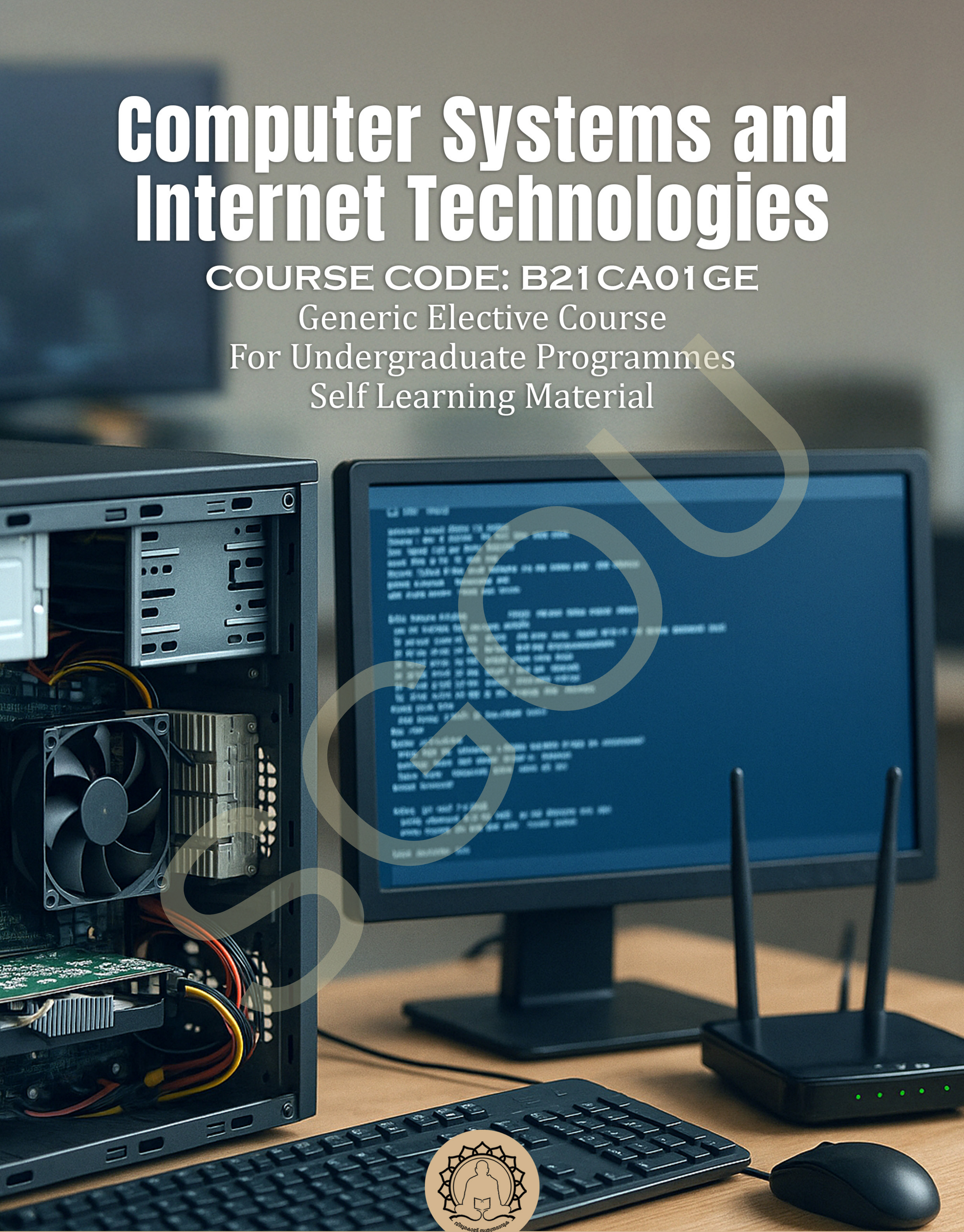
Computer Systems and Internet Technologies

COURSE CODE: B21CA01GE

Generic Elective Course
For Undergraduate Programmes
Self Learning Material



SREENARAYANAGURU
OPEN UNIVERSITY

SREENARAYANAGURU OPEN UNIVERSITY

The State University for Education, Training and Research in Blended Format, Kerala

SREENARAYANAGURU OPEN UNIVERSITY

Vision

To increase access of potential learners of all categories to higher education, research and training, and ensure equity through delivery of high quality processes and outcomes fostering inclusive educational empowerment for social advancement.

Mission

To be benchmarked as a model for conservation and dissemination of knowledge and skill on blended and virtual mode in education, training and research for normal, continuing, and adult learners.

Pathway

Access and Quality define Equity.

Computer Systems and Internet Technologies

Course Code: B21CA01GE

Generic Elective Course
For Undergraduate Programmes
Self Learning Material
(With Model Question Paper Sets)

വിദ്യകൊണ്ട് സ്വതന്ത്രരാവുക

SREENARAYANAGURU
OPEN UNIVERSITY

SREENARAYANAGURU OPEN UNIVERSITY

The State University for Education, Training and Research in Blended Format, Kerala

വിദ്യകൊണ്ട് സ്വതന്ത്രരാവുക

SREENARAYANAGURU
OPEN UNIVERSITY

COMPUTER SYSTEMS AND INTERNET TECHNOLOGIES

Course Code: B21CA01GE
Generic Elective Course
For Undergraduate Programmes

Academic Committee

Dr. Aji S.
Sreekanth M. S.
P. M. Ameera Mol
Dr.Vishnukumar S.
Shamly K.
Joseph Deril K. S.
Dr. Jeeva Jose
Dr. Bindu N.
Dr. Priya R.
Dr. Ajitha R. S.
Dr. Anil Kumar
N. Jayaraj

Development of the Content

Anjitha A.V., Dr. Kanitha D.K.,
Shamin S., Subipriya laxmi S.B.N.,
Aswathy V.S., Suramya Swamidas P.C.,
Sreerekha V.K., Greeshma P.P.,
Dr. Jennath H.S., Lekshmi A.C.

Review and Edit

Dr. Vijayalakshmi A.

Linguistics

Dr. Vijayalakshmi A.

Scrutiny

Anjitha A.V., Dr. Kanitha D.K.,
Shamin S., Subipriya laxmi S.B.N.,
Aswathy V.S., Sreerekha V.K.,
Greeshma P.P., Lekshmi A.C.

Design Control

Azeem Babu T.A.

Cover Design

Jobin J.

Co-ordination

Director, MDDC :
Dr. I.G. Shibi
Asst. Director, MDDC :
Dr. Sajeevkumar G.
Coordinator, Development:
Dr. Anfal M.
Coordinator, Distribution:
Dr. Sanitha K.K.

Scan this QR Code for reading the SLM on a digital device.

Edition
May 2025

ISBN 978-81-986991-4-5

9 788198 699145

www.sgou.ac.m

YouTube

Visit and Subscribe our Social Media Platforms

MESSAGE FROM VICE CHANCELLOR

Dear learner,

I extend my heartfelt greetings and profound enthusiasm as I warmly welcome you to Sreenarayanaguru Open University. Established in September 2020 as a state-led endeavour to promote higher education through open and distance learning modes, our institution was shaped by the guiding principle that access and quality are the cornerstones of equity. We have firmly resolved to uphold the highest standards of education, setting the benchmark and charting the course.

The courses offered by the Sreenarayanaguru Open University aim to strike a quality balance, ensuring students are equipped for both personal growth and professional excellence. The University embraces the widely acclaimed "blended format," a practical framework that harmoniously integrates Self-Learning Materials, Classroom Counseling, and Virtual modes, fostering a dynamic and enriching experience for both learners and instructors.

The University aims to offer you an engaging and thought-provoking educational journey. The Generic Elective course "Computer Systems and Internet Technologies" has been carefully crafted to equip undergraduate learners with essential knowledge of modern computing systems and internet-based technologies. This course introduces the core concepts of computer hardware, software, and networking, while exploring practical applications of internet tools through engaging examples and real-world scenarios. The Self-Learning Material has been meticulously crafted, incorporating relevant examples to facilitate better comprehension.

Rest assured, the university's student support services will be at your disposal throughout your academic journey, readily available to address any concerns or grievances you may encounter. We encourage you to reach out to us freely regarding any matter about your academic programme. It is our sincere wish that you achieve the utmost success.

Warm regards.
Dr. Jagathy Raj V.P. 01-04-2025

Contents

BLOCK
01

Computer System Fundamentals

Unit 1

Fundamentals of Computer

Learning Outcomes

On completion of this unit, the learner will be able to:

- Identify different types of computers based on size, purpose, and data processing.
- Recall the functions of hardware and software in a computer system.
- Name the types of computer memory and storage devices.
- Recognise examples of portable and mobile devices.

Background

Understanding the fundamentals of computers is essential in today's technology-driven world. We rely on computers for communication, education, work, entertainment, and countless other daily tasks. Learning about how computers have evolved, how they function, and how to choose the right system helps individuals use technology more effectively and make informed decisions, whether buying a new device, troubleshooting issues, or using software for work or study.

A student attending online classes needs to know whether a tablet, laptop, or desktop suits their needs based on performance, portability, and cost. Similarly, a small business owner must understand basic hardware and software concepts to manage data securely and efficiently. This foundational knowledge empowers users to adapt to new technologies confidently and use them to their full potential.

Keywords

Supercomputer, Virtual memory, Solid-state drives, Hard Disk Drive, Digital Literacy, Hardware and Software, System Selection.

Discussion

1.1.1 Evolution of Computers

The development of computers has progressed from simple calculation tools like the abacus to today's advanced AI-powered machines. It started with mechanical calculators and the Analytical Engine, then moved to electronic computers in the 20th century.

- **First Generation (1940–1956): Vacuum Tubes**

These computers, which used vacuum tubes and magnetic drums, were large, slow, and consumed a lot of power. Programming was complex until the concept of the stored program by John von Neumann improved functionality.

- **Second Generation (1956–1963): Transistors**

Transistors replaced vacuum tubes, making computers smaller, faster, cheaper, and more reliable. Programming became easier with high-level languages like FORTRAN and COBOL.

- Third Generation (1964–1971): Integrated Circuits

Integrated Circuits (ICs) allowed many transistors to be embedded on a single chip, increasing speed, reducing size and cost, and improving reliability. Key models included the IBM System/360.

- **Fourth Generation (1971–2010): Very Large Scale Integration**

This generation used microprocessors and semiconductor memory, enabling the development of personal computers and laptops. The Intel 4004 marked the start of this era.

- **Fifth Generation (2010–Future): Ultra Large Scale Integration**

Focused on Artificial Intelligence, these computers can process natural language, learn from experience, and handle multitasking more efficiently, making them more user-friendly and intelligent.

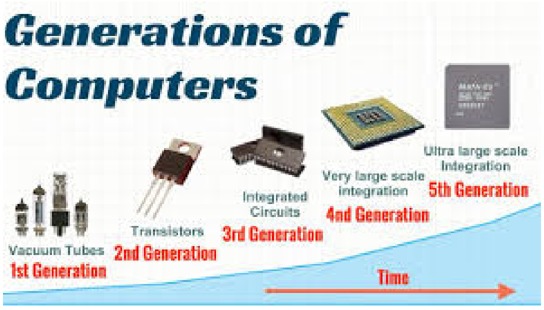


Fig 1.1.1 Core components in various generations of computers

1.1.2 Types of Computers

A computer is like a high-tech tool that takes raw, unprocessed data and turns it into useful information. It does this by following a set of instructions or programs given by the user. Whether the input is numbers, text, images, or something else, the computer processes this information according to the instructions and produces meaningful and useful output. This ability allows computers to handle everything from basic calculations to complex data analysis, making them incredibly versatile for tasks in science, business, education, and entertainment. There are mainly three major classifications of computers: they are

1. Classification based on size and power
2. Classification based on purpose
3. Classification based on the kind of data they process

1.1.2.1 Classification by Size and Power

Computers come in various sizes and can be grouped into four main types: supercomputers, mainframe computers, minicomputers, and microcomputers.

- **Supercomputers**

Supercomputers are the fastest and most powerful computers, and they are known for their incredible speed, as measured in petaFLOPS. These massive machines can be as big as a small building and use multiple processors to solve complex problems, supporting hundreds of users at once. Developed in the 1960s by pioneers like Seymour Cray, they have advanced from simple systems to sophisticated clusters that run on specialised Linux versions. Their high performance comes at a steep cost, ranging from $200,000 to over $100 million.

Supercomputers are used for various complex tasks, including scientific exploration to study diseases and develop treatments, military technology for designing and testing new equipment, and gaming to ensure smooth online experiences. They also help meteorologists predict weather patterns and natural disasters, support research in nuclear and space sciences, and assist Hollywood in creating realistic animations and visual effects.

- **Mainframe Computers**

Mainframe computers are the reliable workhorses of the tech world, designed to handle large amounts of data and multiple tasks simultaneously. Unlike supercomputers that focus on speed, mainframes are excellent at supporting many users across networks, making them vital for large organisations and government agencies. They are commonly used in banks and hospitals for essential functions like payroll and patient record management, and they support many communication and reservation systems. Notable examples include the IBM System z9 and Fujitsu ICL VME, which operate on robust systems like z/OS.

Mainframes play a crucial role in various applications, including processing ATM transactions, credit and prepaid card transactions, and online transactions for shopping and banking. They also provide cloud storage infrastructure, manage hospital patient records, and help airlines with travel reservations. Mainframes are used to process and analyse survey data, such as census counts and elections, ensuring accurate and timely results.

- **Minicomputers**

Minicomputers, also known as midrange computers, appeared in the late 1960s as a cost-effective alternative to mainframes. They provided more power than personal computers but less than mainframes. Designed to handle specific control tasks for mid-sized organisations, minicomputers could support multiple users, usually up to six at a time. Although they are less common now, having been largely replaced by more advanced personal computers, they were appreciated for their simpler construction and lower cost.

Minicomputers were used for various practical tasks, including managing switchboard operations, handling specialised graphics and computer design tasks, enabling time-sharing for multiple users, monitoring manufacturing processes, and managing laboratory equipment.

- **Microcomputers**

Fig. 1.1.2 Types of Microcomputers

Microcomputers, or personal computers (PCs), are the versatile and affordable devices found in homes, schools, and small offices, designed for individual use. Emerging in the 70s and 80s with the advent of microprocessor chips, PCs became a popular choice due to their lower cost and capability for personal and small business tasks, contrasting with the larger, more expensive systems of the time. While they offer less memory and processing power than supercomputers and mainframes, their introduction paved the way for a shift towards more personal and cost-effective computing. By the mid-1990s, PCs had become ubiquitous, marking the beginning of the mobile age and the rise of smaller devices, including wearables. Today, they operate on various systems like Windows, Mac OS X, Linux, iOS, and Android.

1.1.2.2 Classification by Purpose (General Purpose, Special Purpose)

Computers come in two main types based on what they're designed to do: general-purpose and special-purpose.

a. General-purpose Computers

General-purpose computers are incredibly versatile and are what most people use every day. These computers can handle a wide range of tasks, from processing documents and performing calculations to managing data and accounting. They're commonly found in offices, schools, and various other settings because they can adapt to many different uses. Examples of general-purpose computers include mainframes, minicomputers, microcomputers, and laptops. Each of these is designed to handle a broad spectrum of functions, making them a staple in many work and learning environments.

b. Special-purpose Computers

Special-purpose computers are built with a very specific function in mind. They're designed to do just one job and nothing else. Because they are programmed with fixed instructions at the time of manufacturing, they're highly efficient at their designated task. For example, robots used in factories are specialised for production tasks, while mobile phones are dedicated to communication. Other examples include calculators, which handle mathematical operations, digital watches, and computers used in petrol pumps. Each of these devices excels at its particular function, demonstrating how technology can be tailored to meet specific needs.

1.1.2.3 Classification based on the kind of data they process

Computers can also be categorised based on the kind of data they process, falling into three main types: digital, analogue, and hybrid.

1. Digital computers

Digital computers are the most common ones we encounter daily. They work with discrete data, which is represented in binary code (0s and 1s). This allows them to handle everything from numbers to letters. They operate based on simple "ON" and "OFF" states. Think of digital devices like televisions with digital volume controls, digital watches, or calculators; these are all examples of digital computers in action.

2. Analogue computers

Analogue computers deal with continuous data and are designed to measure physical quantities like temperature, pressure, or speed. They're often used for specific tasks and are very good at what they do because they're tailored for particular functions. Analogue devices include thermometers that use mercury to show temperature, petrol pumps that measure fuel flow, and scales that weigh parcels.

3. Hybrid computers

Hybrid computers bring together the best of both digital and analogue worlds. They are built to handle both types of data by integrating digital and analogue components into one system. While they can be pricier, their ability to process diverse data makes them highly valuable. An example is in a hospital's Intensive Care Unit, where analogue devices might monitor a patient's vital signs, and then the information is converted into digital data for immediate alerts and analysis.

1.1.3 Computer Software and Hardware

Computer software and hardware are the two fundamental components that make a computer system function effectively, each playing a distinct yet interdependent role. Hardware refers to the physical elements of a computer, such as the CPU, memory, hard drives, and peripherals like keyboards and monitors, that provide the necessary infrastructure for computing. On the other hand, software encompasses the programs and operating systems that run on this hardware, instructing it on how to perform specific tasks and processes.

1.1.3.1 Software

Software is the brain of our modern devices, turning them from mere metal and plastic into smart, functional tools. It consists of instructions and data that direct computers and gadgets on what to do, acting as a bridge between users and hardware. Whether you're writing a document, browsing the web, or playing a game, software makes these activities possible. Software comes in two main types: system software and application software.

1. System Software

System software is a group of programs that help manage and coordinate the hardware and software resources of a computer. It creates a reliable environment where other software applications can run smoothly. System software can be broken down into the following two subcategories.

a. Operating Systems

An operating system is a key component of system software that oversees and coordinates a computer's hardware and software resources. It serves as a bridge between the user and the hardware, offering an intuitive interface and handling essential functions such as process management, memory allocation, file system organisation, and device control. Popular examples of operating systems are Windows, macOS, and Linux.

b. Utility Programs

Utility software is a type of system software that plays a crucial role in keeping your computer running smoothly. It helps you with tasks like analysing, configuring, optimising, and maintaining your computer's performance. Instead of focusing on user tasks like regular applications, utility software works behind the scenes to ensure the computer's infrastructure is in good shape. Some common examples of utility software include tools for formatting disks, handling files, managing hardware drivers, compressing files, checking for viruses, defragmenting disks, and backing up data. Two main classifications of utility software are Language Processors and Device Drivers.

A **language processor** is a program that helps translate and understand code written in programming languages. It takes human-readable code and converts it into something the computer can understand and execute.

There are different types of language processors:

Compilers convert the whole program at once, **Interpreters** process the code line by line, and **Assemblers** convert low-level code (like assembly language) into machine code.

A **device driver** is a small program that allows the operating system to communicate with hardware devices, like printers, keyboards, or graphics cards. It acts as a translator between the hardware and the software, making sure the operating system can use the device correctly. For example, if you connect a printer to your computer, the printer driver allows the computer to send print jobs to the printer in a language it understands. Without the right driver, the device may not work properly or at all.

2. Application Software

Application Software refers to programs designed to help users perform specific tasks or activities, such as writing documents, managing data, or browsing the internet. It operates on top of system software and is aimed at improving user productivity or providing entertainment.

Classification of Application Software:

a. **General-purpose Software:** Used for a wide range of tasks by various users.

Examples: Microsoft Word, Google Chrome, Excel.

b. **Special-purpose Software:** Designed for specific tasks or industries.

Examples: AutoCAD (design), Adobe Photoshop (image editing), Oracle Database (data management).

The main difference between system software and application software lies in their role and necessity for the computer's operation. System software, such as the operating system, is essential because it manages the computer's hardware and ensures it runs smoothly. Without system software, the computer wouldn't function. In contrast, application software is not required for basic computer operations but is used to perform specific tasks that enhance user experience, like writing documents or playing videos. While the computer can operate without application software, it wouldn't provide the tools needed for tasks like productivity or entertainment.

1.1.3.2 Hardware

Hardware refers to the physical parts of a computer, including components like the CPU, memory, input/output devices, and storage. The CPU acts as the brain, processing instructions and coordinating tasks with other parts, while memory (RAM and ROM) provides data storage. Input devices, like the keyboard and mouse, allow users to interact with the computer, and storage devices, such as hard drives and SSDs, save data permanently for future use.

1.1.4 Computer Memory

Memory is a vital component of any computer, storing programs and data for processing. It consists of multiple types of storage, each with varying speeds and costs, that work together to ensure efficient data handling. The main memory interacts directly with the CPU, managing active tasks but cannot store all data. Computers use a tiered memory system to balance speed and cost, with auxiliary storage providing large capacity but slower access, while cache memory offers faster access at a higher cost.

1.1.4.1 Register Memory

Register memory is located in the CPU and is the fastest type of memory, designed to hold essential data and instructions for immediate processing. Registers act as a temporary storage area for data that the CPU needs quickly, providing rapid access and facilitating efficient processing.

1.1.4.2 Cache Memory

Cache memory is a high-speed memory unit placed between the CPU and the main memory to speed up data access. It stores frequently used data and instructions, allowing the CPU to retrieve them quickly, reducing the time spent waiting for data from slower main memory. Cache memory significantly enhances system performance by matching the CPU's faster processing speed.

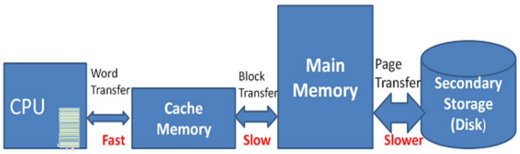


Fig.1.1.3 Cache Memory

1.1.4.3 Auxiliary Memory/ Secondary Storage

Auxiliary or secondary memory provides storage for data and programs that are not actively used by the CPU. It has a larger capacity than primary memory but slower access speeds. Examples include hard disk drives (HDDs), solid-state drives (SSDs), USB flash drives, optical discs (CDs/DVDs), and magnetic tapes. These storage devices are essential for long-term data storage, backups, and file transfers.

1.1.4.4 Virtual Memory

Virtual memory is a memory management technique that allows a computer to use part of the hard drive as if it were additional RAM. This technique enables the system to run larger applications or multiple programs even when physical RAM is limited, enhancing multitasking capabilities and system performance.

1.1.5 Secondary Storage

Storage devices are essential for keeping your computer's files and information safe and readily accessible. Hard drives offer substantial space for long-term data storage, while solid-state drives (SSDs) provide faster performance, enhancing your computer's speed and responsiveness. Optical drives, which handle CDs and DVDs, are useful for media playback and backups. Portable options like USB flash drives and external hard drives allow you to easily transport your data. Understanding these different storage devices helps you effectively manage your files, ensuring that your information is secure and easy to retrieve whenever needed.

1. HDD

A Hard Disk Drive (HDD) is a crucial component inside your computer

responsible for storing all your data. Mounted in a drive bay and connected to the motherboard via cables such as ATA, SCSI, or SATA, the HDD features spinning platters within a protective case. A magnetic head moves across these platters to read and write data. The hard drive holds everything from your operating system and installed programs to personal files, making it essential for the smooth operation and storage of your computer's information. Figure 1.1.3 shows the image of the HDD.

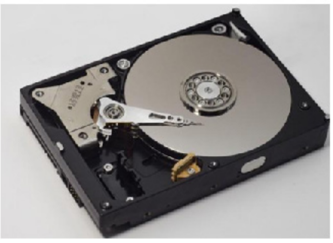


Fig. 1.1.4 Image of hard drive

2. SSD

A Solid State Drive (SSD) is a storage device that uses non-volatile memory to keep and access data, which means it doesn't lose your information when the power is off. Unlike traditional hard drives, SSDs don't have moving parts, so they can access data much faster, work quietly, and are generally more reliable and energy efficient. Figure 1.1.4 shows the image of the SSD.

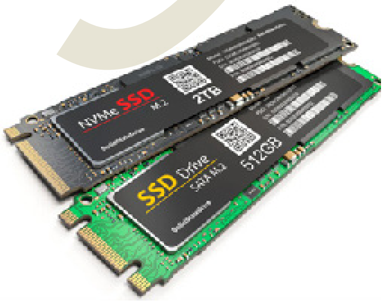


Fig. 1.1.5 Image of SSD

A Solid State Drive (SSD) is a modern storage device that uses non-volatile memory to retain data even when the power is off. Unlike traditional hard drives, SSDs have no moving parts, allowing for faster data access, quieter operation, and greater reliability and energy efficiency. Recently, SSDs have become more affordable and are popular for both desktops and laptops, as well as smaller devices like netbooks. SSDs connect through the SATA interface, offering speeds up to 750 MB/s, or the faster PCIe interface, with speeds up to 4 GB/s for the latest PCIe M.2 models. External SSDs, connecting via eSATA, FireWire, or USB, are convenient for backing up files, adding extra storage, and transferring large data between computers.

1.1.6 Portable Devices

Portable devices are compact and lightweight electronic gadgets specifically designed to be easily carried from place to place. Unlike traditional stationary electronics such as desktop computers or home entertainment systems, portable devices are mobile by nature, making them convenient for use in a wide range of environments at home, in the office, during travel, or even outdoors. These gadgets usually run on rechargeable batteries, enabling users to use them for long periods without needing to be plugged into a power source. For example, students use tablets and laptops for online classes, digital textbooks, note-taking, and research, both in and outside the classroom.

1.1.6.1 Key Characteristics of Portable Devices

1. **Mobility:** These devices are built for easy portability, allowing users to carry them effortlessly in a pocket, bag, or by hand, which makes them ideal for on-the-go use.

2. **Battery Powered :** They usually operate on rechargeable batteries, giving users the freedom to use them without needing a constant power supply.
3. **Wireless Connectivity :** Portable gadgets commonly feature wireless options like Wi-Fi, Bluetooth, and mobile networks, enabling seamless internet access and device pairing without cords.
4. **Touchscreen or Compact Controls:** They are equipped with intuitive touch screens or minimal buttons that make navigation and operation simple and efficient, even in compact designs.
5. **Compact Size:** Their lightweight and space-saving build ensures they can be easily transported and stored without hassle.

1.1.6.2 Types of Portable Devices

a. Smartphones

Smartphones are multifunctional devices that provide a wide range of services, including voice calls, messaging, internet browsing, and multimedia functions like photography and video streaming. Smartphones typically have powerful processors, high-resolution cameras, and a variety of apps to cater to personal, educational, and professional needs. Popular examples of smartphones are the Apple iPhone and Samsung Galaxy S series.

b. Tablets

Tablets have larger screens than smartphones and are ideal for reading, drawing, streaming, and light office work. Devices such as the iPad and Samsung Galaxy Tab are popular examples of tablets.

c. Laptops and Ultrabooks

These portable computers are powerful enough for heavy tasks like programming and video editing. Ultrabooks are lighter for travel. Devices such as the MacBook Air and Dell XPS are examples of this category.

d. Portable Gaming Consoles

These handheld devices allow users to play high-quality games anywhere without needing a TV or traditional console. Popular examples include the Steam Deck and PlayStation Portal.

e. Smartwatches and Fitness Trackers

Worn on the wrist, they track health stats, show notifications, and support fitness goals by syncing with smartphones, with examples including the Apple Watch and Fitbit Charge.

f. E-Readers

E-readers are lightweight devices designed for comfortable digital reading using e-ink displays that mimic paper, such as the Amazon Kindle and Kobo Clara.

g. Portable Media Players & Bluetooth Speakers

These devices focus on music and media playback. Bluetooth speakers let users enjoy loud, wireless sound. For instance, the iPod Touch provides portable media access, while Bluetooth speakers like the JBL Clip deliver loud, wireless sound.

h. Wearable Tech (AR/VR Headsets, Smart Glasses)

These high-tech wearables provide immersive experiences by blending virtual or augmented reality into real life, with devices like the Meta Quest 3 offering VR interaction and Ray-Ban Meta Glasses integrating smart features into everyday eyewear.

1.1.7 Mobile Devices

Mobile devices are compact gadgets designed for on-the-go convenience, fitting easily into your pocket. Unlike traditional computers, they lack disk drives and instead rely on built-in memory or small memory cards for storing apps and data. These devices can connect wirelessly to the Internet, enabling you to chat, email, and browse the web from virtually anywhere. Despite their small screens, they are usually vibrant and bright. Common types include smartphones, personal digital assistants (PDAs), e-book readers, handheld computers, portable media players, and digital cameras. Each device is crafted to enhance connectivity and entertainment, seamlessly integrating into your daily life.

1.1.7.1 PDAs to Smartphones

The PDA revolutionised our digital lives by making technology portable and convenient, moving us away from bulky desktop computers. This compact device allowed us to manage schedules, tasks, and stay connected while on the go, greatly simplifying daily life. Modern PDAs have evolved with advancements in AI, now handling everything from reminders and calendars to controlling smart home devices. Despite their productivity benefits, PDAs can face issues like limited battery life and occasional AI misinterpretations. Nevertheless, they continue to be invaluable tools for both personal and professional use. As technology progresses, PDAs are expected to become even more efficient and integrated, enhancing our connectivity and organisation. When selecting a PDA, consider its features, compatibility with other devices, and app support to maximise its benefits.

A smartphone is a marvel of modern technology, compact yet packed with features. This pocket-sized device combines a high-definition display, a versatile camera, ample storage, and a touchscreen, making it an all-in-one gadget. It supports a wide range of apps for various tasks, from checking emails and browsing the web to playing music and watching movies. The built-in GPS helps with navigation, while voice commands simplify typing on the small keyboard. With its capability to capture photos and videos, and a multitude of apps for fitness tracking, star identification, document management, and gaming, the smartphone is a powerful and versatile tool that keeps you connected and entertained on the go.

1.1.8 Selecting a System Specification Based on Requirements

When choosing a computer, start by thinking about how you'll use it. If you're into gaming or graphic design, you'll need a powerful machine with a strong graphics card, plenty of memory, and a fast processor to keep things running smoothly. On the other hand, if your computer time mostly involves browsing the web or checking emails, you don't need all the bells and whistles.

Check the specs of the programs you want to run; video editing software needs a beefy processor and lots of RAM to handle large files. It's also wise to plan for the future. Technology changes fast, so picking a computer with a bit of extra power can help it stay relevant longer. Look for features like extra memory slots or more storage space that will make upgrades easier down the road.

Lastly, think about your budget. High-end computers can be pricey, but sometimes, spending a bit more on things like an SSD can boost performance without breaking the bank. By matching your needs with what you can afford, you'll get a computer that's both practical and budget-friendly.

Recap

- A **computer** is an electronic device that processes data and performs tasks using hardware and software.
- Computers have **evolved** through five generations, from vacuum tubes to artificial intelligence and ultra-large scale integration.
- They are **classified** by size (supercomputers to microcomputers), by purpose (general vs. special), and by data type (digital, analog, hybrid).
- **Hardware** includes physical parts like CPU, RAM, storage devices; **software** includes system software (OS, utilities) and application software.
- Memory types include **registers**, **cache**, **main memory**, **secondary storage**, and **virtual memory**.
- **Portable and mobile devices** include smartphones, tablets, laptops, smartwatches, e-readers, and more.
- When **choosing a computer**, match system specifications to your needs, software requirements, and budget.

Objective Questions

1. What is the physical part of a computer called?
2. Which generation of computers used vacuum tubes?
3. What is the main component that processes data in a computer?
4. What is the smallest and fastest type of memory?
5. Which type of computer is used for complex scientific calculations?
6. What is the name of the software that manages hardware resources?
7. What type of computer is designed for a specific task only?
8. Which memory type is used to expand RAM using the hard disk?
9. What storage device uses flash memory and has no moving parts?
10. What type of computer was introduced with microprocessors?

11. What software is used for tasks like word processing or browsing?
12. Which company introduced the 4004 microprocessor?
13. What is the most common type of computer used at home?
14. What is a computer that handles both analog and digital data called?
15. Which memory is faster: RAM or Cache?

Answers

1. Hardware
2. First
3. CPU
4. Register
5. Supercomputer
6. Operating System
7. Special purpose
8. Virtual
9. SSD
10. Microcomputer
11. Application
12. Intel
13. PC
14. Hybrid
15. Cache

Assignments

1. **Explain the evolution of computers** from the first to the fifth generation, highlighting the major technological advancements in each stage.
2. **Differentiate between hardware and software** with suitable examples for each.
3. **Classify computers based on their size and power.** Describe each type with examples and uses.
4. **Compare general-purpose and special-purpose computers.** Provide at least two real-world examples of each.
5. **Define and differentiate** between the following types of memory: Register, Cache, Main Memory, and Auxiliary Memory.

Reference

1. Rajaraman, V. (2018). *Fundamentals of Computers* (6th ed.). PHI Learning Pvt. Ltd.
2. Sinha, P. K., & Sinha, P. (2007). *Computer Fundamentals* (6th ed.). BPB Publications.
3. Norton, P. (2003). *Introduction to Computers* (6th ed.). McGraw Hill.
4. Brookshear, J. G., & Brylow, D. (2021). *Computer Science: An Overview* (13th ed.). Pearson Education.
5. Null, L., & Lobur, J. (2018). *Essentials of Computer Organization and Architecture* (5th ed.). Jones & Bartlett Learning.

Suggested Reading

1. Rajaraman, V. (2010). Fundamentals of Computers (6th ed.). PHI Learning.
2. Sinha, P. K., & Sinha, P. (2017). Computer Fundamentals (8th ed.). BPB Publications.
3. Norton, P. (2017). Peter Norton's Introduction to Computers (8th ed.). McGraw Hill.
4. Brookshear, J. G., & Brylow, D. (2020). Computer Science: An Overview (13th ed.). Pearson.

Unit 2

Operating System Concepts

Learning Outcomes

On completion of this unit, the learner will be able to:

- Identify the basic functions of an operating system, such as process and memory management
- Describe the role of the kernel in controlling hardware and system resources
- Recognise how file systems organise and store data on storage devices
- List examples of real-time operating systems and mobile operating systems used in various devices
- Recall how the operating system manages network connections and ensures data security

Background

To understand operating systems is to understand the backbone of any computing device. Whether it's a laptop, smartphone, or embedded system, the OS governs how hardware is utilised and ensures that applications run smoothly. Learning about operating systems enables users to troubleshoot issues, optimise performance, and enhance security. Real-life examples include troubleshooting why your smartphone is slow (possibly due to inefficient process management) or why a company's network is vulnerable (poor security management).

When you install a new application on your laptop, the operating system uses its process and file management capabilities to allocate resources and store the app data. If the OS is not well optimised or secure, it could lead to slow performance, data loss, or security breaches, which makes the understanding of OS principles invaluable for both users and IT professionals. Similarly, understanding file system management helps in managing large datasets, such as in cloud services or when working with large amounts of media data.

Keywords

Kernel, Process Management, File System, Real-Time Operating System (RTOS), Security Management

Discussion

1.2.1 Operating Systems

An operating system (OS) is fundamental software that acts as the backbone of a computer system, managing both hardware and software resources. It is an intermediary between users and the computer hardware, facilitating communication and operational efficiency. Without an OS, users would struggle to interact with their devices, as the OS handles all interactions required among various resources by executing commands. The OS manages processes, memory, devices, and files, ensuring that the computer operates smoothly and efficiently. It also provides a user interface, which can be either command-line based or graphical, allowing users to interact with the system in a more intuitive manner. Furthermore, security and protection are important components of an OS, safeguarding the system against unauthorised access and ensuring the integrity and confidentiality of data. By managing these various aspects, the OS enables users to run applications and perform tasks seamlessly, making it an indispensable part of modern computing.

1.2.2 Operating Systems Components

The following are the important OS components: (Refer fig 1.2.1)

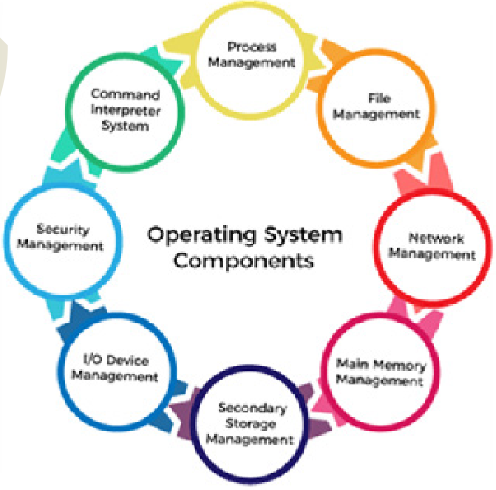


Fig 1.2.1 Operating System Components

1.2.2.1 Kernel

The kernel is the fundamental part of the operating system that interacts directly with the hardware. It is responsible for managing system resources like the CPU, memory, I/O devices, and security. The kernel controls process execution, memory allocation, hardware communication, and system calls, ensuring the smooth and efficient operation of the system. There are different types of kernels, including monolithic, microkernel, and hybrid, each with its design and method of interacting with the system components.

1.2.2.2 Process Management

Process management ensures that the operating system can execute multiple processes simultaneously, allowing for multitasking. The OS handles the lifecycle of processes, which includes their creation, scheduling, and termination. The process scheduler assigns CPU time to processes based on priorities, ensuring fair and efficient resource allocation. The OS maintains a process control block (PCB) to track each process's state, resources, and execution context. It also handles inter-process communication (IPC) and synchronisation, allowing processes to safely exchange data and coordinate execution.

1.2.2.3 File System Management

File system management deals with how files and directories are organised, stored, and accessed on storage devices. The OS provides mechanisms for creating, deleting, reading, and writing files. It uses a hierarchical file system structure to help users and programs manage data efficiently. File systems like NTFS, FAT32, and ext4 dictate how data is structured, allocated, and accessed. The OS ensures security through file permissions, controlling who can access or modify files. It also keeps track of file metadata, such as file size, type, ownership, and modification times.

1.2.2.4 Command Interpreter

The command interpreter, often referred to as the shell, is a crucial interface for users to interact with the operating system. It interprets user commands and executes them, acting as a bridge between the user and the kernel. Command interpreters can be text-based, such as the Unix shell or the Windows Command Prompt, or graphical, such as the Windows GUI. They allow users to run programs, manage files, and control system processes. Shells support scripting and automation, enabling users to write scripts to perform repetitive tasks efficiently.

1.2.2.5 System Calls

System calls provide an interface between user-level applications and the OS kernel. They are essential for programs to request various services from the operating system, such as reading or writing files, creating processes, allocating memory, and handling I/O operations. System calls abstract the underlying hardware and OS complexities, providing a secure and controlled means for applications to access system resources. Common system calls include read(), write(), fork(), exec(), and exit().

read() - This system call is used to read input from files or standard input.

write() - This system call is used to output data to files or standard output.

fork() - This system call is used to create a new process.

exec() - This system call will run a new program in place of the current program.

exit() - This system call is used to stop the execution of a process.

They are critical for ensuring that user programs do not directly access hardware resources, which could lead to system instability.

1.2.2.6 Signals

Signals are used for communication between processes or to notify processes of specific events. The operating system sends signals to a process to indicate events like errors, interrupts, or requests to terminate. For example, a signal might notify a process that a resource is available, that it should stop, or that it encountered an exception like division by zero. Processes can handle signals via signal handlers, allowing them to respond appropriately. Signals enable asynchronous event handling and are vital for real-time applications, error management, and system monitoring.

1.2.2.7 Network Management

Network management in the operating system involves configuring and maintaining communication between different devices in a network. The OS ensures efficient data transmission, connectivity, and security by managing network protocols like TCP/IP. It monitors network traffic, configures IP addresses, and handles connections to wired and wireless networks. Network management utilities within the OS allow administrators to diagnose and troubleshoot issues, configure firewalls, and ensure secure data transfer through encryption and authentication protocols.

1.2.2.8 Security Management

Security management in the OS is crucial for safeguarding data and protecting against unauthorised access. It involves user authentication (verifying user identity) and authorisation (defining user permissions for access to resources). The OS enforces security policies by implementing access controls, file permissions, and encryption. It also supports secure communication protocols (e.g., SSL/TLS) to protect data during transmission. Security management includes monitoring system activities for abnormal behaviour, defending against malware, and applying updates to fix vulnerabilities, ensuring the integrity and confidentiality of system resources.

1.2.2.9 I/O Device Management

I/O device management is responsible for coordinating the communication between the operating system and external devices like printers, disk drives, and USB devices. The OS uses device drivers to provide a standardised interface for interacting with diverse hardware. It manages data transfer between the CPU and peripherals, ensuring that data is sent and received accurately and efficiently. I/O management also involves buffering, where data is temporarily stored before it is transferred, as well as spooling, which helps manage tasks like printing by queuing them for sequential processing.

1.2.2.10 Secondary Storage Management

Secondary storage management involves managing non-volatile storage devices such as hard drives, solid-state drives (SSDs), and optical disks. The OS handles tasks like partitioning storage, formatting drives, and allocating space for files. It also ensures data integrity through error detection and correction mechanisms. In addition to these functions, the OS supports data organisation through file systems and performs maintenance tasks such as defragmentation and backups. Effective secondary storage management ensures that data is reliably stored and efficiently retrieved, contributing to the overall system performance.

1.2.2.11 Main Memory Management

Main memory management is responsible for efficiently allocating and deallocating RAM to processes. The OS ensures that each active process has the necessary memory resources, using techniques such as paging, segmentation, and virtual memory. Paging allows the OS to break memory into fixed-size blocks and allocate space for processes, while segmentation allows for logical division based on process needs. Virtual memory extends the system's addressable memory by swapping data between RAM and secondary storage, allowing large applications to run even with limited physical memory. Effective memory management minimises fragmentation, prevents memory leaks, and optimises system performance.

1.2.3 Common Operating Systems

Operating systems (OS) are essential software that manage computer hardware and software resources, providing a stable environment for applications to run. Different operating systems have been developed to meet various user needs, each with its unique features and strengths. The most common operating systems include Microsoft Windows, macOS, Linux, and Unix. These OSs are widely used in personal computers, servers, and other devices, offering a range of functionalities and user experiences. Understanding these common operating systems helps users choose the right one for their needs and enhances their ability to interact effectively with different computing environments. (Refer Fig 1.2.2)

Fig 1.2.2 Examples of Operating Systems

1.2.3.1 Microsoft Windows

Microsoft Windows is one of the most widely used operating systems in the world, known for its user-friendly interface and extensive software compatibility. It offers a range of versions tailored to both personal and professional use, making it a versatile choice for various computing needs.

1.2.3.2 macOS

macOS, developed by Apple Inc., is the operating system for Mac computers. Renowned for its sleek design and seamless integration with other Apple products, macOS provides a robust and intuitive user experience, which is recommended by many creative professionals and general users alike.

1.2.3.3 Linux

Linux is an open-source operating system that is highly customisable and widely used in servers, desktops, and embedded systems. It is known for its stability, security, and flexibility, with various distributions like Ubuntu, Fedora, and CentOS catering to different user requirements.

1.2.3.4 Unix

Unix is a powerful, multi-user operating system that has influenced many other OSs, including Linux and macOS. Unix is often used in academic, research, and enterprise environments, providing a reliable platform for complex computing tasks. It is well known for its stability and scalability.

1.2.4 Real-Time Operating System (RTOS)

A Real-Time Operating System (RTOS) is designed to build real-time applications that process data as it comes in, typically without buffering delays. The primary purpose of an RTOS is to ensure computing tasks are performed within strict time constraints, making it crucial for applications that require immediate processing. RTOSs are commonly used in embedded systems, such as automotive controls, industrial robots, and medical devices, where response times are critical. They prioritise tasks to ensure high-priority tasks are executed first using preemptive multitasking. This ensures that the most critical operations are performed first, maintaining system stability and reliability. Moreover, RTOSs are optimised for minimal latency and high determinism, which are essential for maintaining system performance under varying loads. The efficiency and reliability of RTOS make them indispensable in environments where timing is critical.

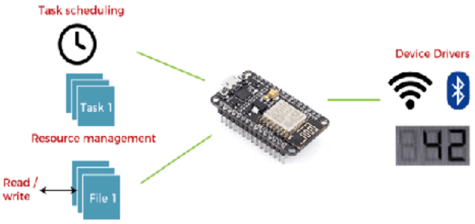


Fig 1.2.3 Real time operating system

RTOSs differ from general-purpose operating systems in their ability to manage hardware resources to meet specific timing requirements. They offer features such as task scheduling, inter-task communication, and real-time clock management to ensure that tasks are completed within defined time frames. (Refer Fig 1.2.3) RTOSs typically have a smaller footprint and are designed to run on resource-constrained devices. This makes them ideal for embedded applications where memory and processing power are limited. Moreover, RTOSs provide mechanisms for handling asynchronous events, ensuring the system responds swiftly to external inputs. The main components of RTOS are shown in Fig 1.2.4.

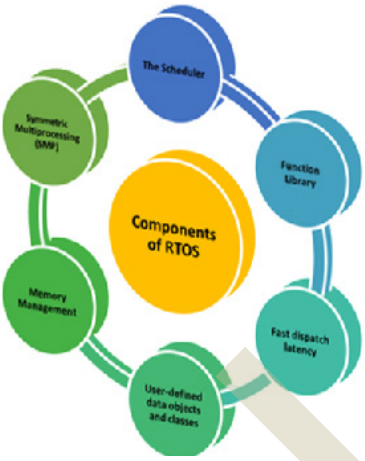


Fig 1.2.4 Components of RTOS

These features collectively enable RTOSs to deliver predictable and consistent performance, vital for safety-critical applications. As technology advances, the role of RTOSs continues to expand, supporting more complex and interconnected systems in various industries.

1.2.4.1 FreeRTOS

FreeRTOS is an open-source RTOS that is widely used in embedded systems. It is known for its simplicity, small footprint, and ease of integration. FreeRTOS supports a wide range of microcontroller architectures and offers features such as task prioritisation, inter-task communication, and time management. It is often used in applications like home automation, industrial control systems, and IoT devices, where reliable real-time performance is essential.

1.2.4.2 VxWorks

VxWorks is a commercial RTOS developed by Wind River Systems. It is designed for high-performance, safety-critical applications and is used in industries such as aerospace, automotive, and telecommunications. VxWorks provides features like real-time multitasking, memory protection, and fast context switching. Its reliability and robustness make it suitable for mission-critical systems, such as spacecraft, medical devices, and industrial robots.

1.2.4.3 QNX Neutrino

QNX Neutrino is a microkernel-based RTOS developed by BlackBerry Limited. It offers better scalability, reliability, and real-time performance. QNX Neutrino is used in various industries, such as automotive, medical, and industrial automation. Its microkernel architecture ensures high modularity and fault isolation, making it suitable for systems that require high availability and stringent safety standards.

1.2.4.4 ThreadX

ThreadX is an RTOS developed by Express Logic and is now part of Microsoft. It has a small footprint, fast performance, and ease of use. ThreadX supports advanced features like real-time scheduling, preemption threshold scheduling, and event chaining. It is used in a variety of applications, such as consumer electronics, industrial automation, and medical devices. The Azure RTOS suite, which includes ThreadX, offers seamless integration with Microsoft's Azure cloud services, making it ideal for IoT applications.

1.2.5 Mobile Operating Systems

Mobile Operating Systems (Mobile OS) are specifically designed to run on smartphones, tablets, and other mobile devices. They provide the necessary platform for mobile applications, managing hardware and software resources to ensure smooth operation. Popular mobile operating systems include Android, iOS, and, to a lesser extent, Windows Phone and BlackBerry OS. Each Mobile OS offers a unique user experience, with features tailored to the capabilities and constraints of mobile hardware. Mobile OSs are designed to handle various tasks such as touch input, location services, camera functions, and connectivity options like Wi-Fi and Bluetooth. They also include app stores, which provide a vast ecosystem of applications that users can download and install, enhancing the functionality of their devices.

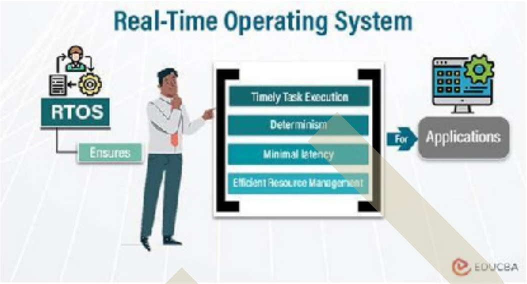


Fig 1.2.5 Real Time Operating System

Android, developed by Google, is the most widely used Mobile OS, known for its open-source nature and extensive customization options. iOS, developed by Apple, is renowned for its seamless integration with Apple's ecosystem and its focus on security and user privacy. Both operating systems have evolved significantly, offering advanced features like voice assistants, mobile payments, and augmented reality. Mobile OSs also prioritise battery efficiency and resource management, ensuring that devices can operate for extended periods on limited power. They incorporate robust security measures to protect user data and privacy, which is critical given the sensitive information often stored on mobile devices. As mobile technology continues to advance, Mobile OSs are becoming increasingly sophisticated, providing users with powerful tools and applications in the palm of their hands.

1.2.6 Files and File Systems in Operating Systems

Files are the fundamental units of storage in a computer system, representing collections of related data or information. They are essential for organising, storing, and retrieving data in an efficient and manageable manner. Operating systems (OS) provide a structured way to store and manage these files through file systems. A file system defines how data is stored, organised, and accessed on a storage device, such as a hard disk, SSD, or USB drive. It acts as an intermediary between the user and the physical storage, ensuring data integrity, security, and accessibility. Understanding the role and functionality of files and file systems is crucial for efficient data management and system performance.

1.2.6.1 Structure and Components of File Systems:

File systems are composed of several key components that work together to manage files. The primary components include directories, file allocation tables, and metadata. Directories, also known as folders, are used to organise files in a hierarchical structure, making it easier to locate and manage them. (Refer Fig 1.2.6) The file allocation table (FAT) or similar structures like inode tables in UNIX-based systems track the physical location of files on the storage device. Metadata contains essential information about each file, such as its name, size, creation date, and permissions. These components ensure that the file system can efficiently manage space, keep track of files, and provide quick access to data.

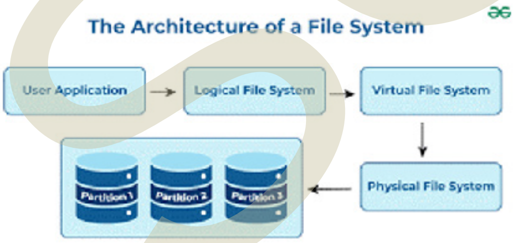


Fig 1.2.6 Architecture of File System

1.2.6.2 Types of File Systems

Various types of file systems have been developed to meet different requirements and use cases. Some common file systems include FAT32, NTFS, ext4, and APFS. FAT32 is widely used for compatibility across different operating systems and devices. NTFS is used primarily in Windows and has advanced features such as file compression, encryption, and disk quotas. The ext4 file system is commonly used in Linux distributions and provides robust performance and reliability. APFS, developed by Apple, is designed for macOS and iOS (mobile OS), offering high efficiency and security features. Each file system has its strengths and weaknesses, making them suitable for specific environments and applications.

1.2.6.3 File System Operations and Management

File systems support a variety of operations to manage files and directories effectively. Common operations include creating, reading, writing, and deleting files. When a file is created, the file system allocates space for it and updates the directory structure and metadata. Reading and writing involve accessing the file's data and updating its contents, respectively. Deleting a file removes its entry from the directory and marks its allocated space as available for reuse. File systems also handle permissions and security, ensuring that only authorised users can access or modify files. Advanced file system management tasks include disk formatting, defragmentation, and backup, which help maintain optimal performance and data integrity.

1.2.7 BIOS and Booting in Operating Systems

The Basic Input/Output System (BIOS) is a fundamental component of a computer's motherboard. It is the first software to run when a computer is powered on, performing crucial tasks to initialise hardware components and prepare the system for loading the operating system (OS). Stored on a non-volatile ROM chip on the motherboard, the BIOS provides essential low-level control and diagnostic functions. It contains a set of instructions for hardware initialisation during the boot process and provides runtime services for operating systems and programmes. The BIOS also offers an interface for configuring hardware settings such as boot sequence, system clock, and device management.

1.2.7.1 Functions and Configuration of BIOS:

One of the primary functions of the BIOS is the Power-On Self-Test (POST), a diagnostic testing sequence that checks the computer's hardware components, such as the CPU, RAM, and storage devices, to ensure they are functioning correctly. If any issues are detected, the BIOS provides error messages or beep codes to alert the user. In addition, the BIOS allows users to configure hardware settings through a setup utility accessible during the boot process. Users can adjust parameters like system date and time, boot order, and enable or disable integrated peripherals. These configurations are stored in a complementary metal oxide semiconductor (CMOS) chip, which is powered by a small battery to retain settings even when the computer is turned off.

1.2.7.2 Boot Process and the Role of BIOS

The boot process begins when the computer is powered on, with the BIOS playing a critical role in starting the system. After completing the POST, the BIOS identifies the bootable devices based on the configured boot order. It then locates the Master Boot Record (MBR) or GUID Partition Table (GPT) on the primary storage device, which contains the bootloader. The bootloader is a small programme responsible for loading the operating system kernel into memory. Once the bootloader is executed, it transfers control to the OS, which continues with the initialisation process, loading necessary drivers and setting up the system environment for user interaction. This sequence ensures that the hardware and software are correctly initialised and ready for operation.

1.2.8 Remote Connections

Remote connections allow users to access and manage computers and networks from a distance, which is much needed in today's interconnected world. They enable users to work on a remote system as if they were physically present, providing flexibility and convenience for requirements like remote work, technical support, and server management. Remote connections rely on protocols and tools designed to ensure secure, reliable, and efficient communication between devices over the Internet or other networks.

Several protocols facilitate remote connections, each with unique features and use cases. The Secure Shell (SSH) protocol is widely used for securely connecting to remote servers and executing commands, offering encryption and strong authentication. Remote Desktop Protocol (RDP) (developed by Microsoft) allows users to access Windows-based systems with a graphical interface, enabling a seamless desktop experience remotely. Virtual Network Computing (VNC) provides remote desktop access across various operating systems. Security is a prime concern, and strong authentication methods like multifactor authentication (MFA) help verify users' identities. Encryption protocols like Transport Layer Security (TLS) protect data transmitted over remote connections. Additional measures like firewalls, virtual private networks (VPNs), and intrusion detection systems (IDS) further enhance security.

1.2.9 Protocols and Security for Remote Connections

1.2.9.1 Remote Desktop Protocol (RDP)

RDP is a Microsoft protocol that allows users to remotely access and control a Windows-based computer. It provides a graphical interface for interacting with the remote system's applications and resources, commonly used for remote administration and support.

1.2.9.2 Secure Shell (SSH)

SSH is a cryptographic protocol used for secure remote access to Unix-based systems. It ensures encrypted communication, preventing eavesdropping and man-in-the-middle attacks, and is widely used for secure logins and file transfers.

1.2.9.3 Virtual Network Computing (VNC)

VNC is a cross-platform protocol that enables users to remotely control another computer's desktop. It transmits screen updates to the local client, allowing interaction as if the user were at the remote machine.

1.2.9.4 Remote Procedure Call (RPC)

RPC is a protocol that allows a program on one machine to execute procedures on another machine. It abstracts network communication, making it simpler to invoke services across different systems in distributed networks.

1.2.9.5 Telnet

Telnet is an older protocol that provides text-based remote access to systems. It allows command-line interaction but lacks encryption, making it vulnerable to security risks. It has been largely replaced by SSH.

1.2.9.6 Simple Network Management Protocol (SNMP)

SNMP is used for managing and monitoring network devices such as routers and switches. It enables administrators to collect data, configure devices, and track network performance.

1.2.9.7 File Transfer Protocol (FTP) / Secure File Transfer Protocol (SFTP)

FTP is a standard protocol for transferring files between a client and a server. SFTP, an extension of SSH, adds encryption to secure the file transfer, making it more suitable for sensitive data.

1.2.9.8 Remote Access Service (RAS)

RAS is a Microsoft service that allows users to remotely access network resources and systems. It supports methods like dial-up and VPN connections, facilitating secure remote connectivity for telecommuting.

Recap

- **Operating systems** manage **hardware** and **software**, handling tasks like **process**, **memory**, **file**, and **security management**
- The **kernel** controls system resources, and **process management** efficiently schedules tasks
- The **file system** organizes and manages **files**, while the **command interpreter** allows user interaction with the OS
- **System calls** provide an interface for programs to request **OS services**, and **security management** protects data and system integrity
- **I/O device management** handles communication with **peripherals**, while **memory management** ensures efficient use of **memory**
- Common **operating systems** include **Windows**, **macOS**, **Linux**, and **Unix**, with **real-time operating systems** used for time-sensitive tasks
- **File systems** determine how **data** is stored and accessed
- **BIOS** starts the computer, checks **hardware**, and loads the **operating system**
- **Remote connections** allow secure access to systems through protocols like **RDP**, **SSH**, and **FTP**

Objective Questions

1. What is the core part of an operating system responsible for managing resources?
2. Which operating system is known for its open-source nature and flexibility?
3. What protocol is used for secure remote login to Unix-based systems?
4. Which component checks hardware during the boot process?
5. Which operating system is commonly used in Apple devices?
6. Which OS is specifically designed for time-sensitive applications?
7. Which file system is commonly used in Windows?
8. Which device does I/O device management handle communication with?
9. What is used to establish remote connections for accessing systems?
10. Which system is responsible for organizing files and directories on a storage device?

Answers

1. Kernel
2. Linux
3. SSH
4. BIOS
5. macOS
6. RTOS
7. NTFS
8. Peripherals
9. Protocols
10. File System

Assignments

1. Explain the role of the Kernel in an operating system. How does it manage system resources like memory, processes, and I/O devices?
2. Discuss the boot process of a computer system. What role does BIOS play, and how does it transition control to the operating system?
3. Discuss the role of file system management in an operating system. How do file systems organize data, and what are some common file systems used by modern operating systems?
4. Compare and contrast Secure Shell (SSH) and Telnet in terms of security features, performance, and use cases. Which one is preferred in modern computing environments and why?

Reference

1. Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating system concepts* (10th ed.). Wiley.
2. Tanenbaum, A. S., & Bos, H. (2014). *Modern operating systems* (4th ed.). Prentice Hall.
3. Shotts, W. E. (2012). *The Linux command line: A complete introduction* (2nd ed.). No Starch Press.
4. Nemeth, E., Snyder, G., Hein, T. R., Whaley, B., & Mackin, D. (2017). *Unix and Linux system administration handbook* (5th ed.). Prentice Hall.
5. Raymond, E. S. (2003). *The art of UNIX programming*. Addison Wesley.

Suggested Reading

1. TutorialsPoint. (n.d.). *Operating systems tutorials*. TutorialsPoint. Retrieved April 30, 2025, from https://www.tutorialspoint.com/operating_system/
2. Russinovich, M., Solomon, D. A., & Ionescu, A. (2012). *Windows internals* (6th ed.). Microsoft Press.
3. Anderson, R. (2014). *Operating systems: Three easy pieces*. Retrieved from https://pages.cs.wisc.edu/~remzi/OSTEP/

Unit 3

Choosing and Installing Operating System

Learning Outcomes

On completion of this unit, the learner will be able to:

- Familiarise themselves with an operating system and its role in managing computer resources
- Identify the key factors involved in choosing an appropriate operating system based on user requirements
- Identify the key components required to install an operating system
- Differentiate between proprietary and open-source operating systems
- Explain the importance of troubleshooting in maintaining operating system functionality

Background

Imagine you just bought a new laptop to start a small online business from home, and you plan to do tasks like managing spreadsheets, sending emails, designing posters, and joining video meetings. After setting it up, you find that some of the apps you need don't work properly, the system feels slow, and updates are confusing to install. This happens because the operating system (OS) that came pre-installed might not be the best fit for your specific needs. The OS is like the manager of your computer; it controls how hardware and software work together and affects everything from speed to security. Choosing the right OS ensures that the programs you use every day run smoothly and efficiently. If you prefer user-friendly tools and built-in office apps, Windows or macOS might be ideal. If you value customisation and free software, a Linux-based OS could be a better choice. Also, installing the OS properly helps avoid technical problems and makes future maintenance easier. A wrong or poorly installed OS can slow you down, waste time, and cause frustration. That's why it's important to understand your requirements before choosing and installing an operating system.

Before moving into the selection, installation, and troubleshooting of operating systems, it is important to have a foundational understanding of several key concepts. These basics will help ensure a smoother learning experience and allow learners to apply the concepts effectively in real-world scenarios.

First and foremost, basic computer literacy is essential. Learners should be familiar with the main components of a computer system, such as the processor, RAM, storage devices, and input/output peripherals. Understanding how these elements work together provides the context needed for installing and managing an operating system.

It is also helpful to have a general awareness of the major operating systems available today. Familiarity with Windows, macOS, and various Linux distributions can help learners make informed decisions when choosing the right OS for a specific need or environment. Being able to identify issues, analyse their causes, and apply appropriate solutions is a key part of managing and maintaining any operating system.

Keywords

System Software, Hardware Management, User Interface, Microsoft Windows, Bootable Media, Backup, Driver Installation.

Discussion

An operating system (OS) is the backbone of every computing device. It acts as the intermediary between the user and the hardware, managing resources and providing essential services. It is system software that manages computer hardware, software resources, and provides common services for computer programs. It plays the role of a coordinator, manager, communicator, and enables effective interaction between users and machines. Popular OS includes Microsoft Windows, macOS, Linux distributions (e.g., Ubuntu, Fedora, Mint), etc.

1.3.1 Choosing the Operating System

Choosing the operating system (OS) is an important decision that depends on the user's specific requirements, technical skills, and hardware capabilities. An OS serves as the foundation for a computer's functionality, and the right choice can significantly enhance productivity, user experience, and system performance. The first step in choosing an operating system is to determine the primary purpose of the computer. For general usage such as web browsing, office work, and media consumption, Windows and macOS are commonly preferred due to their ease of use and compatibility with a wide range of software. Gamers usually choose Windows, as it supports the largest selection of games and is compatible with hardware. Developers and programmers often opt for Linux or macOS because they offer powerful command-line tools and support open-source development environments. For creative professionals involved in graphic design, video editing, or music production, macOS is frequently recommended because of its optimised support for creative software. In server environments, Linux is widely used due to its lightweight nature, high stability, and strong security features.

Each operating system has its own set of characteristics. Windows is a versatile and user-friendly OS that dominates the personal and enterprise market. It offers extensive software and hardware compatibility. The macOS, developed by Apple, provides a clean and visually appealing interface, along with seamless integration with other Apple products. It is known for its stability and security but is limited to Apple hardware. Linux is a free and open-source operating system, available in many distributions (distros) such as Ubuntu, Fedora, and Debian. It is highly customisable and is popular among technical users and professionals who require control over their system configuration. Chrome OS, developed by Google, is a web-based OS that is lightweight and designed primarily for internet use. It is widely used in educational institutions and among users who rely on cloud-based applications.

Software compatibility is a key factor in OS selection. Users must ensure that the required applications are supported by the chosen OS. Microsoft Office and Adobe Creative Suite are fully supported on Windows and macOS, while open-source tools like LibreOffice and GIMP are available across multiple platforms. Developers working with programming languages or containerised environments such as Python and Docker often prefer Linux due to better compatibility and performance.

Cost is another important consideration. Linux distributions are typically free, while Windows usually requires a paid licence. macOS comes pre-installed on Apple devices, so you don't pay for it separately, but the hardware itself is more expensive.

Finally, think about support and community. Windows and macOS have extensive official support and user-friendly help systems. Linux support mainly comes from its strong online communities, forums, and documentation, which can be very helpful, especially for users with some technical background.

1.3.2 Installing the Operating System

Installing an operating system (OS) is a crucial step in setting up a computer for use. It involves loading the core software that manages all hardware and software resources on the computer.

1. **Backup the existing data:** Installing a new OS often involves formatting the drive where the old one resides, which means all your files, photos, documents, and everything else will be gone. Copy everything important to an external hard drive, USB drive, or cloud storage.

2. **Verify System Requirements:** Ensure your computer meets at least the

minimum requirements for the OS you intend to install.

3. **Obtain Installation Media:** This typically comes in one of two forms: Bootable USB Drive or DVD.

4. **Gather Necessary Information:** Depending on the OS, you might need certain information during the installation process. Product Key/ License Key (Many commercial operating systems like Windows require a product key for activation.), Network Information (Optional but Recommended), and Partitioning Scheme (If Custom).

5. **Configure Boot Order in BIOS/ UEFI:** Your computer needs to boot from the installation media (USB drive or DVD) instead of your existing hard drive. To do this, you'll need to access the BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) settings. Restart the computer and enter the BIOS/UEFI setup (usually by pressing F2, F12, Delete, or Esc at startup).

6. **Change the boot order** to prioritise the USB drive.

7. **Save and exit** BIOS/UEFI. The system will boot into the installation environment.

8. **Follow the on-screen instructions**, which typically involve:

   a. Choosing a language and keyboard layout.

   b. Selecting installation type (clean install, dual boot, upgrade).

   c. Partitioning the disk.

   d. Setting user details and passwords.

- **Begin installation** and wait for the process to complete.
- **Restart** the system when prompted, and remove the USB drive.

1.3.3 Understanding Proprietary and Open Source

1.3.3.1 Operating Systems

In the world of operating systems, the software that governs how your computer behaves comes in two main categories: proprietary and open source.

A proprietary operating system is developed, owned, and maintained by a company or individual, and its source code is not available to the public. Users must purchase a licence to use the software, and modifications are generally not allowed. These systems are polished, user-friendly, and supported by large companies. Examples of proprietary operating systems include Microsoft Windows, macOS (by Apple), IBM AIX, and Oracle Solaris (later versions), etc.

An open-source operating system is released with a licence that allows anyone to view, modify, and distribute the source code. Most open-source operating systems are developed collaboratively by communities or foundations. Open-source systems are often free of cost, but their true value lies in freedom and flexibility. Developers, enthusiasts, and privacy-conscious users appreciate the ability to customise the system to their needs or even contribute to its improvement. Examples of open-source operating systems include Linux (Ubuntu, Fedora, Debian, Arch Linux, etc.), FreeBSD, OpenSolaris (early versions), ReactOS, and Haiku OS, etc.

1.3.4 Proprietary Vs Open Source OS

Table 1.3.1 Proprietary vs Open Source OS

Features	Proprietary OS	Open Source OS
Source Code	Not available to users	Freely available and modifiable by anyone.
License Type	Commercial, paid, or restricted licence	Free and open source licences (e.g., GPL)
Ownership	Owned and controlled by a company or individual	Developed and maintained by a community
Updates	Regular updates from vendor	Updates depend on community contributions
Customisation	Limited customisation options.	Highly customisable based on user needs.
Examples	Microsoft Windows, macOS, iOS	Linux (Ubuntu, Fedora, Debian), FreeBSD

1.3.5 Partitioning, installing and troubleshooting

Partitioning is the process of dividing a computer's hard disk or storage drive into separate sections known as partitions. Each partition behaves like an independent disk and can be formatted with its own file system. Before installing any operating system, the hard disk must be partitioned to organise data and define where the OS will reside. There are different types of partitions: primary, extended, and logical. A Primary Partition is a main section of the hard drive where you can install and run an operating system. An Extended Partition cannot hold data directly but is used to create logical partitions inside it. Logical Partitions are created inside an extended partition and are used to store files or install additional operating systems.

The following are some of the benefits of disk partitioning:

- Separates system files from user data.
- Allows installation of multiple operating systems.
- Improves data management and backup practices.
- Helps in performance optimisation and disk maintenance.

Installing an operating system means placing all necessary system files, drivers, and services onto a hard disk so that the computer can boot and operate. It is usually the first step in setting up a new or reformatted computer.

Troubleshooting is the process of diagnosing and resolving problems that occur during or after installing an operating system. It involves both technical knowledge and analytical skills. Effective troubleshooting provides:

- Minimises system downtime
- Prevents data loss
- Maintains user productivity
- Reduces maintenance costs
- Ensures system reliability and security

It helps to determine whether the problem lies with the hardware, software, or user configuration and provides a structured path to resolution. A standard troubleshooting process often follows these steps:

1. **Identify the Problem**
    - Collect information from the user.
    - Observe symptoms or error messages.
    - Check logs and system behaviour.

2. **Establish a Theory**

   - Consider possible causes based on symptoms.
   - Check common or recent changes.

3. **Test the Theory:** Confirm the cause by testing or replicating the issue.

4. **Establish a Plan of Action:** Plan how to resolve the issue with minimal disruption.

5. **Implement the Solution:** Apply the fix, such as reinstalling a driver or repairing the boot loader.

6. **Verify System Functionality:** Ensure that the issue is resolved and no other problems occur.

7. **Document the Process:** Record the issue and solution for future reference.

Recap

- The operating system (OS) acts as the interface between the user and the computer hardware, managing resources and running applications.
- Choosing the right OS depends on the user's needs, hardware, and technical expertise. Windows is suitable for general use and gaming, macOS is ideal for creative professionals, and Linux is favoured by developers and technical users.
- The installation process of an OS involves backing up data, preparing installation media, configuring BIOS/UEFI to boot from the media, and following the on-screen instructions to set up the system.
- BIOS/UEFI settings must be changed to prioritise booting from the installation media, such as the USB or DVD.
- Once the boot order is set, follow the on-screen steps to install the OS, including selecting language and partitioning the hard drive.
- Proprietary OS like Windows and macOS are closed systems developed by companies. They require paid licences to use.
- Open source OS like Linux is free and customisable. Users can modify and share the software as needed.
- Partitioning involves dividing the hard drive into separate sections, or partitions, to organise data and improve system performance.
- Partitioning is useful because it separates system files from user data, making it easier to manage and back up.
- Partitioning the hard drive helps with data management, system performance, and backup.

- Troubleshooting is necessary when problems occur during or after OS installation. It involves identifying and fixing the issue.
- Effective troubleshooting can reduce system downtime, prevent data loss, and keep the system running smoothly.

Objective Questions

1. What is the main function of an operating system?
2. What is the purpose of partitioning a hard drive?
3. What is a common reason for troubleshooting an operating system?
4. Which tools are used to access and change the boot order in a computer?
5. Which OS is pre-installed on Apple devices?
6. What does the acronym "BIOS" stand for?
7. Which file system is most commonly used by Linux operating systems?
8. What is the main advantage of open source operating systems?
9. Which operating system is known for its high security and is often used for servers?
10. What is the main reason for creating multiple partitions on a disk?
11. What is the main advantage of using a dual boot system?
12. Which operating systems can be used to run applications such as Microsoft Office and Adobe Photoshop?
13. What is the function of a "boot loader" in an operating system?
14. What is the function of the "Swap" space in Linux?
15. What does the acronym "UEFI" stand for?

Answers

1. Manage hardware resources
2. To organise data and improve system performance
3. Software errors or crashes
4. BIOS/UEFI
5. macOS
6. Basic Input/Output System
7. ext4
8. They are free to use and modify
9. Linux
10. To organise and manage data more efficiently
11. To allow the user to run multiple operating systems on one machine
12. Windows
13. To load the operating system into memory
14. To extend physical memory by using hard drive space
15. Unified Extensible Firmware Interface

Assignments

1. Explain the role of an operating system in a computer system?
2. Differentiate between proprietary and open source operating systems.
3. Explain the process of installing an operating system?
4. Explain the role and benefits of partitioning in system performance and security?
5. Describe the key steps involved in troubleshooting a failed operating system installation?
6. What are the advantages and disadvantages of using open source operating systems like Linux in enterprise environments?

Reference

1. Tanenbaum, A. S., & Bos, H. (2015). *Modern Operating Systems* (4th ed.). Pearson.

2. Stallings, W. (2018). *Operating Systems: Internals and Design Principles* (9th ed.). Pearson.

3. Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating System Concepts* (9th ed.). Wiley.

4. Sahoo, S. K., & Verma, S. (2019). *Understanding Windows Operating System: Concepts and Techniques*. Springer.

5. Araujo, M., & Lopes, M. (2020). *Practical Linux Security Cookbook*. Packt Publishing.

Suggested Reading

1. Frisch, Æ. (2002). *Essential System Administration* (3rd ed.). O'Reilly Media.

2. Raymond, E. S. (2003). *The Art of UNIX Programming*. Addison Wesley.

3. Nemeth, E., Snyder, G., Hein, T. R., Whaley, B., & Mackin, D. (2017). *Unix and Linux System Administration Handbook* (5th ed.). Prentice Hall.

4. McHoes, A. M., & Flynn, I. M. (2018). *Understanding Operating Systems* (8th ed.). Cengage Learning.

Unit 4

System Security and Protection

Learning Outcomes

On completion of this unit, the learner will be able to:

- Define network security and its purpose in protecting digital systems.
- List common types of malware such as viruses, worms, and trojans.
- Identify the function of a firewall in a network environment.
- Recall various types of phishing attacks like spear phishing and smishing.
- Name the key components of a secure network infrastructure.

Background

Before studying network security, it is important to have a foundational understanding of how computer networks function. This includes knowledge of essential components such as routers, switches, servers, and network protocols like IP addressing, DNS, and HTTP/HTTPS. A basic grasp of how data travels through a network and the roles of operating systems (e.g., Windows or Linux) in managing resources is also necessary. Additionally, understanding how files are stored and accessed, as well as some basic troubleshooting skills, can help learners better visualise and engage with security mechanisms.

This foundational knowledge is crucial because network security builds directly upon these core concepts to identify, prevent, and mitigate cyber threats. Without an understanding of how networks are structured and how data moves within them, it becomes challenging to comprehend how vulnerabilities arise or how security tools like firewalls, encryption, and antivirus software function. Studying these basics allows learners to more effectively analyse risks, design secure systems, and apply protection strategies across digital infrastructures.

Keywords

Network Security, Malware, Firewall, Phishing, Data Protection

Discussion

Network security is crucial for protecting sensitive data and maintaining the integrity of information systems. It helps safeguard against unauthorised access, cyberattacks, and data breaches that can lead to financial losses or damage to an organisation's reputation. By ensuring secure communication channels, network security protects the confidentiality of transmitted information. It also plays a key role in ensuring the availability of network resources and minimising downtime. Robust network security measures are essential for maintaining trust and continuity in digital operations.

1.4.1 Importance of Network Security

Network security involves all the measures taken to protect a computer network's integrity and the data it holds. It is essential because it safeguards sensitive information from cyber threats and ensures the network remains reliable and functional. Effective network security strategies use a combination of security tools to defend users and organisations against threats like malware and cyber attacks, including distributed denial of service (DDoS) attacks.

A network consists of various interconnected devices, such as computers, servers, and wireless networks, many of which can be targeted by attackers. To secure these devices, a range of software and hardware tools are employed, either directly on the network or through software as a service. As networks become more complex and businesses increasingly depend on them, the importance of security grows. Security practices must adapt to new attack methods developed by malicious actors targeting these intricate networks.

Regardless of the specific security methods or strategies an organisation uses, security is generally considered a shared responsibility. Every user on the network can potentially be a weak point, making it crucial for everyone to contribute to maintaining network security. Fig. 1.4.1 shows a network security implementation.

Network security is crucial because it prevents cyber criminals from accessing valuable and sensitive data. If hackers obtain this data, they can cause significant issues, such as identity theft, financial loss, and damage to a company's reputation.

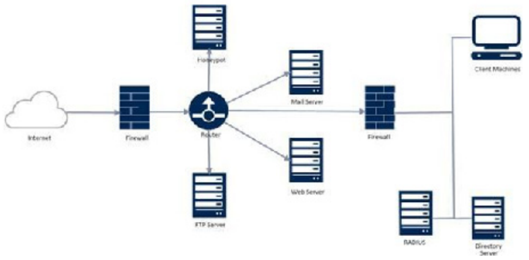


Fig. 1.4.1 Sample diagram of network security implementation

1.4.1.1 Key Reasons for Protecting Networks and Data

Operational Risks

Without adequate network security, disruptions due to cyberattacks, viruses, malware, or unauthorised access can result in operational downtime. Such disruptions can halt business operations, affect productivity, and even compromise the availability of essential services. For example, a ransomware attack could lock out critical systems, preventing employees from accessing files and causing significant business losses. The absence of proper security protocols also makes it easier for cybercriminals to target vulnerabilities, leading to disruptions in both internal and external communication.

Financial Risks

Data breaches, especially those involving Personally Identifiable Information (PII) like Social Security numbers, passwords, and financial details, can lead to substantial financial losses. The financial consequences extend beyond the immediate costs of addressing the breach such as paying for cybersecurity responses, legal costs, and recovery into the longer-term costs associated with reputational damage. Organisations may face lawsuits, regulatory fines, and lost business opportunities. According to the IBM 2022 report, the average cost of a data breach is $4.35 million, reflecting the severe financial implications that result from compromised security.

Intellectual Property Theft

Intellectual Property (IP) theft can cause substantial damage to an organisation's financial stability and long-term competitive position. If a business's proprietary information, such as trade secrets, product designs, or source code, is stolen, it could lead to the loss of unique advantages in the marketplace. Competitors may gain access to valuable insights, or the stolen IP could be sold on the black market. The cost of replacing lost intellectual property and regaining market trust can be extremely high, making IP protection a central element of network security.

Regulatory Compliance

Many industries are subject to data security regulations that require companies to protect sensitive information. For example, medical organisations must comply with the Health Insurance Portability and Accountability Act (HIPAA) to safeguard patient data. In the EU, the General Data Protection Regulation (GDPR) mandates the secure handling of customer data, with strict penalties for non-compliance. Failing to follow these regulations can result in severe penalties, legal action, and restrictions, further emphasising the need for comprehensive network security measures to avoid legal and financial risks.

1.4.2 Advantages of Network Security

Operational Continuity

Effective network security ensures smooth business operations by preventing disruptions such as data breaches, denial of service (DoS) attacks, or system downtime. When network security is robust, businesses can continue their operations without interruption, maintain access to critical systems, and serve their customers without risking the functionality of essential IT infrastructure.

Data Protection

Network security ensures the confidentiality, integrity, and availability of sensitive data. By implementing encryption, secure access controls, and data loss prevention (DLP) tools, organisations can protect critical information from cyber threats.

This is especially important for sectors like healthcare, finance, and education, where personal data is handled regularly. Protecting customer and employee data also helps to comply with regulations like HIPAA and GDPR, avoiding legal consequences.

Intellectual Property Protection

Strong network security helps prevent unauthorised access to valuable intellectual property (IP). Whether it's product designs, proprietary software, patents, or business strategies, protecting these assets from cyber threats is crucial for maintaining a competitive edge. Cyberattacks targeting IP theft can cause irreparable damage to a company's position in the market.

Regulatory Compliance

Network security supports compliance with various regulatory frameworks by implementing policies, tools, and measures that ensure the proper handling of sensitive data. This includes the use of encryption, secure storage, and regular auditing of systems to ensure that data protection protocols align with relevant legal requirements. Ensuring compliance with standards like GDPR (for the EU) or HIPAA (for healthcare organisations) helps avoid legal penalties and fosters a positive reputation.

Customer Trust

When businesses maintain robust network security, they build trust with their customers. Consumers are more likely to engage with a business they believe is committed to protecting their data. Trust is a key driver for customer loyalty, especially in industries where data privacy is a critical concern, such as banking, e-commerce, and healthcare. Companies with secure systems are also better positioned to win and retain clients who prioritise their own privacy.

Employee Accountability

By implementing strong network security protocols, companies can promote accountability among employees, encouraging them to follow best practices like using strong passwords, avoiding suspicious links, and regularly updating their devices. With effective security measures in place, employees are less likely to engage in risky behaviour that could inadvertently compromise the network. Employee awareness training is a key part of fostering a culture of security.

1.4.3 Malware

Malware is software designed with malicious intent to damage or disrupt systems, steal data, or gain unauthorised access to devices. It comes in various forms, each with different methods of attack and objectives:

- **Viruses:** These attach themselves to legitimate programmes and spread when the programme is executed. Viruses can cause system crashes, data corruption, or even render systems inoperable.
- **Worms:** Unlike viruses, worms can self-replicate and spread independently across networks without user intervention. They often exploit network vulnerabilities to infect multiple systems.
- **Trojans:** These malware types masquerade as legitimate software to trick users into installing them. Once inside the system, they provide backdoor access for cybercriminals.
- **Ransomware:** This form of malware encrypts the victim's data and demands payment for decryption. Ransomware can paralyse entire organisations, demanding a ransom in exchange for restoring access to encrypted files.
- **Spyware:** Secretly gathers sensitive information, such as login credentials

or browsing habits, and sends it to a remote attacker.

- **Adware:** Displays unwanted advertisements, often bundled with other malicious software, to track user behaviour and generate revenue for attackers.

Malware exploits unpatched vulnerabilities, social engineering tactics like phishing, and insecure file-sharing practices. Preventing malware requires timely software updates, using advanced threat detection tools, and employing a layered security approach like firewalls, antivirus software, and multi-factor authentication (MFA).

1.4.4 Firewall

A firewall is a critical network security device that monitors and controls the traffic flowing in and out of a network based on predefined security rules. It acts as the first line of defence against external threats by blocking malicious traffic and allowing legitimate communication.

Types of Firewalls

- **Packet filtering firewalls:** These firewalls inspect packets of data and decide whether to allow or block them based on security rules. They work at the network layer and offer basic protection.
- **Stateful inspection firewalls:** These track the state of active connections and make security decisions based on the context of the traffic. They are more sophisticated than packet filtering firewalls and can detect certain types of attacks that other firewalls may miss.
- **Proxy firewalls:** These firewalls act as intermediaries between users and the services they access, ensuring that direct communication between the two is blocked. They can hide the internal network's addresses, providing an extra layer of anonymity and security.

Firewalls can prevent unauthorised access, block malicious traffic, and ensure that only trusted users can access network resources. Additionally, they provide a means of monitoring traffic for suspicious activities, helping to detect and mitigate potential threats in real time.

1.4.5 Antivirus

Antivirus software helps protect systems by identifying, preventing, and removing malicious software. Antivirus tools typically operate by scanning files, programmes, and memory for known malware signatures and unusual behaviours. They play a vital role in defending systems against viruses, worms, Trojans, and other forms of malware.

Key Features of Antivirus Software

- **Real-time scanning:** Continuously monitors files and applications as they are accessed or executed, ensuring that malicious files are detected immediately.
- **Signature-based detection:** Compares files and programmes to a database of known malware signatures to identify and flag threats.
- **Heuristic analysis:** Detects new or unknown malware by analysing suspicious behaviour or code patterns, even if the malware has never been encountered before.
- **Quarantine and removal:** Infected files are isolated in a quarantine zone to prevent further damage, while the antivirus software removes the threat from the system.

Antivirus software is essential for proactively identifying and mitigating threats. While it is not a silver bullet, it plays a key role in the multi-layered security approach necessary to protect devices and networks.

1.4.6 Phishing

Phishing is a cyberattack technique used to deceive individuals into disclosing sensitive information, such as login credentials, credit card details, or other personal data. Attackers use social engineering tactics to impersonate trustworthy entities and manipulate users into making security mistakes.

Types of Phishing Attacks

- **Spear phishing:** Highly targeted attacks that focus on specific individuals or organisations, often using personalised information to increase the likelihood of success.
- **Whaling:** A type of spear phishing aimed at high-profile individuals, such as executives or decision-makers, with the goal of gaining access to sensitive company information.
- **Vishing (Voice Phishing):** Attackers use phone calls to impersonate legitimate organisations, like banks or tech support, to extract personal details from victims.
- **Smishing (SMS Phishing):** A form of phishing that uses text messages to trick users into revealing private information or downloading malicious software.

Phishing attacks are a major source of data breaches and can have devastating consequences for individuals and businesses. To defend against phishing, organisations should:

- **Educate users:** Regularly train employees on how to recognise phishing attempts and avoid falling victim to them.
- **Implement email filtering:** Use spam and malware filters to block phishing emails before they reach the inbox.
- **Use multi-factor authentication (MFA):** Even if credentials are compromised, MFA adds an extra layer of security.

1.4.7 Clickjacking

Clickjacking is a type of cyberattack where an attacker tricks a user into clicking on something they did not mean to click. The word comes from combining "click" and "hijacking" because the attacker takes control of your clicks. This attack works by placing dangerous or unwanted content behind something that looks normal, like a video, button, or link. The person thinks they are doing something harmless, like clicking "Play" or "Submit," but they are really clicking on something hidden. That hidden click might cause actions like liking a page, changing account settings, or sending money without the person realising it happened.

Imagine you visit a website with a big button that says, "Claim Your Free Gift." It looks harmless, but the attacker has secretly placed a transparent "Send Money" button from your bank account underneath it. When you click the gift button, you are clicking the hidden button and unknowingly sending money to the attacker. You think you are getting a prize, but instead, you have been tricked into doing something harmful.

1.4.7.1 Types of Clickjacking Attacks

1. Cursorjacking

Cursor Jacking is a trick that confuses your mouse pointer. It makes you think the pointer is on one thing, but it is actually on something else. So, when you click, you might click the wrong thing by mistake. In this attack, the pointer you see is fake—it is just a picture. The real pointer is a little to the side, usually to the right. So, if you try to click a button, you might accidentally click on something else without knowing.

When you move your mouse, a hidden code makes a fake pointer move with it. You think you are clicking a YES button, but your real click happens somewhere else, like on a hidden Tweet button. Hackers used this trick to fool security tools like NoScript's ClearClick.

2. Likejacking

This is a type of clickjacking that targets Facebook's "Like" button. Scammers trick users into clicking "Like" by showing something tempting, like a video, photo, or coupon offer. Once clicked, the post spreads to the user's friends, helping the scam reach more people. As the number of likes increases, so does the post's visibility. Some security experts believe these scams may also try to steal Facebook login details or personal information.

You see a post offering a free coupon or funny video. You click "Like," but the scam post is shared with your friends, spreading the scam. The hacker might also try to steal your Facebook details, like your profile or login info.

3. Filejacking

Filejacking is a method where attackers exploit the browser's ability to access files on your computer. They trick the user into using the browser's file selection feature, allowing the attacker to access and steal personal information. This technique lets hackers break into a victim's computer and steal files or sensitive data.

You visit a website offering a free tool and are asked to upload a file. When you choose a file, the browser lets the attacker access your computer's files, giving them potential access to your personal documents or information.

4. CookieJacking

It is a type of clickjacking where a hacker steals your cookies (small pieces of data websites store) by tricking you into doing something simple, like dragging an item on a website. Once you do this, your cookies are sent to the hacker, who can then use them to pretend to be you on a website.

You visit a website that asks you to drag a picture to a specific spot to unlock a "special feature." Once you drag the picture, your web cookies are sent to the hacker without you realising it. The hacker can then use those cookies to log in as you on a website, like your social media account, and pretend to be you.

5. Browserless clickjacking

This is a technique that mimics traditional clickjacking in apps that do not run in a web browser. It is commonly used on Android phones because of how pop-up alerts work. There is a short delay between when a pop-up notice is triggered and when it appears on the screen. Attackers use this brief delay to place a fake icon under the real notification, which you may accidentally click.

You get a pop-up notification on your Android phone, like a message from an app. Before the message fully appears, a hacker places a fake icon under it. When you try to close the notification, you actually tap the fake icon, and it triggers an action, like giving the hacker access to something on your phone.

1.4.8 Spamming

Spamming is the practice of sending unwanted, irrelevant, or repetitive messages to a large number of people, usually through digital communication channels like email, social media, SMS, or websites. These messages are often sent in bulk and without the recipient's consent.

You open your email and see a message from an unknown sender saying, "Congratulations! You have won a free iPhone. Click here to claim." You never entered a contest, and the link might lead to a fake site that tries to steal your information. This is a classic example of email spam.

The main goal of spamming is often to advertise products, promote scams, spread malware, or simply annoy users. Since spam is usually automated, it can quickly flood inboxes, comment sections, or chat boxes, making it hard for people to find useful content.

1.4.8.1 Types of Spamming

1. Email Spam

Email spam is when someone sends unwanted emails to a large number of people, usually for advertising, scams, or spreading viruses. These emails often contain fake offers, dangerous links, or attachments.

Consider you open your email and see a message from deals@superstore.com saying, "Claim your free rupees 50 gift card click here now." You never signed up for anything, and if you click the link, it will either ask for your credit card info or try to install malware on your computer.

2. Social Media Spam

Social media spam happens on platforms like Facebook, Instagram, and Twitter. Spammers post fake deals, tag random people, or send links in messages to trick users. It often comes from fake or hacked accounts.

You get an Instagram direct message from someone you do not know, claiming you have been tagged in a private vid and asking you to click a link to watch it. When you tap the link, you are taken to a fake login page where scammers steal your username and password, or the link automatically makes your account follow dozens of spam profiles, causing the unwanted posts to spread even further.

3. SMS Spam

SMS spam is when you receive unwanted text messages on your phone. These messages often promise free prizes, special offers, or ask you to click on suspicious links. The sender is usually a random number or a bot.

You get a text message from an unknown number saying, "Your voicemail is full click here to listen." When you tap the link, you are taken to a fake site that asks for your phone number and password, letting scammers steal your account details or install malware on your device.

4. Web Spam

Web spam appears on websites, blogs, or forums. Spammers post irrelevant comments, repeat the same message, or add links to unrelated websites. Their goal is usually to get attention, sell something, or improve their search engine ranking. A blog might have a comment like "Great post! Visit my site for free stuff," posted over and over. This kind of spam makes sites look messy and untrustworthy.

5. Instant Messaging Spam

Instant messaging spam shows up in chat apps like WhatsApp, Messenger, or Telegram. Spammers send fake offers, suspicious

links, or files in messages. Sometimes, these come from hacked accounts or unknown numbers. Consider you get a text message from an unknown number saying, "Your voicemail is full, click here to listen." When you tap the link, you are taken to a fake site that asks for your phone number and password, letting scammers steal your account details or install malware on your device.

6. Voice Spam (Spam Calls)

Voice spam, also known as spam calls or robocalls, is when you receive unwanted phone calls, often from automated systems. These calls pretend to be from your bank, tech support, or even government services. They might tell you there is a problem with your account and ask you to press a button or give personal details. An example of this is a voice message that might say, "Your bank account is locked. Press 1 to fix it," but it is a scam trying to steal your information.

1.4.8.2 Spam prevention methods

1. **Use Spam Filters**

Spam filters are crucial for detecting unwanted emails. These filters analyse incoming messages based on specific characteristics like suspicious links, keywords, or the sender's reputation. The best approach is to enable a combination of content-based and reputation-based filters and use machine learning-based systems, such as Gmail's filtering, which improves over time. It's important to regularly update your spam filter's rules to keep up with evolving spam tactics.

2. **Require Double Opt-In**

A double opt-in process ensures that subscribers genuinely want to receive your emails. After a user subscribes, they receive a confirmation email with a link to verify their intent. This reduces accidental or fraudulent sign-ups. To enhance this process, make sure the confirmation email clearly explains what the user is opting into and avoid using a single opt-in process. Use time-limited confirmation links to deter bot sign-ups.

3. **Authenticate Outgoing Mail (SPF, DKIM, DMARC)**

Email authentication methods like SPF, DKIM, and DMARC are vital for preventing impersonation and ensuring that your emails are from trusted sources. SPF specifies authorised IP addresses for sending emails on your behalf, DKIM adds a digital signature for verification, and DMARC helps you define how receiving servers should handle unauthenticated emails. Implementing all three methods boosts your email deliverability and protects your brand. Monitoring DMARC reports regularly ensures any authentication issues are promptly addressed.

4. **Include an Unsubscribe Link**

Including an unsubscribe link in your emails is both a legal requirement and a best practice. It should be easy to find and allow users to unsubscribe immediately. The process must be simple and not require users to log in or provide personal details. Avoid deceptive language or multistep processes that make unsubscribing difficult, as this can frustrate users and increase complaints.

5. **Use CAPTCHAs on Web Forms**

CAPTCHAs are essential for differentiating between human users and automated bots, particularly on web forms like contact pages or sign-up forms. Modern CAPTCHA services like Google's reCAPTCHA are effective and user-friendly, ensuring that only legitimate users can submit forms. Invisible or "soft" CAPTCHAs can be implemented to trigger only when suspicious activity is detected, providing a better user experience.

6. **Validate and Sanitize Input**

To prevent spam from entering your system through form submissions, it's important to validate and sanitize user input. This involves filtering out unwanted characters, scripts, or links that may indicate spam. Regular expressions can help with this, and rate limiting submissions can reduce the risk of bulk attacks. Server-side validation is essential for flagging hidden fields or malicious content, further protecting your system.

7. **Limit Message Rate**

Setting limits on the frequency of messages sent helps mitigate spam, especially in bulk attacks. You can implement rate limiting, such as one message per second, for actions like form submissions or email registrations. Applying these limits at both the user and IP address levels can help prevent large-scale spam attacks. For email systems, consider throttling bulk senders to avoid overloading your system and to prevent spam campaigns.

8. Keep Software Updated

Keeping your software up to date is essential for closing vulnerabilities that spammers might exploit. Set up automated updates for all your software, including CMS platforms, email servers, and plugins. Regularly check for security patches and apply them immediately. Using a security service that actively scans for vulnerabilities can further protect your systems from being compromised by spammers.

9. Educate Users

User education plays a critical role in preventing spam-related issues. Providing training on how to recognise phishing attempts and other malicious activities can significantly reduce the success rate of spam attacks. In your emails, clearly highlight potential risks and advise users to avoid clicking on links from unknown sources. Encouraging users to report suspicious messages to your security team can also help identify threats early.

10. Block and Blacklist

Maintaining updated blacklists of known spammy IP addresses, domains, or phone numbers is an effective strategy for blocking unwanted messages. You can use public blacklists like Spamhaus or maintain a custom list of flagged senders. Automating the process of adding and removing addresses from your blacklist can save time and reduce errors. Implementing a dynamic system that flags suspicious senders based on behaviour patterns enhances your ability to stop spam before it reaches your inbox.

Recap

- **Importance of Network Security** – Protects networks from cyber threats and ensures safe, continuous operations.
- **Key Reasons for Protecting Networks and Data** – Prevents data breaches, financial losses, IP theft, and regulatory penalties.
- **Advantages of Network Security** – Enables data safety, business continuity, legal compliance, and user trust.
- **Malware** – Malicious software like viruses, worms, and ransomware that disrupt or steal from systems.
- **Firewall** – A security tool that monitors and filters network traffic based on rules.
- **Antivirus** – Software that detects, blocks, and removes malware using real-time and behavioural analysis.
- **Phishing** – A scam that uses fake communication to steal personal or sensitive information.
- **Clickjacking** – A trick that hides harmful actions behind harmless-looking clicks.
- **Spamming** – Sending bulk, unwanted messages to trick users or spread malware.
- **Types of Spamming** – Includes email, SMS, social media, and voice spam, each with deceptive intent.

Objective Questions

1. What is the general term for software designed with malicious intent?
2. What network security device monitors and controls incoming and outgoing traffic?
3. What type of attack tricks users into clicking on something unintended?
4. What is the term for unwanted, irrelevant, or repetitive digital messages sent in bulk?
5. What is a common type of malware that attaches to legitimate programs?
6. What type of targeted phishing focuses on high-profile individuals?
7. What security software helps identify, prevent, and remove malicious software?
8. What is the act of impersonating trustworthy entities to obtain sensitive information?
9. What type of firewall tracks the state of active connections?
10. What is the term for text message-based phishing attacks?

Answers

1. Malware
2. Firewall
3. Clickjacking
4. Spamming
5. Virus
6. Whaling
7. Antivirus
8. Phishing
9. Stateful
10. Smishing

Assignments

1. Why is network security essential for maintaining operational continuity and protecting sensitive information?
2. Explain the impact of malware on a network and describe two common types.
3. What are firewalls and how do different types (packet filtering, stateful inspection, proxy) enhance network protection?
4. Describe phishing and list two methods attackers use to trick individuals.
5. What is clickjacking? Provide an example to illustrate how it works.

Reference

1. Shotton, M. A. (1989). *Computer addiction? A study of computer dependency*. Taylor & Francis. (While older, this is a real book title and follows the basic APA format.)
2. Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. Simon & Schuster. (Another actual book that explores technology's impact on identity.)
3. Rheingold, H. (1993). *The virtual community: Homesteading on the electronic frontier*. Addison Wesley Publishing Company. (A foundational book in the study of online communities.)
4. Castells, M. (2000). *The rise of the network society* (2nd ed.). Blackwell Publishers. (An influential work on the societal impact of network technologies, with an edition noted.)
5. Lanier, J. (2010). *You are not a gadget: A manifesto*. Alfred A. Knopf. (A more contemporary book offering a critical perspective on digital culture.)

Suggested Reading

1. McClure, S., Scambray, J., & Kurtz, C. (Year of publication). *Hacking exposed: Network security secrets & solutions* (Latest Edition). McGraw Hill.

2. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (Year of publication). *Firewalls and internet security: Repelling the wily hacker* (Latest Edition). Addison Wesley Professional.

3. Szor, P. (Year of publication). *The antivirus book: The Sophos guide to computer security*. John Wiley & Sons.

4. Hadnagy, C. (Year of publication). *Social engineering: The art of human hacking*. Wiley.

Unit 5

Managing Web and Email

Learning Outcomes

On completion of this unit, the learner will be able to:

- Describe the importance of web content and email communication management
- Describe effective password policies for improved security
- Describe the role of CAPTCHA and Two-Way Authentication in protecting online accounts
- Explain how browsing history works and its impact on privacy and usability
- Explain different types of cookies and describe effective session management techniques

Background

You are probably familiar with the need to create strong passwords for your online accounts, and you may have already encountered CAPTCHA when trying to verify that you are not a robot. You've likely seen pop-up ads while browsing the internet and know how they can be frustrating. Perhaps you've also received an email asking you to confirm your identity with a second step for added security; this is known as two-way authentication. In this course, we'll build on your existing experiences and dive into password policies to understand how to create safer online accounts, explore how CAPTCHA works to protect websites, and learn the importance of two-way authentication for extra security. We will also explore cookies and session management, which help websites remember your preferences and login information. You'll discover practices for managing your browsing history to keep your online activity secure and learn how to block ads and pop-ups that can affect your browsing experience. Additionally, we will discuss the safe and efficient use of email, ensuring you understand how to manage your inbox and keep your communication secure.

Keywords

Password Policy, Multi-Factor Authentication (MFA), Two-Factor Authentication (2FA), Ad Blockers, Pop-up Blockers, Phishing.

Discussion

1.5.1 Introduction

In the digital era, the effective management of web content and email communications is essential for personal productivity and organisational efficiency. Web content management involves creating, organising, and maintaining digital content across various platforms, ensuring that information is accurate, accessible, and aligned with the organisation's objectives. This process often utilises Content Management Systems (CMS) that offer user-friendly interfaces, allowing even non-technical users to manage content efficiently. A well-structured CMS can enhance collaboration, streamline workflows, and improve search engine optimisation, making it a vital tool for businesses and individuals alike.

Similarly, managing email communications effectively is crucial for maintaining professionalism and ensuring timely responses. Implementing best practices such as establishing clear email policies, utilising filters and labels, and scheduling regular email check-ins can significantly enhance productivity. Maintaining professional email etiquette through clear subject lines, appropriate greetings, and concise content helps in conveying messages effectively and fostering positive relationships. By integrating these strategies, individuals and organisations can manage their digital communications more efficiently, reducing clutter and improving overall workflow.

Furthermore, integrating web content and email management systems can lead to a more cohesive digital strategy. Linking email communications with content management platforms allows for seamless sharing of updates, promotions, or newsletters directly from the CMS to targeted email lists. This integration ensures consistency in messaging, enhances audience engagement, and streamlines the process of disseminating information. By adopting a holistic approach to managing both web content and email communications, organisations can create a unified and efficient digital presence that resonates with their audience.

1.5.2 Password Policies

In today's digital landscape, robust password policies are essential for safeguarding sensitive information and maintaining cybersecurity. A well-structured password policy outlines the requirements for creating, managing, and securing passwords within an organisation, aiming to mitigate unauthorised access and data breaches.

Key Components of an Effective Password Policy

1. **Minimum Password Length and Complexity**: Establishing a minimum password length of at least 8–12 characters is recommended, with a mix of uppercase and lowercase letters, numbers, and special characters. However, recent guidelines suggest prioritising password length over complexity, advocating for longer passphrases instead of complex combinations.

2. **Password Expiration and History**: While traditional practices mandated regular password changes, current recommendations advise against frequent changes unless a breach is suspected. Instead, enforcing a password history policy that prevents users from reusing recent passwords can enhance security.

3. **Multi-Factor Authentication (MFA)**: Implementing MFA adds an additional layer of security by requiring users to provide two or more verification factors, such as a password and a one-time code sent to their mobile device.

4. **Account Lockout Mechanisms**: Setting up account lockout procedures after a specified number of failed login attempts helps prevent brute force attacks.

5. **User Education and Awareness**: Regular training sessions should be conducted to educate users about the importance of strong passwords, recognising phishing attempts, and adhering to the organisation's password policies.

By integrating these components, organisations can establish a comprehensive password policy that not only enhances security but also fosters a culture of cybersecurity awareness among users.

1.5.3 CAPTCHA

CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart." It is a tool used on websites to make sure that the user is a human, not a computer or robot (bot). Many websites use CAPTCHA to protect themselves from fake users, spam, and hacking attempts. When you try to log in to a website or submit a form, it may ask you to:

- Type some distorted letters or numbers.
- Click on images showing a specific object (like cars or bicycles).
- Or check a box saying "I'm not a robot."

1.5.3.1 Importance of CAPTCHA

- **Blocks bots:** It stops automated software (bots) from filling out forms, creating fake accounts, or posting spam.
- **Improves security:** Helps protect login pages and registration forms from hacking.
- **Protects resources:** Stops websites from being overloaded by fake traffic.

1.5.3.2 Types of CAPTCHA

- **Text CAPTCHA:** Shows jumbled letters or numbers that you must type.
- **Image CAPTCHA:** Asks you to select certain images, like all traffic lights.
- **Audio CAPTCHA:** Plays a sound that you must type in (for people who can't see well).
- **reCAPTCHA:** A newer version by Google. You might just have to click "I'm not a robot" or it checks in the background automatically.

1.5.3.3 Advantages and Disadvantages of CAPTCHA

Advantages:

- Easy for humans, hard for bots.
- Helps reduce spam and fake traffic.

Disadvantages:

- May be difficult for people with disabilities.
- Can slow down user experience.

1.5.4 Two-Way Authentication

Two-Way Authentication (also called Two-Factor Authentication or 2FA) is a method that adds extra security to your online accounts. Instead of just using a password, it asks for a second way to prove your identity. This second step makes it much harder for hackers to access your account, even if they know your password.

1.5.4.1 Working of Two-Way Authentication

When you log in, the first step is to enter your password. After that, you are required to provide a second form of verification, such as a code sent to your mobile phone or email, or by using a fingerprint or face scan. This two-step process significantly enhances the security of your account, making it much harder for unauthorised users to gain access.

Types of Second Step Verification Methods

- One-time password (OTP) sent by SMS or email.
- Code generated by an app like Google Authenticator or Authy.
- Fingerprint or face scan.
- USB security key.

1.5.4.2 Importance of Two-Way Authentication

Even if someone guesses or steals your password, they won't be able to log in without the second code. This extra layer of protection is especially important for securing sensitive accounts such as online banking, email accounts, cloud storage, and social media. By requiring both your password and a second form of verification, two-way authentication helps ensure that only you can access your valuable personal information.

1.5.4.3 Advantages and Disadvantages

Advantages

- Stronger security than just a password.
- Reduces risk of hacking, phishing, and password theft.

Disadvantages

- May need a mobile phone or internet.
- Can be inconvenient if you lose access to your second method.

1.5.5 Browsing History

Browsing history is a feature found in all web browsers that keeps a record of the websites and web pages you have visited. This information includes the URLs (website addresses), page titles, and the time and date of the visits. It helps users revisit websites easily and allows browsers to autofill addresses or suggest frequently visited pages.

If you regularly visit a website like www.wikipedia.org, your browser will save this site in your history, making it easier to access the next time you need it. Browsing history can be a helpful tool, allowing users to go back to previously visited websites without needing to search for them again. This can be especially useful when dealing with research or multiple open tabs. Also, many websites use your history to personalise your experience, such as showing content you are most likely to be interested in. For instance, if you visit "https://www.wikipedia.org" on a browser, the following information is stored in the browsing history:

- URL: https://www.wikipedia.org
- Page Title: Wikipedia
- Timestamp: The exact time you visited the site.

1.5.5.1 Purpose of Browsing History

- **Autofill Suggestions**: When you start typing in the address bar, the browser will suggest previously visited websites based on your history.
- **Easy Navigation**: If you want to go back to a website you visited earlier, you can simply check the history instead of searching for it again.
- **Website Personalisation**: Some websites may change their content or appearance based on your browsing history.

When you start typing "goog" in the address bar, your browser might automatically suggest "www.google.com" because it's a frequently visited site.

1.5.5.2 Privacy Concerns

Storing browsing history can raise privacy concerns. Anyone who has access to your device can see your online activity. That's why browsers also give the option to clear your history manually, or to set automatic deletion after a certain period. Using incognito or private browsing mode is another way to prevent browsers from saving your history during a session. Main concerns are:

1. Browsing history is stored locally on your device, and anyone with access to your device can see the websites you've visited.
2. Browsers also send browsing history to third-party services and advertising networks for targeted ads and tracking.
3. **Incognito Mode:** This mode disables the saving of browsing history and cookies, helping you maintain privacy.

How to Clear Your Browsing History

In Google Chrome, you can clear your browsing data by clicking on the three dots (menu) at the top right corner of the browser, then selecting "History" and choosing "Clear browsing data." From there, you can decide whether to delete browsing history for a specific time frame, such as the last hour or the last 24 hours, or you can choose to clear all history.

1.5.6 Cookies and Session Management

1.5.6.1 Cookies

Cookies are small text files that store information about your preferences such as language preferences, items in a shopping cart, login status, and browsing activity. When you visit a website, the website sends a cookie to your browser, which is stored locally on your device. These cookies help websites remember information about you. If you log into a website like Facebook, the site sends a cookie that remembers your login credentials. The next time you visit Facebook, the website reads the cookie and automatically logs you in, so you don't have to enter your username and password again.

Types of Cookies

1. **Session Cookies**

Temporary cookies that are deleted once you close your browser. For example, when you log into an online store, a session cookie helps maintain your login until you close the browser.

2. Persistent Cookies

Persistent cookies stay on your device for a set period, even after you close your browser. They are used to remember preferences or settings for future visits. For example, when you visit a website like YouTube, persistent cookies store your language preferences or video recommendations.

3. Third-Party Cookies

Third-party cookies are set by domains other than the one you are currently visiting (often advertisers or analytics services). For example, when you visit a website that displays an advertisement from Google Ads, Google sets a third-party cookie to track your activity across various websites.

Managing cookies involves adjusting the settings in your browser. Most modern browsers give users the ability to view, delete, or block cookies from specific websites. You can also use browser extensions like Privacy Badger or uBlock Origin to block third-party cookies. For users who prioritise privacy, browsers like Brave are specifically designed to block trackers and advertisements by default.

1.5.6.2 Session Management

Session management refers to the process by which a website tracks your actions during your visit, such as logging in or interacting with the page. It refers to how a website tracks and manages a user's activity during a session (a period of time a user is logged in or actively using the site). Websites often use session IDs stored in cookies to track the session. Good session management includes features like automatic logouts after inactivity, secure handling of login information, and protection from session hijacking (when attackers steal session IDs to gain unauthorised access). Secure websites use HTTPS and encryption to keep session data safe.

How Session Management Works

When you log into a website, a session ID is created and stored either in a cookie or the URL.

The session ID allows the website to "remember" who you are and maintain your session until you log out or the session expires.

Session management helps websites maintain a continuous experience for users. However, it can also be vulnerable to attacks such as session hijacking or session fixation. In a session hijacking attack, an attacker steals a valid session ID, which allows them to impersonate a legitimate user. This can be prevented by using HTTPS (Hypertext Transfer Protocol Secure) for secure communication and ensuring that session data is properly encrypted. Session timeouts can also be used to automatically log users out after a period of inactivity, reducing the window for attacks.

A common scenario that illustrates session management is logging in to an online banking website. You enter your username and password, and the bank creates a session ID that is stored in a cookie, allowing you to remain logged in while navigating different parts of the site. If you leave and return shortly after, the session ID helps the website remember you and continue the session without requiring another login.

Security Risks in Session Management

While session management enhances user experience, it also introduces certain security risks. One major threat is session hijacking, where an attacker steals your session ID and uses it to impersonate you. Another threat is session fixation, in which an attacker sets a known session ID before you log in, allowing them to gain access once you authenticate. To prevent such attacks, websites use secure protocols like HTTPS, implement proper encryption, and enforce session timeouts after periods of inactivity.

Preventing Session Hijacking

To reduce the risk of session hijacking, several protective measures can be implemented. The most important step is to always use HTTPS to ensure secure communication between the browser and the server. Also, enabling session timeouts helps protect user accounts by automatically logging users out after a period of inactivity, limiting the opportunity for unauthorised access.

1.5.7 Ad and Pop-up Blocking Practices

Ads and pop-ups are common features on websites, but they can be incredibly annoying and even harmful. Many websites rely on advertising as their main source of income, and so they display a variety of ads such as banners, pop-ups, or autoplay videos. However, not all ads are benign. Some pop-ups can lead to malvertising, a type of malicious ad designed to infect your computer with malware or steal personal information. Others might redirect you to phishing sites or display false information.

Ad blocking tools and pop-up blockers help users avoid these issues. Many browsers come with built-in pop-up blockers, which prevent unwanted windows from opening while you browse. In addition, there are various browser extensions such as AdBlock, uBlock Origin, and Ghostery that block most types of ads. These tools enhance your privacy by preventing third-party advertisers from tracking your online activity across websites. For example, if you're browsing a website like YouTube, ad blockers can prevent video ads from appearing before your content starts, saving time and reducing interruptions. These extensions are easy to install, and most of them allow you to whitelist certain websites if you want to support the creators who depend on ads for revenue.

However, there are drawbacks to ad blocking. Many websites depend on ads to generate revenue and provide free content. If users block ads entirely, it can negatively impact the site's revenue, potentially leading to reduced functionality or a paywall for content. Some websites may even detect that you are using an ad blocker and request that you disable it to access their content.

Disadvantages of Blocking Ads and Pop-ups

- **Interruptive:** Pop-ups often interfere with user experience and can disrupt navigation.
- **Security Risks:** Malicious ads (malvertising) can lead to malware or phishing attacks.
- **Data Privacy:** Many ads use third-party trackers to collect personal information.

Tools and Techniques for Blocking Ads and Pop-ups

Browser Extensions

- **AdBlock Plus:** Blocks most ads on websites.
- **uBlock Origin:** A more advanced ad blocker with greater customisation options.
- **Ghostery:** Focuses on blocking trackers and ads that monitor your browsing behaviour.

For instance, if you install AdBlock Plus, most video ads, banner ads, and pop-ups on YouTube or news websites will be automatically blocked.

1. **Built-in Browser Features:**Browsers like Google Chrome, Mozilla Firefox,

and Safari have pop-up blockers that prevent unwanted pop-ups from appearing while you browse.

2. **Security Software:**Some antivirus software comes with built-in ad and pop-up blockers to protect you from malicious ads.

Potential Downsides of Blocking Ads

- **Decreased Revenue for Websites:** Many websites rely on ad revenue to provide free content. Blocking ads may prevent websites from earning money, leading to reduced services or paywalls.
- **Some Sites May Not Load Properly:** Certain websites may display error messages if they detect ad-blocking software.

1.5.8 Email Usage

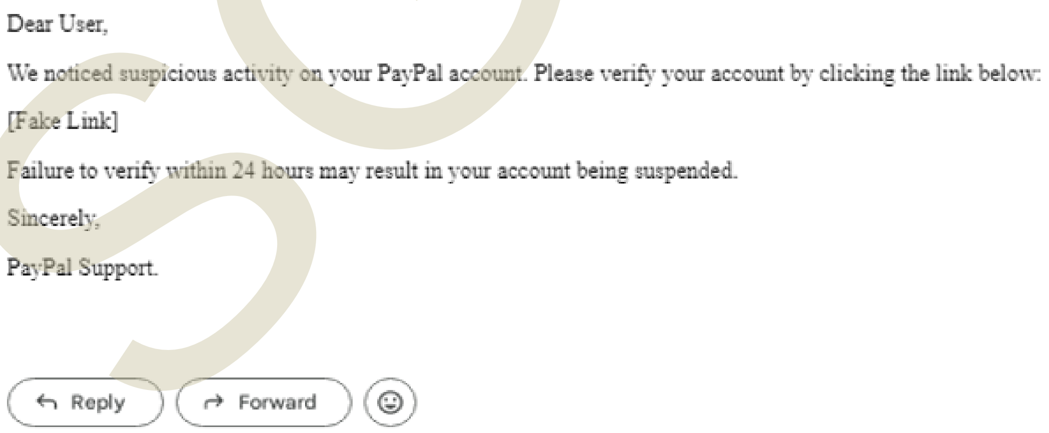
Email is one of the most widely used communication tools, both for personal and professional purposes.

Emails are categorised into types:

- **Personal emails** are used to communicate with friends and family.
- **Work or professional emails** are for job-related communication and should be formal and respectful.
- **Spam or promotional emails** include advertisements or junk mail, and sometimes carry malware.

Email accounts are also a common target for hackers, scammers, and cybercriminals. To maintain a secure and effective email environment, users need to follow a few best practices. When creating an email account, it's important to use a strong password that combines letters, numbers, and special characters. A strong password makes it harder for attackers to guess or crack your account. Also, enabling two-factor authentication (2FA) is a great way to add an extra layer of security. With 2FA, even if someone gets hold of your password, they will also need to access a second factor, such as a text message code or a mobile app approval, to log into your account.

Avoid clicking on suspicious links or downloading attachments from unknown senders, as these could be phishing attempts. One of the major threats in the email world is phishing. Phishing emails are fraudulent messages that impersonate legitimate organisations, such as your bank, social media sites, or popular online stores. These emails often ask you to click on a link or open an attachment, which can steal your personal information or install malware on your device. A common phishing email might look like a message from PayPal saying your account is locked and asking you to click a link to verify your information. These links often lead to fake websites that look like



Dear User,

We noticed suspicious activity on your PayPal account. Please verify your account by clicking the link below:

[Fake Link]

Failure to verify within 24 hours may result in your account being suspended.

Sincerely,

PayPal Support.

Fig 1.5.1 Phishing Email

real ones, but their purpose is to capture your login credentials.

A common phishing email might appear as follows:

Besides phishing, another frequent email-based threat is malware, which can be delivered through attachments or embedded links. These files may appear harmless, such as an invoice in PDF format, but once opened, they can install harmful software on your device without your knowledge.

To stay protected, always avoid clicking on unfamiliar links or downloading attachments from suspicious emails. If an email appears to come from a legitimate organisation, take a moment to verify it by contacting the source directly using an official phone number or website, never through the email itself.

Furthermore, effectively managing spam (unwanted or unsolicited emails) is important for maintaining a clean and secure inbox. Most email services, such as Gmail and Outlook, come with built-in spam filters that automatically detect and redirect suspicious emails to a spam folder. To improve these filters, you should regularly mark unwanted messages as spam, helping your email provider identify and block similar messages in the future.

Recap

- **Web Content Management**: CMS tools help users, even those without technical skills, efficiently create, organise, and maintain web content.
- **Password Policies**: Strong, lengthy passwords combined with multi-factor authentication (MFA) and password history rules enhance security.
- **Multi-Factor Authentication (MFA)**: MFA adds a second layer of security by requiring multiple forms of verification to access an account.
- **CAPTCHA**: CAPTCHA systems protect websites by ensuring that users are human and preventing bot-related activities.
- **Two-Factor Authentication (2FA)**: 2FA strengthens security by requiring a second authentication method, like an OTP or biometric scan.
- **Browsing History**: Browsing history allows easy navigation of visited sites but raises privacy concerns, which can be managed by clearing history or using Incognito Mode.
- **Cookies and Session Management**: Cookies store preferences and session data to improve user
- experience, but can also present privacy risks such as session hijacking.
- **Ad and Pop-up Blocking**: Ad and pop-up blockers improve user experience by removing intrusive content, though they can affect website revenue.
- **Email Usage and Security**: Securing email accounts through strong passwords, 2FA, and careful handling of phishing and malware threats is essential for privacy and protection.

Objective Questions

1. What is the name of the system used to manage digital content on websites?
2. What security method requires two steps for user verification?
3. Which tool is used to differentiate humans from bots online?
4. What file type is stored by websites to remember user preferences?
5. What is the full form of MFA?
6. Which browser feature keeps track of visited websites?
7. What is a common method used by attackers to trick users into revealing sensitive information?
8. What type of cookie is deleted when the browser is closed?
9. Which protocol ensures secure communication between a user and a website?
10. What is used to block ads and trackers on websites?
11. What feature logs users out after a period of inactivity?
12. What do we call unsolicited or junk emails?
13. What Google service is a popular form of CAPTCHA?
14. Which code is sent to a mobile phone in Two-Factor Authentication?
15. What kind of blocker stops automatic browser pop-up windows?

Answers

1. CMS
2. 2FA
3. CAPTCHA
4. Cookie
5. Multi-Factor Authentication

6. History
7. Phishing
8. Session
9. HTTPS
10. AdBlocker
11. Timeout
12. Spam
13. reCAPTCHA
14. OTP
15. Pop-up blocker

Assignments

1. Explain the role of a Content Management System (CMS) in managing web content. Give an example of a popular CMS and describe its basic features.
2. Discuss the importance of having strong password policies in organisations. What are the latest recommendations regarding password complexity and expiration?
3. What is CAPTCHA? Describe two types of CAPTCHA and explain how they contribute to cybersecurity.
4. Describe how Two-Factor Authentication (2FA) works and explain its advantages and disadvantages with real-life examples.
5. What are cookies, and how do they impact user privacy and browsing experience? Differentiate between session cookies and persistent cookies with examples.
6. What are some common threats to email security? Provide examples of phishing and malware attacks and suggest ways to prevent them.
7. Explain how ad and pop-up blockers work. What are the pros and cons of using them, particularly for both users and content creators?

Reference

1. Brooks, C., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. Wiley.
2. Stamp, M. (2011). *Information security: Principles and practice* (2nd ed.). Wiley.
3. Kurose, J. F., & Ross, K. W. (2020). *Computer networking: A top down approach* (8th ed.). Pearson.
4. Google Safety Center. (n.d.). *Explore tools to help you stay safe online*. https://safety.google

Suggested Reading

1. Barker, D. (2016). *Web content management: Systems, features, and best practices*. O'Reilly Media.
2. Taylor, S. (2017). *Email essentials: How to write effective emails and build great relationships one message at a time*. Marshall Cavendish.
3. Krug, S. (2014). *Don't make me think: A common sense approach to web usability* (3rd ed.). New Riders.
4. Andress, J. (2019). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (3rd ed.). Syngress

BLOCK 02

INTERNET TECHNOLOGY

Unit 1

FUNDAMENTALS OF NETWORKING

Learning Outcomes

On completion of this unit, the learner will be able to:

- Understand the fundamentals of networking.
- Identify and describe network devices.
- Explore the difference between wired and wireless connections.
- Familiarise themselves with the concept of IP addressing.

Background

Imagine being able to connect with anyone, anywhere in the world with just a few clicks, or even better, understanding how this seamless communication happens behind the scenes. The world of networking is where this magic begins, and it's all about understanding the systems that power everything from sending an email to streaming your favourite video. The intricate web of devices, connections, and protocols is what keeps us connected, and by exploring these fundamental concepts, you'll gain the knowledge to be the architect of this digital universe.

In today's fast-paced digital age, a solid understanding of how data flows through networks and how different devices work together is more important than ever. From setting up your own network to troubleshooting common issues, this topic is a gateway to mastering the skills that keep our online world functioning. You'll discover how seemingly simple devices like routers and switches play a crucial role in guiding the data where it needs to go, ensuring everything works smoothly.

By learning how networks operate, you'll unlock the ability to understand not only how the internet works but also how to optimise and secure networks for better performance. It's like being given the keys to a highly efficient, yet intricate system that keeps the digital world running. Get ready to dive into this fascinating world where technology connects us all, and start discovering the building blocks that make it all possible!

Keywords

Hub, switch, router, modem, IP addressing, MAC addressing

Discussion

2.1.1 Networking concepts

Networking is the practice of connecting computers and other devices so they can share information and resources. In a network, devices such as desktops, laptops, printers, and servers are linked through wired or wireless connections, allowing them to communicate with each other. This communication enables the sharing of files, access to the internet, use of shared printers, and running of applications on remote systems. Whether it's a small setup at home or a large-scale system in an organisation, networking enables efficient and centralised management of data and resources.

At the most basic level, a network communication system consists of three fundamental components:

1. **Sender**: This is the device that originates the message or data. It could be a computer, smartphone, or any other digital device that sends information over the network.
2. **Transmission Media**: This refers to the channel through which the data travels from the sender to the receiver. It can be wired (such as Ethernet cables or fibre optics) or wireless (such as radio waves, WiFi, or Bluetooth).
3. **Receiver**: This is the device that receives the message or data sent by the sender. Like the sender, it can also be a computer, smartphone, server, or any other device capable of receiving and processing network data.

2.1.2 Network Devices

Network devices are physical devices used in computer networks. The primary purpose of these network devices is to connect various devices, including computers and printers. By connecting these devices, they form a network that helps the devices communicate and share resources. The connected devices can share data and interact with each other, ensuring that the information reaches the correct destinations. Various types of network devices are available, and some of them are listed below:

1. Hub
2. Switch
3. Router
4. Modem
5. Access point

2.1.2.1 Hub

A hub is a network connection device used in the physical layer of the OSI model. The hub acts as a central device that connects multiple devices in a network. The pictorial representation of a hub is shown in Figure 2.2.1. A hub contains multiple ports, and each of these ports can be used for connecting different computers in the network. Any device in the network can be a sender that can send information or data to any other computer or device in the network. The devices that receive that information are termed receivers, as shown in Figure 2.1.1.

2.1.2.2 Switch

A switch is a network connection device that works in the data link layer of the OSI model and uses packet switching to send and receive data over the network. A switch contains multiple ports to connect different components, as shown in Figure 2.1.3.

Fig 2.1.3 Switch

When data arrives, the switch extracts the destination address from the packet and references a table to determine the appropriate

A hub is a fundamental networking device that links several devices together within a Local Area Network (LAN).

Fig 2.1.1 Hub

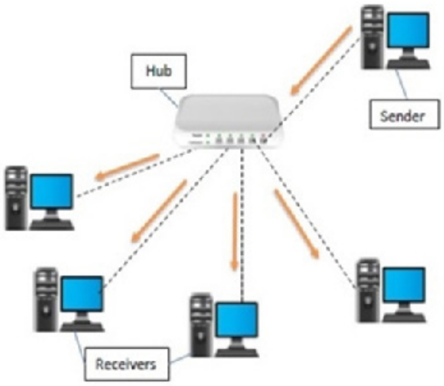


Fig 2.1.2 Network connection using Hub

forwarding path. Consequently, it directs the signal to specific devices rather than broadcasting it to all devices. It can handle the simultaneous forwarding of multiple packets. Ethernet switches are commonly used in homes and offices to connect multiple devices, thereby creating Local Area Networks (LANs) or facilitating Internet access. The working principle of the switch is the packet switching method. When a device (source) sends data over a network, the data is divided into smaller units called packets. A switch receives these packets through its ports. After receiving the packets, the switch must forward them to their destination (target device) within the network.

2.1.2.3 Router

A router is a network device that operates in the network layer of the OSI model. A router is similar to a switch, but it performs the function of directing data packets based on their IP addresses. A router connects a home or office network (LAN) to the Internet, allowing devices within the network to access websites, online services, and other external resources. Routers handle the task of receiving, analysing, and directing data packets between connected computer networks. Upon receiving a data packet, the router examines its destination address, checks its routing tables to determine the best path, and then sends the packet along that path. If two devices on different networks need to communicate, a router is required to facilitate their interaction. Figure 2.1.4 shows the network connection using the router.

2.1.2.4 Modem

A modem, which stands for Modulator/Demodulator, is a networking device utilised to establish an Internet connection for devices within a network. The primary function of a modem is to transform analog signals received from telephone lines into a digital format. In digital format, these converted signals are represented as binary digits, or 0s and 1s. The modem is also referred to as a signal translator because it converts signals from one form to another. It modulates digital signals into analog signals for transmission and subsequently demodulates incoming analog signals back into digital form.

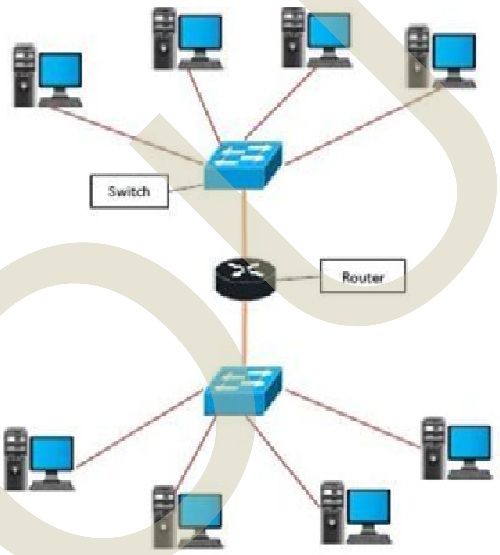


Fig. 2.1.4 A network connecting through a switch and a router

Examples of Modem

1. **Cable Modem:** Connects to cable internet services, allowing high-speed internet access.
2. **DSL Modem:** Used with DSL internet services, providing internet connectivity via telephone lines.

2.1.3 Network Connections

Network connections in computers are the links that let devices communicate and exchange data. Imagine you're talking to your friend. You can talk face-to-face or on a phone call. Both are different ways of communication, just like computers and devices use different ways to "talk" to each other. Connections can be classified based on:

1. How devices are physically connected.
2. How many devices are involved in the communication?

2.1.3.1 Classification based on how devices are physically connected

These connections can happen in two main ways: wired and wireless.

Wired Connection

A wired connection uses physical cables (like Ethernet) to link devices together. The most common wired network cable is the Ethernet cable (LAN cable). The cable carries data signals from one device to another, like a road for cars.

There are three main types of network cables used for data communication. Twisted pair cables are the most common, especially in local area networks (LANs). They consist of pairs of copper wires twisted together and are available in different categories like Cat5, Cat6, and Cat7. These cables are mainly used to connect computers to switches and routers.

Coaxial cables have a single copper wire core surrounded by insulation and shielding. Though less common today, they are still used for cable television and some broadband internet connections.

Fiber optic cables transmit data using light signals through thin strands of glass or plastic. They offer extremely high speed and are suitable for long-distance communication. Fiber optic cables are typically used in high-speed internet and large-scale network backbones.

Examples of wired connection:

1. A desktop computer connected to the internet using a LAN cable,
2. A printer connected to a computer with a USB or Ethernet cable,
3. An office network where all computers are linked through a switch using Ethernet cables.

Wired connections have some disadvantages. One major drawback is limited mobility, as devices must remain close to the cable, restricting movement. Another issue is cable clutter, since managing multiple wires can become messy and difficult, especially in larger setups.

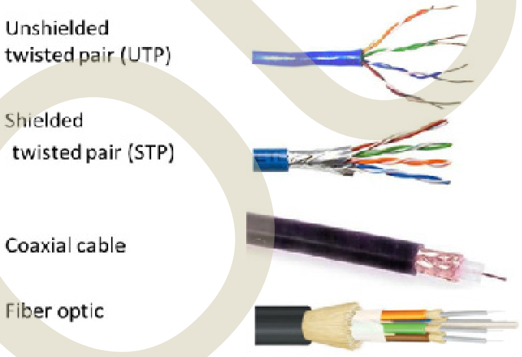


Fig. 2.1.5 Types of cables

Wireless Connection

A wireless connection sends data through the air using radio signals, so no physical cables are needed. Devices use built-in antennas to send and receive signals from a wireless router or access point.

Your smartphone connects to home WiFi, laptops use WiFi in a library or café, Bluetooth earbuds connect to your phone, etc.

Wireless Personal Area Network (WPAN)

WPANs are short-range wireless networks that typically cover just a few meters. They are mainly used for personal devices like smartphones, headphones, smartwatches, and laptops, often connected through Bluetooth. Because of their limited range, WPANs are ideal for communication between devices that are close to each other.

Wireless Local Area Network (WLAN)

WLANs cover a larger area than WPANs and are commonly used in homes, offices, and schools. The most popular example is the WiFi network. However, not all WLANs use WiFi. Other radio-based technologies can also be part of a WLAN. These networks usually work within a range of up to 100 meters and use radio waves or infrared signals to connect devices within a local area.

Wireless Metropolitan Area Network (WMAN)

WMANs can cover areas as large as 50 kilometres and are designed to connect locations across a metropolitan region. They are often used to link buildings of an organisation or to provide wireless internet access to entire towns or cities. A common example of a WMAN technology is WiMAX.

Wireless Wide Area Network (WWAN)

WWANs offer broad coverage using mobile towers or satellites and can span across cities, regions, or even remote areas. These networks support devices like smartphones, tablets, and laptops that need internet access while on the move. Although WWANs are great for mobile connectivity, they often provide slower speeds compared to smaller networks due to the large infrastructure and long distances involved.

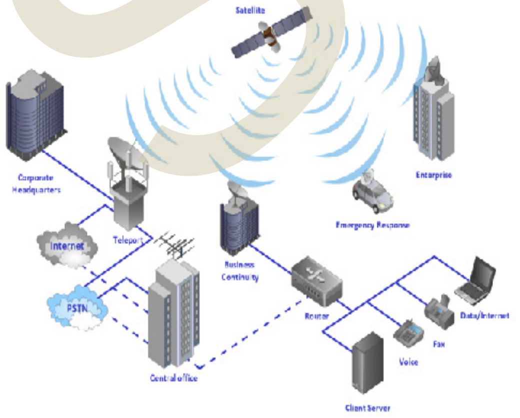


Fig. 2.1.6 Wired and Wireless Connections

2.1.3.2 Classification based on how many devices are involved in the communication

Computer networks can be classified based on the number of devices they connect and the way they enable communication. These networks range from small, local setups to vast, global systems. Depending on how devices interact and the number of devices involved, network connections can be categorised into three basic types:

Point-to-point connections enable communication between two devices. For example, two phones can pair to exchange contact details or pictures.

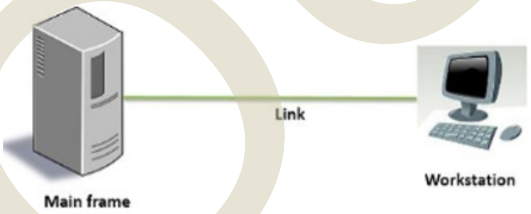


Fig. 2.1.7 Point-to-Point connection

1. Multipoint connections let one device communicate with multiple devices at the same time, sending messages to all of them simultaneously.

2. Broadcast/multicast connections allow a device to send a message to the network, with copies of the message being delivered to multiple recipients.

2.1.4 Understanding Network Performance: Bandwidth, Speed, and Interfaces

1. Bandwidth

Bandwidth refers to the capacity or maximum amount of data that can be transferred over a network connection in a given period, usually measured in bits per second (bps). To visualise it, think of bandwidth like a highway: the wider the highway (with more lanes), the more cars (data) can travel at once. For example, if your internet connection has a bandwidth of 100 Mbps, it means 100 megabits of data can be sent every second. The higher the bandwidth, the more data can be transferred at once, which helps make activities like large file downloads and high-quality video streaming smoother.

2. Speed

Speed refers to how quickly data can be transmitted over the network. Although it's often confused with bandwidth, speed is different. While bandwidth is about capacity, speed is about how fast the data travels. To illustrate, if bandwidth is like the width of a highway, speed is like the rate at which cars (or data) are moving. For example, you might have a high bandwidth connection, but if the speed is low, it can still take time for the data to reach you. Speed is commonly measured in terms like Mbps (Megabits per second) or Gbps (Gigabits per second).

3. Interfaces

Interfaces are the points of connection between devices on a network. These can either be physical ports, such as USB ports or Ethernet jacks, or wireless communication methods like WiFi or Bluetooth. To explain further, think of interfaces as the doors or gateways that allow data to flow between devices, similar to how doors connect different rooms in a house. An Ethernet interface connects your computer to a router with a cable, while a WiFi interface allows your phone to connect wirelessly to a network.

2.1.5 IP Addressing

IP addressing is like giving a unique home address to every device that connects to a network, such as the internet. This address allows devices to communicate with each other and find where to send data, similar to how letters are delivered to a specific house based on the address written on the envelope.

There are two main types of IP addresses:

1. **IPv4 (Internet Protocol Version 4)**: This is the most common type of IP address. It consists of four sets of numbers separated by periods. Each set can range from 0 to 255, for example, 192.168.1.1; think of this as a "street address" for your device. IPv4 allows about 4 billion unique addresses, but with so many devices connected to the internet today, we are running out of IPv4 addresses.

2. **IPv6 (Internet Protocol Version 6)**: To solve the problem of running out of IPv4 addresses, IPv6 was introduced. IPv4 uses 32 bits, whereas IPv6 uses 128 bits for its address space. With 128 bits, it can generate 2^128 unique addresses. It uses longer addresses made up of eight groups of four alphanumeric characters separated by colons, like 2001:0db8:85 a3:0000:0000:8a2e:0370:7334.

Example to Understand IP Addressing

Let's say you are using your phone to send a message to a friend's phone over the internet.

- Your phone has its own IP address (like 192.168.1.10) and your friend's phone has another (like 192.168.1.20).
- When you send a message, your phone's IP address is used as the "return address," while your friend's phone address is used to send the message to the right place.
- The network, using the IP system, ensures your message goes from one address to the other and that both phones can communicate properly.

In short, IP addressing is the system that assigns unique addresses to each device on a network, ensuring that data can be correctly routed to and from the right devices. It's like making sure that a letter sent across the world gets to the right destination based on its address.

2.1.6 MAC Address

To transfer data between computers, an address is required. In computer networks, different types of addresses are introduced, each functioning at a specific layer. The MAC address, short for Media Access Control Address, is a physical address that operates at the Data Link Layer. This article focuses on addressing the Data Link Layer, specifically the MAC address. A MAC address is a unique **48-bit**hardware number embedded into a network card, also known as a Network Interface Card (NIC), during its manufacturing. It is also referred to as the physical address of a network device. According to the IEEE 802 standard, the Data Link Layer is divided into two sublayers:

Logical Link Control (LLC) Sublayer: The LLC sublayer manages communication between the network layer and the data link layer. It is responsible for identifying network protocols, ensuring error checking, and controlling frame synchronisation. Essentially, it provides the logic needed to manage and maintain the link between devices.

Media Access Control (MAC) Sublayer: The MAC sublayer controls how devices on a network gain access to the physical medium (such as cables or wireless spectrum) and permission to transmit data. It ensures that data packets are placed onto the network medium correctly and determines how to address frames using MAC addresses. The MAC sublayer is critical in coordinating access to the shared medium in a network to avoid collisions and ensure data integrity.

The MAC address is utilised by the Media Access Control (MAC) sublayer of the Data Link Layer. Since there are millions of network devices worldwide, each one needs a unique identifier, which is provided by the MAC address.

MAC Address format

To fully grasp what a MAC address is, it's crucial to first understand its format. A MAC address is a 12-digit hexadecimal number (essentially a 6-byte binary number), typically represented in Colon Hexadecimal notation. The first 6 digits (for example, 00:40:96) of a MAC address identify the manufacturer, known as the OUI (Organisational Unique Identifier). These MAC prefixes are assigned to registered vendors by the IEEE Registration Authority Committee. The rightmost six digits represent the Network Interface Controller, which is assigned by the manufacturer.

Some OUIs of well-known manufacturers

D8:30:62	Apple Inc.
CC:46:D6	Cisco
AC:5F:3E	Samsung Electronics
3C:D9:2B	Hewlett Packard
3C:5A:B4	Google, Inc.
00:9A:CD	HUAWEI TECHNOLOGIES CO., LTD

IP Address vs MAC Address

Table 2.1.1 Comparison of IP Address and MAC Address

IP Address	MAC Address
IP stands for Internet Protocol	MAC tands for Media Access Control
It is a logical address	It is a physical address
It is provided by ISP	It is provided by the computer manufacturer
It can be changed by changing ISP	It is a fixed address for a particular device
It is applicable on the Network layer of the OSI model	It is applicable to the Data Link layer of the OSI model
The length of IPv4 is 32 bits and IPv6 is 128 bits	The length of a MAC address is 48 bits

Recap

- Networking: Involves connecting devices to share information and resources.
- Network Devices:
  - Hub: Broadcasts data to all connected devices.
  - Switch: Forwards data based on MAC addresses to specific devices.
  - Router: Directs data between networks using IP addresses.
  - Modem: Converts signals for internet access (digital to analogue).
  - Access Point: Connects wireless devices to a wired network.
- Connection Types:
  - Wired: Uses cables like Ethernet, coaxial, and fibre optics.
  - Wireless: Uses radio signals (WiFi, Bluetooth).
- IP Addressing:
  - IPv4: 32-bit addressing, limited to 4 billion addresses.
  - IPv6: 128-bit addressing, supports a vast number of devices.
- MAC Address: Unique hardware address for devices on a network.

Objective Questions

1. What device connects multiple devices within a local area network (LAN)?
2. What type of network uses wireless radio signals?
3. What does a router use to forward data between networks?
4. What is the 32-bit addressing scheme used in networking?
5. What is the unique hardware address for devices on a network?
6. What device converts digital signals to analogue for internet access?
7. What technology is used to connect wireless devices to a network?

8. What network device forwards data to a specific device based on MAC address?
9. What network cable type is commonly used for Ethernet connections?
10. What protocol is used to transfer files over the internet?

Answers

1. Switch
2. Wireless
3. IP Address
4. IPv4
5. MAC Address
6. Modem
7. Access Point
8. Switch
9. Ethernet
10. FTP

Assignments

1. Explain the difference between a switch and a router in terms of their function in a network.
2. Describe the purpose and function of an IP address in networking.
3. Discuss the key differences between IPv4 and IPv6 addressing schemes.
4. Illustrate the process of data transmission in a wireless network, highlighting key devices involved.
5. Explain how a MAC address is used in networking to identify devices on a local area network (LAN).

Reference

1. Tanenbaum, A. S., & Wetherall, D. (2011). *Computer Networks* (5th ed.). Pearson Education.

2. Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top Down Approach* (7th ed.). Pearson.

3. Forouzan, B. A. (2012). *Data Communications and Networking* (5th ed.). McGraw Hill.

Suggested Reading

1. Stallings, W. (2013). *Data and Computer Communications* (10th ed.). Pearson.

2. Comer, D. E. (2018). *Computer Networks and Internets* (6th ed.). Pearson.

3. Limoncelli, T. A., & Chalup, C. J. (2016). *The Practice of Cloud System Administration* (2nd ed.). Addison Wesley.

4. Peterson, L. L., & Davie, B. S. (2011). *Computer Networks: A Systems Approach* (5th ed.). Morgan Kaufmann.

5. Behrouz, A. F. (2008). *Data Communications and Networking* (4th ed.). McGraw Hill.

Unit 2

Cloud Computing

Learning Outcomes

On completion of this unit, the learner will be able to:

- Define cloud computing and identify its key characteristics
- Differentiate between the types of cloud services
- Explain the application of cloud computing
- Explain different types of cloud deployments

Background

Cloud computing is an exciting and rapidly growing field, and you might already be familiar with using applications like Google Drive, Dropbox, or even online shopping websites. These are examples of how cloud computing impacts our daily lives. In this topic, we will explore cloud computing in more detail and understand how it provides essential services for data storage, backup, big data analysis, and much more.

You may already know that saving files on your computer or mobile device takes up space and can be limiting. With cloud computing, all your data can be stored online, accessible from anywhere, and without worrying about storage limitations. We'll look at how this works, especially in areas like data backup and recovery, which are critical for businesses and individuals who need to secure their data.

In addition, if you're interested in fields like big data, app development, or e-commerce, cloud computing is key in powering these services. We'll also dive into how cloud computing supports innovations in education, IoT (Internet of Things), and wearable devices—topics that are shaping the future of technology.

Keywords

Private Cloud, Public Cloud, Community Cloud, Hybrid Cloud, SaaS, PaaS, IaaS, IoT

Discussion

2.2.1 What is Cloud Computing?

Cloud computing refers to the delivery of computing resources over the Internet. Instead of owning and maintaining physical servers or data centres, individuals and organisations can access technology services like servers, storage, databases, networking, software, and analytics on demand from a cloud service provider.

In simple terms, cloud computing allows users to use computing services as utilities, similar to electricity or water, without needing to understand or control the underlying infrastructure.

2.2.2 Key Characteristics of Cloud Computing

1. **On-Demand Self Service:**Users can provision resources like storage and computing power automatically, without human interaction with the service provider.
2. **Broad Network Access:**Services are available over the internet and accessible via standard devices like laptops, smartphones, and tablets.
3. **Resource Pooling:**Resources are pooled to serve multiple users using a multi-tenant model, with resources dynamically assigned based on demand.
4. **Rapid Elasticity:**Resources can be scaled up or down quickly, depending on workload needs.
5. **Measured Service:**Usage is monitored, controlled, and reported, providing transparency for both provider and user.

2.2.3 Types of Cloud Deployments

The cloud deployment model determines how cloud resources are allocated, accessed, and managed across users and organisations. The four primary cloud deployment models are private cloud, public cloud, community cloud, and hybrid cloud. Each model differs in terms of scalability, reliability, security, and cost, depending on how resources are shared and controlled.

2.2.3.1 Private Cloud

In a private cloud deployment, cloud infrastructure is dedicated exclusively to a single organisation. This setup offers enhanced control, customisation, and a high level of security since all resources are confined within the organisation. However, it often involves higher costs due to the need for dedicated infrastructure and in-house maintenance.

2.2.3.2 Public Cloud

The public cloud model delivers cloud services over the internet to multiple users or organisations. Resources are shared and delivered on a pay-per-use basis, making it highly scalable and cost-efficient. However, compared to private clouds, it may offer less control and reduced data security.

2.2.3.3 Community Cloud

Community cloud services are shared among several organisations that have similar operational concerns or objectives, such as regulatory compliance or security needs. This model strikes a balance between public and private clouds, offering resource sharing with improved security tailored to the community's requirements. Costs are typically distributed among the participating organisations.

2.2.3.4 Hybrid Cloud

The hybrid cloud model combines features of private, public, and sometimes community clouds. Organisations use a blend of on-premises infrastructure and cloud-based resources, enabling them to allocate workloads as per specific needs. While this model provides flexibility and optimised performance, it also introduces challenges related to integration, data consistency, and overall management.

2.2.4 Cloud Service Models

A cloud can interact with a client in a variety of ways through capabilities called services. Across the web, three major types or models of services have emerged.

2.2.4.1 Software as a Service (SaaS)

Software as a Service (SaaS) is a convenient way to access applications over the internet, letting users work through a web browser without needing to install or maintain software on their devices. SaaS can be used in different cloud setups: private, public, community, and hybrid. In a private cloud, the software runs on dedicated servers for one organisation, offering strong security and control that can be customised to meet specific needs. In contrast, public cloud SaaS shares infrastructure with other users, making it cost-effective and flexible, which is great for businesses that want to save money and reduce IT management. Community cloud SaaS brings together multiple organisations that have similar interests, allowing them to share resources and improve security.

Hybrid clouds mix both private and public cloud resources, giving organisations the best of both worlds. They can enjoy the scalability and flexibility of public cloud services while keeping their sensitive information secure in a private cloud. This setup is especially useful for businesses that need to balance strong security with cost savings.

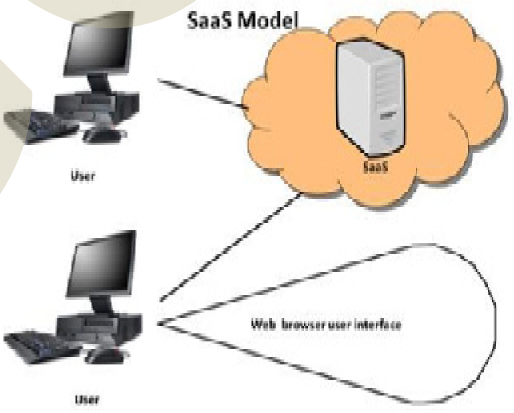


Fig. 2.2.1 illustrates the SaaS model.

Fig 2.2.1 SaaS Model presents a cloud-based application

2.2.4.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) is a system that helps developers create and manage applications without needing to handle all the technology involved. Normally, developers would have to set up and maintain things like servers, operating systems, and databases themselves. With PaaS, these are provided and managed by the platform, making the development process much easier. PaaS gives access to virtual servers, pre-set operating systems, ready-to-use databases, and tools that make coding and deploying apps simpler and faster.

Fig 2.2.2 PaaS Model provides an underlying platform for running applications.

In this system, developers don't have to worry about things like keeping the servers up to date or ensuring the databases are secure and running smoothly. Instead, they can focus on writing the code and developing the features of their application. The platform takes care of all the technical stuff in the background, making sure everything is working properly. This way, developers can launch their applications more quickly and efficiently while knowing the platform can grow and adapt to their needs.

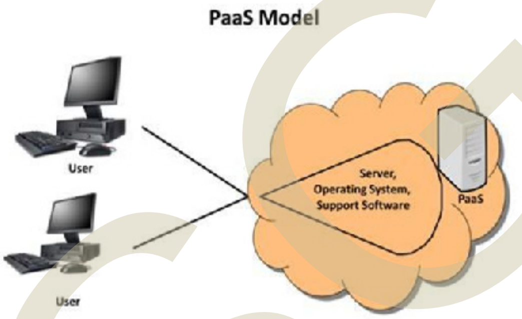


Figure 2.2.2 illustrates the PaaS Model.

2.2.4.3 Infrastructure as a Service (IaaS)

The Infrastructure as a Service (IaaS) model provides a virtual workspace in the cloud where you can access computing resources like servers and storage. It's like renting the building (infrastructure) but still being responsible for setting up the furniture (software). You get physical and virtual servers that can grow or shrink as needed, and the storage is flexible too, allowing you to increase or decrease it depending on how much data you need to handle.

However, with IaaS, while the provider takes care of the building (the hardware), you are in charge of installing and managing everything inside, like the operating system, databases, and other tools needed for your applications to run smoothly. It gives you the freedom to customise everything according to your needs but also requires you to monitor, update, and secure the systems to ensure everything is running efficiently.

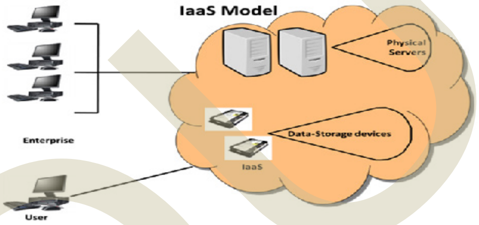


Figure 2.2.3 illustrates IaaS.

Fig 2.2.3 The IaaS model provides the underlying hardware (Servers and storage)

2.2.5 Applications of Cloud Computing

Cloud computing has transformed the way individuals and organisations access and manage computing resources. Below are some of the most important and widely adopted applications:

2.2.5.1 Online Data Storage

Cloud computing enables users to store, manage, and retrieve data over the internet instead of using local storage devices. This application is especially beneficial for users who need access to their data across multiple devices or locations.

Some of the key features of cloud computing include:

- Scalable storage capacity (you can increase or decrease as needed)
- Accessibility from anywhere with an internet connection

- Enhanced data sharing and collaboration
- Automatic synchronisation across devices

Well-known cloud storage services that demonstrate these features include Google Drive, Dropbox, Microsoft OneDrive, and iCloud, each offering convenient solutions for storing and managing files online.

2.2.5.2 Backup and Recovery

Data loss due to system crashes, accidental deletions, or natural disasters can be devastating. Cloud computing offers automated and secure backup solutions, allowing users to recover their data quickly and efficiently.

Important features of cloud-based backup services include:

- Scheduled automatic backups
- Version history (retrieve older versions of files)
- Fast recovery time
- Redundancy across multiple data centres for reliability

Popular platforms that offer such cloud backup capabilities include Acronis, Carbonite, AWS Backup, and Google Cloud Backup, each designed to ensure data availability and protection even in the face of unexpected disruptions.

2.2.5.3 Big Data Analysis

Cloud platforms offer powerful tools and infrastructure to process and analyse large and complex datasets (big data). This helps businesses gain insights into customer behaviour, market trends, and operational efficiency.

- Some of the important features of cloud-based big data solutions include:
- High-performance data processing tools
- Scalable computing power for real-time analytics
- Integration with AI and machine learning services

Among the widely used cloud solutions for big data analytics are Amazon EMR (Elastic MapReduce) offered by Amazon Web Services (AWS), BigQuery from Google Cloud, and Azure Data Lake along with Synapse Analytics provided by Microsoft Azure.

2.2.5.4 Software Development and Testing

Cloud computing provides developers with platforms and tools to build, test, and deploy applications quickly and efficiently without the need for costly physical infrastructure.

Key features of cloud-based development environments include:

- On-demand development environments
- Simulated real-world testing conditions
- Version control and collaboration features
- Continuous integration and continuous delivery (CI/CD)

Prominent services that support these capabilities include Microsoft Azure DevTest Labs, which provides quick environment setup; AWS CodeBuild and CodePipeline, which automate build and deployment tasks; and Google Cloud Build, designed for scalable CI/CD workflows in the cloud.

2.2.5.5 Cloud Computing Concepts in E-Commerce Applications

In the digital age, e-commerce platforms have become a major part of our daily lives, allowing us to buy and sell products and services from anywhere at any time. Behind the smooth functioning of these platforms lies a powerful technology known as cloud computing.

Cloud computing provides on-demand access to computing resources such as storage, servers, and software through the internet. This means that e-commerce businesses do not need to invest heavily in physical infrastructure. Instead, they can use cloud services to run their online stores, manage large volumes of customer data, process transactions, and ensure their services are available 24/7.

Why is Cloud Computing Important in E-Commerce?

E-commerce websites (online shopping platforms) need to:

- Manage thousands of users at the same time
- Store huge amounts of product and customer data
- Process payments securely
- Scale up or down during festivals or sales

Key Cloud Computing Features in E-Commerce

a. On-Demand Self-Service

This means that businesses can quickly get the computing resources they need (like storage space, servers, or software) without needing human assistance from the cloud provider. Everything can be managed through a web interface or dashboard. For example, during Diwali sales, Flipkart can increase server capacity to handle more users.

b. Scalability and Elasticity

Scalability means the ability to grow when needed. Elasticity means the ability to increase or decrease resources automatically based on demand. To illustrate this, consider a small boutique shop launching its online store. In the beginning, it requires only minimal computing resources. As customer traffic increases over time, cloud services allow the business to seamlessly scale up its infrastructure to meet the growing demand, ensuring smooth performance and uninterrupted service.

c. Pay-As-You-Go Model

This concept means that businesses only pay for the cloud resources they use, just like a utility service such as electricity or water. Imagine a startup that uses cloud storage services for just one month while testing its website. The company will only be billed for that specific month. If no services are used the following month, there will be no charges, making this model highly cost-effective and flexible.

d. Data Backup and Recovery

Cloud computing automatically backs up data to secure servers. If something goes wrong, like a system crash, power failure, or cyberattack, the data can be recovered without loss.

To illustrate this, consider an online clothing store that experiences a sudden power failure, making its local server inaccessible. Without a cloud backup solution, crucial customer order information could be lost. However, with cloud storage in place, the store can quickly retrieve all the data and resume operations with minimal downtime.

2.2.5.6 Cloud Computing in Education

Cloud computing has significantly transformed the educational landscape by providing flexible, cost-effective, and scalable technological solutions. It allows educational institutions to deliver learning content, manage administrative tasks, and support communication and collaboration through internet-based services. Cloud computing eliminates the need for physical infrastructure and offers a more efficient and accessible environment for both learners and educators.

Key Benefits of Cloud Computing in Education

1. Easy Access and Flexibility

Cloud services allow students and teachers to use learning materials and take part in classes from anywhere in the world, at any time. This was very helpful during the COVID-19 lockdowns when many schools and colleges moved to online learning. Tools like Google Classroom and Microsoft Teams helped schools to continue teaching by sharing notes, conducting online classes, and collecting assignments.

2. Saves Money

Using cloud services means that schools and colleges do not need to buy expensive computers or software. They can use cloud-based tools by paying only for what they use, which is often cheaper. Instead of buying software for every computer, a school can use free or low-cost tools like Google Workspace for Education.

3. Teamwork and Sharing Made Easy

Cloud tools help students and teachers work together on the same project or document at the same time, even if they are in different places. For example, students can work together on group assignments using Google Docs. Everyone can write and edit the file at the same time and give comments.

4. Safe Data Storage and Easy Backup

Important data like notes, student marks, and assignments are safely stored in the cloud. Even if a computer crashes, the data can be recovered. A university can save all course materials and student records on cloud services like Dropbox or OneDrive, so nothing is lost if something goes wrong.

5. Automatic Updates and Less Maintenance

Cloud software is always kept up to date by the service providers. This means schools do not have to worry about installing updates or fixing technical issues. Online test platforms are updated automatically, so colleges can use the latest tools for exams without needing any technical staff.

Cloud computing applications in education

Table 2.2.1 Cloud computing applications in education

Cloud Service	Purpose in Education	Example
Google Classroom (SaaS)	Online class management, assignment submission	Used by schools for remote learning
Microsoft Teams (SaaS)	Video conferencing, collaboration, and file sharing	Used by colleges for online lectures
Dropbox / OneDrive (SaaS)	Secure file storage and sharing	Used by teachers to share study materials
Amazon EC2 (IaaS)	Hosting virtual servers for educational platforms	Used by universities to run LMS (Learning Management Systems)
Google App Engine (PaaS)	Developing custom academic applications	Used for building student portals
Zoom (SaaS)	Conducting live online classes and webinars	Used for hosting guest lectures

2.2.6 Application of Cloud Computing in IoT and Wearable Devices

Cloud computing plays a crucial role in enabling the Internet of Things (IoT) and wearable technology by providing the infrastructure, storage, and computing power required to handle the massive amount of data generated by these devices.

Key Features

1. Data Storage and Accessibility

IoT devices and wearables generate continuous streams of data. Cloud computing provides scalable and centralised data storage, allowing real-time and historical data access from anywhere. Smartwatches like Apple Watch store health metrics such as heart rate and steps in the cloud, enabling users and doctors to view the data anytime through mobile apps.

2. Real-Time Processing and Analytics

Cloud platforms offer real-time data processing capabilities, helping to analyse information instantly and support timely decision-making. **IoT-based** fire alarm systems send smoke or temperature sensor data to the cloud. If dangerous levels are detected, alerts are triggered immediately on the user's phone.

3. Remote Monitoring and Control

Cloud computing enables users to monitor and control devices remotely using a web or mobile dashboard, making operations more efficient and responsive. Using a cloud-based app, a user can monitor the condition of smart home appliances or wearable fitness devices while travelling.

4. Data Backup and Recovery

The cloud ensures automatic backups and easy recovery of device data in case of failure or loss, increasing reliability and safety. If a person loses their fitness tracker, all their data is still available in the cloud and can be restored to a new device.

5. Security and Privacy

Cloud providers implement strong encryption, user authentication, and access control, protecting sensitive personal or industrial data collected by IoT and wearable devices. A wearable medical device tracking a patient's glucose levels encrypts and uploads the data to a secure cloud server, accessible only by authorised healthcare professionals.

6. Automatic Updates and Maintenance

The cloud allows automatic delivery of software or firmware updates to devices, ensuring they stay up to date with the latest features and security patches. For example, wearable devices receive new fitness features or health tracking improvements through cloud-based updates without user intervention.

7. Integration and Interoperability

Cloud services facilitate easy integration of data from different types of IoT and wearable devices into a unified system. For example, a smartwatch can share data with a cloud-based fitness app, diet tracker, and healthcare provider all at once, enabling better health monitoring.

Recap

- Cloud computing delivers computing services like servers, storage, databases, networking, software, analytics over the internet.
- Key Characteristics of Cloud Computing
- On-Demand Self-Service: Provision resources without human intervention.
- Broad Network Access: Services accessible over standard devices.
- Resource Pooling: Shared resources serve multiple users dynamically.
- Rapid Elasticity: Scale resources up or down instantly.
- Measured Service: Transparent monitoring and billing of usage.
- Types of Cloud Deployments
- Private Cloud – Exclusive infrastructure for one organisation.
- Public Cloud – Shared infrastructure, accessible via the internet, cost-effective.
- Community Cloud – Shared among similar organisations (e.g., universities, banks).
- Hybrid Cloud – Combination of public/private clouds for flexibility and performance.
- Cloud Service Models
- Software as a Service (SaaS) : Delivers applications via the internet. No installation needed. Example: Google Workspace, Microsoft 365.
- Platform as a Service (PaaS) : Provides platforms for developers to build and deploy apps. Example: Google App Engine, Microsoft Azure App Services.
- Infrastructure as a Service (IaaS): Offers virtual servers, storage, and networking resources. Example: Amazon EC2, Google Compute Engine.
- Applications of Cloud Computing
- Online Data Storage: Centralised data access, sharing, and backup across devices. Examples: Dropbox, Google Drive.
- Backup and Recovery: Automated, reliable data protection solutions. Examples: AWS Backup, Carbonite.
- Big Data Analysis: Large-scale data processing for business insights. Examples: AWS EMR, Azure Synapse.
- Software Development and Testing: On-demand environments for agile app development. Examples: AWS CodePipeline, Azure DevTest Labs.

- Cloud in E-Commerce: Supports scalability, uptime, secure transactions, and global access.Examples: Flipkart using cloud to scale during festive sales.
- Cloud in Education: Enables remote learning, resource sharing, and virtual classrooms. Examples: Google Classroom, Microsoft Teams for Education.

O Objective Questions

1. What is the term for the delivery of computing services over the internet?
2. Which model of cloud computing provides infrastructure resources like servers and storage?
3. What is the cloud service model where applications are hosted and provided over the internet?
4. Which service model provides a platform for building, running, and managing applications?
5. What term refers to storing and accessing data over the internet, rather than on a local server?
6. What is the practice of automatically adjusting computing resources based on demand in the cloud?
7. What is the term for a cloud infrastructure dedicated to a single organisation?
8. Which cloud deployment model involves sharing computing resources between multiple organisations?
9. What term refers to a cloud setup that combines both public and private clouds?
10. What type of cloud service provider offers computing infrastructure like storage, networking, and virtual machines?

A Answers

1. Cloud
2. IaaS

3. SaaS
4. PaaS
5. Cloud storage
6. Scalability
7. Private
8. Public
9. Hybrid
10. IaaS

Assignments

1. Define cloud computing and explain its basic concept in your own words.
2. List and describe the three main service models of cloud computing.
3. Differentiate between public, private, and hybrid cloud deployment models with examples.
4. Explain the advantages of using cloud computing in daily life or business.
5. Write a short note on virtualisation and its role in cloud computing.

Reference

1. https://nptel.ac.in/courses/106105167

Suggested Reading

1. Kavis, Michael. Architecting the cloud. Wiley, 2023.
2. Thomas, Erl, Mahmood Zaigham, and Puttini Ricardo. "Cloud computing concepts, technology & architecture." (2013).
3. Coulouris, George F., Jean Dollimore, and Tim Kindberg. Distributed systems: concepts and design. Pearson Education, 2005.
4. Buyya, Rajkumar, Rodrigo N. Calheiros, and Amir Vahid Dastjerdi, eds. Big data: principles and paradigms. Morgan Kaufmann, 2016.

Unit 3

Wireless and Mobile Technologies

Learning Outcomes

On completion of this unit, the learner will be able to:

- Identify the main features of wireless communication technologies such as Bluetooth, WiFi, WiMAX, and ZigBee
- Describe how Bluetooth and WiFi enable wireless communication between devices
- Familiarise with the essential components of mobile and positioning technologies
- Explore the key features and real-world applications of GPS and GPRS in everyday life
- Explain the core differences between 3G, 4G, and 5G mobile network technologies

Background

In today's world, communication is instant and wireless, whether it's through smartphones, smartwatches, or smart home devices. You've probably used Bluetooth to share a file or connected your phone to WiFi to browse the internet. These technologies have become an everyday part of our lives, helping us stay connected with ease. But have you ever wondered how these systems actually work, or why newer mobile networks like 4G and 5G offer faster data speeds?

Think about streaming a video on your phone while riding a bus. It plays smoothly without buffering, thanks to mobile data. Or consider your home, where multiple devices like phones, laptops, and smart TVs can all use the same WiFi network without slowing down. This is possible because of advanced technologies like WiFi and 4G, and with 5G, even faster speeds and greater connectivity are being introduced. Understanding how technologies such as Bluetooth, GPS, GSM, WiFi, and mobile networks like 3G, 4G, and 5G function can help you appreciate the way they shape our connected lives.

In this unit, we will explore various wireless and mobile communication technologies that have revolutionised how we interact and share information. We'll start with short-range technologies like Bluetooth and Zigbee, then move on to broader systems such as WiFi and WiMAX. You'll also learn how mobile networks have progressed from early 2G and 3G systems to advanced networks like 4G LTE, VoLTE, and the emerging 5G. By understanding the principles and uses of these technologies, you'll gain a deeper insight into their role in our increasingly connected world.

Keywords

Bluetooth, WiFi, GSM, GPS, GPRS, 3G, 4G, 4G LTE, VoLTE, 5G

Discussion

2.3.1 Bluetooth

Bluetooth is a short-range wireless communication technology that enables devices to exchange data over a limited distance without the need for cables. It is widely used in mobile devices, laptops, headphones, speakers, and various other devices for wireless data transfer and connectivity.

Features of Bluetooth

Bluetooth is a wireless technology that lets devices communicate with each other over short distances, typically within 10 metres. In some cases, especially with certain device types, the range can extend up to 100 metres. It is designed to use very little power, which makes it ideal for battery-powered devices such as smartphones, smartwatches, and wireless earphones. Bluetooth works on the 2.4 gigahertz ISM frequency band, which is shared by many other wireless technologies.

To reduce interference from other devices using the same frequency band, Bluetooth uses a method called frequency hopping. This means it rapidly switches between different frequencies while sending data, helping maintain a stable connection. Before two devices can exchange information, they must first connect through a secure pairing process. Bluetooth allows moderate speed data transfers, with earlier versions supporting up to 3 megabits per second and newer versions like Bluetooth 5.0 reaching up to 50 megabits per second. This makes it useful for both simple tasks like sending files and more complex uses like streaming audio.

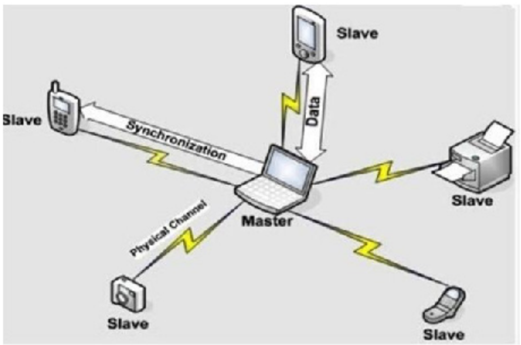


Fig 2.3.1 Master and slave connections in Bluetooth

2.3.2 WiFi

WiFi, also known as Wireless Fidelity, is a LAN (Local Area Network) technology based on the IEEE 802.11 standards. Its main purpose is to offer broadband connectivity within buildings, enabling devices such as smartphones, laptops, and tablets to connect to the internet or communicate with each other wirelessly. Using radio waves, typically at 2.4 GHz and 5 GHz frequencies, WiFi facilitates data transmission over short ranges, making it perfect for setting up wireless networks in homes, offices, and public areas. Continuous improvements in WiFi standards have greatly enhanced its speed, reliability, and security, establishing it as a key technology in modern digital communications.

The main part of a WiFi network is the WiFi router. The router connects to your internet source (like a modem) and sends out radio signals so your devices can connect wirelessly. Devices with built-in WiFi, such as smartphones and laptops, detect these signals. When a device comes close to the router, it looks for available networks. If it finds a known one, it tries to connect by entering the correct password. Once connected, the device can access the internet. The data is sent in small pieces called packets, which travel through the router and get reassembled on the receiving device. This allows fast and easy communication without any wires.

Applications of WiFi

1. Enables wireless internet access on any WiFi-capable device
2. Allows streaming or casting audio and video wirelessly for entertainment
3. Supports high-speed file and data sharing between computers or mobile devices.
4. Enables wireless printing with WiFi printers, which is widely used today

2.3.3 WiMAX

WiMAX, which stands for Worldwide Interoperability for Microwave Access, is a technology that allows people to access the internet wirelessly. It provides high-speed internet over long distances, making it different from WiFi, which typically covers a smaller area.

2.3.3.1 Features of WiMAX

WiMAX is a wireless technology that provides long-range internet access, making it especially useful in rural or remote areas where fibre optic or cable internet is not widely available. It can cover distances of up to 30 miles (50 kilometres), allowing more people to get connected even in hard-to-reach locations. WiMAX also offers high data speeds, similar to those of wired broadband, which means users can stream videos, play online games, and work from home smoothly without delays. It is mainly used for fixed wireless access, meaning it is designed to deliver internet to stationary places like homes and offices, rather than to mobile devices that move around.

WiMAX offers several advantages, making it a strong option for internet access in areas lacking wired infrastructure. Its long-range coverage of up to 30 miles (50 kilometres) is ideal for rural regions. It also allows for faster and more cost-effective deployment compared to laying fibre optic cables. Another key benefit is its scalability; WiMAX networks can easily expand to accommodate more users. It provides high data speeds similar to wired broadband, supporting activities like streaming, gaming, and remote work without noticeable lag.

However, WiMAX also has some limitations. It is primarily designed for fixed wireless access, which makes it less suitable for mobile use, such as with smartphones or tablets that are often on the move. Signal strength can also be affected by obstacles like buildings and trees, leading to reduced performance in certain areas. Furthermore, there are fewer devices that support WiMAX compared to more common technologies like WiFi, which can limit its accessibility for general users.

2.3.3.2 Applications of WiMAX

1. **Rural Broadband:** WiMAX has been used in rural areas to deliver high-speed internet to communities that lack good internet service.
2. **Enterprise Networks:** WiMAX can be utilised to establish private wireless networks for businesses, offering connectivity for offices, warehouses, and other locations. This serves as a cost-effective alternative to wired networks, particularly in large or widely spread areas.
3. **Public WiFi:** Some cities and local governments have set up WiMAX networks to offer public WiFi access in parks, plazas, and other communal spaces. This initiative can help boost economic growth and attract tourists.

Table 2.3.1 Comparison between WiFi and WiMAX

Feature	WiFi	WiMAX
Range	Shorter range, typically within a home or small business.	Longer range, capable of covering several miles.
Speed	Generally offers speeds up to 1 Gbps	Provides speeds comparable to wired broadband, typically ranging from 1 to 10 Mbps
Mobility	Supports mobile devices, enabling user mobility.	Designed for fixed access, less effective for mobile devices on the move.
Deployment Cost	Generally lower setup costs, especially for home networks;	Higher initial deployment costs due to base station installation, but can be cost-effective for large areas.
Applications	Ideal for home networks, offices, and small businesses.	Suitable for rural broadband, enterprise networks, and public WiFi in large areas.

2.3.4 ZigBee

Zigbee is a wireless communication technology made for short-distance use and low power consumption. It is commonly used in smart homes, factories, and Internet of Things (IoT) applications. Devices using Zigbee, such as smart lights or thermostats, can work for several years on a small battery, making them very energy efficient. It usually works within 300 feet indoors and can reach even farther outside. One special feature of Zigbee is mesh networking, where devices connect with each other and pass messages along, improving network coverage. It also uses security methods like encryption to keep data safe.

Zigbee is widely used in home automation, such as smart lighting and door locks, and in industries to monitor machines or manage processes. It's also useful in healthcare for tracking patient health and in buildings for managing lights and air systems. Some main advantages of Zigbee include its low power use, long range (especially outdoors), mesh networking that improves reliability, and easy scaling by adding more devices. However, it has some drawbacks: it offers slower data speeds compared to Wi-Fi or Bluetooth, which makes it unsuitable for things like video streaming. It also operates on the crowded 2.4 GHz band, so it may face interference, and some networks may have limits on how many devices can be connected.

2.3.5 GPS

GPS, or Global Positioning System, is a navigation system that utilises satellites to help users find their exact location anywhere on the planet. It provides real-time positioning information by communicating with satellites orbiting the Earth. This technology enables accurate location tracking for various applications worldwide.

Components of GPS

- The GPS system includes three main components:
  - **Satellites:**A minimum of 24 satellites circle the Earth, ensuring comprehensive global coverage.
  - **Ground Stations:**These facilities oversee the satellites, ensuring they operate properly and stay in their designated orbits.

Receivers: These are devices that capture GPS signals to determine the user's location. Common examples include smartphones, vehicle navigation systems, and specialised GPS units.

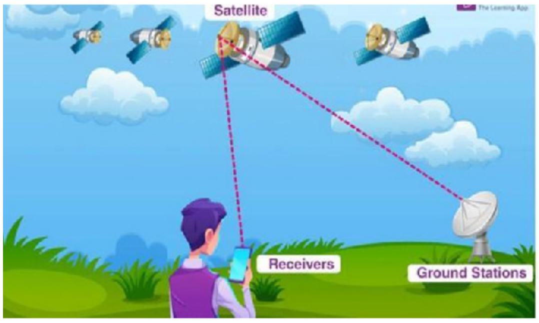


Fig 2.3.2 GPS

2.3.5.1 Applications of GPS

- **Navigation:**GPS is used in cars and smartphones for detailed directions, helping users find the best routes to their destinations.
  - **Tracking:**GPS enables the location tracking of vehicles, assets, and individuals. This is especially useful in logistics and fleet management, allowing companies to monitor delivery trucks in real time.
  - **Aviation:**GPS is essential for navigation in aviation, assisting pilots in locating themselves and offering guidance for takeoffs, landings, and in-flight navigation.
  - **Mapping and Geographic Information Systems (GIS):**GPS technology is vital for creating detailed maps and enhancing geographic information systems, enabling precise data collection and analysis in areas like urban planning, environmental monitoring, and disaster management.

2.3.6 GPRS

GPRS (General Packet Radio Service) is a mobile data service that facilitates the wireless transfer of data across cellular networks. It is a cellular technology that utilises packet switching, allowing data to be divided into smaller packets and transmitted more efficiently over the network compared to traditional circuit switching.

Consider a real-life example to understand the concept of GPRS by imagining you're out with friends and want to discover a new restaurant, so you pull out your smartphone and open a map app. GPRS (General Packet Radio Service) comes into play right away when you search for the restaurant. Your phone sends a request to the map service using GPRS, which breaks your request into small packets of data rather than maintaining a constant connection like a traditional phone call. These packets are transmitted over the cellular network to your service provider, which then communicates with the internet to locate the restaurant. With packet switching, multiple users can send their requests simultaneously without interference; while you're looking up directions, another user might be streaming music or checking emails. Once the map service processes your request, it sends the information back in packets. Your phone quickly reassembles these packets, displaying the restaurant's location and directions on your screen.

Features of GPRS

- **Packet Switching:**GPRS sends data in small packets instead of using circuit-switched technology for voice calls. This enables multiple users to share the same channel at the same time, enhancing efficiency.
  - **Continuous Connectivity:** GPRS offers uninterrupted internet access, enabling users to send and receive data without having to create a new connection every time.
  - **Support for Multiple Services:**GPRS can manage different types of data services, such as web browsing, email, multimedia messaging (MMS), and application services, allowing for a diverse array of mobile applications.
  - **Scalability:**GPRS networks can be easily expanded to support additional users and devices, making them flexible to increasing mobile data demands.
  - **Data Rates:**GPRS offers speeds between 56 kbps and 114 kbps, depending on network conditions and demand. Although slower than newer technologies like 3G, it was an upgrade from earlier mobile data services.

Table 2.3.2 Comparison between GPS and GPRS

Feature	GPS	GPRS
Definition	A satellite-based navigation system	A mobile data service for transmitting data
Primary Purpose	Determines location and provides navigation	Enables wireless internet access
Technology Type	Uses satellites to provide location	Uses cellular networks for data transmission
Data Transmission	Does not transmit data; only receives signals	Transmits data in packets over a network
Application	Navigation, mapping, tracking	Internet browsing, email, app usage
Data Charges	No data charges; GPS signals are free	Typically charged based on data usage

2.3.7 GSM

GSM (Global System for Mobile Communications) is a mobile network standard developed in the late 1980s to allow voice and data communication on mobile phones. It became the most widely used mobile communication system in the world and laid the foundation for newer technologies like 3G, 4G, and 5G. GSM brought significant changes in the way people connect, making mobile communication more reliable and accessible.

GSM uses digital signals, which provide clearer sound and better use of available bandwidth compared to older analog systems. It relies on SIM cards to store user information, making it easy to switch phones without losing contacts or services. GSM supports international roaming, allowing users to stay connected in different countries. It also offers many services, such as voice calls, text messages (SMS), internet access, and multimedia messages (MMS). GSM uses a method called TDMA to let several users share the same channel efficiently. In addition to calls and texts, GSM supports location-based services like navigation and tracking, enhancing the overall mobile experience.

2.3.8 3G

3G (Third Generation) is a mobile technology that offers increased data speeds and enhanced multimedia features compared to earlier generations such as 2G (GSM). It utilises a broader spectrum of frequencies and more sophisticated modulation methods to attain these higher data rates.

3G is a mobile communication technology that offers significantly higher data transfer speeds compared to earlier generations, typically ranging from 200 kilobits per second to several megabits per second. This increase in speed allows users to enjoy a wide range of multimedia services such as video streaming, online gaming, and video calls. One of the key features of 3G is mobile internet access, enabling users to browse the web, check emails, and use social media directly from their mobile devices. 3G uses a method called packet switching, which makes network usage more efficient and supports various data-based applications simultaneously.

Applications of 3G

- **Mobile Internet:**3G provided faster and more reliable internet access on mobile devices, enabling users to browse websites, check emails, and download content more efficiently.
  - **Video Streaming:**The faster data speeds of 3G enabled streaming of videos, movies, and TV shows directly on mobile devices.
  - **Mobile Gaming:**3G facilitated the creation of more sophisticated mobile games with enhanced graphics and improved gameplay.
  - **Location-based Services:**The combination of 3G and GPS technology enabled features like navigation, augmented reality, and local searches.
  - **Video Conferencing:**3G allowed video calls on mobile devices, supporting remote communication and work.

2.3.9 3.5 G

3.5G is a term used for technologies that act as a bridge between 3G and 4G mobile networks. It includes improvements to existing 3G systems that offer faster and better data performance. Some of the main technologies under 3.5G are HSPA, which increases download (HSDPA) and upload (HSUPA) speeds; DC HSPA, which combines two 3G channels for even faster data; and LTE, which is technically 4G but is often grouped with 3.5G because it works well with 3G networks.

The main features of 3.5G are higher data speeds, better network coverage, and smoother performance. These technologies allow users to stream videos, play online games, and join video calls with fewer interruptions. 3.5G also helped mobile service providers and users gradually move from 3G to full 4G, making the upgrade process easier and more cost-effective.

2.3.10 4G

4G, or the Fourth Generation of mobile network technology, marks a major advancement over earlier generations like 3G and 2G in terms of speed, performance, and functionality. It was designed to address the increasing need for faster data transfer, richer multimedia experiences, and better connectivity. With 4G, mobile device usage has been revolutionised, supporting applications such as high-definition video streaming, real-time video calls, and sophisticated mobile gaming.

Features of 4G

- **High Data Speeds:**4G networks provide much higher data transfer speeds than 3G, enabling smooth activities such as HD video streaming, online gaming, and video conferencing with little to no lag.
- **Low Latency:**4G technology minimises data travel time, allowing for real-time applications such as video calls, online gaming, and augmented reality.
- **Enhanced Multimedia Services:**4G enables high-quality multimedia services like HD video streaming, music streaming, and enriched mobile content experiences.
- **IP Based Network:**4G relies on Internet Protocol (IP) for data transmission, facilitating seamless integration with various internet services and enhancing the efficiency of mobile data applications.
- **Voice over LTE (VoLTE):**4G networks enable voice calls over LTE (VoLTE), offering improved voice quality and more efficient utilisation of network resources.

2.3.11 4G LTE (Long Term Evolution)

4G LTE (Long Term Evolution) is a wireless communication standard that marks a major improvement in mobile technology. Created as part of the fourth generation (4G) of mobile networks, LTE aims to boost data speeds, increase network capacity, and enhance the overall user experience compared to previous generations like 3G and 2G.

4G LTE offers faster data speeds, making it ideal for activities like streaming HD videos, online gaming, and quick content uploads and downloads. It also features low latency, ensuring smooth real-time applications such as video calls and gaming. 4G LTE uses Internet Protocol (IP) for efficient data transfer, which enhances integration with various internet services and mobile apps. It supports Voice over LTE (VoLTE), providing clear voice calls over the data network. 4G LTE also ensures reliable connections for users on the move, whether travelling in a car or on public transportation, while offering improved reliability through stronger signals and better network management.

2.3.12 VoLTE

Voice over LTE (VoLTE) is an advanced technology enabling voice calls to be made over a 4G LTE (Long Term Evolution) network. Unlike conventional voice calls that depend on circuit-switched systems, VoLTE utilises an Internet Protocol (IP) based framework to transmit voice data in packets, allowing it to operate alongside other data services like internet browsing and video streaming.

Features of VoLTE

VoLTE (Voice over LTE) offers high-definition voice quality, making calls clearer and sharper. It also reduces the time it takes to connect calls, ensuring faster call setup. With HD Voice, conversations sound more natural. One of the key benefits of VoLTE is that it allows users to make voice calls while using data services, such as browsing the internet or streaming videos, without interrupting the call. VoLTE also supports video calling, letting users see each other during conversations, and enables a wider range of multimedia services, such as sending messages or starting video calls while on a voice call.

2.3.13 5G

5G, or Fifth Generation, is the newest standard in mobile telecommunications, marking a major improvement over earlier generations like 4G. It is engineered to deliver faster speeds, reduced latency, and greater capacity, addressing users' increasing needs for uninterrupted connectivity and enhanced mobile experiences. An important characteristic of 5G is its capacity to provide exceptionally high data rates, achieving speeds of up to 10 Gbps or even higher.

Features of 5G

- **High Data Speeds:**5G delivers much higher data transfer rates, reaching up to 10 Gbps or beyond, allowing for smooth streaming, rapid downloads, and real-time application performance.
    - **Minimal Latency:**5G reduces latency to as little as 1 millisecond, enabling almost instant communication, which is crucial for real-time uses like self-driving cars, online gaming, and remote medical procedures.
    - **Extensive Device Connectivity:**5G can handle numerous connected devices at once, making it perfect for Internet of Things (IoT) applications, smart cities, and automation in industries.
- **Increased Network Capacity:**5G supports more data and can manage a higher number of users and devices simultaneously, ensuring smooth performance even in crowded places like cities and stadiums.
- **Enhanced Stability:**5G networks offer greater reliability, delivering a consistent and uninterrupted connection, especially for mission-critical applications.

2.3.13.1 Applications of 5G

- **Smart Cities:**With 5G, connected devices can communicate faster and more efficiently, enhancing urban infrastructure management, improving traffic systems, and increasing public safety.
- **Autonomous Vehicles:**The ultra-low latency of 5G is essential for self-driving cars, enabling real-time interactions between vehicles, road systems, and other devices, enhancing safety on the roads.
- **Healthcare:**5G technology enhances telemedicine, enables remote surgeries, and allows for real-time patient monitoring, improving the accessibility and effectiveness of healthcare services.
- **Internet of Things (IoT):**5G supports the widespread use of IoT devices, making smart homes, industrial automation, and connected appliances more efficient and scalable.

Recap

- Bluetooth:
  - Short-range wireless communication for data exchange without cables.
  - Working involves device discovery, pairing, and data transmission.
- WiFi:
  - LAN technology enables broadband connectivity via 2.4 GHz and 5 GHz frequencies.
  - Components: WiFi router and WiFi enabled devices.
  - Working involves broadcasting a signal, network scanning, authentication, and data transmission.
  - Applications include wireless internet access, media streaming, file sharing, and wireless printing.
- WiMAX:
  - High-speed wireless internet access over long distances.
  - Features: long range, high data rates, and fixed wireless access.
  - Applications include rural broadband, enterprise networks, and public WiFi.
- ZigBee:
  - Low power, short-range wireless communication for smart home, IoT, and industrial automation.
  - Features include low power consumption, short range, mesh networking, and secure communication.
  - Applications: home automation, industrial automation, healthcare, and building automation.
- GPS
  - GPS (Global Positioning System) is a satellite-based navigation system for real-time location tracking.
- GPRS
  - GPRS (General Packet Radio Service) is a mobile data service that uses packet switching for wireless data transfer.
  - Applications: GPS for navigation; GPRS for internet services.
  - GSM

    □ GSM (Global System for Mobile Communications) is a digital mobile network standard for voice and data communication.

    □ Applications:

□ Voice Communication: Enables reliable voice calls.

□ Text Messaging (SMS): Widely used communication method.

□ Location Based Services: Supports navigation and tracking.

- 3G
  - Higher Data Rates: Speeds range from 200 kbps to several Mbps.
  - Enhanced Multimedia: Supports video streaming, online gaming, and video conferencing.
  - Mobile Internet Access: Allows web browsing, email, and social media.
  - Packet Switching: Efficiently utilises network resources for various applications.

- 3.5G
  - HSPA Technologies: Includes HSDPA and HSUPA for faster data speeds.
  - DC HSPA: Combines two 3G carriers for higher speeds.
  - Transition to 4G: Facilitates the upgrade from 3G to 4G networks.

- 4G
  - High Data Speeds: Facilitates HD video streaming, online gaming, and video conferencing.
  - Low Latency: Reduces the time it takes for data to travel, supporting real-time applications.
  - IP Based Network: Improves the integration of internet services.
  - VoLTE Support: Enhances voice quality and optimises resource use.

- 4G LTE
  - High Speed Data Transfer: Accelerates downloads and uploads, improving the experience for streaming and gaming.
  - Low Latency: Crucial for applications that require real-time interaction, such as video calls. IP Based Network: Ensures seamless integration with various internet services.

- VoLTE
  - High Quality Voice Calls: Offers high-definition voice clarity.
  - Quicker Call Setup: Minimises the time needed to connect calls.
  - Concurrent Voice and Data Usage: Permits simultaneous voice calls and data activities.
  - Video Calling: Supports video calls during voice conversations.

- 5G
  - High Data Speeds: Reaches data rates of 10 Gbps or more.

- Low Latency: Lowers latency to just 1 millisecond.
- Broad Device Connectivity: Accommodates numerous connected devices for the Internet of Things (IoT).
- Enhanced Network Capacity: Effectively handles large volumes of users and devices.

Objective Questions

1. What technology does Bluetooth primarily use for communication?
2. In Bluetooth communication, which device controls the connection?
3. What is the main frequency band used by WiFi?
4. What type of access does WiMAX primarily provide?
5. What is the typical range of ZigBee communication?
6. What network topology does ZigBee utilise for device connectivity?
7. What system is used for navigation and location tracking?
8. What component captures GPS signals to determine location?
9. What type of data transmission does GPRS use?
10. What does GSM stand for?
11. Which technology allows continuous internet access without creating new connections?
12. What does GPS stand for?
13. What type of data transmission does GPRS use?
14. What does 3G stand for?
15. What technology is used in 3.5G to boost data speeds?
16. What does 4G LTE stand for?
17. What is the primary benefit of 5G technology?

Answers

1. Radio
2. Master
3. 2.4 GHz
4. Fixed
5. 100 metres
6. Mesh
7. GPS
8. Receiver
9. Packet
10. Global System for Mobile Communications.
11. GPRS
12. Global Positioning System
13. Packet Switching
14. Third Generation
15. HSPA
16. Long Term Evolution
17. Speed

Assignments

1. Describe the Bluetooth communication process, detailing the steps involved in device discovery, pairing, and data transmission, and explain the importance of the master-slave architecture in this context.
2. Differentiate between WiFi and WiMAX regarding their range, speed, mobility, and common applications.
3. Explain the characteristics and operational principles of ZigBee technology. In what ways do its energy efficiency and mesh networking features enhance its suitability for smart home applications?

4. Explain the advantages and disadvantages of WiMAX technology. In what ways does its extensive range make it a practical choice for delivering internet access in rural regions?

5. Explain the key components of the GPS system and discuss their roles in determining a user's location.

6. Differentiate between the functionalities of GPS and GPRS. How do their purposes and technologies differ?

7. Examine the characteristics of GSM technology and explain how it improves mobile communication in comparison to previous technologies.

8. Explain the key features of 3G technology.

9. Discuss the main characteristics of 4G technology and how it addresses the growing demand for faster data transfer and improved multimedia experiences.

10. Differentiate between the features of 4G LTE and 5G. What are the key differences that enhance user experience in 5G technology?

Reference

1. Rappaport, T. S. (2002). *Wireless Communications: Principles and Practice* (2nd ed.). Prentice Hall.

2. Stallings, W. (2017). *Wireless Communications and Networks* (2nd ed.). Pearson.

3. Zhang, Y., & Wang, X. (2009). *Wireless and Mobile Networks: Concepts and Protocols*. Wiley.

Suggested Reading

1. Schiller, Jochen. *Mobile Communications*. Pearson Education Ltd, 2003.

2. Stüber, Gordon L., and Gordon L. Steuber. *Principles of Mobile Communication*. Vol. 2. Boston: Kluwer Academic, 2001.

3. Lin, Yi Bang, and Imrich Chlamtac. *Wireless and Mobile Network Architectures*. John Wiley & Sons, 2000.

4. Kukushkin, Alexander. *Introduction to Mobile Network Engineering: GSM, 3G WCDMA, LTE and the Road to 5G*. John Wiley & Sons, 2018.

Unit 4

Web Pages Creation and Hosting

Learning Outcomes

On completion of this unit, the learner will be able to:

- identify the roles of web clients and web servers
- describe the HTTP request-response cycle
- list the basic steps involved in web page creation
- define key terms related to web hosting
- outline the process of uploading a web page to a hosting server

Background

Imagine you want to borrow a book from the library. You go in, ask the librarian for the book, and the librarian finds it and hands it to you. This is similar to how the internet works. Your web browser, such as Google Chrome, acts like the person asking for the book; it sends a request to a web server. The web server, like the librarian, responds by sending the requested web page back to your browser. This exchange of asking and receiving is known as the HTTP request-response cycle.

Now, think of creating a web page like designing a poster for a school event. You begin with a plain sheet (HTML) to build the structure, then decorate it with colours, fonts, and images (CSS) to make it visually appealing. To make it even more exciting or interactive, you might add some moving or clickable parts (JavaScript). Just like a poster is designed to grab attention and share information, a web page is created to be both attractive and informative for visitors.

Finally, if you want others to see your poster, you would pin it on a public notice board. That's similar to web hosting. Once your web page is ready, you upload it to a server so it's available online, like placing your poster on the internet's bulletin board. You also need a domain name, the web address that tells people where to find your site. Understanding these steps prepares you to start creating and publishing your own web pages for others to see.

Keywords

Web clients, Web servers, HTTP request-response, Web page creation, Web hosting

Discussion

2.4.1 Web Pages Creation and Hosting

Creating and hosting web pages is an important skill in today's digital world. A web page is a digital document that we can view on the Internet. It includes text, images, videos, and other multimedia elements. To make a web page, we use different coding languages, such as HTML for the structure, CSS for styling, and JavaScript for interactivity. HTML is like the framework of a house, CSS is like the paint and decorations, and JavaScript adds special features like moving parts. Understanding these basics helps you create a functional web page.

Once you have created a web page, it needs to be hosted on a server so that it can be accessed and seen by others online. Think of hosting as placing your web page on a giant bulletin board that everyone can access. There are different types of hosting services you can use. Shared hosting means your web page shares space with others on the same server, which is good for small websites. Virtual Private Server (VPS) hosting gives you more dedicated resources, making your website faster and more reliable. Dedicated hosting provides an entire server just for your website, which is ideal for large websites with a lot of traffic.

To make your web page accessible, you also need a domain name. A domain name is the address people type in their web browsers to visit your website, like www.example.com. Registering a domain name is like getting your address on the Internet. Once you have your domain name, you connect it to your hosting server so people can find your web page. Hosting services often provide additional features like email accounts, database support, and security measures to protect your

website from hackers and other threats.

The process of creating and hosting web pages involves several steps, but each one is important. Designing the web page with HTML, CSS, and JavaScript ensures it looks good and works well. Choosing the right hosting service ensures your web page is always available and performs well. Registering a domain name makes it easy for people to find your site. By following these steps, you can create a web page that is both functional and easy to access.

In short, learning how to create and host web pages is a valuable skill that allows you to share information and connect with others online. Whether making a simple personal website or a complex site for a business, understanding the basics of web development and hosting is essential. With practice, you can become proficient in these skills and create web pages that are both beautiful and functional. This knowledge opens up many opportunities in the digital world.

2.4.2 Web Client

A web client is a software application that allows you to access and interact with web pages on the Internet. The most common example of a web client is a web browser, such as Google Chrome, Mozilla Firefox, or Safari. When you type a web address into your browser's address bar and press enter, the web client sends a request to a web server to fetch the web page you want to see. The web server then sends the web page back to your browser, which displays it for you to view and interact with. This process is called the HTTP request-response cycle.

Web clients do more than just display web pages; they also help manage your browsing experience. For example, they can save your favourite websites as bookmarks, store your login information for different sites, and keep a history of the pages you've visited. Web clients also support extensions or add-ons to enhance their functionality, like ad blockers or language translators. These features make web clients powerful tools for navigating and using the Internet efficiently.

Another important aspect of web clients is their role in ensuring online security. Modern web browsers include various security features to protect us from threats such as malware, phishing attacks, and harmful websites. They do this by checking the websites you visit against a list of known dangerous sites and warning you if a site looks suspicious. Web clients also use encryption to keep our data safe when we enter sensitive information, like passwords or credit card numbers, on a website. By using a secure web client, you can browse the Internet confidently, knowing your information is protected.

2.4.3 Web Server

A web server is a computer system that stores and delivers web pages to users over the Internet. When you want to visit a website, your web browser sends a request to the web server where the website is hosted. The web server then processes this request and sends back the required web page so you can view it on your browser. This exchange of information between your web browser and the web server happens very quickly, allowing you to access websites almost instantly.

Web servers do more than just store web pages; they also handle multiple requests from users all over the world at the same time. They use special software to manage these requests efficiently, ensuring that each user gets the right web page without delays. Popular web server software includes Apache, Nginx, and Microsoft's Internet Information Services (IIS). These programs help the web server run smoothly and securely, handling tasks like load balancing to distribute traffic evenly and prevent the server from becoming overloaded.

Security is also very important for web servers. They protect websites from online threats, especially hacking attempts and data breaches. Web servers use firewalls and encryption to safeguard the data they store and transmit. They also regularly update their software to fix any security vulnerabilities. By implementing these security measures, web servers ensure that the websites they host are safe for users to visit and interact with.

In addition to delivering web pages, web servers can also host other services, like email, file storage, and databases. This makes them versatile tools for both personal and business use. For example, a company might use a web server to host its website, store customer data, and manage email communications all in one place. Understanding how web servers work helps you see how the Internet functions and how information is shared and protected online.

2.4.4 Web Page Creation and Web Hosting

Creating a web page involves several steps to ensure it looks good and functions properly. The first step is to use HTML (Hypertext Markup Language) to build the page's structure. HTML provides the basic layout and content of the web page, such as headings, paragraphs, and links. For example, if you want to add a heading, use HTML tags like and so on. These tags help organise the content and make it easier for browsers to display it correctly. Once the basic structure is in place, you can style the page to make it visually appealing.HTML BasicsHTML is a markup language used to create the structure of web pages. It consists of elements, which are the building blocks of a web page. Each HTML element is defined by tags, which are enclosed in angle brackets. For example,

is a tag used to create a top-level heading, while is used for paragraphs. Tags often come in pairs, with an opening tag and a closing tag, like and to enclose content.

Creating Structure with HTML

To design a web page, you start by using HTML to set up the basic structure. The core elements include:

- The root element that contains the entire HTML document.
- Contains meta information about the document, such as the title and link to stylesheets.
- Contains the visible content of the web page, including text, images, links, and other multimedia elements.

CSS (Cascading Style Sheets) is used to style the web page created with HTML. CSS allows you to change the colours, fonts, spacing, and layout of the content. For example, you can set the background colour of a page, adjust the font size of text, and position elements on the page. CSS is written in a separate file that links to your HTML file, which keeps the design and content separate. This separation makes it easier to update the page's look without changing the content. Good CSS design ensures that your web page is attractive and easy to read.

Formatting and Styling

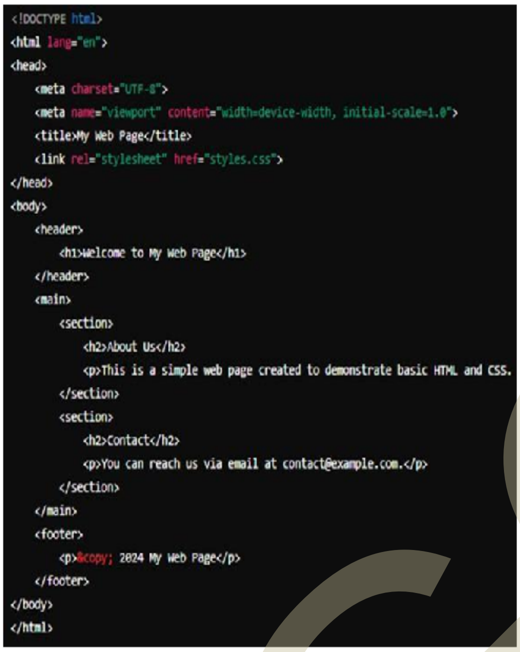
While HTML defines the structure, styling uses CSS (Cascading Style Sheets). CSS allows you to control the appearance of your web page by defining styles for various HTML elements. You can set colours, fonts, spacing, and layout properties to make your web page visually appealing. For example, you might use CSS to change the background colour of a

element or adjust the font size of headings.

2.4.4.1 Example Web Page Creation

HTML Content

HTML (Hypertext Markup Language)is used to create the structure and content of a web page. Here is an example of a simple web page using HTML:



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>My Web Page</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body>
    <header>
        <h1>Welcome to My Web Page</h1>
    </header>
    <main>
        <section>
            <h2>About Us</h2>
            <p>This is a simple web page created to demonstrate basic HTML and CSS.
        </section>
        <section>
            <h2>Contact</h2>
            <p>You can reach us via email at contact@example.com.</p>
        </section>
    </main>
    <footer>
        <p>&copy; 2024 My Web Page</p>
    </footer>
</body>
</html>
```

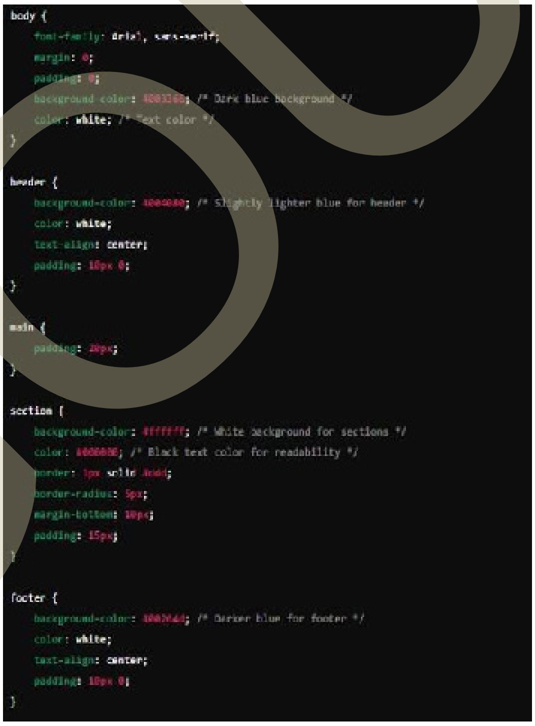
Fig 2.4.1 Example of HTML Page

HTML Page Explanation

- This declaration defines the document type and version of HTML being used (HTML5 here).
- This element is the root of the HTML document and specifies that the language is English.
- Contains meta information about the web page, such as the character set (UTF-8), viewport settings for responsive design, the title of the page, and a link to the CSS file for styling.
- Contains the visible content of the web page. It includes:
- Displays the website title and navigation menu.
- Provides links to different sections of the page (Home, About, Contact).
- Holds the main content of the page, divided into sections.
- Defines different parts of the page, each with its heading and content.
- Displays the footer with copyright information.

CSS Styling

CSS (Cascading Style Sheets)is used to style the HTML content, making the web page look attractive. Here's an example of CSS for the HTML above:



```
body {
    font-family: Arial, sans-serif;
    margin: 0;
    padding: 0;
    background-color: #003366; /* Dark blue background */
    color: white; /* Text color */
}

header {
    background-color: #004080; /* Slightly lighter blue for header */
    color: white;
    text-align: center;
    padding: 10px 0;
}

main {
    padding: 20px;
}

section {
    background-color: #ffffff; /* White background for sections */
    color: #000000; /* Black text color for readability */
    border: 1px solid #ddd;
    border-radius: 5px;
    margin-bottom: 10px;
    padding: 15px;
}

footer {
    background-color: #00264d; /* Darker blue for footer */
    color: white;
    text-align: center;
    padding: 10px 0;
}
```

Fig 2.4.2 Example of CSS for HTML

CSS Page Explanation

- **body**: Fig 2.4.2 depicts the example for setting the body font to Arial, removing default margins and padding, and giving a light grey background to the page.
- **header**: Styles the header with a green background and white text, and centres the text. Adds padding for spacing.
- **main**: Adds padding around the main content area.

- **section**: Styles each section with a white background, a light border, rounded corners, and padding inside the section.
- **footer**: Styles the footer with a dark background and white text, and centres the text. Adds padding for spacing.

2.4.4.2 Adding Interactivity

HTML on its own provides the structure and content, but to add interactivity to our web pages, we use JavaScript. JavaScript enables dynamic features, such as form validation, interactive galleries, or live updates. By integrating JavaScript, you can create a more engaging user experience.

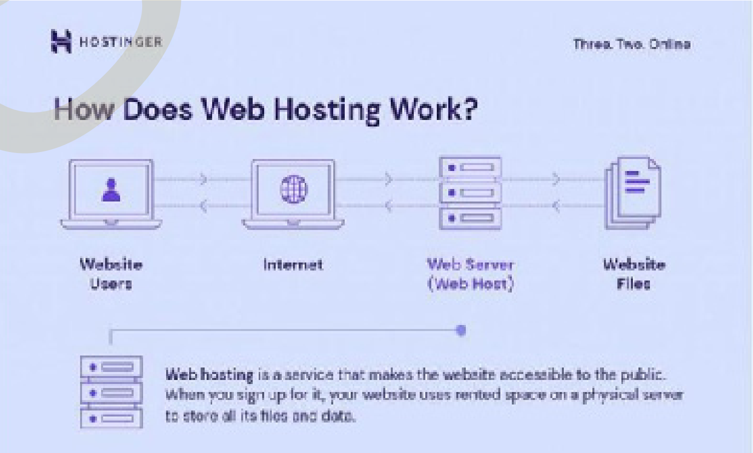
JavaScript adds interactivity to your web page, making it more dynamic and engaging. With JavaScript, you can create features like slideshows, pop-up windows, and interactive forms. For example, you can use JavaScript to validate user input on a form before it is submitted, ensuring that the information is correct. JavaScript is written in a separate file or directly in the HTML file, and it interacts with both HTML and CSS. In short, using JavaScript can enhance the user experience and make our web page more functional.

Once your web page is created and styled, it needs to be hosted on a web server so that others can view it online. Web hosting involves uploading your web page files to a server that is connected to the Internet. There are different types of hosting services available, such as 1. shared hosting, where multiple websites share the same server, and dedicated hosting, where a server is used by only one website. Choosing the right type of hosting depends on factors like the size of your website, the expected traffic, and your budget.

After choosing a hosting service, we need to register a domain name, the web address people will use to access your website. A domain name is like an address for your website, such as www.example.com. Registering a domain name ensures that users can find your site easily. Once you have your domain name, you need to connect it to your hosting server. This process involves configuring DNS (Domain Name System) settings so that when someone types your domain name into their browser, they are directed to your web page.

2.4.5 Web Hosting

Web hosting is a service that allows individuals and organisations to make their websites accessible on the Internet. When you create a web page, it consists of files and data that need to be stored on a server, a powerful computer which is always connected to the Internet. If you create a personal blog or an online store, you need to use web hosting to store and serve your blog posts, product images, and other content to visitors.



Web hosting is a service that makes the website accessible to the public. When you sign up for it, your website uses rented space on a physical server to store all its files and data.

Fig 2.4.3 How does Web Hosting work

When we choose a web hosting service, we essentially rent space on one of these servers. For example, HostGatorprovides web hosting services to manage the server's upkeep and ensure it is operational 24/7 (24 hours, 7 days a week). This means our website, whether it's a small blog or a large e-commerce site, will be accessible to anyone with an Internet connection at any time. Many hosting services, like Bluehost, also offer additional features such as domain name registration, email hosting, and security measures to protect your site from threats.

There are different types of web hosting to suit various needs and budgets. Shared hostingis the most basic and affordable type, where multiple websites share the same server resources. This is a good option for small websites with low to moderate traffic. For example, Bluehostoffers shared hosting plans that are perfect for personal blogs or small business sites. VPS (Virtual Private Server) hostingprovides more dedicated resources and better performance, as it allocates a portion of the server specifically for our site. InMotion Hostingoffers VPS hosting with more control and reliability for growing websites.

Dedicated hostingprovides the highest level of performance and control, as you have an entire server to yourself. This type of hosting is ideal for large or high-traffic websites. For example, Liquid Webspecialises in dedicated hosting solutions. They offer premium hardware and fully managed servers, making them suitable for high-demand sites. Cloud hostingis another modern option that uses a network of servers to host your website. This type of hosting, offered by services like A2 Hosting, offers flexibility and scalability, handling large amounts of traffic and growing with your needs. Cloud hosting is more reliable because your site is hosted on multiple servers, reducing the risk of downtime.

Choosing the right web hosting service depends on factors like the size of your website, the amount of traffic you expect, and your budget. By understanding the different types of hosting and considering examples from various providers, you can select the best option to ensure that your website is always available to visitors and performs efficiently.

Recap

- Web Client
  - A web client is a software application that allows you to access and interact with web pages, such as a web browser (e.g., Google Chrome, Mozilla Firefox).
  - When you enter a web address, the web client sends an HTTP request to a web server and displays the response.
  - Web clients manage browsing experiences by saving bookmarks, storing login information, and providing security features like encryption.
- Web Server
  - A web server is a computer system that stores and delivers web pages to users over the Internet.

- The server processes HTTP requests from web clients and sends back the requested web pages.
    - Examples of web server software include Apache, Nginx, and Microsoft IIS.
    - Web servers handle multiple user requests, ensure security through firewalls and encryption, and can also host additional services like email and databases.
- Creating a Web Page
    - Web pages are digital documents on the Internet containing text, images, videos, and multimedia.
    - HTML (Hypertext Markup Language) provides the page structure (like a house's framework).
    - CSS (Cascading Style Sheets) styles the page (like paint and decorations).
    - JavaScript adds interactivity and dynamic features (like moving parts).
- Web Hosting
    - Web hosting makes your web page accessible online by storing it on a server.
    - Shared Hosting (e.g., HostGator): Multiple websites share the same server, suitable for small sites.
    - VPS Hosting (e.g., InMotion Hosting): Offers more dedicated resources for growing sites.
    - Dedicated Hosting (e.g., Liquid Web): Provides an entire server to one website, ideal for large or high-traffic sites.
    - Cloud Hosting (e.g., A2 Hosting): Uses multiple servers for flexibility, scalability, and reliability.
- Domain Name
    - A domain name is your website's address on the Internet (e.g., www.example.com).
    - Registering a domain name ensures users can find your site easily.
    - Connect the domain to your hosting server by configuring DNS settings to direct users to your web page.

Objective Questions

1. What is HTML used for in web page creation?
2. Define the purpose of CSS in web design.
3. What role does JavaScript play in enhancing web pages?
4. What is web hosting, and why is it necessary for making websites accessible on the Internet?
5. Explain the function of a web client.
6. What is the primary job of a web server?
7. Describe what an HTTP request is and how it is used.
8. An HTTP response consists of the requested web page or resource and status information.
9. A web browser sends an HTTP request to a web server, which then sends back the requested web page for display.
10. A domain name is a unique web address used to locate a website on the internet.
11. Shared hostinginvolves multiple websites sharing the same server resources, while VPS hostingprovides dedicated resources for each site on the same server.
12. Dedicated hostinginvolves renting an entire server exclusively for one website, usually for high-traffic sites.
13. Cloud hostinguses a network of servers to host a website, offering scalability and flexibility.
14. Linking a domain nameto a web hosting server involves configuring DNS settings to direct web traffic to the server.
15. The background colour property in CSSsets the background colour of an element.
16. HTML creates a hyperlinkusing the tag with the href attribute.
17. The font size property in CSScontrols the size of the text.
18. Security measuresin web hosting protect against threats like hacking and data breaches.
19. An HTTP status codeof “200 OK” indicates that the request was successful and the web page was delivered.
20. Web clientsmanage and enhance browsing by saving bookmarks, managing passwords, and providing security features.

Answers

1. HTML is used for defining the structure and content of web pages.

2. CSS is used for styling the appearance of web pages, including layout, colours, and fonts.

3. JavaScript adds interactivity and dynamic features to web pages.

4. Web hosting provides space on a server to store and make web pages accessible online.

5. A web client is a software application, like a web browser, that requests and displays web pages.

6. A web server stores and delivers web pages to users over the internet.

7. An HTTP request is a message sent by a client to a server asking for a web page or resource.

8. An HTTP response consists of the requested web page or resource and status information.

9. A web browser sends an HTTP request to a web server, which then sends back the requested web page for display.

10. A domain name is a unique web address used to locate a website on the internet.

11. Shared hosting involves multiple websites sharing the same server resources, while VPS hosting provides dedicated resources for each site on the same server.

12. Dedicated hosting involves renting an entire server exclusively for one website, usually for high-traffic sites.

13. Cloud hosting uses a network of servers to host a website, offering scalability and flexibility.

14. Linking a domain name to a web hosting server involves configuring DNS settings to direct web traffic to the server.

15. The background colour property in CSS sets the background colour of an element.

16. HTML creates a hyperlink using the tag with the href attribute.

17. The font size property in CSS controls the size of the text.

18. Security measures in web hosting protect against threats like hacking and data breaches.

19. An HTTP status code of "200 OK" indicates that the request was successful and the web page was delivered.

20. Web clients manage and enhance browsing by saving bookmarks, managing passwords, and providing security features.

Assignments

1. Design and code a basic web page using HTML and CSS. Your page should include a header, navigation menu, main content section with at least two different types of content (e.g., text, image, video), and a footer. Apply CSS to style the page, ensuring it is visually appealing and responsive.

2. Write a detailed explanation of the HTTP request-response cycle. Describe the process from when a user enters a URL into a web browser to when the web page is displayed. Include the roles of the web client, web server, and the information exchanged during the request and response.

3. Research and compare different web hosting services (shared hosting, VPS hosting, dedicated hosting, and cloud hosting). Write a report outlining the pros and cons of each type, and recommend which type of hosting would be suitable for different scenarios (e.g., a personal blog, a small business website, or a large e-commerce site).

Reference

1. Felke Morris, Terry. *Web Development and Design Foundations with HTML5*. Pearson, 2018.
2. Gourley, David, and Brian Totty. *HTTP: The Definitive Guide*. O'Reilly Media, 2002.
3. Carter, James M. *Web Server Administration*. Apress, 2009.
4. Duckett, Jon. *HTML and CSS: Design and Build Websites*. Wiley, 2011.
5. Duckett, Jon. *JavaScript and JQuery: Interactive Front End Web Development*. Wiley, 2014.
6. Kent, Peter, and Steve Holzner. Web Hosting For Dummies. Wiley, 2010.

Suggested Reading

1. Frain, Ben. *Responsive Web Design with HTML5 and CSS*. Packt Publishing, 2015.
2. Felke Morris, Terry. *Web Development and Design Foundations with HTML5*. Pearson, 2018.
3. Beaird, Jason. *The Principles of Beautiful Web Design*. New Riders, 2014.

Unit 5

Cyber Literacy And Etiquette

Learning Outcomes

On completion of this unit, the learner will be able to:

- Familiarise with the usage of search engines and their needs
- Efficiently utilise search engines for content searching
- Make others aware of Google Scholar for locating academic resources
- Narrate the relevance and appropriate use of various social media platforms
- Interact on social media platforms with proper etiquette

Background

In today's life, it is essential to have a basic understanding of Internet usage, including navigating search engines and social media platforms. A traveller relies on search engines to find nearby restaurants and landmarks. Search engines allow people to quickly find information on a wide range of topics, such as looking up recipes, local events, or books, etc.

Consider a graduate student researching for a science project; they might use Google to find information but may struggle to differentiate between credible sources and unreliable ones. By introducing them to Google Scholar, they can access peer-reviewed articles, which enhances the quality of their research.

Understanding the relevance and appropriate use of social media platforms is crucial, especially when interacting online. If someone carelessly shares sensitive information in an unprotected email or social media post, it could be intercepted and misused by malicious actors. By following good online behaviour and practising good cyber etiquette, individuals will contribute to a safer and more respectful digital space for everyone.

Keywords

Search engine optimisation, Privacy, Google Scholar, Content Authenticity, Fact-checking, Social Media

Discussion

2.5.1 Search Engines

Search engines are vital tools for quickly accessing information from a vast array of online sources. They help users locate relevant content, making research and learning more efficient and accessible across various fields.

Google Scholar is essential for academic research as it provides access to a wide range of scholarly articles, theses, and books. It allows researchers to easily search for peer-reviewed literature across various disciplines, ensuring credible and reliable sources. This platform also helps in tracking citations, enabling users to follow the impact and relevance of specific works in the academic community. Additionally, social media is important for facilitating communication and the exchange of ideas among individuals and communities. It also serves as a platform for disseminating information, enabling rapid access to news, trends, and public discussions.

In today's digital era, search engines are essential tools for navigating the vast amount of information available online. Platforms such as Google, Bing, and Yahoo have revolutionised the way we retrieve information, enabling users to find relevant content in mere seconds. This topic discusses the evolution of search engine usage, its impact on various aspects of daily life and business, and its implications for users and organisations.

2.5.1.1 Evolution of Search Engines

Search engines originated in the early 1990s with the development of simple directories and keyword-based search systems. Early search engines like Archie and Lycos offered basic functionalities by indexing web content and allowing users to perform text-based searches. The launch of Google in 1998 marked a major advancement with its PageRank algorithm, which provided more accurate and relevant search results by evaluating the quality and quantity of backlinks to web pages. This innovation set new standards for search engine effectiveness and user satisfaction.

Over time, search engines have evolved from basic tools into complex systems that integrate machine learning, natural language processing, and artificial intelligence. Modern search engines now use sophisticated algorithms to understand user intent, deliver personalised results, and directly answer questions within search results. Features such as voice search, autocomplete suggestions, and integrated knowledge panels have further enhanced the user experience, making it easier to find and consume information.

2.5.1.2 Search Engine Impact on Daily Life

Search engines have dramatically changed how we conduct research, make decisions, and engage with digital content. They are a primary source of information for various tasks, ranging from academic research and job hunting to finding local services and entertainment. The ability to quickly access a wide range of information has empowered users to make informed decisions and interact with content more effectively. Fig. 2.5.1 shows a sample search engine window.

For example, in healthcare, patients often use search engines to learn about symptoms, treatments, and medical conditions. While this can lead to better-informed individuals, it also raises concerns about the accuracy of medical information and the potential for misinformation. This situation underscores the need for search engines to prioritise authoritative and reliable sources in their results.

In education, search engines have become vital tools for students and educators, facilitating access to academic resources, research papers, and educational materials. However, the vast amount of available information can also create challenges, such as information overload and difficulty in discerning credible sources. This highlights the importance of digital literacy and critical thinking skills in navigating search engine results.

2.5.1.3 Impact on Business Marketing

Fig. 2.5.1 Search Engine

For businesses, search engines are crucial components of digital marketing strategies. Search engine optimisation (SEO) involves optimising websites and content to rank higher on search engine results pages (SERPs), thereby driving organic traffic and enhancing online visibility. Effective SEO practices can lead to increased brand awareness, higher conversion rates, and competitive advantages in the marketplace. Pay-per-click (PPC) advertising is another key aspect of search engine marketing, allowing businesses to place advertisements on search engine results pages and pay only when users click on their advertisements. This model provides targeted advertising opportunities, enabling businesses to reach specific audiences based on keywords, demographics, and user behaviour.

The competitive nature of search engine marketing requires businesses to continually adapt to changing algorithms and search trends. Staying updated with SEO best practices, understanding user intent, and leveraging data analytics are essential for achieving and maintaining high search rankings. This dynamic environment emphasises the importance of ongoing investment in digital marketing and search engine optimisation.

2.5.2 Exploring Google Scholar

Google Scholar (GS) is a specialised, free academic search engine that serves as an academic counterpart to the broader Google search engine. Unlike Google, which indexes the entire web, Google Scholar focuses on academic repositories, including:

- Publishers
- Universities
- Scholarly websites

This targeted approach provides access to a more curated subset of scholarly sources. Despite its utility, Google Scholar includes a broader range of sources than subscription-based academic databases like Scopus and Web of Science. Consequently, users must critically assess the credibility of resources found through Google Scholar.

Google Scholar offers several advantages over standard Google searches for academic research:

2.5.2.1 Familiar Interface

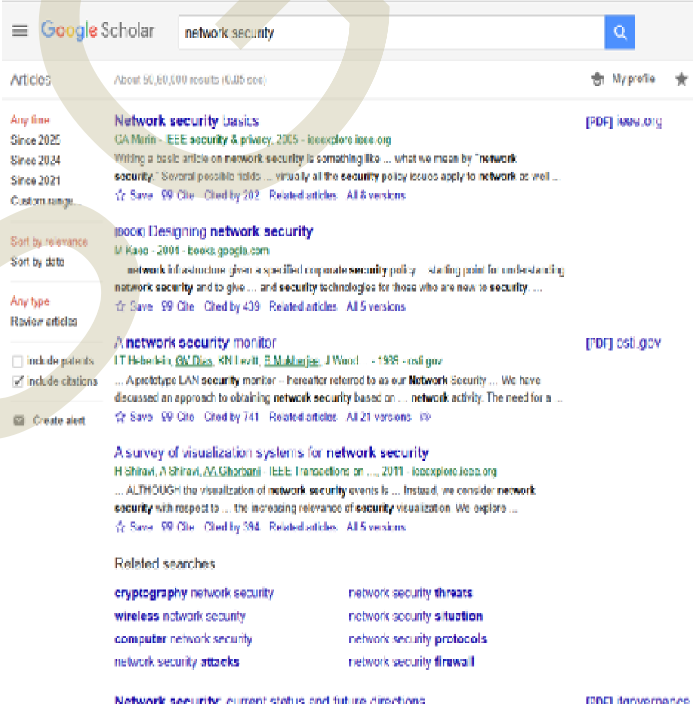
Google Scholar features a familiar user interface that mirrors the design and layout of Google's main search engine. This similarity reduces the learning curve, making it easy for users to navigate and find scholarly information without needing extensive training. Users can quickly perform searches using the simple search bar, just as they would when searching the web. The clean and intuitive design allows for easy access to filters, advanced search options, and related articles. This familiar interface helps both beginners and experienced researchers streamline their search for academic resources efficiently.

2.5.2.2 Citation Tools

Google Scholar provides built-in citation tools that allow users to easily copy formatted citations in various styles, such as MLA, APA, and Chicago. This feature is especially helpful for students, researchers, and writers who need to properly credit sources in their work. Users can export bibliographic data in formats like BibTeX and RIS, which can be directly imported into reference management software like EndNote, Zotero, or Mendeley. This capability saves time and ensures that references are consistently formatted. By simplifying the citation process, Google Scholar makes academic writing and research more efficient.

2.5.2.3 Citation Tracking

Google Scholar offers a powerful feature called citation tracking, which allows users to see how many times a particular resource has been cited by other works. This provides a quick way to assess the impact and relevance of a publication in its field. Users can also explore the list of articles



Network security basics [PDF] ieee.org
CA Marin - IEEE security & privacy, 2005 - ieeexplore.ieee.org
Writing a basic article on network security is something like ... what we mean by "network security." Several possible fields ... virtually all the security policy issues apply to network as well ...
☆ Save 99 Cite Cited by 202 Related articles All 8 versions

[BOOK] Designing network security
M Kaeo - 2004 - books.google.com
... network infrastructure given a specified corporate security policy ... starting point for understanding network security and to give ... and security technologies for those who are new to security. ...
☆ Save 99 Cite Cited by 439 Related articles All 5 versions

A network security monitor [PDF] osti.gov
LT Heberlein, GV Dias, KN Levitt, B Mukherjee, J Wood ... - 1989 - osti.gov
... A prototype LAN security monitor -- hereafter referred to as our Network Security ... We have discussed an approach to obtaining network security based on ... network activity. The need for a ...
☆ Save 99 Cite Cited by 741 Related articles All 21 versions

A survey of visualization systems for network security
H Shiravi, A Shiravi, AA Ghorbani - IEEE Transactions on ..., 2011 - ieeexplore.ieee.org
... ALTHOUGH the visualization of network security events is ... Instead, we consider network security with respect to ... the increasing relevance of security visualization. We explore ...
☆ Save 99 Cite Cited by 394 Related articles All 5 versions

Related searches

cryptography network security	network security threats
wireless network security	network security situation
computer network security	network security protocols
network security attacks	network security firewall

Network security: current status and future directions [PDF] dergipark...

Fig. 2.5.2 A typical Google Scholar page

that have cited the original work, enabling them to follow the research trail and discover more recent studies on the same topic. Citation tracking is useful for identifying influential papers and gaining insights into the ongoing academic discussion around a specific subject. This helps researchers stay current with developments in their fields.

2.5.2.4 Navigating the Google Scholar Search Result Page

The layout of Google Scholar's search results page differs from Google's standard search results.

Each Google Scholar search result includes core bibliographic information that provides essential details about the document. Fig. 2.5.2 shows a typical Google Scholar page. The title of the work, whether it's an article, book, or chapter, is prominently displayed, often with a clickable link that directs users to the publisher's page for more details. This page usually includes additional resources like abstracts and, in some cases, PDFs for further reading. Bibliographic details such as the authors' names, the journal or book title, the publication year, and the publisher are also listed, giving users a quick snapshot of the source's background. Some results may feature direct links to the full text, though these versions may not always be the final published ones.

Additional helpful links enhance the research process. The "Cited by" link displays other articles that have cited the resource, which is useful for tracking more recent research and assessing the source's credibility. Google Scholar also offers alternative versions of the work through the "Versions" link, where users might find free access through different databases. A built-in citation tool provides formatted citation options, such as MLA, APA, or Chicago styles. It allows users to export the citation data in formats like BibTeX or RIS for easy integration into reference management software. This set of features makes Google Scholar an invaluable tool for efficiently accessing and managing scholarly resources.

2.5.2.5 Scope and Limitations

Google Scholar is a vast and continually expanding academic resource with an estimated 160 million records, offering access to a wide range of scholarly materials such as journal articles, books, conference proceedings, patents, and court opinions. It provides a rich selection of academic sources, including peer-reviewed articles, book chapters, and recent research, making it a valuable tool for general academic research. However, its coverage is not exhaustive, especially in areas like multimedia content or highly specialised collections, which may require users to consult local library catalogs or other platforms.

Despite its broad content, Google Scholar has limitations, particularly in the consistency and accuracy of its metadata, which can make it challenging to locate precise information or reliable citations. It also indexes materials from both reputable and predatory journals, emphasising the need for critical evaluation of sources. While Google Scholar is an accessible and convenient research tool, it should be used alongside other databases and library resources to ensure comprehensive and high-quality research. Understanding its strengths and limitations enables researchers to effectively incorporate Google Scholar into their work while supplementing it with other resources for a more thorough investigation.

2.5.3 Social Media

The purpose of social media is to facilitate the sharing and exchange of ideas, information, and content among users through digital platforms. It enables individuals and organisations to connect, communicate, and engage with a global audience in real time. Social media serves various functions, including personal networking, professional development, and marketing, by providing a space for user-generated content, interactive communication, and community building. Its versatility makes it a powerful tool for fostering relationships, spreading information, and driving engagement across diverse sectors of society.

Social media platforms initially emerged to facilitate personal interactions, enabling users to connect with friends and family. Over time, these platforms expanded their functions, integrating various features to serve diverse purposes. For example, early platforms like MySpace paved the way for future networks by attracting large user bases and establishing the concept of online social networking.

Subsequent platforms such as Facebook and Twitter (now X) built on this foundation, transforming how information is shared and consumed. Facebook enabled users to connect globally and engage with a wide range of content, while Twitter introduced real-time updates, changing the dynamics of information dissemination.

As social media continued to evolve, new platforms emerged, each offering unique features. TikTok focuses on short-form video content, while Signal and Clubhouse have introduced innovations in privacy and audio-based interactions. This ongoing development reflects the adaptability and growth of social media as a central element of digital communication.

2.5.3.1 Social Media Family

Social media encompasses a wide variety of digital platforms designed to enable users to create, share, and engage with content across the globe. These platforms serve as hubs for communication, interaction, and the exchange of ideas in various formats, including text, images, videos, and more. By offering diverse ways to connect, social media platforms have become a key part of daily life for billions of people. Each platform provides unique features tailored to different types of content and interaction, allowing users to engage with information and communities in different ways.

One of the largest and most well-known social media platforms is Facebook, which offers a space for users to connect with friends, family, and communities. It allows people to share updates, photos, videos, and participate in discussions within various groups and events. Facebook's versatility makes it a central platform for both personal and professional connections, as well as for news sharing and business promotion. Instagram, another major player in the social media landscape, focuses primarily on photo and video sharing. With features like Stories, Reels, and IGTV, Instagram caters to users looking for creative, visually engaging content. It has become a go-to platform for influencers, brands, and individuals who want to showcase their lives and interests through images and short videos.

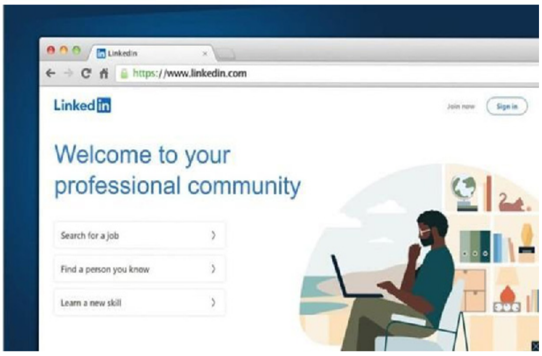


Fig 2.5.3 LinkedIn Homepage

LinkedIn is a professional social media platform designed to help individuals and businesses connect, network, and grow professionally. Fig. 2.5.3 shows a LinkedIn Homepage. Unlike other social media platforms focused on personal updates or entertainment, LinkedIn emphasises career development, industry networking, and business opportunities. Users can create profiles showcasing their work experience, skills, and educational background, making it a digital resume for potential employers and collaborators. LinkedIn offers features like job postings, where users can apply directly to job opportunities, and recommendations, allowing colleagues to endorse each other's skills. The platform also includes LinkedIn Learning, offering professional development courses on various topics. In addition, LinkedIn's news feed keeps users updated on industry trends, thought leadership posts, and company updates. For businesses, LinkedIn provides tools for creating company pages, promoting products or services, and connecting with potential clients or partners, making it a powerful tool for professional networking and career advancement.

X (formerly Twitter) is known for its real-time updates and brief, to-the-point content. With its 280-character limit, users can share thoughts and news and engage in discussions on a variety of topics, making it a popular platform for commentary on current events, politics, and trending topics. This platform fosters a fast-paced environment where ideas are exchanged quickly and publicly, often serving as a barometer for global conversations. Meanwhile, YouTube stands as the dominant platform for video sharing, where users can upload, view, and comment on video content. From educational tutorials to entertainment, YouTube's vast array of content appeals to a wide audience, making it an essential resource for creators and consumers of all kinds.

In addition to these major platforms, there are other popular social media tools globally, each offering unique functionalities. WhatsApp is widely known for its messaging capabilities, allowing users to send texts, voice messages, images, and make voice or video calls, making it especially popular for personal communication. Similarly, Facebook Messenger, integrated with Facebook, allows users to chat, share media, and connect directly. Telegram has gained popularity for its emphasis on privacy and secure messaging, offering encrypted communication and the ability to manage large group chats.

For visual content enthusiasts, Pinterest provides a platform to bookmark, share, and explore visual ideas on topics like fashion, home decor, and DIY projects. It serves as a digital inspiration board where users can "pin" images and ideas for future reference. Snapchat appeals to users who enjoy multimedia messaging with a twist. It offers temporary content that disappears after being viewed, along with features like augmented reality filters, making it popular for sharing quick, playful snapshots.

These platforms demonstrate a wide range of functionalities and content-sharing options available on social media today. Each one offers unique opportunities for interaction, creativity, and communication, making them indispensable tools in both personal and professional settings. Globally, social media usage exceeds 5 billion people, which represents about 62% of the world's population. This widespread adoption highlights social media's role as a significant component of modern communication and information sharing. Fig 2.5.4 shows some social media logos.

Fig 2.5.4 Sample Social Media Logos

2.5.3.2 Categories and Uses of Social Media

Social media platforms can be broadly categorised into several types, each offering unique functions and catering to different user needs. Social networking platforms, such as Facebook and LinkedIn, are designed for building personal and professional connections. Facebook allows users to connect with friends and family, join groups, and share updates, making it a hub for both social interaction and community engagement. LinkedIn, on the other hand, focuses on professional networking, allowing users to build relationships with colleagues, showcase their work experience, and engage in career-oriented discussions. Both platforms play a crucial role in fostering connections and facilitating communication on a global scale, but each serves distinct purposes such as personal interaction versus professional growth.

Another category is social bookmarking platforms, with Pinterest being a prime example. Pinterest enables users to save, categorise, and share links to web content, whether it's articles, images, or ideas related to personal interests like fashion, home decor, recipes, or DIY projects. Users can create themed boards to organise content and share it with others, helping them discover new hobbies, trends, or creative inspiration. Social bookmarking platforms are especially useful for curating large amounts of content in an organised and visually appealing way. Social news platforms, like Reddit, focus on the collective sharing and discussion of news articles and updates. Reddit is community-driven, with users posting news, voting on the relevance of content, and engaging in discussions on a wide variety of topics. Different subreddits cater to specific interests, ranging from politics and technology to niche hobbies, allowing users to go deeply into specialised communities. This type of platform is particularly valuable for crowdsourcing opinions, sharing current events, and fostering debates that are often more dynamic and community-oriented than traditional news outlets.

2.5.4 Social Media Interactions

1. **Social Media Interactions:** Social media allows people to connect and communicate by sharing updates, photos, videos, and interacting through likes, comments, and shares. It supports real-time communication and helps build relationships with individuals, communities, and organisations. These platforms also offer spaces for discussions, joining interest-based groups, and participating in online communities.

2. **Privacy and Security:** Protecting privacy is vital on social media. Sharing too much personal information can lead to identity theft, stalking, or fraud. Users should avoid posting sensitive details like home addresses, phone numbers, and bank information. Strong, unique passwords and two-factor authentication add extra layers of security, helping protect personal data and online accounts from hackers.

3. **Digital Footprint :** Everything shared online contributes to a digital footprint, which can be permanent. Even deleted posts may remain through screenshots or archives. A thoughtless post today could affect future job opportunities or relationships. It's important to think before posting and understand how content may be viewed by different audiences over time.

4. **Misinformation and Mental Health:** False information can spread quickly on social media, creating confusion and harm. Always verify facts using trusted sources before sharing content.

Additionally, constant use of social media can impact mental health, leading to stress or low self-esteem especially when comparing oneself to others. Taking breaks and balancing offline activities helps maintain emotional well-being.

5. **Online Etiquette:** Respectful communication is essential. Even during disagreements, users should avoid cyberbullying, trolling, or hate speech, as these behaviours can deeply hurt others and damage reputations. Being mindful of cultural and social sensitivities also supports a more inclusive and respectful online space.

6. **Responsible Posting:** Social media users should post thoughtfully, considering their audience be it friends, family, or coworkers. Harmless-looking content can sometimes offend or be misunderstood. Responsible posting includes being mindful of how often you post, the tone of your content, and ensuring it reflects your values respectfully.

7. **Legal Considerations:**Users must be aware of laws that apply to online activity. Sharing copyrighted content without permission or making defamatory statements can lead to legal issues. It's important to credit original creators and avoid using protected material without consent. Understanding platform rules also helps avoid account penalties.

8. **Platform Policies:** Every social media platform has its own terms of service and community guidelines. Violating these can result in content removal or account suspension. Knowing how each platform moderates content helps users stay compliant and use the platform more effectively.

9. **Purposeful Use**: Using social media with a clear goal like networking, learning, or staying connected improves productivity. Following accounts that match personal interests adds value to your feed. This focused approach helps avoid aimless scrolling and creates more meaningful online experiences.

10. **Diverse Perspectives and Critical Thinking**: Social media algorithms often show users content they already agree with, creating echo chambers. To stay informed, it's important to seek out diverse viewpoints and think critically about the content you see. Asking questions and verifying facts promotes balanced thinking and informed online participation.

2.5.5 Credibility and Fact-Checking in Cyberspace

The expansive nature of the Internet has revolutionised information dissemination, presenting challenges related to credibility and fact-checking. Evaluating the trustworthiness of online content is critical as individuals make decisions based on the information they encounter. Credible information is essential for making informed choices in areas such as health, finances, education, and politics.

The Importance of Credibility

Credibility is the reliability of information available online, and it has become increasingly important in an age where anyone can publish content, regardless of its accuracy. A person might come across health advice on social media shared by a friend, but that information may not be backed by scientific research or expert opinion. This democratisation of information allows for diverse perspectives but also raises concerns about the trustworthiness of what is being shared. Therefore, assessing the credibility of sources is essential to ensure that decisions are based on accurate and reliable data. By critically evaluating the origins and evidence behind the information, individuals can make informed choices rather than relying on potentially misleading or false claims.

Several factors influence the credibility of online information. The source of information plays a significant role; content from reputable organisations, such as established news outlets or academic institutions, is generally more reliable. The author's expertise and credentials also impact credibility, as information from subject matter experts is often more trustworthy. Citations and references enhance credibility by allowing verification of information. The design and presentation of websites can also affect perceptions of credibility, although appearance alone should not be the sole criterion.

The Role of Fact-Checking

Fact-checking is crucial for ensuring information accuracy online. It involves verifying claims against reliable sources to correct errors and prevent misinformation. Fact-checking organisations and tools, such as Snopes and PolitiFact, provide evidence-based assessments of claims. This practice helps protect individuals from making decisions based on inaccurate information and builds trust in the accuracy of online content. Fig. 2.5.5 shows some fact-checking steps.

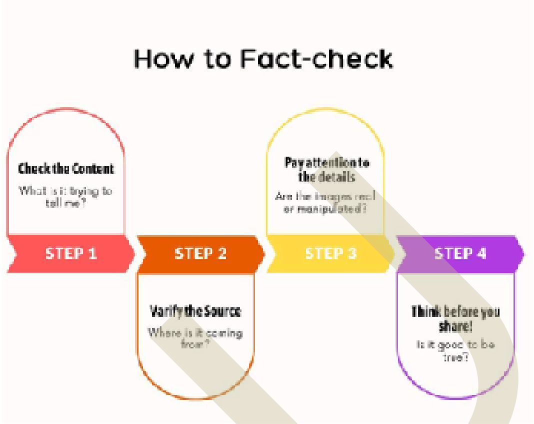


Fig 2.5.5 Fact-check before Sharing

Fact-checking faces challenges, including the sheer volume of information and the rise of sophisticated misinformation technologies like deepfakes. The vast and constantly changing nature of the Internet complicates the verification process. Confirmation bias can hinder the effectiveness of fact-checking, as individuals may reject information that contradicts their beliefs. Despite these challenges, prioritising credibility and fact-checking is essential for navigating cyberspace effectively.

Recap

- Search engines are essential tools for quickly accessing and retrieving information online.
- Early search engines like Archie and Lycos used simple keyword-based systems.
- Google's PageRank algorithm, introduced in 1998, significantly improved search result relevance.
- Modern search engines use AI, machine learning, and natural language processing to enhance user experience.

- Search engines impact daily life by facilitating research, decision-making, and access to various services.
- In healthcare, search engines help patients find information but raise concerns about misinformation.
- Search engines are vital for education, providing access to academic resources but also creating challenges like information overload.
- Search engines require constant adaptation to changing algorithms and trends.
- Privacy concerns arise from search engines collecting user data for personalisation.
- Regulations like GDPR address privacy and data protection in search engine usage.
- Google Scholar is a specialised academic search engine focusing on scholarly sources.
- Google Scholar offers citation tools, citation tracking, and full-text access but has limitations compared to subscription-based databases.
- Social media started as a way to connect with friends and family.
- Platforms like MySpace paved the way for modern social networking.
- Facebook and Twitter introduced global connections and real-time updates.
- Social media platforms serve as key communication tools in daily life.
- Platforms like LinkedIn support professional networking and career growth.
- Instagram and YouTube are popular for sharing visual and video content.
- Messaging apps like WhatsApp allow instant personal communication.
- Social media enables users to connect, share, and explore ideas globally.

Objective Questions

1. What is the major purpose of using search engines?
2. Which algorithm did Google introduce in the search engine?
3. What is the main use of Google Scholar?
4. What does SEO stand for?
5. What method is crucial to enhance digital account security?
6. What may persist even after a post is deleted?
7. What should be verified before sharing?
8. Excessive social media use can lead to what?
9. What should be avoided to maintain respect online?
10. What should be considered when posting content?
11. What must be respected to avoid legal issues?
12. LinkedIn is which type of social media network?
13. What helps make social media use more productive?
14. What should be actively sought to avoid echo chambers?

Answers

1. To find information on searched topics or links related to it.
2. PageRank
3. Research
4. Search Engine Optimisation
5. Passwords
6. Footprint
7. Need to do fact check

8. Stress
9. Bullying
10. Credibility
11. Copyright
12. Professional
13. Intent of use
14. Perspectives

Assignments

1. Analyse the impact of search engines on daily life, focusing on their influence on healthcare and education. Evaluate both the benefits and potential challenges that arise from using search engines in these contexts.
2. Assess the advantages and limitations of Google Scholar as a research tool compared to other academic databases like Scopus and Web of Science.
3. Evaluate the benefits and challenges associated with social media marketing.
4. Discuss how businesses leverage social media for customer interaction, advertising, and trend identification. Assess the impact of social media on customer behaviour and the potential challenges businesses face in maintaining effective social media strategies.

Reference

1. Ribble, M. (2015). Digital Citizenship in Schools: Nine Elements All Students Should Know (3rd ed.). International Society for Technology in Education (ISTE).
2. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.
3. Kennedy, M. (2016). Cyber Literacy: Navigating the Digital World. Wiley.

Suggested Reading

1. Couzin G, Grappone J. Search Engine Optimisation: An Hour a Day. Wiley Publishing; 2008.

2. Evans L. Social Media Marketing: Strategies for Engaging in Facebook, Twitter & Other Social Media. Pearson Education; 2010 Jun 18.

3. Kawasaki G, Fitzpatrick P. The Art of Social Media: Power Tips for Power Users. Penguin; 2014 Dec 4.

MODEL QUESTION PAPER SETS

SREENARAYANAGURU OPEN UNIVERSITY

QP CODE: ………   Reg. No.: ………..............

Name: ……....…………...

MODEL QUESTION PAPER I
FIFTH / SIXTH SEMESTER - UG DEGREE EXAMINATION
GENERAL ELECTIVE COURSE – B21CA01GE
COMPUTER SYSTEMS AND INTERNET TECHNOLOGIES
(CBCS - UG)
2022-23 - Admission Onwards

Time: 3 Hours   Max Marks: 70

Section A

I Answer any 10 questions. Each carries one mark

1. Which generation of computers used microprocessors?
2. What is the full form of RTOS?
3. Name one open-source operating system.
4. What storage device uses flash memory and has no moving parts?
5. What is the function of a modem?
6. What does SaaS stand for in cloud computing?
7. Name one wireless communication technology.
8. Which file system is commonly used in Windows?
9. What is a computer that handles both analog and digital data called?
10. What protocol is used for secure remote login to Unix-based systems?
11. What does the acronym "UEFI" stand for?
12. What is used to block ads and trackers on websites?
13. What is the practice of automatically adjusting computing resources based on demand in the cloud?
14. What does 4G LTE stand for?
15. What should be actively sought to avoid echo chambers?

(10×1=10 marks)

Section B

II Answer any 5 questions. Each question carries 2 marks

16. Differentiate between volatile and non-volatile memory.
17. What is the function of a kernel in an operating system?
18. State two differences between Windows and Linux operating systems.
19. How does an IP address differ from a MAC address?
20. What are the benefits of using public cloud deployment?
21. What is the main reason for creating multiple partitions on a disk?
22. What is phishing in cybersecurity?
23. Define web hosting with an example.
24. Mention any two advantages of Captcha.
25. What is Virtual Memory?

(5×2=10 marks)

Section C

III Answer any 5 questions. Each question carries 4 marks

26. Explain the evolution of computers from first to fifth generation.
27. Describe different functions of an operating system with examples.
28. Explain the steps to install an operating system on a new device.
29. Discuss the key networking devices and their roles.
30. Explain the difference between a switch and a router in terms of their function in a network.
31. Describe the features of 3G, 4G, and 5G mobile technologies.
32. Discuss the advantages of Portable Devices.
33. Explain the types of IP Addresses

(5×4=20 marks)

Section D

IV Answer any 3 questions. Each question carries 10 marks

34. Compare different operating systems based on usability, performance, and security.

35. Describe major types of cybersecurity threats and the preventive techniques to mitigate them.

36. What is Spamming?Explain the different types.

37. Explain the different cloud service models.

38. Discuss the various types of network connection methods used in computer networking.

39. Compare and contrast Bluetooth, ZigBee, and WiFi as short-range wireless technologies.

(3×10=30 marks)

SREENARAYANAGURU OPEN UNIVERSITY

QP CODE: ………   Reg. No.: ………...............

Name: ……...…………...

MODEL QUESTION PAPER II
FIFTH / SIXTH SEMESTER - UG DEGREE EXAMINATION
GENERAL ELECTIVE COURSE – B21CA01GE
COMPUTER SYSTEMS AND INTERNET TECHNOLOGIES
(CBCS - UG)
2022-23 - Admission Onwards

Time: 3 Hours   Max Marks: 45

Section A

I Answer any 10 questions. Each carries one mark

1. What is the fastest type of memory in a computer?
2. What does BIOS stand for?
3. What is the default file system in Windows OS?
4. What device connects LANs together?
5. What is the full form of IaaS?
6. Which technology uses satellites for positioning?
7. Which unit is responsible for email and web content security?
8. What is the general term for software designed with malicious intent?
9. What does GPS stand for?
10. Which device does I/O device management handle communication with?
11. What type of firewall tracks the state of active connections?
12. What term refers to storing and accessing data over the internet, rather than on a local server?
13. What does a router use to forward data between networks?
14. What type of computer is designed for a specific task only?
15. Which operating system is known for its open-source nature and flexibility?

(10×1=10 marks)

Section B

II Answer any 5 questions. Each question carries 2 marks

16. What are the different types of computer memory?
17. What are system calls? Give two examples.
18. State two factors to consider while choosing an OS.
19. Explain the role of a Content Management System (CMS) in managing web content.
20. List two advantages of cloud computing in business.
21. How does GPS differ from GPRS?
22. What is the use of pop-up blockers in web browsers?
23. Describe two components of a URL.
24. What is the function of a "boot loader" in an operating system?
25. What are cookies?

(5×2=10 marks)

Section C

III Answer any 5 questions. Each question carries 4 marks

26. Describe different classifications of computers based on size and functionality.
27. Explain the process and components involved in booting a computer.
28. Describe proprietary vs open-source OS with suitable examples.
29. Explain IPv4 vs IPv6 with advantages of each.
30. Differentiate between WiFi and WiMAX regarding their range, speed,mobility, and common applications.
31. Explain the key features of 3G technology.
32. Differentiate Wired and Wireless connection.
33. Why is cloud computing important in E-commerce?

(5×4=20 marks)

Section D

IV Answer any 3 questions. Each question carries 10 marks

34. Explain the entire HTTP request-response cycle in web communication with appropriate diagrams.

35. Discuss web and email security threats and the tools used to manage them.

36. Describe how Two-Factor Authentication (2FA) works and explain its advantages and disadvantages with real-life examples.

37. Explain about computer memory.

38. What is Clickjacking? Explain the types.

39. Illustrate the process of data transmission in a wireless network, highlighting key devices involved.

(3×10=30 marks

സർവ്വകലാശാലാഗീതം

വിദ്യയാൽ സ്വതന്ത്രരാകണം
വിശ്വപൗരരായി മാറണം
ഗ്രഹപ്രസാദമായ് വിളങ്ങണം
ഗുരുപ്രകാശമേ നയിക്കണേ

കൂരിരുട്ടിൽ നിന്നു ഞങ്ങളെ
സൂര്യവീഥിയിൽ തെളിക്കണം
സ്നേഹദീപ്തിയായ് വിളങ്ങണം
നീതിവൈജയന്തി പാറണം

ശാസ്ത്രവ്യാപ്തിയെന്നുമേകണം
ജാതിഭേദമാകെ മാറണം
ബോധരശ്മിയിൽ തിളങ്ങുവാൻ
ജ്ഞാനകേന്ദ്രമേ ജ്വലിക്കണേ

കുരീപ്പുഴ ശ്രീകുമാർ

SREENARAYANAGURU OPEN UNIVERSITY

Regional Centres

Kozhikode
Govt. Arts and Science College
Meenchantha, Kozhikode,
Kerala, Pin: 673002
Ph: 04952920228
email: rckdirector@sgou.ac.in

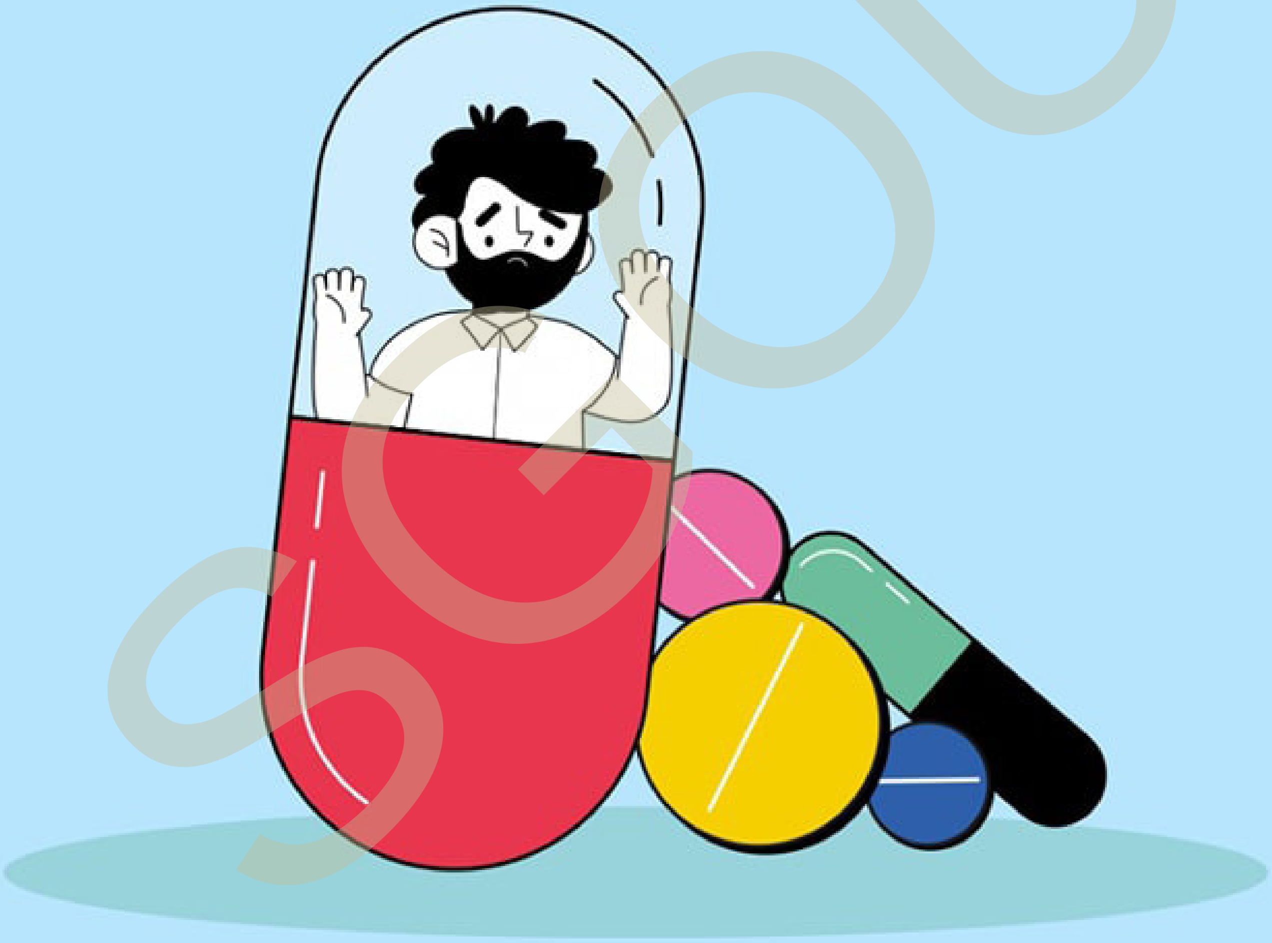
Thalassery
Govt. Brennen College
Dharmadam, Thalassery,
Kannur, Pin: 670106
Ph: 04902990494
email: rctdirector@sgou.ac.in

Tripunithura
Govt. College
Tripunithura, Ernakulam,
Kerala, Pin: 682301
Ph: 04842927436
email: rcedirector@sgou.ac.in

Pattambi
Sree Neelakanta Govt. Sanskrit College
Pattambi, Palakkad,
Kerala, Pin: 679303
Ph: 04662912009
email: rcpdirector@sgou.ac.in

NO TO DRUGS

തിരിച്ചിറങ്ങാൻ പ്രയാസമാണ്



ആരോഗ്യ കുടുംബക്ഷേമ വകുപ്പ്, കേരള സർക്കാർ

Computer Systems and Internet Technologies

COURSE CODE: B21CA01GE

Sreenarayanaguru Open University
Kollam, Kerala Pin- 691601, email: info@sgou.ac.in, www.sgou.ac.in Ph: +91 474 2966841

ISBN 978-81-986991-4-5
9 788198 699145