.It involves strategies such as data backups, redundant systems, and offsite storage, ensuring that organizations can restore critical data and resume operations as quickly as possible. Disaster recovery plans outline step-by-step procedures for responding to emergencies, conducting damage assessments, and initiating recovery processes.

KEYWORDS:

Backup Systems, Business Impact Analysis, Crisis Management, Data Recovery, Emergency Response, Incident Management.

INTRODUCTION

If you own a company, you must prepare for unforeseen circumstances that might affect your information systems and your ability to do business, such as power outages, floods, earthquakes, or terrorist attacks. Planning for disaster recovery creates strategies for resuming computer and communications services once they have been interrupted. Disaster recovery plans are largely concerned with the technical aspects of maintaining systems, such as whether data should be backed up and how backup computer systems or disaster recovery services should be maintained.For instance, MasterCard has a backup computer facility in Kansas City, Missouri, that may be used in case of an emergency at its main facility in St. Louis.

Many businesses use disaster recovery companies, such as Comdisco Disaster Recovery Services in Rosemont, Illinois, and SunGard Availability Services, with headquarters in Wayne, Pennsylvania, rather than building their own backup facilities. These catastrophe recovery companies provide hot sites with extra computers scattered around the nation so that paying companies may operate their vital programs in an emergency. For instance, it takes Champion Technologies only two hours to move its enterprise systems from Houston to a SunGard hot site in Scottsdale, Arizona, where it provides chemicals needed in oil and gas operations[1]–[3].

Planning for business continuity focuses on how the organization can resume operations following a calamity. The business continuity plan identifies key business processes and establishes strategies for addressing mission-critical operations in the event of system failure.

For instance, Deutsche Bank, which offers asset management and investment banking services in 74 different nations, has a solid business continuity strategy that it is constantly updating and improving. In order to coordinate plans addressing loss of premises, staff, or crucial systems so that the business may continue to run should a catastrophic catastrophe happens, it maintains full-time teams in Singapore, Hong Kong, Japan, India, and Australia. The strategy from Deutsche Bank makes a distinction between procedures necessary for maintaining business operations and those required for crisis management, and it works in tandem with the organization's disaster recovery preparations for its data centers.In order to identify the systems and business processes that are most important to the organization, business managers and information technology professionals must collaborate on both kinds of plans. To determine the company's most crucial systems and the effects a system outage will have on the business, they must undertake a business impact study. Management must decide which areas of the company need to be restored first and how long the firm can operate without its systems.

The Impact Auditing Has

How can management know that the security and controls of the information systems are efficient? Organizations must carry out thorough and methodical audits to provide an answer to this issue. An MIS audit looks at both the controls over specific information systems and the company's broader security environment. Using automated audit tools, if necessary, the auditor should run tests and follow a sample transaction's path through the system. Data quality may be examined during the MIS audit.

Technology, processes, paperwork, training, and staff are all examined during security audits. To assess how the technology, information systems, and business people would react to an attack or catastrophe, a comprehensive audit will even mimic one.

All control flaws are ranked and included in the audit along with a probability estimate. The effect of each danger on the economy and the organization is then evaluated. It has a provision for reporting such flaws to management and for management's reaction. Management is required to create a strategy for addressing substantial control gaps.

DISCUSSION

Technologies And Tools for Protecting Information Resources

Businesses may safeguard their information resources using a variety of methods. These technologies manage user identities and guard against illegal access to systems and data while also assuring system uptime and software quality.

The Management and Authentication of Identities

Large and mid-sized businesses have intricate IT infrastructures and a wide variety of systems, each with its own user base. By giving each user a distinct digital identity for system access, identity management software simplifies the process of keeping track of all these users and their system rights. Additionally, it has capabilities for user authentication, user identity protection, and access management. A biometric fingerprint scanner on this computer allows for quick and safe access to networks and information. Biometric identification is now being used by certain new PC models to authenticate users. A user has to be approved and authenticated before they may access a system. The capacity to verify that a person is who they say they are is referred to as authentication. Utilizing passwords that are only known by authorized users is a common way to create authentication. A password is used by an end user to enter a computer system and may also be used to access certain systems and data. But

users often trade passwords, forget them, or choose weak passwords that are simple to guess, which jeopardizes security. Overly strict password policies reduce staff productivity. Employees commonly use shortcuts when they have to change difficult passwords regularly, such as selecting passwords that are simple to guess or leaving their credentials at their workstations where they are visible to others. Additionally, passwords may be "sniffed" if sent across a network or taken through social engineering.

Some of these issues are resolved by new authentication technologies including tokens, smart cards, and biometric authentication. A token is a tangible object that serves as a user's identity proof, much like an identification card. Tokens are tiny devices with regularly changing passcodes that commonly fit on key rings. A smart card is a small, credit card-sized object containing a chip that is pre-formatted with data and access permissions. The data on the smart card is interpreted by a reader device, which then grants or refuses access.

To give or reject access, biometric authentication employs technologies that scan and interpret distinctive human characteristics like fingerprints, irises, and voices. The foundation of biometric authentication is the measurement of a physical or behavioral characteristic that distinguishes one person from others. It determines if there are any disparities between a person's distinctive traits and the recorded profile by comparing them to a person's unique attributes, such as their fingerprints, face, or retinal picture. Access is given if the profiles match. Many PC laptops come with fingerprint scanners, and other models come with built-in cameras and face recognition software. Fingerprint and facial recognition technologies are only starting to be employed for security purposes.

Avoidance Software, Intrusion Detection Systems, And Firewalls

It would be very risky to connect to the Internet without defense against viruses and intrusions. Antivirus software, intrusion detection systems, and firewalls are becoming fundamental corporate tools.

Firewalls

Unauthorized users cannot access private networks because of firewalls. An apparatus that regulates the flow of incoming and outgoing network traffic is known as a firewall. Although firewalls may also be used to separate one area of a company's network from the rest of the network, they are often positioned between the organization's private internal networks and untrustworthy external networks, such as the Internet. Before allowing a user access to a network, the firewall serves as a gatekeeper, checking their credentials. Incoming traffic's identities, IP addresses, programs, and other details are identified by the firewall. This data is compared to the access rules that the network administrator set into the system. Unauthorized communication into and out of the network is stopped by the firewall.

No incoming request may directly access private network resources since the firewall, which is often located on a dedicated computer distinct from the rest of the network in big enterprises, prevents this. Static packet filtering, stateful inspection, Network Address Translation, and application proxy filtering are a few of the technologies used for firewall screening. In order to offer firewall protection, they are commonly used in conjunction. Data packets that are flowing back and forth between the trusted network and the Internet are subjected to packet filtering, which looks at certain fields in the headers while inspecting each packet separately. Numerous other assaults may be missed by this screening mechanism. By evaluating whether packets are a part of an ongoing conversation between a sender and a recipient, stateful inspection adds an extra layer of security. It creates states to keep track of data over several packets. Whether a packet is a part of an authorized discussion or is seeking

to establish a genuine connection determines whether it will be accepted or refused. When static packet filtering and stateful inspection are used, network address translation may provide an additional layer of security. To stop sniffer programs running outside the firewall from learning the IP addresses of the organization's internal host computer and exploiting that knowledge to breach internal systems, NAT conceals the addresses.

Application proxy filtering looks at the packets' application content. Outside-originating data packets are blocked by a proxy server, which also inspects them and sends a proxy to the opposite side of the firewall. When a user outside the business wishes to speak with a user within the company, the outside user first "talks" to the proxy program, which then speaks with the internal computer of the company. Similar to this, a user of a computer within the company uses the proxy to communicate with a computer outside. An administrator must keep up-to-date internal rules that specify which users, programs, or addresses are accepted or disallowed in order to build a reliable firewall. Firewalls should be considered one component of a comprehensive security strategy since they may hinder, but not entirely prohibit, outsiders from accessing your network.

Systems for detecting intrusions

Commercial security vendors increasingly provide intrusion detection technologies and services in addition to firewalls to safeguard against unauthorized network access attempts and suspicious network traffic. In order to continuously identify and prevent offenders, intrusion detection systems include instruments for continuous monitoring positioned at the weakest points or "hot spots" of corporate networks. If the system discovers a suspicious or unusual occurrence, it generates an alert.

Scanning software analyzes for patterns suggestive of well-known computer attack techniques, such using poor passwords, verifies if crucial files have been deleted or changed, and issues alerts for vandalism or system management faults.

Monitoring software looks at events as they happen to find active security assaults. A network's most sensitive area may be configured to be shut down if it receives illegal traffic using the intrusion detection tool.

Software for antivirus and antispyware

Every PC must have anti-malware protection in defensive technology strategy for both consumers and organizations. Malware, such as Trojan horses, spyware, adware, and computer viruses, is prevented, found, and eliminated by antivirus software. However, the majority of antivirus programs only work against malware that was already well-known at the time the programs were built. The antivirus software must be updated regularly to stay functional[4]–[6].

Systems for Unified Threat Management

Security manufacturers have incorporated firewalls, virtual private networks, intrusion detection systems, Web content filtering, and antispam software into a single appliance to aid enterprises in cost reduction and management. Unified threat management systems are the name given to these complete security management tools. UTM products are accessible for all network sizes, while being originally targeted for small and medium-sized organizations. Leading UTM manufacturers include Check Point, Fortinet, and Crossbeam, while networking manufacturers like Cisco Systems and Juniper Networks integrate some UTM functionality in their products.

Wireless Networks Security

Wired Equivalent Privacy, the first security standard created for Wi-Fi, is not particularly successful since its encryption keys are quite simple to decipher. However, if users remember to activate it, WEP offers a little degree of protection. When accessing internal company data, businesses may further increase Wi-Fi security by combining it with virtual private network technologies. The 802.11i protocol, which replaces WEP with more robust security measures, was completed in June 2004 by the Wi-Fi Alliance industry trade organization. The new standard employs significantly longer keys that are constantly changing rather than the static encryption keys used in WEP, making them more difficult to decipher. To guarantee that only authorized users access the network, it also uses an encrypted authentication system with a central authentication server.

A Public Key Infrastructure for Encryption

Many companies employ encryption to safeguard the digital data they keep, physically move, or transmit online. The process of converting ordinary text or data into encrypted text, which can only be read by the sender and the intended recipient, is known as encryption. A secret numerical code known as an encryption key is used to encrypt data, turning plain text into cipher text. The recipient needs to decode the message. SSL and S-HTTP are two techniques for encrypting network data on the Web. Client and server computers may control encryption and decryption operations as they interact with one another during a secure Web session thanks to Secure Sockets Layer and its descendant Transport Layer Security. Another technique for encrypting data moving over the Internet is called Secure Hypertext Transfer technique, but it just encrypts individual messages, while SSL and TLS are intended to create a secure connection between two computers.

The Internet client browser software and servers come with the ability to create secure sessions. The key and degree of security to employ are decided upon by the client and server. All communications sent and received during a secure connection between a client and a server are encrypted.

Symmetric key encryption and public key encryption are two further encryption techniques. In symmetric key encryption, the sender and receiver create a single encryption key and deliver it to the recipient so they both have access to the same key, resulting in a secure Internet connection. The bit length of the encryption key serves as a gauge for its security. A common key today will be 128 bits long. All symmetric encryption methods have the drawback of requiring the key to be exchanged in some way between senders and receivers, making it accessible to third parties who may be able to intercept and decode the key.

Public key encryption, a more secure kind of encryption, employs two keys: one shared and one completely private, as in 8.6. Data encrypted with one key may be decoded using only the second key since the keys are mathematically connected. Communicators first generate unique pairs of private and public keys in order to transmit and receive messages. The private key has to be kept a secret while the public key is stored in a directory.

With the recipient's public key, a communication is encrypted by the sender. The receiver uses his or her private key to decode the message after receiving it. Digital certificates are data files that are used to verify users' identities and the ownership of electronic assets for the security of online transactions. Using a certificate authority, a trusted third party, a digital certificate system verifies a user's identity. Many CAs exist both domestically and internationally, such as Symantec, GoDaddy, and Comodo.

A digital certificate user's identity is offline verified by the CA. This data is entered into a CA server, which creates an encrypted digital certificate with the owner's public key and identity information. The public key's ownership by the specified owner is verified by the certificate. The CA publishes its own public key and makes it accessible in print or potentially online. An encrypted communication's receiver may access the sender's public key and identity details by decrypting the digital certificate that was attached to the message using the CA's public key, confirming that it was really issued by the CA. The receiver may send an encrypted response using this data. A credit card user and a merchant, for instance, might use the digital certificate system to verify that their digital certificates were issued by a reputable and approved third party before exchanging data. In e-commerce, public key infrastructurethe use of public key cryptography in conjunction with a CAis increasingly extensively employed.

Securely Ensure System Availability

Companies need to take extra precautions to make sure that their systems and apps are always accessible as they depend more and more on digital networks for revenue and operations. Fault-tolerant computer systems have been used for many years by businesses with critical applications requiring online transaction processing, such as those in the airline and financial services industries. 100 Digital certificates help establish the identity of people or electronic assets. By offering safe, encrypted internet communication, they defend online transactions. % of accessibility. Online transactions are processed as they are entered, and the computer processes them right away. Every second, many updates to databases, reports, and information requests take place.

Reliable hardware, software, and power supply components are included in fault-tolerant computer systems to provide a continuous, uninterrupted service environment. Fault-tolerant computers may detect hardware problems and switch to a backup device automatically thanks to sophisticated software routines or self-checking logic integrated into their circuitry. These computers' components may be taken out and fixed without affecting the computer system. Both fault tolerance and high-availability computing aim to reduce downtime, however fault tolerance should be separated from high-availability computing. Downtime is the term for times when a system is not functional. However, fault tolerance offers continuous availability and the complete removal of the recovery time, while high-availability computing aids businesses in recovering rapidly after a system breakdown.

For businesses that perform a lot of e-commerce or rely on digital networks for their internal processes, high-availability computing systems are a minimal necessity. High-availability computing necessitates backup servers, processing spread over several servers, large-capacity storage, and effective business continuity and disaster recovery procedures. The computer infrastructure of the company must be very strong and have expandable processing, storage, and bandwidth. Recovery-oriented computing is a method that researchers are looking at as a means to help computers recover even more quickly from errors. As part of this effort, systems that recover fast are designed, and capabilities and tools are implemented to make it easier for operators to identify the root causes of problems in multi-component systems and promptly fix their errors. Deep Packet Inspection for Network Traffic Control Have you ever attempted to utilize the university network and discovered it to be really slow? It can be as a result of other pupils downloading music or watching YouTube on the network. Applications that use a lot of bandwidth, such file-sharing programs, Internet phone services, and online videos, may choke business networks and slow them down, resulting in poor performance. For instance, Ball State University in Muncie, Indiana, discovered that a tiny percentage of students were utilizing P2P file-sharing tools to download music and videos, which caused a slowdown in the network.

Deep packet inspection, a technology, assists in resolving this issue. DPI analyses data files and separates out low-priority web content while giving business-critical information a greater priority. It determines whether a single data packet may travel to its destination or should be stopped or delayed while more crucial traffic moves forward based on the priorities set by a network's operators. Ball State was able to restrict the volume of file-sharing traffic and give it a significantly lower priority by using a DPI system from Allot Communications.

The preferred network traffic at Ball State accelerated. Many firms, particularly small enterprises, lack the resources or knowledge necessary to independently offer a secure high-availability computing environment. Many security tasks may be delegated to manage security service providers that keep an eye on network activity and conduct vulnerability assessments and intrusion detection. Leaders in MSSP services include Secure Works, BT Managed Security Solutions Group, and Symantec.

Security Concerns For Mobile Digital Platform And Cloud Computing

Although cloud computing and the newly developed mobile digital platform have the potential to provide significant advantages, they also present new risks to the security and dependability of the system. We now go through some of these difficulties and how to handle them.

Cloud-based security

When processing occurs on the cloud, the organization that owns the sensitive data retains accountability and responsibility for its security. It's crucial to comprehend how the cloud computing company sets up its services and controls the data. The Interactive Session on Technology explains how security lapses may occur in even well developed Web-based businesses. Highly dispersed cloud computing is prevalent. Large distant data centers and server farms that provide business services and data management for several corporate customers are where cloud applications are housed. Cloud computing companies often disperse work to data centers around the world where it can be completed most effectively in order to save money and keep expenses down. You may not be aware of the exact location of your data while using the cloud.

Since cloud computing is distributed, it is difficult to monitor unauthorized behavior. Almost all cloud service providers protect the data they handle during transmission using encryption, including Secure Sockets Layer. However, it's crucial to make sure that any data that are saved on devices that simultaneously contain data from other businesses are secured. Businesses require their systems to stay operational around-the-clock, but cloud service providers haven't always been able to meet this demand. The cloud services of Amazon.com and Salesforce.com have suffered outages on several times during the last few years, causing millions of users' commercial activities to be interrupted[7]–[10].

Users of the cloud must guarantee that, regardless of where their data are hosted, they are safeguarded to the standards set by their organizations. They should specify that the cloud provider must store and handle data in accordance with those countries' privacy laws in order to do so. Customers of cloud services should learn how the cloud provider separates their corporate data from that of other businesses and request evidence that the encryption methods are reliable. It's crucial to understand the cloud provider's response plans in the event of a catastrophe, including if and how quickly your data can be fully restored. Users of the cloud should also inquire about the cloud providers' willingness to submit to outside audits and security certifications. Before concluding a contract with a cloud provider, these sorts of restrictions might be included in the service level agreement.

Mobile Platform Security

Mobile devices must be protected against infection, theft, loss due to accident or theft, unauthorized access, and hacking attempts if they are to perform various computer-related tasks.Special security measures are needed for mobile devices that access business networks and data. Businesses should ensure that mobile devices are covered by their corporate security policy, along with extra information on how mobile devices should be maintained, secured, and utilized. They will require mobile device management technologies to lock down or wipe lost or stolen devices so they can't be hacked, authorize all devices in use, keep accurate inventory records on all mobile devices, users, and apps, and regulate application updates. Companies should establish policies defining the needed software and processes for remote access to business systems, as well as the allowed mobile platforms and software applications. When it's feasible, businesses should encrypt communication. Every user of a mobile device should be compelled to utilize the smartphone's password function. Products like Kaspersky, Lookout, and Droid Security are available for mobile security.

Some businesses demand that staff only use cellphones that are provided by the firm. Because they operate inside their own secure system, BlackBerry handsets are regarded as the safest. However, in order to increase employee availability and productivity, businesses are increasingly enabling staff members to use their own cellphones for work, including iPhones and Android devices. Protective software packages, like those from Good Technology, are now available to separate personal material on mobile devices owned by individuals from business data stored on such devices.

Security For Software Quality

Organizations may increase system quality and dependability in addition to providing effective security and controls by using software metrics and thorough software testing. Software metrics are quantitative measures that serve as an objective evaluation of the system. By continuously using metrics, the information systems division and end users are able to assess the system's performance and spot issues as they arise. Examples In 1998, South Africa's top ISP was MWEB, which had been founded in 1997. It has made a name for itself as a provider of cutting-edge network and service infrastructure as well as first-rate customer care. MWEB now serves 320,000 consumers, including home users, small, medium, and big businesses, as well as corporations. ISP of the Year was given to MWEB during the 2010 My Broadband Conference in Johannesburg. The prize was given based on both client happiness and the effectiveness of its numerous broadband offerings.

In January 1998, MWEB Business, its commercial branch, was established. MWEB Business takes pleasure in being a business partner that is well situated to tap into the potential of Web-based technologies across the board. MWEB Business assists businesses by: Manage corporate data in a manner that improves operations and provides actual value. Integrate current systems with the Internet to bridge the technological, strategic, and financial gaps for the firm. Create, oversee, and upkeep solutions that include all facets of Internet access, website creation and hosting, broadband and wireless apps, e-commerce, and consulting services. Manage internal communication amongst colleagues, as well as between clients and suppliers.

Publicizing its ambitions for the South African Internet market has advanced MWEB. According According to MWEB CEO Rudi Jansen, the firm has to enhance the caliber of its network, which is a concern with both the MWEB and Telkom networks. MWEB employs AVG Internet protection to provide its consumers the finest online protection despite having a less-than-ideal network architecture. The following features are available to MWEB

customers who use AVG Internet Security: Additionally, MWEB automatically shields users from unsolicited email and email-borne malware. Its virus filter makes sure that only email that is free of viruses is sent to customers' inboxes by automatically removing emails from known sources of malware.

In order to protect their ADSL connections from bandwidth theft and account misuse, MWEB encourages its clients to restrict incoming connections to network ports that are often utilized by hackers. Despite the extensive security services provided by MWEB, a number of MWEB Business users had their account information exposed because hackers posted their login and password information online. Initial indications indicated that up to 2,390 MWEB business digital subscriber line subscribers may have been impacted. On October 25, 2010, the business made the security breach public. The self-service management system used by MWEB company to furnish and oversee company accounts that have not yet been moved to the MWEB network seems to have been compromised by hackers.

In the past, MWEB Business sold Uncapped & Fixed IP ADSL services from Internet Solutions. These services were supplied and managed by MWEB utilizing an Internet Solutions-provided Web-based administration interface. The majority of legacy services that have already been transferred, as well as all new Business ADSL services offered after April 2010, employed MWEB's internal authentication mechanisms, which were completely unaffected by this event. MWEB reacted to the hacking incident immediately. About 1,000 customers on the Internet Solutions network had to be transferred from the previous server, which had been hacked, according to Jansen. The majority of the clients had just switched over to MWEB's IPC network, even though the network was rapidly protected. As an additional security step, MWEB would also be contacting these customers to change their passwords. Since their usernames and passwords had been reset and regenerated, Jansen was eager to point out that no personal information was lost and that none of MWEB's clients had experienced any losses. He continued by saying that MWEB effectively fends off 5,000 assaults per day.

CONCLUSION

In conclusion, for guaranteeing the resilience and continuation of corporate activities in the case of catastrophes, DRP and BCP are crucial. Organizations may reduce downtime, safeguard important assets, and uphold consumer confidence by anticipatorily detecting hazards, creating thorough strategies, and using technological improvements. In a company environment that is always changing, keeping prepared requires ongoing evaluation, testing, and adaption of strategies. A comprehensive strategy to DRP and BCP is required because to the complexity of threats, such as cyberattacks and data breaches, which is rising. Cybersecurity measures must be a key component of an organization's planning process. To protect data and systems during and after a catastrophe, it is essential to implement strong security controls, carry out frequent vulnerability assessments, and create incident response plans.

REFERENCES

[1] H. F. Cervone, “Disaster recovery planning and business continuity for informaticians,” *Digital Library Perspectives*. 2017. doi: 10.1108/DLP-02-2017-0007.

[2] A. F. Fahmawati and D. Urumsah, “Faktor-Faktor yang Mempengaruhi Disaster Recovery Planning dan Business Continuity Planning (Studi Empiris pada Perguruan Tinggi di Indonesia),” *Simp. Nas. Akunt. XIX*, 2016.

[3] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, "Integrated business continuity and disaster recovery planning: Towards organizational resilience," *Eur. J. Oper. Res.*, 2015, doi: 10.1016/j.ejor.2014.09.055.

[4] J. Cook, "A Six-Stage Business Continuity and Disaster Recovery Planning Cycle," *SAM Adv. Manag. J.*, 2015.

[5] Ashok Kumar, "Business continuity plan," *South Asian J. Eng. Technol.*, 2020, doi: 10.26524/sajet.2020.2.2.

[6] J. Pinta, "Disaster recovery planning as part of business continuity management," *Agris On-line Pap. Econ. Informatics*, 2011.

[7] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, "Building organizational resilience in the face of multiple disruptions," *Int. J. Prod. Econ.*, 2018, doi: 10.1016/j.ijpe.2017.12.009.

[8] S. Snedaker and C. Rima, *Business Continuity and Disaster Recovery Planning for IT Professionals: Second Edition*. 2013. doi: 10.1016/C2012-0-06206-0.

[9] S. Hamadah, "Cloud-based disaster recovery and planning models: An overview," *ICIC Express Lett.*, 2019, doi: 10.24507/icicel.13.07.593.

[10] Y. Muflihah and A. P. Subriadi, "A basic element of it business continuity plan: systematic review," *J. Inform.*, 2019, doi: 10.26555/jifo.v12i1.a8370.