

Domestic Biometric Data Operator

(Job Role)

Qualification Pack: Ref. Id. SSC/Q2213

Sector: Information Technology and Information
Technology enabled Services (IT-ITeS)

Textbook for Class XI



171105

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी
NCERT

राष्ट्रीय शैक्षिक अनुसंधान और प्रशिक्षण परिषद्
NATIONAL COUNCIL OF EDUCATIONAL RESEARCH AND TRAINING

171105– Domestic Biometric Data Operator

Vocational Textbook for Class XI

ISBN 978-81-949859-6-9

First Edition

March 2021 Phalgun 1942

PD 5T BS

© **National Council of Educational
Research and Training, 2021**

₹ **235.00**

*Printed on 80 GSM paper with NCERT
watermark*

Published at the Publication Division
by the Secretary, National Council
of Educational Research and
Training, Sri Aurobindo Marg, New
Delhi 110 016 and printed at Shree
Vrindavan Graphics (P.) Ltd., E-34,
Sector-7, Noida - 201 301 (U.P.)

ALL RIGHTS RESERVED

- ❑ No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission of the publisher.
- ❑ This book is sold subject to the condition that it shall not, by way of trade, be lent, re-sold, hired out or otherwise disposed off without the publisher's consent, in any form of binding or cover other than that in which it is published.
- ❑ The correct price of this publication is the price printed on this page. Any revised price indicated by a rubber stamp or by a sticker or by any other means is incorrect and should be unacceptable.

OFFICES OF THE PUBLICATION

DIVISION, NCERT

NCERT Campus
Sri Aurobindo Marg
New Delhi 110 016 **Phone : 011-26562708**

108, 100 Feet Road
Hosdakere Halli Extension
Banashankari III Stage
Bengaluru 560 085 **Phone : 080-26725740**

Navjivan Trust Building
P.O. Navjivan
Ahmedabad 380 014 **Phone : 079-27541446**

CWC Campus
Opp. Dhankal Bus Stop
Panihati
Kolkata 700 114 **Phone : 033-25530454**

CWC Complex
Maligaon
Guwahati 781 021 **Phone : 0361-2674869**

Publication Team

Head, Publication Division : *Anup Kumar Rajput*

Chief Editor : *Shveta Uppal*

Chief Production Officer : *Arun Chitkara*

Chief Business Manager : *Vipin Dewan*
(In charge)

Editor : *Bijnan Sutar*

Assistant Production Officer : *Deepak Jaiswal*

Cover and Layout

DTP Cell, Publication Division

FOREWORD

The National Curriculum Framework (NCF)–2005 recommends bringing work and education into the domain of the curricula, infusing it in all areas of learning while giving it an identity of its own at relevant stages. It explains that work transforms knowledge into experience and generates important personal and social values, such as self-reliance, creativity and cooperation. Through work, one learns to find one’s place in society. It is an educational activity with an inherent potential for inclusion. Therefore, an experience of involvement in productive work in an educational setting will make one appreciate the worth of social life and what is valued and appreciated in the society. Work involves interaction with material or people (mostly both), thus, creating a deeper comprehension and increased practical knowledge of natural substances and social relationships.

Through work and education, school knowledge can be easily linked to learners’ life outside the school. This also makes a departure from the legacy of bookish learning and bridges the gap between the school, home, community and workplace. The NCF–2005 also emphasises Vocational Education and Training (VET) for all those children, who wish to acquire additional skills and seek livelihood through vocational education after either discontinuing or completing school education. VET is expected to provide a ‘preferred and dignified’ choice rather than a terminal or last resort option.

As a follow-up of this, NCERT has attempted to infuse work across subject areas and contributed in the development of the National Skill Qualification Framework (NSQF) for the country, which was notified on 27 December 2013. It is a quality assurance framework that organises all qualifications according to the levels of knowledge, skills and attitude. These levels, graded from one to ten, are defined in terms of learning outcomes, which the learners must possess regardless of whether they are obtained through formal, non-formal or informal learning. The NSQF sets common principles and guidelines for a nationally recognised qualification system, covering schools, vocational education and training institutions, technical education institutions, colleges, and universities.

It is under this backdrop that Pandit Sunderlal Sharma Central Institute of Vocational Education (PSSCIVE), Bhopal, a constituent of NCERT, has developed learning outcomes based modular curricula for vocational subjects from Classes IX to XII.

This has been developed under the Centrally Sponsored Scheme of Vocationalisation of Secondary and Higher Secondary Education of the Ministry of Education, erstwhile Ministry of Human Resource Development.

This textbook has been developed as per the learning outcomes based curriculum, keeping in view the National Occupational Standards (NOSs) for the job role and to promote experiential learning related to the vocation. This will enable the students to acquire necessary skills, knowledge and attitude.

I acknowledge the contribution of the development team, reviewers and all institutions and organisations, which have supported in the development of this textbook. NCERT welcomes suggestions from students, teachers and parents, which would help us to further improve the quality of the material in subsequent editions.

New Delhi
September 2020

HRUSHIKESH SENAPATY
Director
National Council of Educational
Research and Training

ABOUT THE TEXTBOOK

The IT-ITeS sector is an important industry in India and abroad, and is growing at a fast pace. With the growth in business opportunities in various domains around the globe, large amount of data is churned and transferred from one place to another, thus creating a need for proper management of the data that is collected. As the companies also need to focus on their core activities, many resort to outsourcing the data entry process. This has led to a huge demand for trained personnel for various job roles, such as biometric data operator.

A biometric data operator is responsible for capturing data that is used for validating and authenticating identity. A 'Domestic Biometric Data Operator' in the IT-ITeS industry is also known as Biometric Technician or Biometric Coordinator. Individuals at this job are responsible for the smooth running of the process of biometric data capture and ensuring that users get maximum benefit from them. Individual tasks vary depending on the size and structure of the organisation, but may include installing and configuring computer hardware operating systems and applications; monitoring and maintaining computer systems and networks, troubleshooting biometric system and network problems and diagnosing and solving hardware or software faults, etc. This job requires the individual to have thorough knowledge of various technology trends and processes as well as have updated knowledge about biometric systems and IT initiatives.

The textbook for the job role of 'Domestic Biometric Data Operator' has been developed to impart knowledge and skills through hands-on learning experience, which forms a part of the experiential learning.

This textbook has been developed with the contribution of subject experts, vocational teachers, and industry experts and academicians for making it a useful and inspiring teaching-learning resource material for the vocational students. Adequate care has been taken to align the content of the textbook with the National Occupational Standards (NOSs) for the job role so that the students acquire necessary knowledge and skills as per the performance criteria mentioned in the NOSs of Qualification Pack (QP).

The NOSs for the job role of 'Domestic Biometric Data Operator' covered through this textbook are as follows:

1. SSC/N3023 – undertake biometric data entry and processing
2. SSC/N9001 – manage work to meet requirements
3. SSC/N9003 – maintain a healthy, safe and secure working environment

Unit 1 covers the fundamentals of data and computing. This unit gives a basic overview of computer system and peripheral devices. It further explains the concept of data and data file formats.

Unit 2 gives a detailed overview of various types of biometric devices and the process to capture the biometric data.

Unit 3 discusses the basics of operating system and system maintenance. Lastly, Unit 4 covers the concept of computer networks, Internet and standards of biometric data.

DEEPAK D. SHUDHALWAR
Professor (CSE) and Head
Department of Engineering and Technology
PSSCIVE, NCERT, Bhopal

© NCERT
not to be republished

TEXTBOOK DEVELOPMENT TEAM

MEMBERS

Avadhut Sakhare, *Manager Production*, WYSE Biometrics, Pune

Gauri Phulaware, *Manager*, Software Department, WYSE Biometrics, Pune

Jayant Mishra, *Consultant—IT-ITeS (Contractual)*, Department of Engineering and Technology, PSSCIVE, NCERT, Bhopal

Mrunalini Nisal, *Manager – Client Support*, WYSE Biometrics, Pune

Prakash Khanale, *Professor and Head*, Department of Computer Science, DSM College, Parbhani, Maharashtra

Suhas Patil, *Technical Senior Engineer*, WYSE Biometrics, Pune

Yogendra Wadaskar, *Managing Director*, WYSE Biometrics, Pune

MEMBER-COORDINATOR

Deepak D. Shudhalwar, *Professor (CSE) and Head*, Department of Engineering and Technology, PSSCIVE, NCERT, Bhopal

ACKNOWLEDGEMENTS

The National Council of Educational Research and Training (NCERT) expresses its gratitude to all members of the Project Approval Board (PAB) and officials of the Ministry of Human Resource Development (MHRD), Government of India, for their cooperation in the development of this textbook. The Council also extends gratitude to all the contributors for sharing expertise and time by positively responding to the request for the development of this textbook.

The Council also acknowledges the contribution of the review committee members — Kamlesh Mittal, *Professor (Retd)*, DCETA, NCERT, New Delhi and Arti Goel, *Assistant Professor*, Hansraj College, University of Delhi, for carefully evaluating and giving suggestions for the improvement of this textbook.

The Council would also like to thank Rajesh Khambayat, *Joint Director*, PSSCIVE, Bhopal, for providing support and guidance in the development of this textbook.

The Council is grateful to Saroj Yadav, *Professor and Dean (A)*, NCERT, and Ranjana Arora, *Professor and Head*, Department of Curriculum Studies, for their sincere efforts in coordinating the review workshops for the finalisation of this textbook. The Council also acknowledges the copy editing and valuable contribution of Shilpa Mohan, *Assistant Editor (Contractual)* in shaping this textbook. The efforts of Pawan Kumar Barriar, *DTP Operator*, and Haridarshan Lodhi, *DTP Operator (Contractual)*, Publication Division, NCERT, for flawless layout design are also acknowledged. Abhinaw Kumar Dwivedi, *Consultant-Media and Entertainment (Contractual)*, PSSCIVE, Bhopal is duly acknowledged for drawing the figures used in this textbook.

CONTENTS

<i>Foreword</i>	<i>iii</i>
<i>About the Textbook</i>	<i>v</i>
Unit 1: Fundamentals of Data and Computing	1
Session 1: Power of Computing	2
Session 2: Data Types and Formats	25
Session 3: Biometric Data	38
Session 4: Collect and Digitise Data	53
Session 5: Store and Handle Data Securely	64
Unit 2: Procedures and Tools for Biometric Data	74
Session 1: Biometric System and Devices	75
Session 2: Setting up Biometric Devices	99
Session 3: Biometric Data Entry	111
Session 4: Interfacing of Biometric Devices	134
Unit 3: Operating System and System Maintenance	141
Session 1: Operating System	142
Session 2: Maintenance of Biometric System	160
Session 3: Updating of Biometric System	177
Unit 4: Computer Networks, Internet and Standards of Biometric Data	185
Session 1: Computer Networks	186
Session 2: Internet and its Application	215
Session 3: Standards of Biometric Data	236
Session 4: IT Practices	252
<i>Answer Key</i>	264
<i>Glossary</i>	269

Do You Know

According to the 86th Constitutional Amendment Act, 2002, free and compulsory education for all children in 6-14 year age group is now a Fundamental Right under Article 21-A of the Constitution.

EDUCATION IS NEITHER A PRIVILEGE NOR FAVOUR BUT A BASIC HUMAN RIGHT TO WHICH ALL GIRLS AND WOMEN ARE ENTITLED

*Give Girls
Their Chance !*



Unit



Fundamentals of Data and Computing



17110SCH01

Biometric technology is a technique to measure physiological or behavioural characteristics of a person to distinguish them from another and convert it into digital data. Biometric devices are connected to the computer system. Fingerprints, face, iris, retinal patterns and voice recognition are common methods used to identify authorised users. In each method, the computer compares the item being scanned with a copy of the item stored in the computer memory. It is essential to have basic knowledge of computer to work with biometric devices. Biometric data is the live data captured and stored in biometric devices. In this unit, you will understand the basics of computer and computing devices, different types of data, biometric data capture, its storage, conversion and handling.

SESSION 1: POWER OF COMPUTING

INTRODUCTION

Aviral, a Class X student, was given a mathematical problem to multiply an eight-digit fractional number with another eight-digit fractional number and divide the result by 67888.9. He took an hour to calculate. He was asked to do the same using a computer and he did it within seconds. Computer is a powerful electronic device with high computing capacity (Fig. 1.1).

Desktop computer, laptop, tablet and phones are major forms of computers available these days. Computer memory can be classified as: primary and secondary. Primary memory is the internal storage in the computer. It stores data and instructions temporarily for immediate access to CPU. Secondary memory on the other hand stores the data on a permanent basis. The devices used for secondary memory are called secondary storage devices. Every computer has an internal hard disk drive (HDD), fixed inside the computer, which is a secondary storage device. The other portable secondary storage devices that can be attached to the computer for backing up data are Compact Disc (CD), Digital Versatile Disc (DVD), USB flash drive or pen drive and external HDD. Apart from these all other devices attached to the computer for input or output operation are peripheral devices, such as printer, scanner, etc.

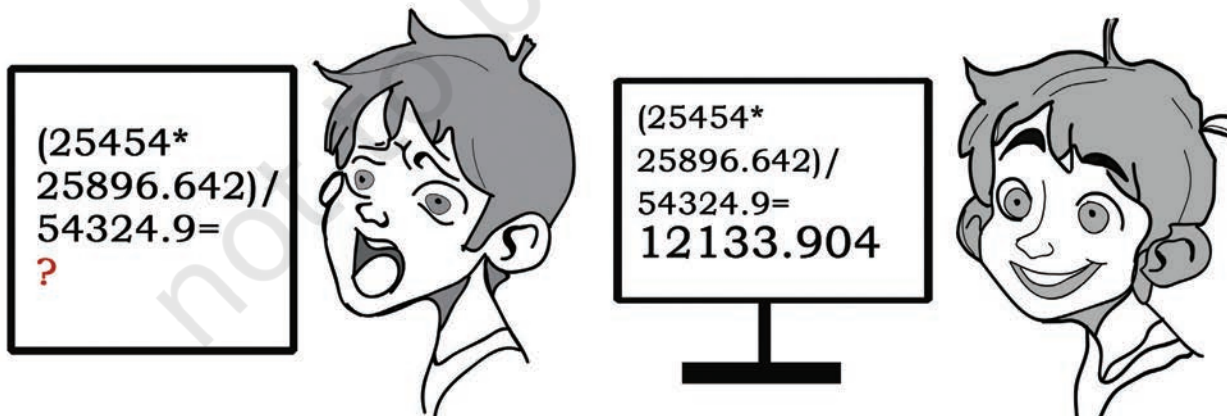
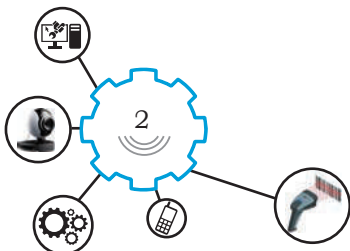


Fig. 1.1: Power of computing



Computer

The word computer is derived from the Latin word ‘*computare*’, which means to calculate. A computer is an electronic computational device that can perform sequences of arithmetic or logical operations based on a set of instructions called computer programs. It is essential to understand the functioning of a computer system to operate biometric devices. These devices are attached to the computer to capture and store data.

Components of a computer system

Every computer system has the following three basic components:

1. Input unit
2. Central processing unit
3. Output unit

While there are other components as well, these three are primarily responsible for making a computer function. Fig. 1.2 shows the diagram of a computer system.

The central processing unit (CPU) comprises arithmetic logic unit (ALU) and control unit (CU). The input and output devices are also connected to the computer.

(a) Input Unit: consists of input devices that are used to enter data in the computer. Data can be in the form of numbers, words, pictures, audio and video. Keyboard is an input device used to enter numbers and characters, whereas a mouse is used to enter directions and commands. Magnetic Ink Character Reader (MICR) and Optical Character Reader (OCR) are also types of input devices. In a biometric system, the fingerprint scanner, palm scanner and iris scanner are used to enter the biometric data.

(b) Central Processing Unit (CPU): after receiving data and commands from users, it processes these according to the instructions provided. The CPU has three elements — Memory Unit, Arithmetic Logic Unit and Control Unit.

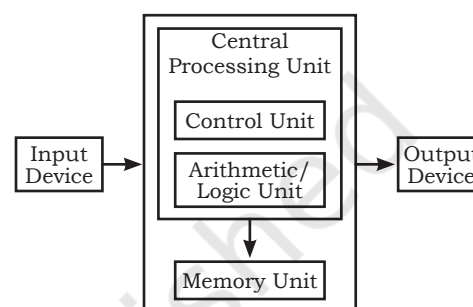
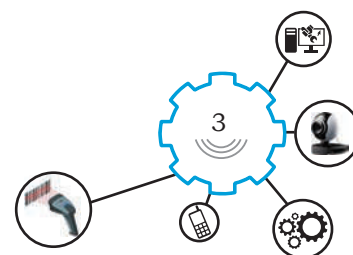


Fig. 1.2: Block diagram of computer system



NOTES

- (i) Memory Unit initially stores the data entered using input devices. This unit holds the data temporarily till the CPU processes it. The memory unit uses a set of pre-programmed instructions to further transmit this data to other parts of the CPU.
- (ii) Arithmetic and Logic Unit (ALU) performs arithmetical and logical operations, such as basic mathematical calculations (addition, subtraction, division, multiplication) and comparison of data.
- (iii) Control Unit coordinates tasks between all components of a computer system. It collects data from input unit and sends it to the processing unit. It also transmits the processed data to output unit for users.
- (c) Output Unit is any hardware device used to send data from a computer to another device or user, for example, monitor, screen, printer and speaker.

Practical Activity 1


Identify the various parts of a computer system

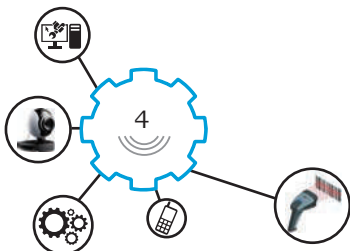
Material required

Computer and peripherals

Procedure

1. Observe the computer system provided to you carefully and identify the parts and peripherals.
2. Prepare a table showing the picture of each component along with its name as shown in the table below.

Picture of the Computer parts	Name of device
	Compact Disk (CD)

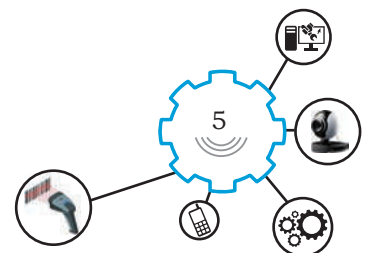


NOTES

	Universal Serial Bus (USB) cable
	
	
	
	
	
	

Role of Computer in Biometric System

Nowadays, computer system is used everywhere for networking and communication. It can process and store huge amount of data. Biometric devices



capture biometric data and store it in a server, which here is a computer. Therefore, computer systems play a critical role in the functioning of biometric systems. Biometric attendance systems can be commonly seen in government and private organisations, schools, colleges or even small shops to maintain the attendance of employees. There are various types of computers, which are used for this purpose depending on the application. Therefore, we must know about the various types of computers and its components.

Different Types of Computer Systems

A computer is a general-purpose device that can be programmed to carry out a finite set of arithmetical or logical operations. There are different types of computer systems—personal computer, workstation, minicomputer, mainframe and supercomputer.



Fig. 1.3: Personal computer



Fig. 1.4: Desktop computer



Fig. 1.5: Workstation

Personal computer (PC)

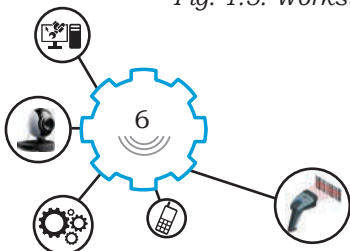
It is a small computer with a microprocessor, designed for use by individual. The modern PCs have touchscreens with built-in connectivity like Bluetooth and Wi-Fi. Fig. 1.3 shows a personal computer.

Desktop

It is also a PC with tower CPU and monitor. The desktop systems are set up in a permanent location. Desktops offer more power, storage and versatility for less cost than a portable computer. Fig. 1.4 shows a desktop computer.

Workstation

It is simply a desktop computer with a powerful processor, high memory, high-end graphics adapters and enhanced capabilities. Workstations are used for engineering applications, desktop publishing, software development, and other types of application that require a moderate amount of computing power and relatively high-quality graphic capabilities. Fig. 1.5 shows a workstation.



Servers

They have powerful processors, more memory, large hard drives and are capable of providing services to other computers over a network. They allow the client computers to share peripheral devices, software and information. In biometric systems, a centralised server is used to process the captured data. Fig. 1.6 shows a server computer.



Fig. 1.6: Server computer

Supercomputer

It is the fastest, most powerful and expensive computer. It can perform over a trillion calculations per second. Supercomputers consist of multiple CPUs working in parallel. They are used at places like atomic research centers, scientific institutes, or weather forecasting stations. Fig. 1.7 shows a supercomputer.

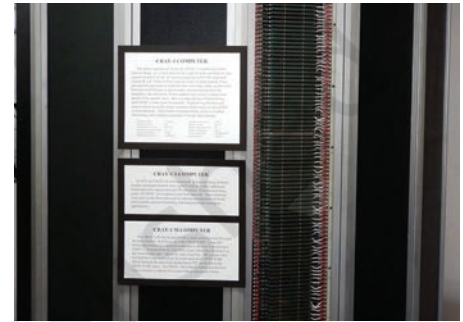


Fig. 1.7: Supercomputer

Laptops

They are portable computers that integrate a display screen, keyboard, a pointing device or trackball, processor, memory and hard drive all in a battery-operated package. Laptops can be folded for transportation, therefore they are ideal for travelling and mobile usage. Fig. 1.8 shows a laptop.



Fig. 1.8: Laptop

Netbooks

These are portable computers, which are smaller and cheaper than traditional laptops. Its internal components are less powerful than those of a regular laptop. They are primarily used for Internet and web surfing. They have small displays as small as 6 or 7 inches, less storage capacity ranging from 32 GB to 128 GB. Fig. 1.9 shows a netbook.



Fig. 1.9: Netbook

Tablet

It is a short name for tablet computer. It is also used as a personal computer. It is smaller than a

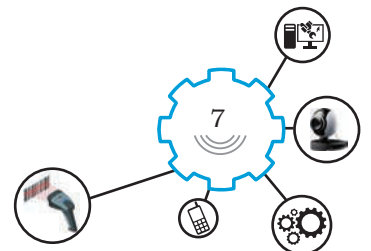




Fig. 1.10 (a): Tablet



Fig. 1.10 (b): Smartphone

netbook but larger than a smartphone. A tablet runs on a mobile operating system and can perform the functions just as in a smartphone, like taking photos, playing games and drawing with a stylus. Tablets usually have a screen size measuring 7 inches or larger, when measured diagonally. Fig. 1.10 (a) shows a tablet and Fig. 1.10 (b) shows a smartphone.



Fig. 1.11: Motherboard

Internal Computer Hardware Components

Internal components are fixed inside the computer system to perform important tasks. The main internal components of a computer system are as explained below.

Motherboard

It is the main circuit board of the computer system fitted inside the cabinet. All other important components, such as processor, memory and hard disk drive are connected with the motherboard. Fig. 1.11 shows a motherboard of a computer system.

Processor

It is an electronic device measuring about one-inch square. It is mounted on the motherboard. A modern processor may contain billions of transistors. It is the main component of a computer system, which performs computing and controls all the other components. Fig. 1.12 shows a processor used in computer system.

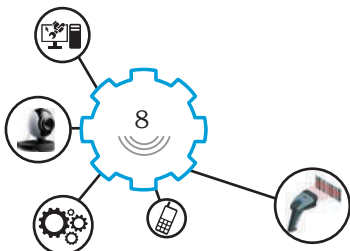


Fig. 1.12: Processor

Internal memory

Memory in a computer system can be primarily divided into four types based on the speed of access, cost and size of the memory. They are as follows:

- Registers
- Cache Memory
- Primary Memory
- Secondary Memory



- (a) **CPU Register** is located inside the CPU. It is extremely fast memory of the computer with an access speed of less than a nano second (1 ns). CPU registers are expensive and, hence, present in limited quantity of about 100 bytes.
- (b) **Cache Memory** is a high speed semiconductor memory, which provides high-speed data access to a processor and stores frequently used computer programs, applications and data. It is the second fastest memory of computer after CPU registers. It acts as a buffer between the CPU and the main memory. The parts of data and programs are transferred from the disk to cache memory by the operating system, from where the CPU can access them. Cache memory is also expensive and hence present in limited capacity in computer in the range of 512 MB or 1024 MB.
- (c) **Primary Memory** are of two types — RAM and ROM. It is also called internal memory or main memory. It holds data and instructions that execute. The primary memory is generally made up of a semiconductor device.
- (i) Random-access memory (RAM) is a type of computer memory that stores data and instructions currently being used. RAM is generally located on the motherboard. RAM allows the reading or writing operation of data in almost the same speed irrespective of the physical location of data inside the memory. It is a volatile and fast type of memory, where stored information is lost if power is turned off. Modern RAM is measured in GB (Gigabytes). Fig. 1.13 shows RAM modules used in a computer system.
 - (ii) Read Only Memory (ROM) permanently holds instructions. These instructions are known as BIOS (Basic Input Output System) or the boot program. The contents of ROM cannot be altered or added to by the

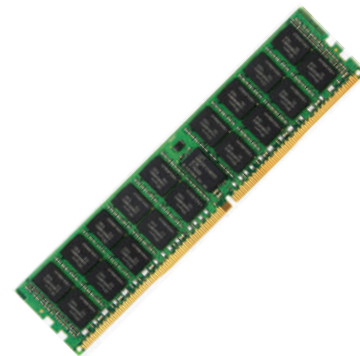
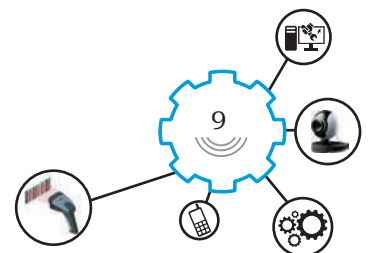


Fig. 1.13: Random Access Memory (RAM)



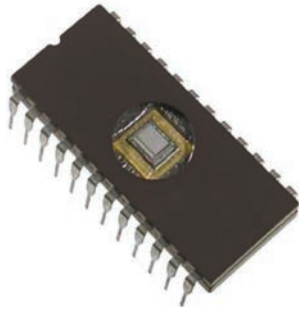


Fig. 1.14: Read Only Memory (ROM)



Fig. 1.15: Internal hard disk

user. Data stored in ROM can be accessed and read quickly. ROM is non-volatile memory, i.e. the stored information is not lost when the power is turned off. Fig.1.14 shows ROM chip.

Different types of ROM are

- PROM—Programmable Read Only Memory
- EPROM—Erasable Programmable Read Only Memory
- EEPROM—Electrically Erasable Programmable Read Only Memory

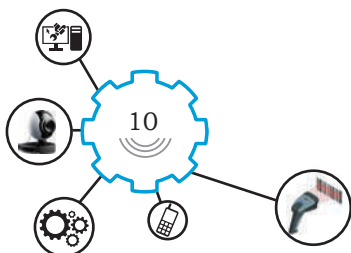
(d) Secondary Memory is used to store data that is not instantly needed by the computer. Secondary storage devices store the data permanently for a long period. These are used to take back-up data. The most common secondary memory is the internal hard disk drive, which is fixed inside the computer. It is connected with the motherboard and receives the power from internal power supply of computer. The hard disk has huge storage capacity as compared to the main memory. The storage capacity of modern hard disk ranges from 500 GB to 1 TB (terabyte). Fig. 1.15 shows an internal hard disk of a computer system.

Practical Activity 2

Identify the memory unit and its size in different computing devices

Material required

Personal Computer System, Laptop, Tablet, etc.



Procedure

1. Start the personal computer, and write steps to observe RAM used in the computer.
2. Start the laptop and write steps to observe the RAM used in the laptop.
3. Start the tablet, and observe the RAM used in the tablet
4. Record your observations in the table given below.

Computing device name	Size of memory used

Peripheral Devices

These devices are additionally connected to the computer system from outside and not from the basic components of the system. They are either input, output or storage devices.

Input devices

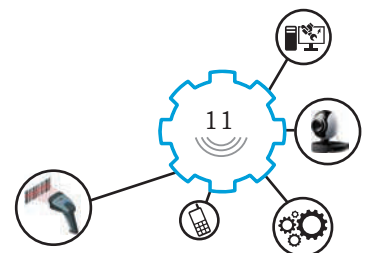
These devices are used to enter various types of data in the computer. Input devices can be divided into two categories.

(a) Manual Input Devices are used to enter data manually by hand.

- (i) Keyboard is used to enter text, number and special symbols by striking on the specific key on the keyboard. It is connected to the computer on serial port. Modern keyboards use USB port to connect to the computer externally. Fig. 1.16 shows the keyboard of a computer system.



Fig. 1.16: Keyboard



- (ii) Numeric keypad is used to enter numbers into the computer system. Most commonly it is used to enter PIN (personal identification number) in ATM and swapping machines. It is useful in large scale numeric data entry. Fig. 1.17 shows the numeric keypad.



Fig. 1.17: Numeric keypad

- (b) Pointing Devices (Mouse, touchpad, trackball)** are used to control pointing cursor, selecting menu options, clicking on icons in Graphical User Interface (GUI). There are three main types of pointing devices — mouse, touchpad and trackball.

- (i) Mouse is the most commonly used input device. Earlier it was connected to the computer on serial port or PS/2 port, but these days the mouse is connected to USB port on the computer. Mouse originally used a ball rolling on an overface to detect motion, but modern mouse often have optical sensors that have no moving parts. A mouse has two buttons and a scroll wheel. The left button is used to click and select icons and the right button is used to open context menus and the scroll wheel is used to scroll the document up and down. Fig. 1.18 shows the mouse used for a computer. Nowadays, cordless keyboard and mouse are also available, which give additional information. They use batteries for interfacing with the computer.

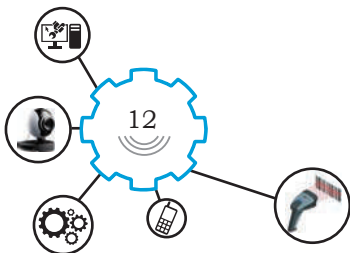


Fig. 1.18: Mouse



Fig. 1.19: Touchpad

- (ii) Touchpad is used in laptops instead of mouse. It has two buttons to work as mouse buttons. A touchpad allows the user to move the cursor with their finger. Fig. 1.19 shows a touchpad of laptop.
- (iii) Trackball performs the same function as a mouse. It is more accurate than a mouse and is used in gaming machines to control gaming characters.



(c) **Remote control** is used to control devices using infrared sign. Buttons on the remote control are used to change the channel number in TV, increase or decrease the volume. Fig. 1.20 shows a remote control.



Fig. 1.20: Remote control

(d) **Joysticks** are used to control objects in video games. They are used in simulators to control in simulated environment. Fig. 1.21 shows a joystick.



Fig. 1.21: Joystick

(e) **Touchscreen** is used to enter input into the computer by pressing on the screen. Touchscreens are used where limited options are available for selection, such as in ATM, airports, etc. Fig. 1.22 shows a touchscreen.



Fig. 1.22: Touchscreen

(f) **Scanners** are use to convert hard copy or printed documents, photographs to soft copy in digital form. The digital data can then be stored and manipulated by the computer. Fig. 1.23 shows a scanner.



Fig. 1.23: Scanner

(g) **Graphics Tablet** is used to create graphics on the computer. Graphics are drawn with a special pen called stylus. The graphics can be saved on the computer and further edited in graphics software. Fig. 1.24 shows a graphic tablet.

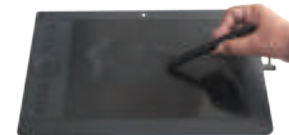


Fig. 1.24: Graphics Tablet

(h) **Microphone** is a sound input device. It accepts the analogue sound signals into computer. These analogue signals are converted into digital signals by the sound card. This digitised sound can be stored and manipulated by the computer. Fig. 1.25 shows a microphone.

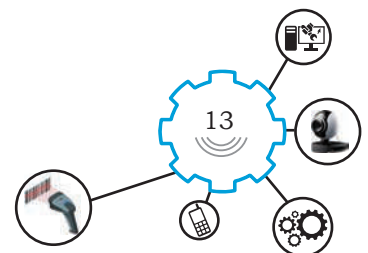


Fig. 1.25: Microphone

(i) **Digital Camera** is used to capture and store photographs (in the memory card), which can be transferred to the computer for viewing and editing. In digital camera, the image quality is measured in megapixels. The higher the megapixel the better the image quality. For example, a 12-megapixel camera produces images made up of 12 million dots. Modern digital cameras are capable of capturing video and sound. Nowadays, smartphones also have



Fig. 1.26: Digital camera



a built-in digital cameras. Fig. 1.26 shows a digital camera.



Fig. 1.27: Web camera

(j) **Web Camera** is attached to the computer for capturing digital photographs and video. The captured photo can be directly stored on the computer and hence it is used to capture face images in biometric system in the Aadhaar Center. Web camera is in-built in the laptop and it is used for video calling by using video calling application. Fig. 1.27 shows a web camera.

(k) **Direct Input Devices** are used to give input directly entered by the device. The examples of direct input devices are as follows.

(i) *Barcode Scanner or Reader* reads the stored barcode through visible red light reflected by barcode scanner, which is translated into digital information. The barcode present on the products holds information about the product ID number and manufacturer. However, it stores the price of the product. The price is stored in the database, which is accessed using product ID. After scanning the barcode the computer can read the information stored on the barcode and access details about the product from the database. Fig. 1.28 shows a barcode scanner.

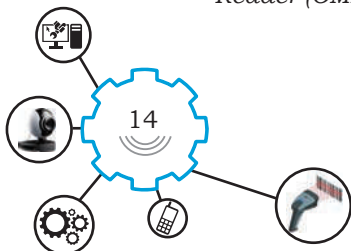


Fig. 1.28: Barcode scanner

(ii) *Optical Mark Reader (OMR)* can read the marks made by pen or pencil. OMR works with a scanner device that shines a beam of light on to the form paper, where answers are marked with pencil and reflects less light on the pencil mark. The reader tells the computer which option is selected. The selected option is matched with the correct answer in the database and thus the answer sheet is evaluated. It can process 4000 sheets per hour. OMR is used to process passport and identity cards and also used to process digitised books. Fig. 1.29 shows an OMR.



Fig. 1.29: Optical Mark Reader (OMR)



(iii) *Optical Character Reader (OCR)* consists of scanner and software. It scans the text on the paper and the software converts the scanned text into digital format. The digital text can be further edited and formatted. Fig. 1.30 shows an OCR.

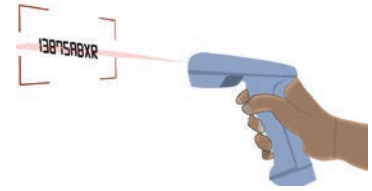


Fig. 1.30: Optical Character Reader (OCR)

(iv) *Magnetic Ink Character Recognition (MICR)* is mainly used to process cheques in banks. The MICR device reads the account number written in the special ink and then converts it into computer understandable form. The converted information is sent to the computer to process the cheques. MICR processes the cheques with speed and accuracy. Fig. 1.31 shows an MICR.



Fig. 1.31: Magnetic Ink Character Recognition (MICR)

Output devices

(a) **Monitor** is an output device that displays information in pictorial form. Older monitors used a CRT (cathode ray tube). These were heavy and bulky. The display device in modern monitors is a thin-film transistor liquid crystal display (TFT-LED) with LED back lighting. These screens are made up of thousands of tiny pixels. Each pixel has three transistors red, green and blue and each transistor can produce different intensities. Fig. 1.32 shows different types of monitors.

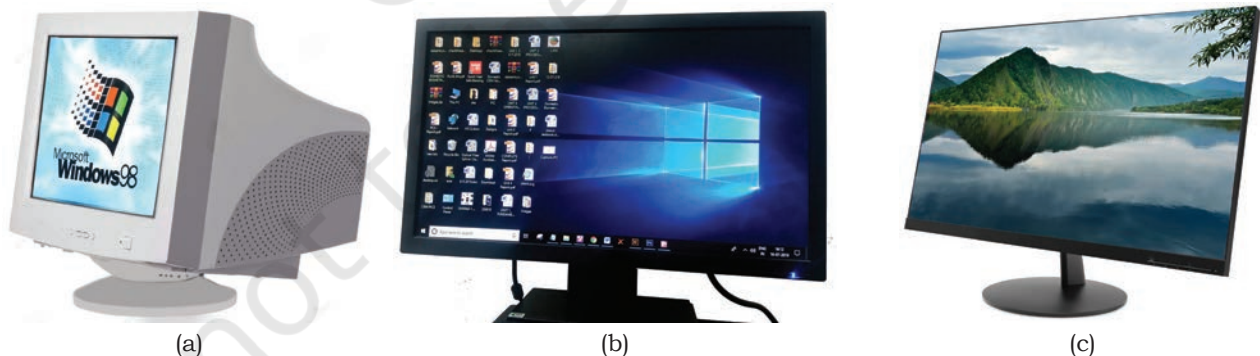
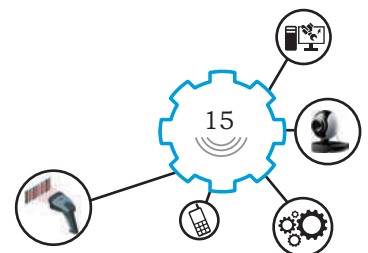


Fig. 1.32: Monitor (a) CRT (b) LCD (c) LED

(b) **Printer** is a peripheral device used to make a persistent human-readable representation of graphics or text on paper.



Printers are mainly divided into two categories — impact and non-impact. An impact printer makes contact with the paper, while a non-impact printer prints without making contact with the paper.

(i) Impact printer is a group of printers that work by banging a head or needle against an ink ribbon to make a mark on the paper. Dot-matrix printers, daisy-wheel printers and line printers are examples for impact printer.



Fig. 1.33 Dotmatrix printer



Fig. 1.34: Line printer

- Dot-matrix printer uses print heads containing 9 to 24 pins. Patterns of dots are produced by these pins on the paper to form the individual characters. The print quality increases with the number of pins used. Dot-matrix printers are inexpensive and typically print at speeds of 100–600 characters per second. Fig. 1.33 shows a dot matrix printer.

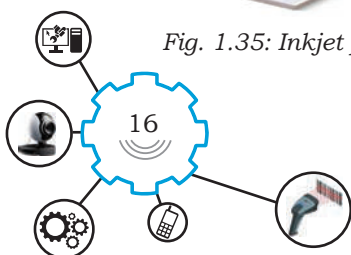
- Line printer is also called line-at-a-time printer that uses a special technology to print a line at a time. Line printers are pretty fast, they can print at the range of 1,200 to 6,000 lines per minute. Drum, chain and band printers are examples of line printers. Fig. 1.34 shows a dot line printer.

(ii) Non-impact printers form characters and images without direct physical contact between the printing mechanism and the paper. These printers do not hammer on paper and hence do not make noise and are faster. Inkjet printers and laser printers are examples of non-impact printer.

- Ink-jet printers print on paper by spraying ink from tiny nozzles through an electrical field that arranges the charged ink particles into characters at the rate of approximately 250 characters per second. A nozzle for black ink is used



Fig. 1.35: Inkjet printer



to print text, and full colour printing is possible with three extra nozzles for cyan, magenta, and yellow. It can produce a copy with a resolution of at least 300 dots per inch (dpi). Fig. 1.35 shows an inkjet printer.

- Laser printer uses a laser and electrical charge model instead of the traditional printing of ink onto paper. Laser printers can print high quality text and graphics and medium quality photographs, with a resolution of 600 dots per inch (dpi) or higher. It repeatedly passes a laser beam back and forth over a negatively charged cylinder called *drum*. The drum then selectively collects electrically charged powdered ink called toner, and transfers the image onto paper. Fig. 1.36 shows a laser printer.



Fig. 1.36: Laser printer

Secondary Storage Devices

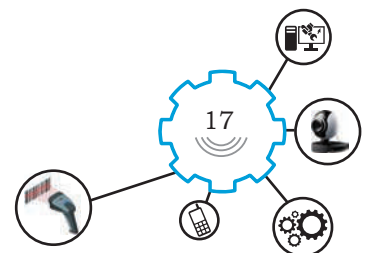
Secondary storage devices provide a way for the computer to store information on a permanent basis. It is non-volatile memory and is not directly accessed by the CPU. Secondary memory devices include flash memory, magnetic disks like drives and floppy disks, optical disks, such as CDs and CD-ROMs and portable hard disk drives.

- (a) Universal Serial Bus (USB) Flash Memory** also popularly known as a thumb drive or pen drive, is a data storage device that includes flash memory with an integrated USB interface. It is removable, re-writable and much smaller than an optical disc. It is non-volatile in nature. Fig. 1.37 shows a USB flash drive.



Fig. 1.37: USB flash memory

- (b) Optical Disks** use storage medium laser to read and write data. An optical disk can store up to 6 GB of data. There are three basic types of optical disks: CD/DVD/Blue Ray Disk (BD) ROM (read-only), write-once read-many (WORM) and



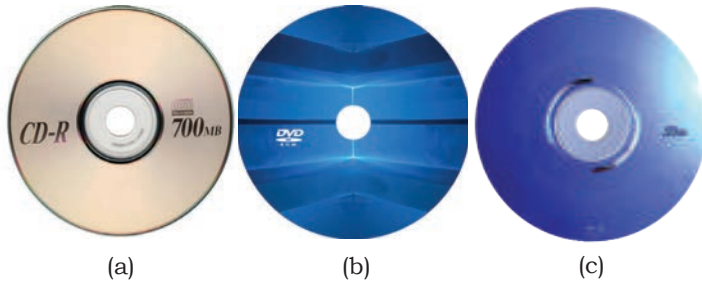


Fig. 1.38: Optical disks (a) CD (b) DVD (c) Blu-ray disc



Fig. 1.39: Hard disk drive



Fig. 1.40: Portable hard disk drive

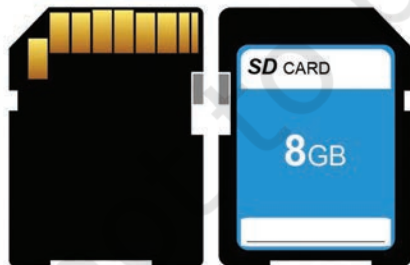


Fig. 1.41: Memory card

erasable optical (EO) disks. Blu-ray disc is the successor of DVD designed to display high definition data with large storage. Fig. 1.38 shows optical discs.

(c) Hard Disk Drive (HDD)

can be internal or external storage device. Every computer has a fixed HDD inside the system. Externally removable HDD is also available. Storage capacity of such HDD is high terabytes (TB) shown on internal and external HDD Fig. 1.39.

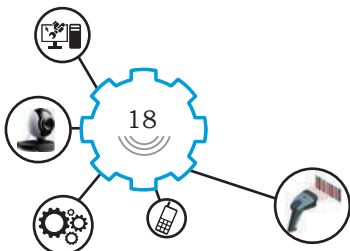
(d) Portable HDD

is a portable storage device that can be attached to a computer through a USB. External hard drives have high storage capacities and are often used to back up data or serve as a network drive. Fig. 1.40 shows a portable HDD.

(e) Memory Card

is another type of flash memory. It is very small in size of about 1×1 inch with thickness in millimeters. Memory cards can also be externally connected to the computer systems. They can also be used with cell phones and tablets. The typical storage

capacity of memory cards varies from 1 GB to 64 GB. Fig. 1.41 shows the commonly used memory cards.



Practical Activity 3

Identify the components of computer system

Material required

Writing material, pictures of processor, memory card, printer, monitor, keyboard, mouse

Procedure

1. Observe Fig. (a) consisting of the main components of a computer system.



Fig. (a)

2. Identify and name each component as shown in Fig. (b).
 - Processor and Primary Memory
 - Output Devices
 - Input Devices
 - Secondary Storage Devices

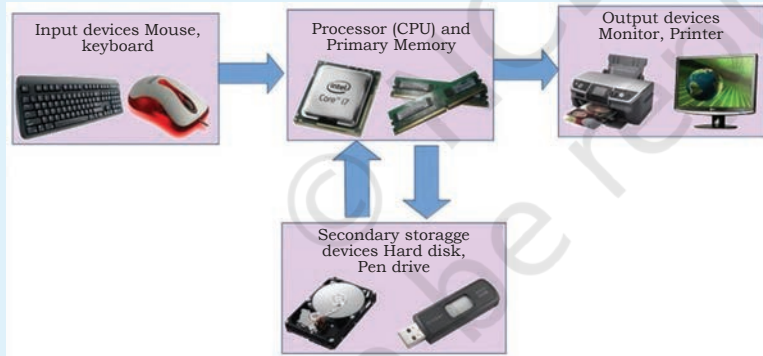


Fig. (b)

Practical Activity 4

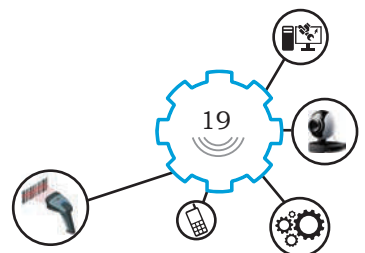
Identify and name the various storage devices

Material required

Hard Disk Drive, Pen Drive, Compact Disc

Procedure

1. Observe the given storage devices carefully, identify and record their name as per their shape and size. Record your observation as shown in the table given below.







Picture of the storage device	Name of the storage device	Storage capacity of the device
	Hard Disk Drive	1 TB
		
		
		



Fig. 1.42: Universal Serial Bus (USB) Hub

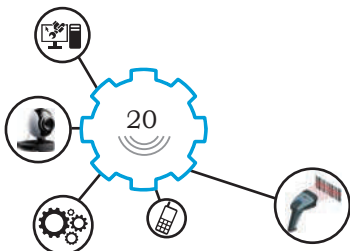


Fig. 1.43: Global Positioning System (GPS) Dongle

(f) **Universal Serial Bus (USB) Hub** is an industry standard for establishing specifications for cables, connectors and is used for connection, communication and power supply between personal computers and their peripheral devices. A computer system or laptop has limited USB ports. Therefore, USB hub is very useful if you want to connect two or more peripheral devices. Fig. 1.42 shows a USB hub.

Global Positioning System (GPS) Dongle

It is a satellite-based radio navigation system owned by the US government, and is made up of a network of 24 satellites. GPS provides information of geographical location and time to the GPS receiver anywhere on the earth or near the earth. A GPS dongle is a GPS receiver



that is used to receive GPS signals. GPS dongle is usually used with laptops, notebooks, tablets and other forms of information devices. Most of the GPS dongles are connected with the system using USB ports. Fig. 1.43 shows a GPS dongle.

Practical Activity 5

Identify and connect peripheral devices to the computer

Material required

Mouse, Keyboard, Printer, Scanner, External Hard Disk Drive, Pen Drive

Procedure

1. Take a peripheral device, such as printer and scanner.
2. Identify the corresponding socket on the CPU of a computer system.
3. Connect the device to the appropriate socket on the CPU of a computer system.
4. Ensure it is connected correctly.
5. Check whether the device is properly connected or not.

Uninterruptible Power Supply (UPS)

It is an electrical system that provides emergency power support when the main power source fails. In case of a power failure, a UPS provides near-instantaneous alternative power by supplying energy stored in its batteries. UPS systems can provide power for a few minutes sufficient enough to start a standby power source or properly shut down the machine. It is typically used to protect hardware, such as computers, data centers, where unexpected power failure can cause damage to the system. Fig. 1.44 shows a UPS.



Fig. 1.44: UPS

Practical Activity 6

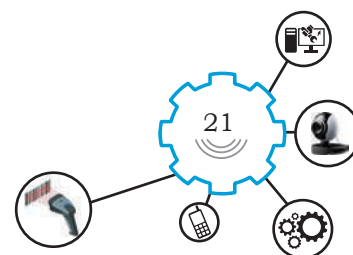
Connect the UPS shown in the adjacent figure to the mains power supply

Material required

Computer, Mains Power Supply, UPS, Battery

Procedure

1. With the help of your teacher, connect the UPS to the computer and then main power supply.
2. Switch ON the mains power supply. Observe that your computer will not go OFF. UPS works till backup exists.



Check Your Progress

A. Fill in the blanks

1. Computer is a _____ electronic machine.
2. The term computer is derived from the Latin word _____.
3. A computer can perform arithmetic and _____ operations.
4. A set of the instructions is called _____.
5. CPU stands for _____.
6. CPU consists of control unit and _____.
7. ALU stand for _____.
8. Keyboard and mouse are _____ devices of a computer system.
9. Monitor and printer are _____ devices of a computer system.
10. USB stands for _____.
11. UPS stand for _____.
12. The fastest access to the memory is _____.
13. The full form of RAM is _____.
14. The full form of ROM is _____.
15. Primary memory is memory that is accessed directly by the _____.
16. RAM is generally located on the _____.
17. Printers are mainly divided into two categories _____ and _____ printers.

B. Multiple choice questions

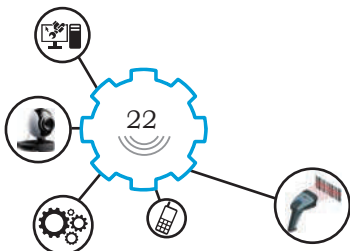
1. Which of the following is a valid type of ROM?

(a) PROM	(b) EPROM
(c) EEPROM	(d) All of these
2. Which of the following is not a type of memory?

(a) RAM	(b) FEPROM
(c) EEPROM	(d) ROM
3. Which of these is a type of memory used in computer system?

(a) PC	(b) Laptop
(c) DRAM	(d) Tablet
4. RAM in PC is used to _____.

(a) store the boot program	(b) store applications
(c) load the operating system	(d) Both (b) and (c)



5. _____ is a secondary storage device.

(a) Keyboard	(b) Mouse
(c) Pen drive	(d) Printer
6. Which of the following is the fastest memory in a computer?

(a) RAM	(b) Registers
(c) HDD	(d) ROM
7. In a _____ printer characters or letters are formed without the use of any mechanical impact.

(a) page	(b) line
(c) impact	(d) non-impact
8. The devices that are used for storing program and data for long term are called _____ device.

(a) volatile	(b) non-volatile
(c) primary memory	(d) CPU registers
9. The thickness of memory cards is given in _____.

(a) millimeter	(b) centimeter
(c) kilometer	(d) None of these
10. Hard copy of the data can be obtained by using a device called _____.

(a) keyboard	(b) mouse
(c) pen drive	(d) printer
11. Printers that make contact with paper are called _____ printers.

(a) non-impact	(b) impact
(c) global	(d) local
12. Printers that do not make any contact with the paper while printing data are called _____ printer.

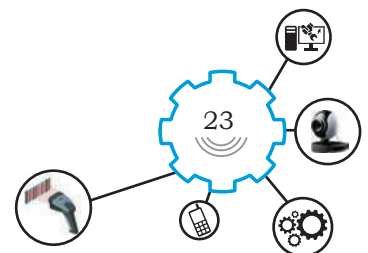
(a) non-impact	(b) impact
(c) global	(d) local
13. Dot matrix printer is a _____ type of printer.

(a) non-impact	(b) impact
(c) global	(d) local
14. Laser printer is a _____ type of printer.

(a) non-impact	(b) impact
(c) global	(d) local
15. _____ is the faster printer.

(a) Dot matrix	(b) Inkjet
(c) Laser	(d) Line
16. High quality printing can be achieved by using _____ printer.

(a) dot matrix	(b) inkjet
(c) laser	(d) line



NOTES

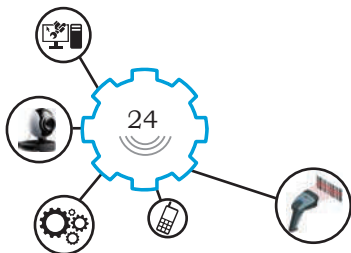
17. Which of the following printers' speed is measured in characters per second?
(a) Inkjet (b) Laser
(c) Dot matrix (d) Drum
18. Usually peripheral devices are connected to the computer system via _____ port.
(a) PCM (b) UCB
(c) USB (d) GPS
19. GPS stands for _____.
(a) Global Positioning System
(b) Global Partitioning System
(c) Google Positioning System
(d) Global Permanent System
20. To identify the geographical position and time information anywhere on the earth we use _____.
(a) GST (b) GMP
(c) GPS (d) GNU

C. State whether the following statements are True or False

1. UPS provides uninterruptible power supply.
2. Electrical generator provides uninterruptible power supply.
3. Electrical generator converts mechanical energy into electrical energy.
4. UPS needs battery for its operation.
5. Mouse and keyboard cannot be connected to the USB port.
6. Speakers of the computer systems are generally connected to the USB port.
7. Modern computer is a analog electronic device.
8. Tablet is a type of computer.
9. Memory of the computer system is measured in bytes.
10. Cache memory is slower and consumes lot of access time than main memory.
11. Cache memory is used to store application programs.
12. The instructions stored in ROM can be changed by the user.

D. Short answer questions

1. Draw the connectivity diagram of UPS and battery.
2. Explain the use of GPS in personal computer.
3. What is the use of USB port?
4. List the devices that can be connected to USB port.
5. Along with a suitable diagram explain the working of laser printer.



6. How are inkjet printers different from laser printers?
7. Explain the uses of line printer.
8. Describe the working of a dot matrix printer
9. List the different types of secondary memory storage devices that are commonly used.
10. List the uses of memory card and pen drive in different applications.
11. What do you mean by memory of a computer system?
12. What is cache memory?
13. What are the characteristics of main memory?
14. What are the major differences between RAM and ROM?

SESSION 2: DATA TYPES AND FORMATS

INTRODUCTION

Suppose you have passed your Class XII examination and you decide to continue your education. What will be the next step? You will seek admission in a college and for that you will have to fill a form as shown in Fig. 1.45.

In the admission form you will have to fill in your name, address, date of birth, telephone number, e-mail ID and attach your photograph. This information is called personal data. Similarly, when you apply for a job, you need to give your bio-data or resume to the organisation you want to work with. In this session, you will understand the different types of data and their application.

Data

The word data is taken from Latin word 'datum'. Data means facts or set of values. It can be measured, collected, reported, analysed and visualised. Data can be in different formats, such as number, text, image, audio or video as shown in Fig. 1.46.

Fig. 1.45: School admission form


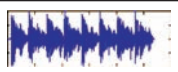

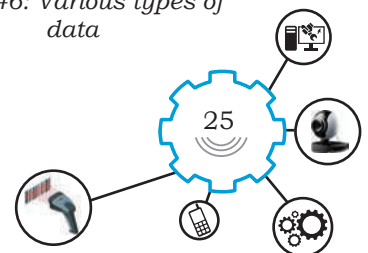
Data type	Example
Number	52354872
Text	Hello world
Image	
Audio	
Video	

Fig. 1.46: Various types of data



Practical Activity 7


Identify data types for the given data values

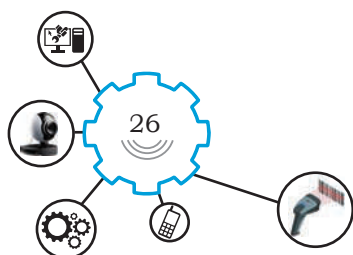
Material required

Writing material, photograph, personal details

Procedure

1. Write down your personal details, such as name, father's name, photograph and other details as given in the table below.
2. Identify the data type for each of the data value provided by you for your personal details.
3. Record the details as shown in the following table.

Personal Details		
Data Item	Data Value	Data type
Name	Ms Devanshi Ghosh	Text
Photo		Image
Father's Name	Mr Aryan Ghosh	Character with text
Mother's Name	Mrs Poorva Ghosh	Character with text
Permanent Address	House Number 215, APJ Kalam Marg, Delhi	Character with text
Present Address	House Number 115, Kasturba Nagar, Bhopal	Character with text
Date of Birth	9 December 1990	Date with number and text
Qualification	B.Sc.	Character with text
Height	158 CM	Number with text
Weight	60 kg	Number with text
Contact Number	987654321	Number



Examples of data

As can be seen in the practical activity, personal information contains different types of data. Personal data is required in every day life. For example, you require your personal data in preparation of Aadhaar card, passport and school ID.

There are two types of data. Some data elements are called individual data. For example, your personal data is individual data. The examples of personal data is shown in Fig. 1.47



Fig. 1.47 (a): Aadhaar card ID



Fig. 1.47 (b): School ID



Fig. 1.47 (c): Passport ID

(a) **Demographic Data** represents a large population. There are many examples of demographic data, such as 'Energy survey data', 'Gross domestic product and stock market data'. The examples of various demographic data are shown in Fig. 1.48 (a-d).

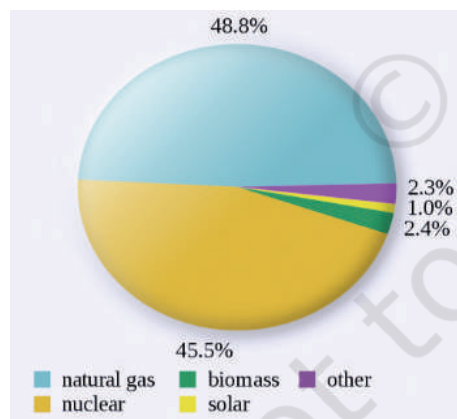
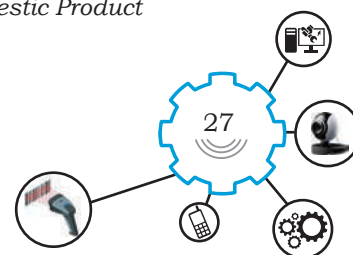


Fig. 1.48 (a): Pie chart for data of Energy Survey



Fig. 1.48 (b): Line graph of Gross Domestic Product



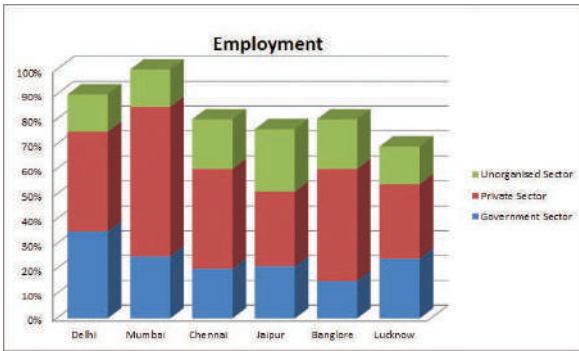
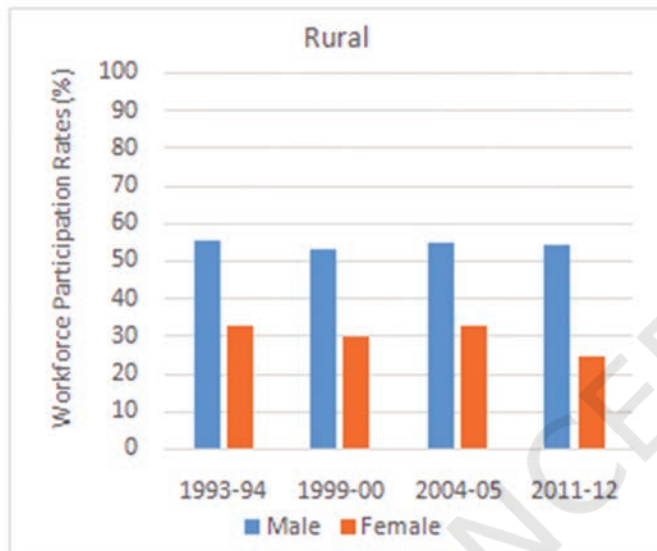


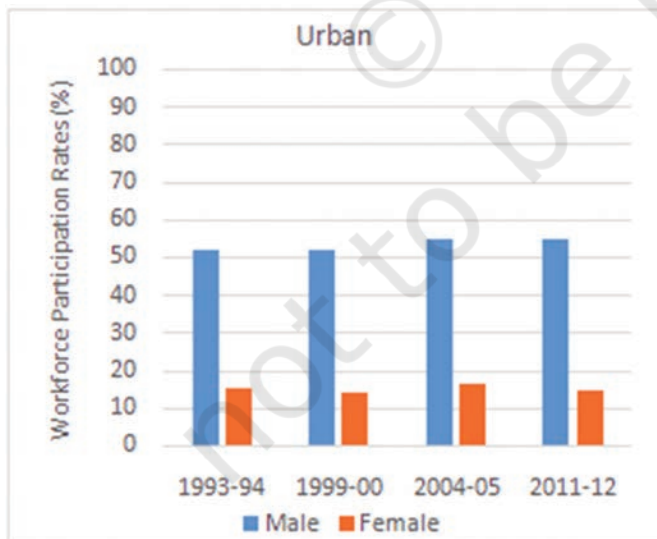
Fig. 1.48 (c): Bar graph of Gross Domestic Product



Fig. 1.48 (d): Line graph for stock market data



(a)



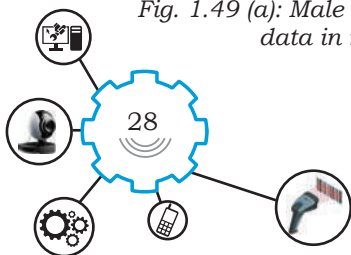
(b)

Fig. 1.49 (a): Male and female workforce demographic data in rural and (b) urban India

Observe that the data can be visualised in various formats, such as pie chart, bar graph and line graph.

Age, society, education, gender and marital status can be considered demographic features. Data associated with these demographic features is called as demographic data. It refers to the public data that normally represents certain demographic features for a large population. By using this data, we can easily understand some common features of large population. For example, India is said to be a young country because the average age of Indian population is around 30–35 years.

By collecting the gender information of population of a country, one can easily infer the percentages of males and females in that country. This information is useful for framing the common policies and taking decisions for an organisation. Figs 1.49 (a) and (b) gives the illustration of male and female workforce demographic data in rural and urban India.



From this data one can understand that the number of working females is less in urban areas and more in rural areas. Also we can infer that the number of working males is more than females both in rural as well as urban areas. Such type of useful conclusions can be easily drawn from the demographic data. These conclusions are useful for government or any organisations to make their decisions or to frame their policies.

Practical Activity 8

Identify the personal data and demographic data from the given data

Material required

Writing material, photograph, data

Procedure

1. Observe the given data carefully and then decide whether it is personal data or demographic data.
2. Write the appropriate name of the data in front of the data item.

Data item/picture	Data type (Personal/ Demographic)
Name of a person	Personal data
Photo of a person	Personal data
Population of India	Demographic data
Average age of Indians	Demographic data
Literacy rate of your state	Demographic data
Educational qualification	Personal data

Practical Activity 9

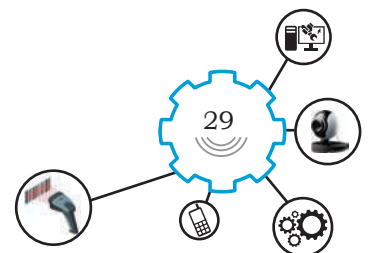
Visualise the data using bar graph, pie chart and line graph

Material required

Computer system with spreadsheet software, paper, given data

Procedure

1. Record the maximum and minimum temperature of your city for a week (see Table).



NOTES

Day	Max. Temperature in degree Celsius	Min. Temperature in degree Celsius
Sunday	41.2	29.1
Monday	40.6	29.6
Tuesday	40.8	29.5
Wednesday	41.1	30
Thursday	41.2	30.1
Friday	41	29.9
Saturday	41.3	30.3

2. Draw a line graph to visualise the data.
3. Draw a pie chart to visualise the data.
4. Enter the data in the spreadsheet and draw a bar graph to visualise the data.

Digital or Electronic Data

Computers can only work with digital information. Digital data is information stored on a computer system in binary language. It is the discrete, discontinuous representation of information or works. Digital data can be either quantitative data or qualitative data.

Qualitative data

Qualitative data is a type of data that describes information. It can be observed but is subjective and therefore difficult to use for the purpose of making comparisons.

For example, the softness of your skin, colour of eyes, face image, thumb image, fingerprint image, iris image and palm image, are all qualitative data. Observe that qualitative data cannot be expressed in the form of numbers but we use a natural language description to express it. The examples of qualitative data are shown in Fig. 1.50 (a-f).

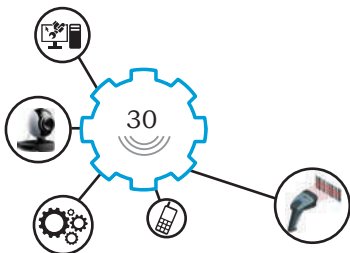




Fig. 1.50 (a): Colour of eyes



Fig. 1.50 (b): Thumb image

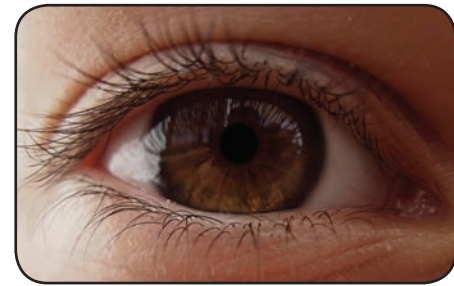


Fig. 1.50 (c): Iris image



Fig. 1.50 (d): Face image



Fig. 1.50 (e): Fingerprint image

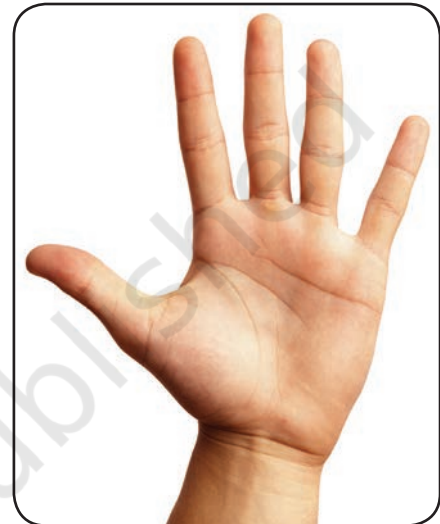


Fig. 1.50 (f): Palm image

Qualitative data can be collected by using various methods, such as group discussions, interviews or a survey. Computer machine and peripherals can also be used for collecting qualitative data. Fig. 1.51 (a – d) show the various ways to collect qualitative data.



Fig. 1.51 (a): Group discussion



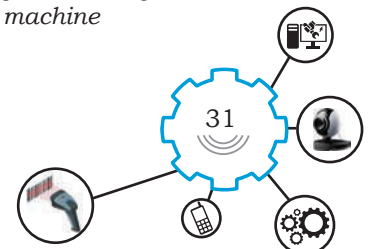
Fig. 1.51 (b): Interview



Fig. 1.51 (c): Survey



Fig. 1.51 (d): Capturing and storing data in computer machine



Applications of qualitative data

Qualitative data is used in various applications, such as scientific research, health and biomedical research, marketing research, education, entertainment, banking, energy and government sector. For example, Government of India uses qualitative data for preparation of Aadhaar card, passport and driving license.

Practical Activity 10

Capturing qualitative data using digital camera

Material required

Digital camera or mobile phone and computer system

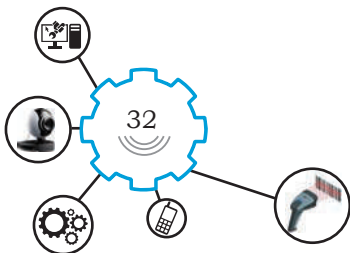
Procedure

1. Capture the face image of your classmates with a digital camera or using a mobile phone.
2. Record your voice using mobile phone.
3. Capture the video of your friend while working.
4. Transfer the picture, audio and video files from the device to computer.
5. Prepare a list of these data items in tabular form and indicate it as qualitative data.

Quantitative data

Quantitative data is data that is expressed only with numbers. It is information that can be measured and represented numerically.

Numerical data can be easily counted and analysed by using analytical method. Quantitative data is also called statistical data. Statistical analysis techniques can be applied to quantitative data. In everyday life we represent the measurement in the form of numbers. For example, height, weight, age and ID number, salary, crop yield, area and air pollution index, etc. It can be represented in the form of graphs and tables. Fig. 1.52 shows the examples of qualitative data.










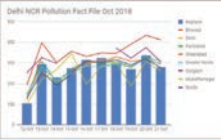
Feature	Height	Weight	Age	ID number	Salary	Crop yield	Area	Air Pollution
Value	5.6 feet	60 kg	17 years	12	₹ 35,000	1.2 tonnes	2500 sq. ft	59 micrograms per cubic metre ($\mu\text{g}/\text{m}^3$)
Related image								

Fig. 1.52: Examples of quantitative data

Quantitative data is expressed in number with specific units, which depend upon the physical quantity that is measured. For example, weight has a unit of kilogram and area is measured in square feet, etc.

Practical Activity 11

Prepare a list of quantitative data

Material required

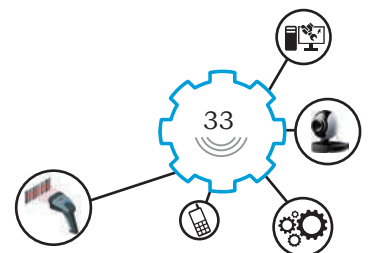
Word or Excel Software, Computer, Printer, software for word processing and spreadsheet

Procedure

1. Prepare the Employee table with various fields, such as Emp ID, Employee salary, Pincode, Bank Account Number, and Mobile Number as shown below.
2. Observe that all values in the fields are represented by numbers. Therefore, this data is a quantitative data.









Employee ID	Employee Salary	Pin Code	Bank Account Number	Mobile Number
101	70000	462011	12454784244	1236544654
102	85000	462024	12544557177	NIL
103	85000	462042	12325336868	1232125564
104	80000	465265	12345657887	1235454787
105	80000	454454	12345467878	1234546578
106	40000	454775	12345547878	1234545678

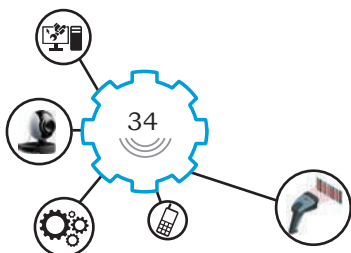
3. From such data you can easily infer following information.
 - Highest salary in the organisation is ₹ 85000/-
 - Lowest salary in the organisation is ₹ 40000/-
 - The number of employees with the same salary are two and the amount is ₹ 85000/-
 - The number of employees who have mobile phones are five.


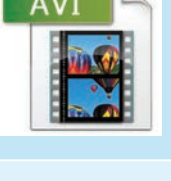


Data File Formats

The most common type of computer files for data files are document file, image file, video file and audio file. They have different file formats. Most data files are saved in binary format. The biometric data is stored in .xml file format for security reasons. The commonly used file formats are given below.

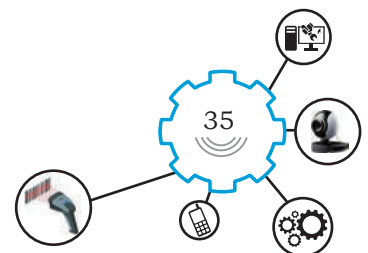
	DOC: is a word processing document created by Microsoft Word. It contains formatted text, images, tables, graphs, charts, page formatting, and print settings.
	DOCX: is created using the Open XML format Microsoft Word 2007. It also contains images, drawn objects, and other document elements.
	RTF: supports rich text. It includes several types of text formatting, such as bold type, italics, different fonts and font sizes, and custom tab settings. RTF files also support objects and images saved within the text file.
	BMP: is an uncompressed raster image with rectangular grid of pixels. It contains a file header and bitmap pixels, each with a different colour.
	JPG: is an image saved in a compressed image format standardised by the Joint Photographic Experts Group (JPEG). It is used for storing digital photos.
	PNG: is a Portable Network Graphic file. It contains a bitmap of indexed colours and uses lossless compression, similar to a .GIF file but without copyright limitations. PNG files are commonly used to store graphics for web images.
	PSD: is an image file created by Adobe Photoshop. It includes image layers, adjustment layers, layer masks, annotations, file information, keywords and other Photoshop-specific elements.
	WAV: is an audio file that uses a standard digital audio file format utilised for storing waveform data. It saves audio recordings.



	<p>TIFF: is a graphics container that stores raster images. It may contain high-quality graphics that support colour depths from 1 to 24-bit and supports both lossy and lossless compression. TIFF files also support multiple layers and pages.</p>
	<p>PDF: is commonly used for saving documents and publications in a standard format that can be viewed on multiple platforms. In many cases, PDF files are created from existing documents instead of from scratch.</p>
	<p>MID: is a Musical Instrument Digital Interface file used by music authoring and mixing programs as well as MIDI hardware devices. It contains music data.</p>
	<p>AVI: is a video file saved in the Audio Video Interleave (AVI) multimedia container format created by Microsoft. It stores video and audio data that may be encoded in a variety of codecs.</p>
	<p>HTML: is a webpage coded in HTML. It is used to format text, tables, images and other content that is displayed on a webpage. HTML files are used for static web pages.</p>
	<p>PHP: is a Hypertext Preprocessor code used for webpage. It includes PHP functions that can process online forms, get the date and time, or access information from a database.</p>

Practical Exercise

1. Open your computer system and note down different data formats that can be used to store text files or documents, image files and audio files.
2. Note down different database file formats used on your computer system.



Check Your Progress

A. Fill in the blanks

1. The word data is taken from the Latin word _____.
2. In 1946 the term _____ was used first time with transmittable and storable computer information.
3. Alphanumeric data contains _____.
4. The data representing a large population is called _____ data.
5. The individual data is called _____ data.
6. Age, society, education, gender are considered as features of _____ data.
7. Government decisions or policies are mostly based upon _____ data.
8. The data captured by the electronic devices is called _____.
9. OTP stands for _____.
10. BHIM stands for _____.
11. The data that can only be described by using words and description is called _____ data.
12. Group discussion, interviews and surveys are used to collect _____ data.
13. The data that is expressed by numbers only is called as _____ data.

B. Multiple choice questions

1. Data may be _____.

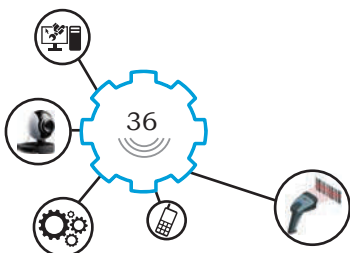
(a) numbers	(b) text
(c) alphanumeric	(d) All of these
2. Quantitative data is expressed in _____.

(a) only numbers	(b) only text
(c) only alphanumeric	(d) Both (a) and (b)
3. Pie chart is used for _____.

(a) data interpretation	(b) designing
(c) showing text	(d) hiding data
4. OTP in credit card transaction is _____.

(a) Odd Transaction Password
(b) Owner Trading Passcode
(c) One Time Password
(d) One Time Pincode
5. Why is one time password safe?

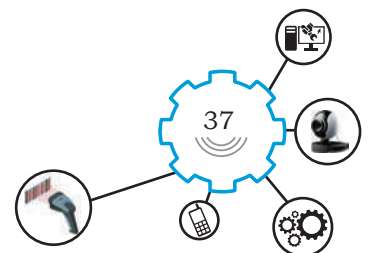
(a) It is easy to generate.
(b) It cannot be shared.
(c) It is different for every access.
(d) It is a complex encrypted password.



6. Electronic data is _____.
(a) digital form of data (b) hard copy of data
(c) only used for shopping (d) only used by apps
7. Height and weight of a person are examples of _____ data.
(a) qualitative (b) quantitative
(c) random (d) global
8. Face image and thumb image are examples of _____ data.
(a) qualitative (b) quantitative
(c) random (d) global
9. .DOC format is used with _____.
(a) text file (b) image file
(c) voice file (d) database file
10. .JPG format is used with _____.
(a) text file (b) image file
(c) voice file (d) database file
11. .MP3 format is used with _____.
(a) text file (b) image file
(c) video file (d) database file
12. .SQL format is used with _____.
(a) text file (b) image file
(c) video file (d) database file
13. Statistical data is also called _____ data.
(a) qualitative (b) quantitative
(c) random (d) global
14. All physical quantity data is _____.
(a) qualitative (b) quantitative
(c) random (d) global
15. Stock market data is an example of _____.
(a) demographic data (b) demographic data
(c) random (d) global

C. State whether the following statements are True and False

1. Data means facts or set of values.
2. Useful knowledge about data can be obtained without processing it.
3. Data cannot be measured and analysed.
4. Data can be visualised.
5. Quantitative and qualitative are the two types of data.
6. Demographic data is personal data.
7. Energy survey data and stock market data are the examples of demographic data.



NOTES

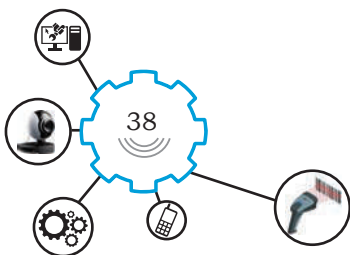
8. Pie chart, bar graphs and line graph can be used to visualise data.
9. Useful conclusions cannot be drawn by using demographic data.
10. Data generated by electronic devices, such as mobile phone is called analog data.
11. The colour of skin and colour of eyes is qualitative data.
12. The crop yield and air pollution is the quantitative type of data.
13. .txt format is used for image file.
14. .wav format is used for voice file.
15. .mdb format is used for image file.
16. .gif format is used for image file.

D. Short answer questions

1. Explain the different types of text file formats using suitable examples.
2. What is data file format? Explain the format used for video files.
3. Along with suitable examples explain the different image file formats.
4. What are the different types of data? .
5. How is data processed?

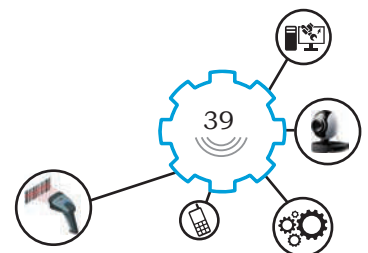
SESSION 3: BIOMETRIC DATA

You must have noticed that there are a large number of students in your school and all of them look different from each other. If you minutely observe, the fingerprint or the signature of each student is different from the other. When you use the fingerprint detection on your smartphone rather than providing a four-digit security code, you are using biometrics. Simply placing a finger over the start button is all that is needed to register you as the user. Many laptops and tablets now give you the choice of using fingerprint or facial recognition to gain access to the system. This is a quick and efficient way to log in without the need to remember a password. This is called biometric data. In this session, you will understand different types of biometric data, such as fingerprint, palm and face data, its importance, qualities and types.



Some important definitions associated with biometric are as follows—

- **Biometrics:** is used to describe a characteristic or a process in biometric identification systems. It is measurable, physiological and behavioural characteristic that can be used for automated recognition.
- **Biometric Data:** the word biometric is derived from the Latin words 'bio' and 'metric'. Greek or Latin Greek word bio means life and metric means the standard of measurement. Biometric data is used to describe the information collected during enrolment, verification, or identification process, but does not apply to end user information, such as user name, demographic information and authorisations.
- **Biometric Technologies:** is the technology of detecting and recognising human characteristics. This is done by measuring and analysing biological data using various electronic technologies
- **Biometric Verification:** refers to a specific task in which the system tries to confirm an individual's claimed identity by means of comparing a submitted biometric sample to a database of templates.
- **Enrolment:** is the act of creating a record in a biometric system. The enrolment phase goes from biometric sample acquisition and storage to biometric feature extraction, up to the creation of the biometric reference to be stored for subsequent comparisons.
- **Biometric Capture:** is the process of collecting a biometric sample from an individual via a sensor.
- **Live Biometric Capture:** is the biometric data capture device, which captures the data immediately in a digital format and makes it ready for comparison to a database. For example, a fingerprint capture device that electronically captures fingerprint images using a sensor, iris or retinal scanner and immediately



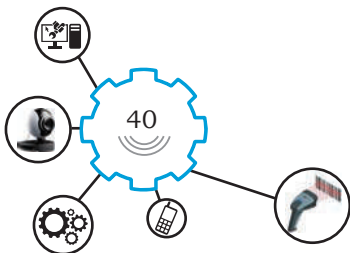
NOTES

provides appropriate information for database comparison or digital image of face.

- **Biometric Identification:** is the process of searching a database, by way of biometric comparison, against one or more biometric templates corresponding to the acquired data. It is one-to-many comparison and does not envisage a biometric claim.
- **Biometric Sample:** is the analog or digital representation obtained from a biometric sensor device. For example, images of a face or fingerprint.
- **Biometric Feature:** is the information extracted from a biometric sample and used for comparison;
- **Biometric Feature Extraction:** is the process by which key features of the sample are selected particular frequencies and patterns. A digital picture may pull out particular measurements, like the relative positions of the ears, forehead, cheekbones and nose. Iris prints will encode the mapping of furrows and striations in the iris.
- **Biometric Comparison:** is the comparison of biometric data to determine their similarities or dissimilarities, usually based on statistical methods and metrics that are typical of the selected technological environment and biometric system.

Biometric system consists of various components like sensors, matching algorithm and result display, that combine to make an operational biometric system. A biometric system is an automated system capable of

1. capturing a biometric sample from an end user,
2. extracting and processing the biometric data from that sample,
3. storing the extracted information in a database,
4. comparing the biometric data with data contained in one or more references and



5. deciding how well they match and indicating whether or not an identification or verification of identity has been achieved.

Biometric data represent certain biometric characteristics of a person. It can be physical or behavioural characteristics, which can be used for recognition of a person. The characteristics, such as face, iris, retina, finger, thumb are biometric data elements of a person. The behavioural characteristics, such as signature, way of walking, voice are also biometric data elements of a person. Fig. 1.53 illustrates various biometric data elements of a person.

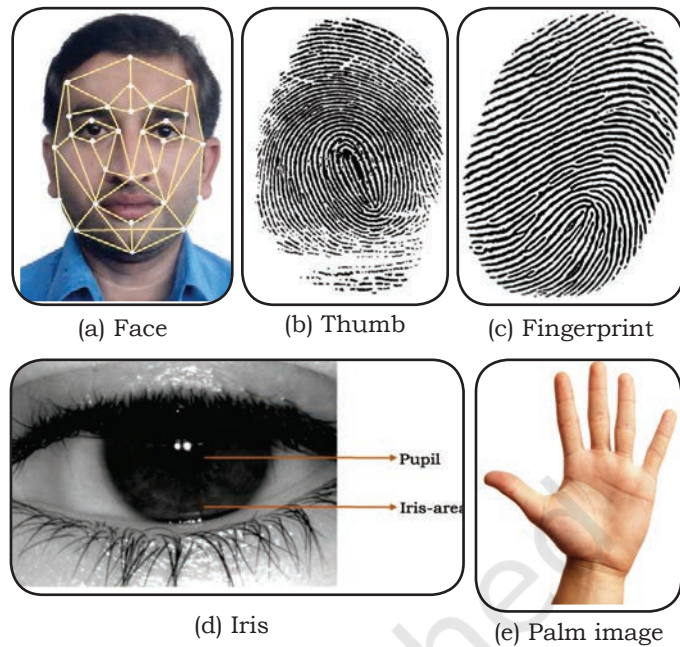


Fig 1.53 (a–e): Various biometric data elements

Types of Biometrics

Biometrics are based on the measurement of distinctive physiological or behavioural characteristics. Fingerprint, face, iris, hand and retina are considered physical, or physiological, biometrics, as they are based on direct measurements from parts of the human body. Physical biometrics directly measures characteristics of the human body. On the other hand, voice recognition, gait and signatures are considered behavioural biometrics, as they are based on measurements and data derived from an action and human body composition, such as the shape of the vocal cords in a voice scan, or the agility of hands and fingers in signature recognition. Therefore, behavioural biometrics measures these human body characteristics indirectly. These physiological and behavioural classifications are a useful way to view the different types of biometric technology traits. Fig. 1.55 shows types of biometrics.

Physiological biometric data

- (a) **Fingerprints:** are used for personal identification of human. The high accuracy of fingerprints helps to identify an individual in biometric

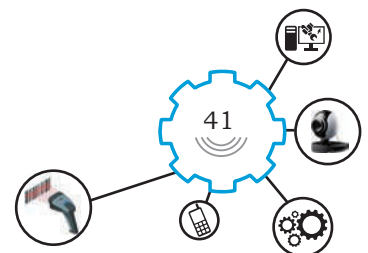




Fig. 1.54: Sample fingerprint images

applications. The curves or ridges on the skin of our fingertips form a unique pattern and this pattern is called fingerprint. A fingerprint pattern is recognised as a series of dark lines that represent the ridges or high areas of the skin, and white space or low areas, which are the valleys. Some sample fingerprint images are shown in Fig. 1.54.

Every fingerprint contains a core part, bifurcation, cross over, ridge ending, island, delta and pore as shown in Fig. 1.55. The pattern formed by the ridges on the fingertips is called minutiae.

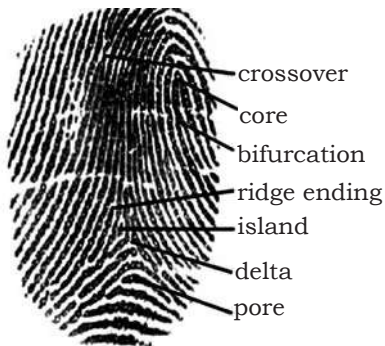


Fig. 1.55: Parts of fingerprint

The fingerprint of the individual person is unique. It can be easily collected and measured or compared. Therefore, the fingerprint biometric data is used widely and about 65 per cent biometric system makes use of fingerprint data. Most of the time the fingerprint of thumb or first finger is used for the purpose of identification.

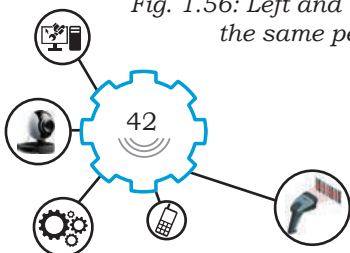
Fingerprint identification is a cheap, fast, convenient and reliable way to identify someone and is one of the most known and widely accepted biometric modalities available. There are several sensor types for collecting fingerprint images including optical, capacitive, ultrasound, and thermal. Fingerprint recognition may be unsuitable for a small percentage of the population because of genetic, environmental, and even occupational factors

(b) Hand Geometry: the human hand includes bones, muscles and joints, to make up our five fingers, the palm and the wrist. The anatomy of the human hand shape depends upon geometry of hand, length, width of fingers and the span of the hand in different dimensions. The left and right hands of an individual have similar geometric features as shown in Fig. 1.56. Fingerprints or iris show distinct differences between left and right.



Fig. 1.56: Left and right hand of the same person

Hand geometry systems achieve high performance in accuracy and also have a very



high user acceptance rate. This system also combines several physiological and behavioural features, which not only include the shape and length of the hand but also in the way that the person offers their hand to the sensor for scanning. Hand geometry scanners measure the width, length and thickness of the palm and fingers as shown in Fig. 1.57. The technology uses a digital camera to record the hand's three-dimensional image and ignores any lines, scars and dirt that may be present.

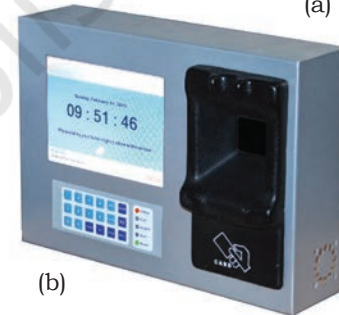


Fig. 1.57: Hand geometry scanner

(c) **Palm:** the complete left-hand fingerprint except the thumb can be captured simultaneously and it is called palm biometric data. In the same way all the fingers of the right hand except the thumb can be scanned simultaneously. This scanning is useful for the purpose of identification instead of a single fingerprint. Palm print information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis or top layer of the skin. A palm print, therefore, illustrates the physical properties of skin patterns, such as lines, points, minutiae, and texture and has the capability to uniquely identify a person among many others. Palm scanner is used to capture the palm biometric data (Fig. 1.58).



(a)



(b)

Fig. 1.58 (a): Palm (b) Palm scanner

(d) **Vein:** it can be identified in the same way as fingerprint and palm print by ridges and valleys. The pattern of veins is unique to every individual, even among identical twins. The veins are the internal structure responsible for carrying blood from one body part to the other. Veins are present in the fingers, palm and back of the hand surface as shown in Fig. 1.59. Vein biometric systems are used to record the vein patterns under the skin using infrared scanners to produce a distinctive feature set.



Fig. 1.59: Vein biometrics

(e) **Face:** every individual's face has different characteristics than others. The size and shape of every individual's face is different. Also the shape of the nose, the distance between eyes

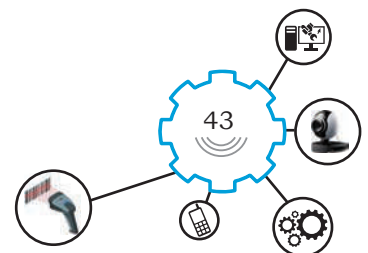




Fig. 1.60: Face images

is different for every individual. The skin of the face and its colour can also be an important parameter in face biometric data. A typical image of the face is shown in Fig. 1.60.

Faces are unique. They can be easily captured by using ordinary cameras. The face measurement can be easily done by using the available face recognition algorithms. About 11% of biometric systems make use of face biometric data for the purpose of identification.



Fig. 1.61: Human eye

- (f) **Retina:** is a typical image of the eye is shown in Fig. 1.61. A human eye can be used for the purpose of recognition. Every eye has unique features, such as retina, iris and blood vessel pattern.

Retina is a thin tissue at the back of the eye that has a pattern capillaries and this pattern is unique. No two persons in the world can have the same retina pattern. Also the retina pattern remains unchanged from birth to death.

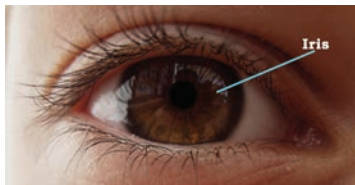


Fig. 1.62: Iris

- (g) **Iris:** is actually an internal part of eye that controls the inflow of light to the eye. Every iris has a unique pattern and it has different features, such as corona, crypts, filaments, freckles, furrows, striations and rings. All these different features of iris form a unique pattern

for every individual person. A typical image or photo of an iris is shown in Fig. 1.62. Iris comparison can give us high accuracy for recognition of a person. It is a very fast technology where without informing the person recognition can be done. This technique is used in almost 5 per cent of biometric recognition systems.

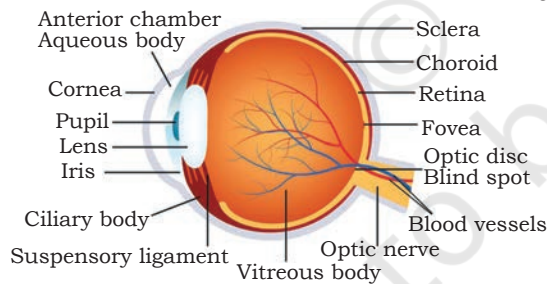
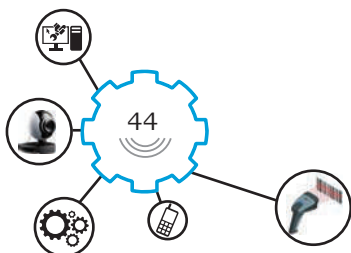


Fig. 1.63: Anatomy of retina

Behavioural biometric data

- (a) **Signature:** is the shape and writing style of signature of every individual person is different from the other. Therefore, signatures can be used for the purpose of authentication. The shapes of different signatures are shown in Fig. 1.63. Parameters associated with signature



are x and y values, pressure, speed, acceleration and delta pressure.

Signature verification can be done either offline or online. In offline method the images are matched and in online method the movement of the pen or motion is matched. Signature authentication is commonly used for most of the financial transactions, such as the bank transactions.



Fig. 1.64: Signatures of different persons

- (b) **Voice:** every individual's voice is different from the other person with respect to the various parameters associated with the voice. The parameters associated with the voice are—pitch, tone, cadence and frequency of voice. Fig. 1.65 shows a typical image of a person's audio and its different parameters. Measurement of these parameters can be performed by using a voice recognition system and this system is practically used in about 5 per cent biometric data recognition systems.

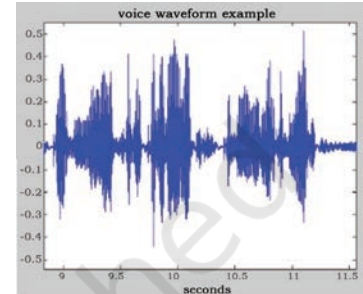


Fig. 1.65: Voice pattern

- (c) **Way of Walking:** even though every person has two legs, the walking pattern of every individual is different from the other. By recording this walking pattern, we can easily recognise a person. Such recognition is called gait recognition. This recognition is useful in the sense that it can be done at a distance. A typical walking pattern of a person is shown in the following Fig. 1.66. By measuring various distances, we can determine working pattern of a person.

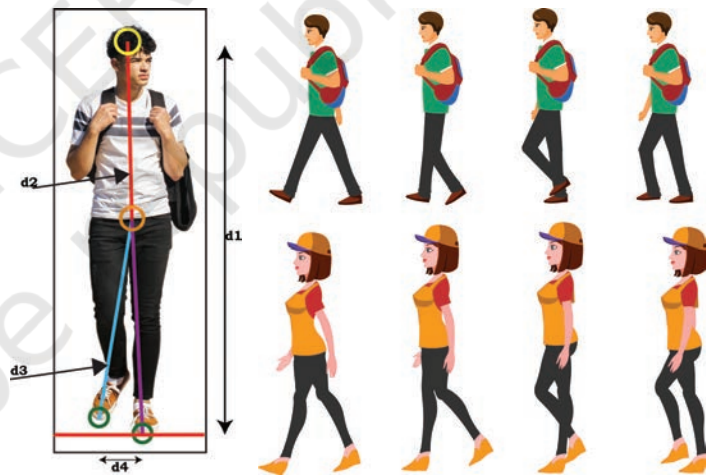


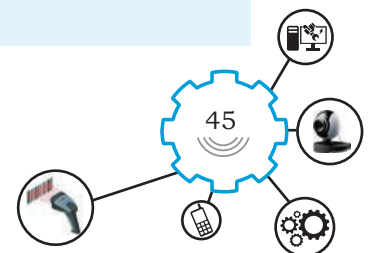
Fig. 1.66: Walking pattern

Practical Activity 12

Identify the parameters of fingerprint biometric data.






Material required

Inkpad, Fingerprint scanner, Paper, Pen, Pencil



Procedure

1. Collect the biometric data of fingerprint of five students of a class.
2. Do this by using an inkpad or by using fingerprint scanner.
3. Plot the parameters of the fingerprint in a tabular form as shown below.

S.No.	Student name	Fingerprint photo	Parameters				
			Core	Position of core	Position of crossover	Position of bifurcation	Position of ridge ending
1.	Aviral		Yes	Centre area	Top left area	Top right area	Top left area
2.	Hriday		Yes	Centre area	Top right area	Centre right area	Centre right area
3.	Peehu		Yes	Centre area	Top right area	Bottom right area	Bottom right area
4.	Suman		Yes	Bottom area	Bottom right area	Bottom right area	Centre area
5.	Kartik		Yes	Centre area	Top right area	Bottom left area	Top centre area

Practical Activity 13



Identify the parameters of face print biometric data.

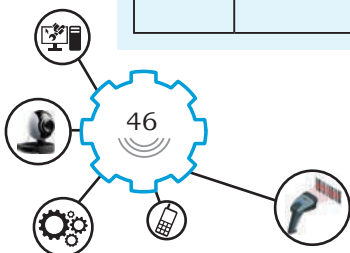
Material required

Camera, Computer, Paper, Pen, Pencil

Procedure

1. Collect the biometric data of face images of five students of a class.
2. Take the photographs of face images using digital camera.
3. Observe these photographs on your computer screen and identify the difference between the face images.
4. Plot the parameters of the face images in a tabular form as shown below.

S.No.	Student name	Face images	Shpae of the face mage	Colour of skin	Colour of hair	Shape of ears
1.	Aviral		Diamond	Fair	Black	Pointed ear
2.	Hriday		Oval	Fair	Black	Round ear



3.	Peehu		Square	Wheatish	Black	Attached lobe
4.	Suman		Heart	Wheatish	Black	Narrow ear
5.	Kartik		Oblong	Dark	Black	Round ear

Practical Activity 14






Identify the parameters of iris biometric data.

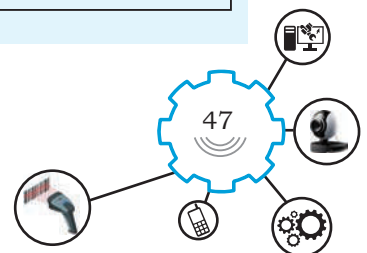
Material required

Iris scanner, Computer, Writing Material

Procedure

1. Collect the biometric data of iris images of 5 students in the class.
2. Take the photographs of iris images using iris camera.
3. Observe these iris images on your computer screen and identify the difference between the iris images.
4. Plot the parameters of the eye images in tabular form as shown below.

S.No.	Student Name	Eye images	Shape of the eye	Colour of eye
1.	Aviral		Almond	Black
2.	Hriday		Almond	Black
3.	Peehu		Almond	Blue
4.	Suman		Thin Almond	Brown
5.	Kartik		Round	Black



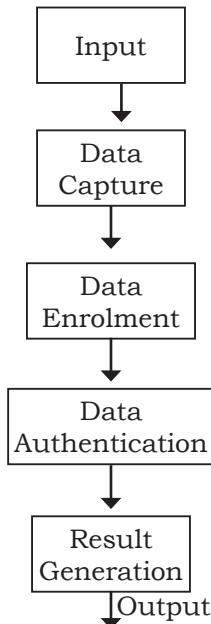


Fig. 1.67: Biometric authentication or recognition system

Biometric System

Biometric system can be used as an identification system or authentication system. Biometric systems are designed to perform following general operations as shown in Fig. 1.67.

- Data capture
- Data enrolment
- Data authentication
- Data matching and result generation

Input biometric data, such as face, fingerprint, iris is captured by an appropriate sensor, such as camera, finger scanner or eye scanner. This captured data is analysed and its unique features are extracted. These features are stored in appropriate file.

When the enrolled user wants to authenticate then its biometric data is again captured and it is compared with the data that is already stored. Finally an algorithm is used to see if there is any match between the stored data and the user data. If appropriate match is found then the system recognises the user or it denies the user.

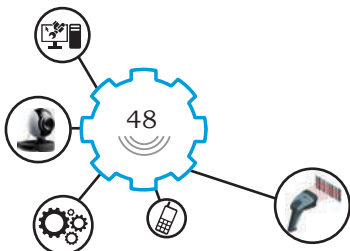
Qualities of Biometric Data

Quality of the biometric data refers to a clear and error free data capture of biometric data. Broadly, a sample should be of good quality if it is to be suitable for automated matching. This viewpoint may be distinct from the human conception of quality. If, for example, an observer sees a fingerprint with clear ridges, low noise and good contrast, then he might reasonably say it is of good quality. However, if the image contains few minutiae, then a minutiae-based matcher would under perform. Likewise, a face recognition algorithm will suffer from blurring of the image.

Quality measurement plays a vital role in improving biometric system's accuracy and efficiency. Neglecting quality measurement will adversely impact accuracy and efficiency of biometric recognition systems.

Limitations of Biometric Data

Biometric data recognition system suffers from many limitations. Some of the limitations are mentioned below.



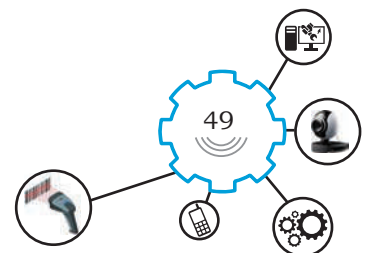
- Change in the face due to increase in the ages.
- Collection of biometric data requires the physical contacts.
- Ridges on the fingers get erased over a period of time.
- Blur face images cannot provide accurate face matching.
- Variation in lighting conditions creates problems during matching of the faces.
- Accidental damage to the eyes can create problem in iris for eye recognition.
- The variation in the signature over a period of time.
- Medical problems or accidental injuries can create problems for behavioural biometric data.
- Biometric system requires computer hardware and software. Both hardware and software need to be maintained over a period of time.
- Biometric system is an online system of which the data must be secured by using appropriate security procedures

Domestic and Global Data

In biometric systems the input data stored is local data, i.e. the biometric data, such as face image, fingerprint image or signature is of the people who are associated with an organisation. Such data can also be called domestic data. For the processing of such domestic data we can use global data for matching purposes.

For example in India, Aadhaar cards are prepared for all citizens. Every citizen gets a unique Aadhaar number. When this person wants to open a bank account, their data is cross verified with the concerned Aadhaar data. In this scenario the Aadhaar data stored on the government server works as global data and data entered by the concerned bank to open an account becomes local data. This process can save time as authentication is done at a higher speed.

A similar process is used by the income tax department and for issuing visas. On the international



NOTES

airports, the authenticity is being verified by cross matching the local and global data of the person. This process ensures proper authentication and saves time and money.

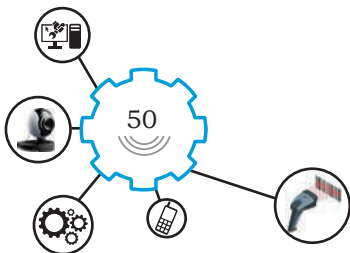
Practical Exercise

1. Collect the face images and fingerprint images of 10 students of your class. List the uniqueness in each individual's face and fingerprint.
2. Collect the palm images of 5 different students of your class. Observe and list the difference in palm images.
3. Collect the signature of 5 different students of your class. Observe the difference in signing.
4. Observe the walking style of 5 different students in a class and list the features and differences in their walking pattern.
5. Check the difference between your fingerprints and your classmate's. To perform this activity you need to have inkpad, a white paper and cloth for cleaning ink from finger and a magnifying glass

Check Your Progress

A. Fill in the blanks

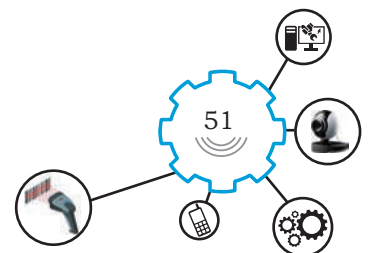
1. The word biometric is derived from the Latin word _____ and _____.
2. Greek word bio means _____ and metric means _____.
3. Biometric is used to identify _____ and _____ characteristics of a person
4. Authentication of a person can be performed by using _____ data.
5. Iris is actually an internal part of the _____ that controls the inflow of light to the eye.
6. The _____ style of signature of every individual person is different from the other.
7. Biometric system can be used as a (an) _____ system.
8. Quality of the biometric data refers to a clear and _____ free data capture of biometric data
9. Changes in the human face occurs due to an increase in the _____.
10. Every citizen gets a/an _____ Aadhaar number.
11. Signature and way of walking are _____ characteristics of a person.
12. Fingerprint and face image are _____ characteristics of a person.



13. Core, crossover and island are the parts of _____ image.
14. Fingerprint of every individual person is _____.
15. About 65 per cent of biometric systems make use of _____ data.
16. In palm biometric image we can observe _____ on the palm.

B. Multiple choice questions

1. Which of the following methods is the best form of authentication?
 - (a) Biometrics
 - (b) Multiple factor
 - (c) Password-based
 - (d) Token-based
2. Hand geometry identification can be performed by using _____.
 - (a) fingerprint image
 - (b) palm image
 - (c) iris image
 - (d) face image
3. Corona, crypts and rings are the different features of _____.
 - (a) fingerprint image
 - (b) palm image
 - (c) iris image
 - (d) face image
4. Face of the human can be used as _____ data.
 - (a) demographic
 - (b) biometric
 - (c) local
 - (d) global
5. Voice of a person is _____ data.
 - (a) physiological
 - (b) non-physiological
 - (c) behavioural
 - (d) non-behavioural
6. Pitch, tone and frequency are features of _____ data.
 - (a) signature
 - (b) iris
 - (c) retina
 - (d) voice
7. Pressure, speed and acceleration are features of _____ data.
8. Skin colour, shape and size are features of _____ data.
 - (a) signature
 - (b) face
 - (c) retina
 - (d) voice
9. About 11 per cent of biometric systems make use of _____ data for the purpose of identification.
 - (a) signature
 - (b) face
 - (c) retina
 - (d) voice
10. Gait recognition means _____.
 - (a) walking pattern recognition
 - (b) face recognition
 - (c) iris recognition
 - (d) fingerprint recognition
11. Which of the following are the elements of biometric recognition system?
 - (a) Data capture
 - (b) Data Enrolment
 - (c) Data authentication
 - (d) All of these



NOTES

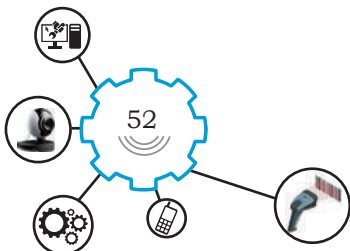
12. Which of the following is the limitation of biometric data?
(a) Biometric data cannot be captured
(b) Biometric data cannot be enrolled
(c) Collection of biometric data requires physical contact
(d) Data authentication is difficult
13. The biometric data of people associated with an organisation is called _____.
(a) domestic data (b) global data
(c) material data (d) None of these
14. The data stored on the Aadhaar server that is used for matching purposes is called _____.
(a) domestic data (b) global data
(c) material data (d) None of these

C. State whether the following statements are True or False

1. Domestic data is a global data.
2. Biometric system is an offline system.
3. Biometric system do not require any hardware and software.
4. Medical problems or accident injuries can create problem for behavioural data.
5. Quality of biometric data refers to clear and error free data.
6. Collection of biometric data does not require physical contact.
7. Face images get changed due to increase in age.
8. Data authentication is performed by using hardware.
9. Data capture is performed by using software only.
10. Voice of every individual person is different from the other person.

D. Short answer questions

1. Define the term biometric data.
2. Define demographics data.
3. What are the characteristics of successful biometric identification methods?
4. What are the qualities of biometric data?
5. State the types of biometric data.
6. Explain the different parts of a fingerprint.
7. Explain the different parts of a palm image.
8. What are the different features associated with the face of a person?
9. State the features of human eye.
10. Draw the diagram of iris and state its different parts.



11. State the features associated with the signature of a person.
12. List the voice features of a person.
13. What is gait recognition?
14. Differentiate between domestic and global data.

SESSION 4: COLLECT AND DIGITISE DATA

Whenever you wish to appear for any board examination, the board asks you to fill the examination form. Through the examination form the board collects the information of students appearing for the examination. This refers to collection of data. Nowadays most of the examination forms are available on the website and one needs to fill these forms by using computer system. This refers to the digital form of data. In this session, you will understand the importance of data collection, advantages and applications of data collection in real life. You will also know the difference between handwritten data and digital data. The process of digitisation has also been discussed in this session.

Data Collection

It is the process of gathering and measuring data for information. Data collection is an integral, usually initial, component of any public activity, such as conduction of examination, admission process in school and colleges, opening of bank accounts in a bank, applying for a post in an organisation, getting loan from a bank and enrolling for hospital treatment. Data collection is also used in commercial activities, such as selling of a product, launching of a new product, launching building projects and popularisation of the product. Data collection is also used by the government in various activities, such as framing of new policy, giving authorisation to the different agencies. Data collection is used in the preparation of Aadhaar card and in the preparation

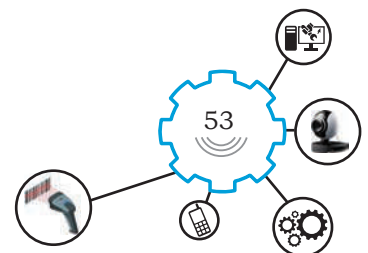




Fig. 1.68: Data collection activity

of passport as well. So we observe that almost in all phases of real life the data is being collected by the various agencies. In the recent years we observe that the data collection plays a vital role in succeeding the businesses. Data collection is also used in the research of all branches, such as social sciences, humanities and physical sciences. Data can be collected by surveys.

Importance of data collection

Data collection means the accurate acquisition of data. Although methods of data collection may differ depending on the field, the emphasis on ensuring accuracy remains the same. Normally the data is collected to get answers for the questions that have been raised within an organisation. For example, a examination board will collect the student information so that they know how many students are appearing for or taking examinations. Depending upon the number of students the board needs to make the arrangements for the examination. A company or business will collect the data to measure the popularity of their product or service. Also, whenever the company decides to launch a new product the requirement of such a new product is measured through the data collection. The deficiencies or limitations of existing services can be overcome only through collection of data.

A college or school collects feedback forms from the students to know the quality of teaching offered by the teachers in the college or school. Also the requirement of infrastructural facilities can be understood through the data collection. So data collection plays a vital role in getting answers to the problems faced by the organisation. The improvement or expansion of the services is possible only through data collection. Fig. 1.69 shows a sample form used for collecting feedback from the students.

Your feedback

We would like your feedback to improve our website.

What is your opinion of this page?

☹️ 😐 😊 😄 😁

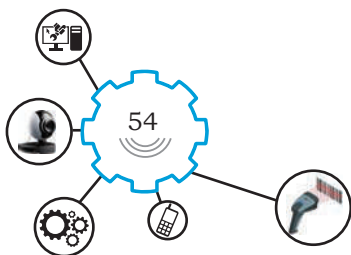
Please select your feedback category below.

Suggestion **Something is not quite right** Compliment

Please leave your feedback below:

Send

Fig. 1.69: Feedback form for data collection



Advantages of data collection

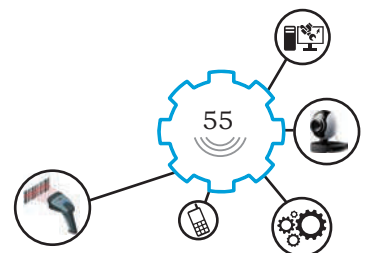
The advantages of data collection are as given below.

- Answers to the questions faced by the organisation can be obtained through data collection.
- Improvement in the existing services or products can be achieved through data collection.
- Extension of existing services is possible through data collection.
- Successful launching of new products or services is achieved through the data collection of such requirement.
- General understanding of the people about the concept or about the government can be obtained through data collection.
- Financial status of the people living in a certain area or country can be understood through data collection.
- Number of migrants in a country can be obtained through data collection.
- Number of users of products or services and their satisfaction level can be measured through data collection.
- Testing of new platforms can be achieved through data collection. The collected data when processed can help draw useful conclusion.

Application of data collection in real life

In real life, almost at every stage data is collected. For example, data is collected in hospitals to offer treatment and the data is collected by the school or colleges for getting admission. The bank also collects the user data for opening a bank account. Government collects the data of citizen to issue the Aadhaar card and passport. Organisations collect the data of their employees.

Some of the real-life applications of data collection are demonstrated in Practical Activity 16.



Practical Activity 15

Data collection process in preparation of Aadhaar card.

Material required

Aadhaar card application form, documents, photograph, pen

Procedure

1. While preparing the Aadhaar card, we know that our data is collected by the Aadhaar card service provider.
2. Aadhaar card cannot be issued to any person without collection of their data.
3. We need to fill the Aadhaar card application form as shown below.



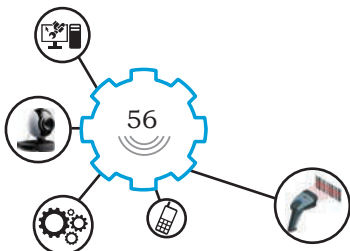
AADHAAR ENROLMENT / CORRECTION FORM

Aadhaar Enrolment is free and voluntary. Correction within 96 hours of enrolment is also free. No charges are applicable for Form and Aadhaar Enrolment. In case of Correction provide your EID, Name and only that field which needs Correction.
In case of Correction provide your EID No here: | dd | mm | yyyy | hh | mm | ss |

Please follow the instructions overleaf while filling up the form. Use capital letters only.

1	Pre-Enrolment ID :	2	NPR Receipt/TIN Number :
3	Full Name:		
4	Gender: Male () Female () Transgender ()	5	Age: Yrs or Date of Birth: DD MM YYYY Declared <input type="checkbox"/> Verified <input type="checkbox"/>
6	Address: C/o () D/o () S/o () W/o () H/o () NAME		
	House No/ Bldg./Apt.	Street/Road/Lane	
	Landmark	Area/locality/sector	
	Village/Town/City	Post Office	
	District	Sub-District	State
	E Mail	Mobile No	PIN CODE
7	Details of: Father () Mother () Guardian () Husband () Wife () <small>For children below 5 years Father/Mother/Guardian's details are mandatory. Adults can opt to not specify this information, if they cannot/do not want to disclose.</small>		
	Name		
	EID/ Aadhaar No.: dd mm yyyy hh mm ss		
8	I have no objection to the UIDAI sharing information provided by me to the UIDAI with agencies engaged in delivery of welfare services.		YES () NO ()
9	Select One of the Below (OPTIONAL) (This data cannot be Corrected after Enrolment)		
	<input type="checkbox"/> I want the UIDAI to facilitate opening of a new Bank/Post Office Account linked to my Aadhaar Number and have no objection to sharing my information for this purpose		
	<input type="checkbox"/> I have no objection to linking my present bank account provided here to my Aadhaar number		
	State	Bank Name/Branch	Account No.
	IFSC Code		
	Verification Type : Document Based () Introducer Based () Head of Family () Select only one of the above. Select Introducer or Head of Family only if you do not possess any documentary proof of identity and/or address. Introducer and Head of Family details are not required in case of Document based Verification.		
10	For Document Based (Write Names of the documents produced. Refer back side of this form for list of valid documents)		
	a. POI	b. POA	
	c. DOB <small>(Mandatory in case of Verified Date of Birth)</small>	d. POR	
11	For Introducer Based – Introducer's Aadhaar No.:	For HoF Based – Details of: Father () Mother () Guardian () Husband () Wife () HoF's Eid/Aadhaar No.: dd mm yyyy hh mm ss	
	I hereby confirm the identity and address of _____ as being true, correct and accurate.		
	Introducer/HoF's Name:	Signature of Introducer/HoF	
	Consent I confirm that information (including biometrics) provided by me to the UIDAI and the information contained herein is my own and is true, correct and accurate.		
	Verifier's Stamp and Signature: <small>(Verifier must put his/her Name, if stamp is not available)</small>		Applicant's signature/Thumbprint
	To be filled by the Enrolment Agency only : Date & time of Enrolment: _____		

Fig. a: Aadhaar card application form



4. Attach the signed copies of your documents, such as school leaving certificates and birth certificates to the application.
5. Once you submit these documents and allow the Aadhaar card service provider to collect your fingerprint, iris and palm images, then only the Aadhaar card processing takes place.

Practical Activity 16

Data collection process in school admission.

Material required

Admission application form, documents, photograph, pen

Procedure

1. Fill the admission form of the school or college you wish to join.
2. A sample form is shown below.

2015001 **ADMISSION FORM**

A - ONE INSTITUTE
S.C.O - 322, TOP FLOOR, SEC - 40 D
CHANDIGARH
PH- 9872662038, 9872642264
WWW.AONEBIOINSTITUTE.COM

AFFIX PHOTOGRAPH

1. Full Name of the Applicant (space should be given between Firstname, Surname & Lastname)
2. Nationality 3. Date of Birth 4. Sex M - Male F - Female 5. Course Opted
6. Father's Name
7. Mother's Name
8. Contact No. Father's No. Mother's No.
9. Complete Address (do not repeat name)
- District State Pin Code
10. E mail :
11. Present School / College
12. Class / Course Marks Obtained %age or CGPA
13. How did you come to know about A - One Institute
 Newspaper Teacher Friends/Relatives Others
14. Reg. Fee Detail Amount Date
15. Do you required P.G / Hostel facility yes No
16. Extra Curricular activities / Awards

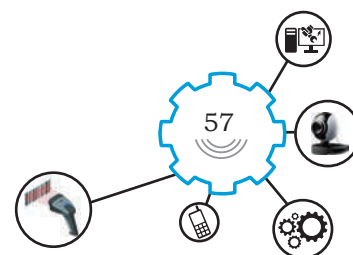
Note: Fees to be paid on the given dates as discussed in Institute during admission of candidate
Institute will not be held responsible for misplacement of vehicle of any candidate

DECLARATION:
I hereby declare that all the particulars stated in this application are true to the best of my knowledge and belief. I have understood all the provisions of the prospectus and agree to abide by them. In the event of suppression or distortion of any fact like educational qualification, study period etc. made in my application form, I understand my admission is liable for cancellation.

Date Place Sig. of Applicant

Fig. a: Admission form

3. Attach the signed copies of your documents, such as school leaving certificates and birth certificates to the application.



RAILWAY CM257
RESERVATION/CANCELLATION REQUISITION FORM

If you are a Medical Practitioner
Please tick () in Box Dr.
(You could be of help in an emergency)

Train No & Name 12138 Punjab Mail Date of Journey 20/08/19
Class 3rd AC No of Berth/Seat 02
Station from NEW DELHI To CSTM
Boarding at New Delhi Reservation upto CSTM

S.No.	Name in Block letter (not more than 15 chars)	Sex (M/F)	Age	Concession/Travel Authority No.	Choice if any
1.	<u>AJEET SINGH</u>	<u>M</u>	<u>40</u>		<input checked="" type="checkbox"/> Lower/Upper berth
2.	<u>SUNITA SINGH</u>	<u>F</u>	<u>36</u>		
3.					<input type="checkbox"/> Veg./Non-veg. Meal for
4.					<input type="checkbox"/> Rajdhani/
5.					<input type="checkbox"/> Shatabdi
6.					<input type="checkbox"/> Express Only

CHILDREN BELOW 5 YEARS (FOR WHOM TICKET IS NOT TO BE ISSUED)

S.No.	Name in Block Letters	Sex	Age
<u>01</u>	<u>AMAN</u>	<u>M</u>	<u>04</u>

ONWARD/RETURN JOURNEY DETAILS

Train No. & Name _____ Date _____
Class _____ Station from: _____ To _____
Name of applicant AJEET SINGH
Full Address D-506, Karol Bagh, New Delhi

Signature of the Applicant/Representative _____
Telephone No., if any 7867532120 Date 17/07/19 Time 1:40 PM

FOR OFFICE USE ONLY

S.No. of Requisition _____ PNR No. _____
Berth/Seat No. _____ Amount collected _____
Signature of Reservation Clerk _____

Note : 1. Maximum permissible passengers is 6 per requisition.
2. One person can give one requisition form at a time.
3. Please check your ticket and balance amount before leaving the window.
4. Forms not properly filled or in illegible forms shall not be entertained.
5. Choice is subject to availability

Fig. 1.70: Photograph of railway reservation handwritten form

	A	B	C	D	E
1	Date	Name	Area	Interviewed By	Status
2	15-05-2019	Rajesh Kumar	Accountant	Vijay Singhania	Selected
3	16-05-2019	Sumit Arora	Programmer	Sunil Kumar	Rejected
4	17-05-2019	Alka Jain	HR Manager	Vijay Singhania	Selected
5	18-05-2019	K. Abhitosh	Marketing	Amit Bajaj	Rejected
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					

Fig. 1.71: Data entry form

Handwritten Data and Digital Data

Whenever you fill any form, such as railway reservation form by writing data in your own handwriting then such data can be called handwritten data. An example of handwritten data is shown in Fig. 1.70.

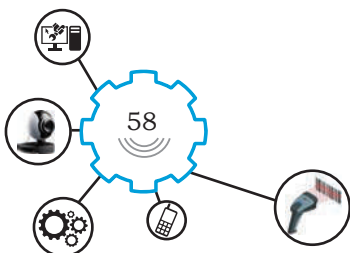
There are chances that the handwritten data is misread or misinterpreted. This is because the handwriting style of every individual is different. Sometimes it is not readable also. While filling in any handwritten form, one must take care that the information entered is clear and is in readable form. This increases the reliability of getting the correct data. To reduce the possible errors, many organisations design their own data entry forms, which consist of one block for one character. Also many fields can be entered just by checking the appropriate check boxes. One such form is given in Fig. 1.71.

Data entered into the computer by using digital codes is called digital data. Digital data is available in binary or machine form. Such data can be stored in computer memory and on the hard drives. Digital data is in electronic form and, therefore, it can be easily processed. Any real-life data, such as text, number, image, video or audio can be converted in digital form by using appropriate digital formats.

Advantages of digital data

The advantages of digital data over handwritten data are as given below.

- Ease of accessibility through computer systems.
- Environment friendly, as digital data do not require any paper.



- Better protection; as digital data can be stored on hard drives and they can be protected from physical harm.
- Storing and retrieving of data is convenient than that of handwritten data.
- A large amount of money can be saved by storing the data on low cost storage devices.
- Digital data increases the productivity of any organisation.
- Chances of errors are reduced while using digital data.

Practical Activity 17

Differentiate between handwritten and digital data.

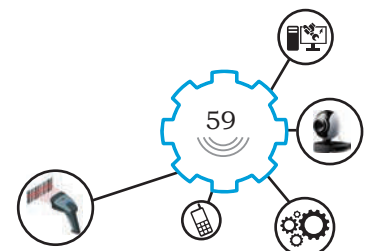
Material required

Handwritten documents, digital documents on computer, pen

Procedure

1. Collect the certain handwritten documents, such as your school leaving certificate or application forms.
2. Collect the digital version of the similar documents.
3. Carefully observe the difference between the two versions and plot the observations in a tabular form as shown below.

Parameter	Handwritten	Digital
Use of paper	This documents require paper	This documents do not require any paper
Font face and colour	It appears in single colour and do not have a specific font and size.	It can appear in any colour and can have a specific font and size.
Undesirability	Handwritten documents are difficult to understand if handwriting is not good	Understanding digital documents is easy as they are in typed format
Processing	Handwritten documents cannot be processed on computer systems	Digital documents can be processed on computer systems
Life of the document	Handwritten documents have a short life, as the life of the paper is short	Digital documents can be stored for a long period of time on storage devices
Effect of virus	There is no effect of virus on handwritten documents	Virus can affect the digital documents



Ph. : 2556707, 2526100

Red Cross Hospital

(X-Ray, Pathology, Blood Bank)
Red Cross Campus, Shivaji Nagar, Bhopal - 462 016 (M.P.)

Name : Deepak Age 47 Date 11/4/19

	EYE	SPHERICAL	CYLINDICAL	AXIS	VISION
DISTANCE	Right	+0.5	+0.25	145	6/6
	Left	+0.75	+0.25	15	6/6
NEAR	Add	+1.75			

P.D. to be measured
Constant Use/ Near Work Progressive Eye Specialist S

Fig. 1.72: Handwritten data

Digitisation of Handwritten Data

Any handwritten data can be converted into digital form. All paper documents can be transformed to electronic form for easy information processing. Working with the files in digital form is cheaper than that of traditional documents. Also each document exists in one copy consequently all changes or notes are visible for all.

Practical Activity 18

Conversion of handwritten data into digital form.

Material required

Handwritten documents, scanner, computer system

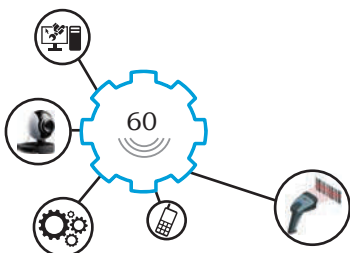
Procedure

1. Identify the documents that you want to convert in digital forms. Double-sided documents or colour documents need to be treated differently.
2. Prepare all the documents along with their notes for digitisation.
3. Scan the documents using appropriate standard scanners available for scanning of the handwritten documents.
4. After scanning, save the scanned documents in images or PDF form on the disk. You can also use optical character recognition (OCR) to convert the scanned images into electronically coded text. You can also store it on virtual servers by using cloud services, such as Google Drive, OneDrive, Dropbox, iCloud.

Check Your Progress

A. Fill in the blanks

1. Data collection is a process of _____ and _____.
2. Data collection is _____ and _____ activity.
3. Data collection is performed by private and _____ agencies.
4. Data collection means the accurate _____ of data.



5. There are chances that handwritten data can be _____ or misinterpreted.
6. Data is collected to get _____ for the questions raised within organisations.
7. Popularity of the product or service can be measured by _____.
8. Improvement in the existing services can be achieved through _____.
9. When we fill a printed form, such data is called _____ data.
10. The reliability of the handwritten data can be increased by _____.
11. Data entered on the computer machine is called _____ data.
12. Digital data is available in _____ form.
13. The data that do not require any paper is _____ data.

B. Multiple choice questions

1. Which of the following are the advantages of digital data?

(a) Ease of accessibility	(b) Environment friendly
(c) Security	(d) All of these
2. Font face and colour can be easily changed in _____ data.

(a) handwritten	(b) digital
(c) Both (a) and (b)	(d) None of these
3. Virus can easily affect _____ data.

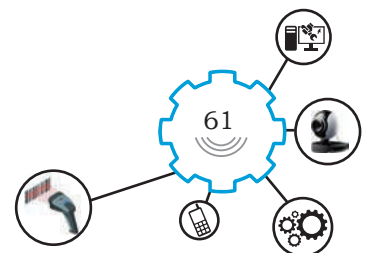
(a) handwritten	(b) digital
(c) Both (a) and (b)	(d) None of these
4. Use of paper is required in the creation of _____ data.

(a) handwritten	(b) digital
(c) both (a) and (b)	(d) None of these
5. Security protection for personal computers includes _____.

(a) internal components	(b) locks and cables
(c) software	(d) All of these
6. Secret words or numbers used for protection of devices is called _____.

(a) biometrics data	(b) backup
(c) passwords	(d) private words
7. In computer security, _____ means that computer system assets can be modified only by authorised parties.

(a) confidentiality	(b) integrity
(c) availability	(d) authenticity

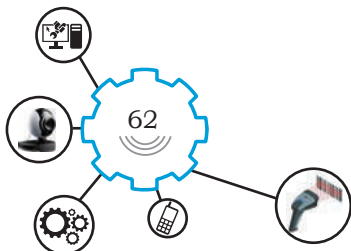


NOTES

8. MICR stands for _____.
(a) Magnetic Ink Control Recognition
(b) Magnetic Ink Character Recognition
(c) Magnetic Ink Character Receiver
(d) Magnetic Item Character Recognition
9. Banks process volumes of cheques quickly and accurately by using _____.
(a) OCR
(b) OMR
(c) MICR
(d) Scanner
10. OMR stands for _____.
(a) Optical Material Reader
(b) Optical Media Reader
(c) Optical Magnetic Reader
(d) Optical Mark Reader
11. PDF stands for _____.
(a) Post Data File
(b) Purchase Data Format
(c) Post Data Format
(d) Picture Data File
12. OCR means _____.
(a) Optical Character Recognition
(b) Open Character Recognition
(c) Optical Character Receiver
(d) Optical Character Recorder
13. Which of the following is an example of cloud services?
(a) Google drive
(b) One drive
(c) Drop box
(d) All of these
14. Digitised documents can be saved on _____.
(a) hard disk drive
(b) virtual servers
(c) ROM
(d) Both (a) and (b)

C. State whether the following statements are True or False

1. Digital documents can be saved in PDF format.
2. Digital documents cannot be saved in image format.
3. Handwritten documents can be scanned by using mobile devices.
4. Before digitising documents you need to remove paper clips and pins attached to the documents.
5. Digital documents cannot be saved on virtual servers.
6. Digital documents can be stored on secondary storage devices.
7. PDF is the most commonly used format for storing a document.
8. In competitive examinations OMR sheets are used to record answers.
9. Banks do not use MICR for processing cheques.
10. Handwritten data can easily get affected by computer virus.
11. Handwritten documents cannot be processed on computer system.



12. Digital documents require use of paper.
13. A large amount of money can be saved by storing the data on low-cost storage devices.

D. Short answer questions

1. What is data collection? Give examples where data collection is required.
2. State any four advantages of data collection.
3. Explain the importance of data collection.
4. Differentiate between handwritten data and digital data.
5. State any four advantages of digital data.
6. What do you understand by digitisation?
7. What are the benefits of digitising documents?
8. Describe security and data security?
9. Give the steps for conversion of handwritten data into digital data.
10. Draw the diagram and explain the working of MICR.
11. Draw the diagram and explain the working of OMR scanner.
12. Write a note on PDF format and state its advantages.
13. Give the steps for storing a document on cloud server.

Practical Exercise

1. Fill the feedback of your travel in Ola or Uber taxi in the feedback form provided as shown in Fig. a below.

Your feedback

We would like your feedback to improve our website.

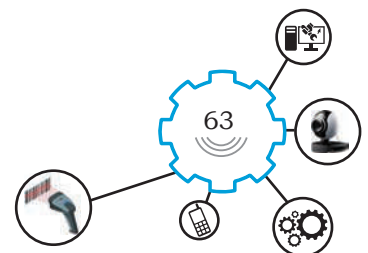
What is your opinion of this page?

Please select your feedback category below.

Please leave your feedback below:

Fig. a: Feedback form by Ola taxi

2. Digitise your Class X marksheet by using the process of digitisation.



SESSION 5: STORE AND HANDLE DATA SECURELY

Suppose your school has asked you to submit all your marksheets in digital form. You convert all your typed marksheets in digital form and carry these in a pen drive to your school. When you reach your school and insert the pen drive in the school computer, you observe that you cannot open the file that contains the digitised marksheets. You are shocked to know that you have lost all of your digital documents. This means that you have not handled your digital documents securely. In this session, you are going to study how to store and handle digital data and the procedures and precautions to be followed. Also you will study the different devices used for storing and handling of digital data. The concept of data security will also be briefly explained.

Storing and Handling of Data

Storing of data means, putting the data in a known place. When we write the data or save the data it means that we are storing the data. The data needs to be stored so that whenever we come back to that place we can get our data back again. Reading of data means retrieving data or opening a data file so that we can get our data back from its storage locations.

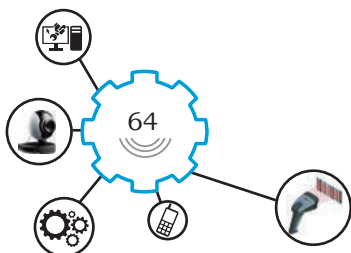
Data handling refers to the process of safe and secure data storing and retrieving. That is whenever we are dealing with the data we need to deal in such a way that no harm is caused to the data.

In some storage devices like hard disk drive, data is stored randomly. In magnetic tapes data is stored sequentially and it is also accessed sequentially. If you want to store the data for a long period then hard disk drives are preferred.

Procedure for Storing and Handling of Data

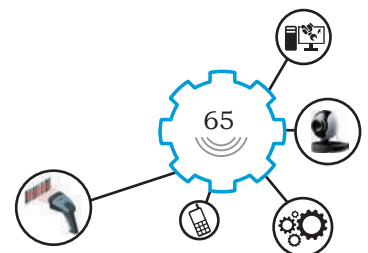
The procedure for storing and handling of data is given below.

Step 1. Understand the existing format of the data. If the data is handwritten or printed text then first convert this handwritten data into digital



form. If the data is readily available in the digital form, then you need not to adopt any conversion process.

- Step 2.** Identify and connect the appropriate storage device for storing of data. There are a large number of storage devices available for storing of data, such as fixed storage devices and removable storage devices. The magnetic coated hard disk is a fixed storage device, while a pen drive or a Compact Disc (CD) ROM are removable storage devices. Based on the data you may decide the requirement of fixed storage device or a removable storage device. Connect the appropriate storage device to your computer system, if it is not readily available.
- Step 3.** Check for virus in externally connected storage device. Many times we use the external storage devices that are already used by other people on other computer machines. There is a strong possibility that these devices may be affected by the viruses present in that system. In such a case you need to check if the storage device is affected by virus by using appropriate antivirus software program. You must clean all the viruses before storing any new data in the externally connected storage devices.
- Step 4.** Understand the size of the data and the space available in the storage device. Some data files are extremely large in size and they require a space in megabytes or gigabytes. Depending upon the size of the data, check if sufficient space is available in the selected storage device.
- Step 5.** Transfer files from computer memory to storage device. Normally the digitised data files are available in computer memory. Such files can be transferred to the storage device by using appropriate operating system commands. Many times you can use some software or application



NOTES

to transfer such files into storage device. For example, if an image file is opened by using paint software in Windows then the file can be saved on the pen drive.

Step 6. Check if the file is properly saved on storage device. Once the file transfer is completed you need to open the storage device and check that the file is available on the storage device. Also, check if the file can be accessed from the storage device itself.

Step 7. Close or end the storing of data and remove the storage device. In this final step we will close all open windows and safely remove the connected storage device from the computer system.

Practical Activity 19

Store the data on computer storage device HDD.

Material required

Computer, software application, such as Word, Excel

Procedure

1. Open the software application associated with the file type you wish to create. You can open the application by double-clicking on it.
2. Click on 'File' along the top of your screen and select 'New.' Some applications use commands like 'Create New File'.
3. Type the new data into the file.
4. Click 'File' and select 'Save' option to save the file.
5. Enter the file name in the 'Save As:' field. Also provide the file extension.
6. Click the 'Save' button. You have successfully created a file.

Practical Activity 20

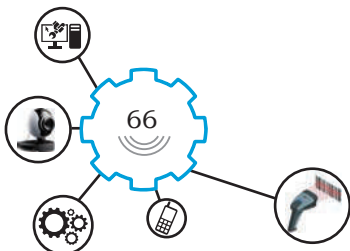
Store the data on pen drive

Material required

Computer, pen drive, software application, such as Word, Excel

Procedure

1. Open the software application associated with the file type you wish to create. You can open the application by double-clicking on it.



2. Click on 'File' along the top of your screen and select 'New.' Some applications use commands like 'Create New File'.
3. Type the new data into the file.
4. Click 'File' and select 'Save' option to save the file.
5. Type the name you want to give the file in the 'Save As': and choose location as USB drive. This is the file extension is by default '.bmp'.
6. Click the 'Save' button.
7. Open USB drive and check if the file has been successfully saved on USB drive.

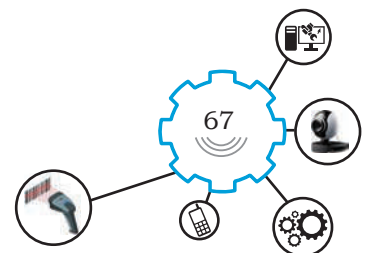
Data Security

It is defined as protection of data against unauthorised modification, destruction, disclosure or transfers either accidentally or intentionally. If data is not provided appropriate security then there are chances that the data can get lost or it can get stolen from your computer system. Sometimes the data can get hacked by hackers. In all such cases the user or owner of the data is at loss. Sometimes it becomes very difficult to re-initiate the data.

The issues related to the data security are mostly handled by using the public key infrastructure (PKI) approach. This approach consists of two keys. Both these keys are the binary strings in the range of 1024 bits to 2048 bits. The first key is the public key that is widely known and the second key is the private key, which is known only to owner of the data. These keys must also be stored securely with proper authentication, such as password or pin

Precautions to be taken while creating a password

- Password length should not be less than 8 and more than 20 characters.
- Password should contain at least one digit [0-9], one alphabet [A-Z] [a-z] and one special character, such as [@#&*!].
- Please avoid choosing a password that is generic in nature, guessable or inferable.



NOTES

- Avoid a password that is related to your personal data, such as name, date of birth, address, telephone number and car or bike registration number.
- It is a good practice to memorise your password rather than write it down somewhere.
- For security reasons, keep changing your password at regular intervals

Practical Activity 21

Logging in to bank account with correct credentials

Material required

Computer, credentials of your bank account

Procedure

1. Visit the website of Internet banking to access your bank account.
2. Enter your login and password.
3. Observe that after entering the correct login and password you will get access to your bank account details and you can do the transactions.
4. If the wrong credentials such as login or password are entered, then you will get the error message and you will not be able to access your bank account details.
5. Change your password by adopting the process of changing password.

Practical Activity 22

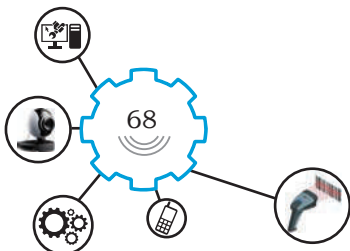
Protect PDF file with password

Material required

Computer, credentials of your bank account

Procedure

1. Take one handwritten document.
2. Digitise this document by using a scanner and save it in the PDF format.
3. While saving the PDF file, set the password in the file security menu.
4. Observe that this file will open, only after providing the correct password.

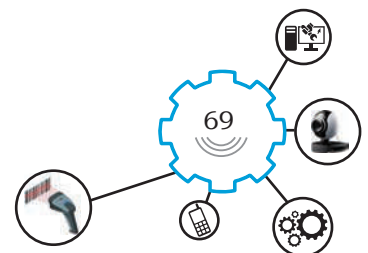


Data security issues in biometric systems

In biometric systems the personal data of employees are collected. This data consists of photographs, signature, date of birth and other personal information. This data must be handled carefully and it should not be leaked to unauthorised personnel. To take care of this many biometric systems assign a field as 'Sensitive' to some of the data elements as shown in the following form.

List of Data Elements

Data Field	Description	Classification
CID		Non-sensitive
ID		Sensitive
Alfa Numeric		Sensitive
Name		Sensitive
Name _Local		Sensitive
E type		Sensitive
Desig _Id		Sensitive
Dept _Id		Sensitive
Reg date		Sensitive
Join date		Sensitive
Reg exp date		Sensitive
Email		Sensitive
Date_Birth		Sensitive
Blood group		Sensitive
Weekly Off		Non-sensitive
Gender		Sensitive
Grade _Id		Non-sensitive
Weekly off flag		Non-sensitive
Religion _Id		H ig hy-sensitive
Nationality _Id		Sensitive



Visa Expiry Date	Sensitive
Passport Expiry Date	Sensitive
Policy_Id	Non-sensitive
Shift_Id	Non-sensitive
RO	Non-sensitive
HR	Non-sensitive
Sub_Dept_Code	Non-sensitive
VIP	Non-sensitive
Person_Id	Sensitive

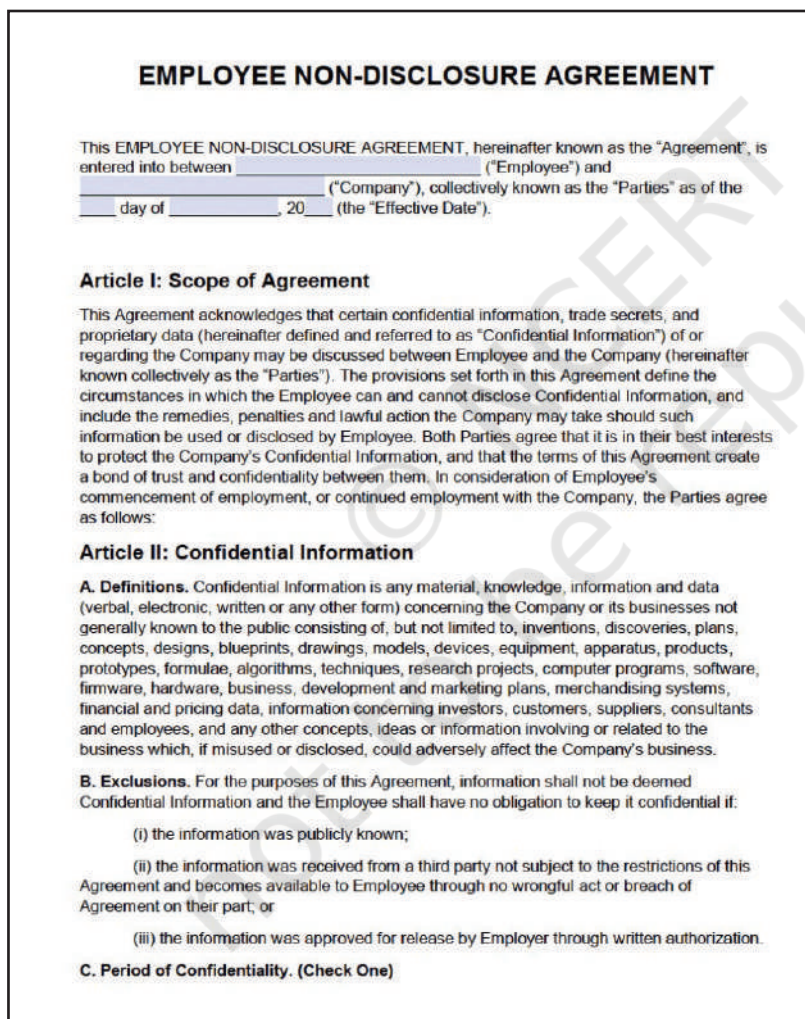


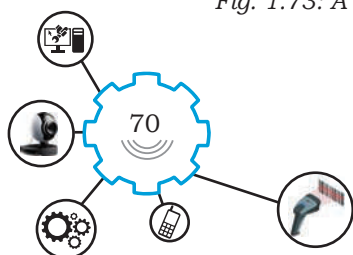
Fig. 1.73: A typical clause of confidentiality agreement

Observe that the data of **Religion_Id** is a highly sensitive data. ID name and date of birth of employee is sensitive data. Company ID (CID) is non-sensitive data. Likewise department code is non-sensitive data.

Highly sensitive data is treated as private data. Higher level of protection is assigned to these fields. Sensitive data is confidential data. This data is also secure.

Non-sensitive data is public data. It is usually unprotected. Sensitive data can be accessed only through the administrator login and password. While non-sensitive data can be accessed easily.

Biometric equipment or devices are protected from unauthorised uses or viruses by using firewall or antivirus programs.



Data confidentiality among the workers in biometric industry

Whenever an employee accepts a work order in Biometric industry, then Biometric industry asks the employee to sign a **Confidentiality Agreement**. This agreement takes care of non-leakages of the personal details of the customers.

The various clauses are included in the agreement (Fig. 1.73). The individual hereby agrees that they shall hold in confidence and shall not assign, license, sell, use, commercialise or disclose in any manner whatsoever except under terms of employment or association with <Biometric Industry>, any Intellectual Property or Confidential Information belonging to <Biometric Industry>, to any person or entity, or else under provision governed by this memorandum except as <Biometric Industry> may approve in writing.

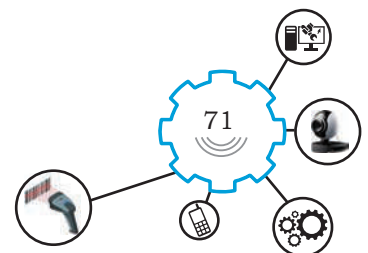
Practical Exercise

1. Store the data prepared on the computer on an appropriate storage device.
2. How will you secure your ATM card pin, credit card pin.
3. You have been provided some storage devices. Perform the following activity to check it for
 - Viruses, if any present in the device.
 - storage capacity of the device.
 - available space on the device.
 - data size to be stored

Check Your Progress

A. Fill in the blanks

1. Writing of the data means _____ of the data.
2. Reading of the data means _____ of the data.
3. Data handling refers to the process of _____ data storing and retrieving.
4. Data handling should not _____ the data.
5. In hard disk drives data is stored _____.
6. In magnetic tape drive data is stored _____.

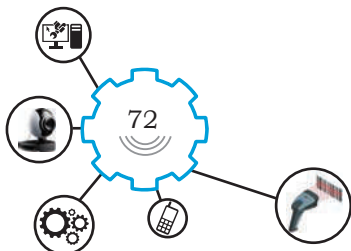


NOTES

7. In optical disk drives data is accessed _____.
8. For long-term storage of the data _____ drives are preferred.
9. Before storing the data conversion of data is necessary if it is in _____ form.
10. Transfer of the files from computer memory to the storage device is performed by using _____ commands of operating system.
11. Before quitting any software application it is necessary to _____ the application.

B. Multiple choice questions

1. Protection of the data against unauthorised modification is called _____.
(a) data security (b) data disclosure
(c) data transfer (d) None of these
2. Chances of data loss are more if _____.
(a) it is modified frequently
(b) it is transferred frequently
(c) it has no security
(d) None of the above
3. PKI stands for _____.
(a) Public Key Infrastructure
(b) Public Key Internet
(c) Public Keyword Infrastructure
(d) Porous Key Infrastructure
4. PKI approach is related to _____.
(a) data modification (b) data destruction
(c) data disclosure (d) data security
5. In PKI approach the first key is called _____.
(a) private key (b) public key
(c) owner key (d) None of these
6. In PKI approach the key that is known to the owner of the data is called _____.
(a) private key (b) public key
(c) owner key (d) user key
7. Generally the length of the password should be minimum _____.
(a) less than 8 characters
(b) equal to 8 characters
(c) more than 8 and less than 20 characters
(d) more than 20 characters
8. Every password must contain _____.
(a) at least one digit
(b) one digit and one alphabet
(c) one digit, one alphabet and one special character
(d) only digits



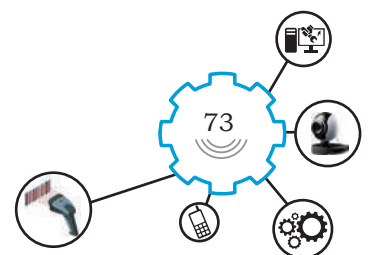
9. Password must be changed _____.
- | | |
|---------------------|--------------------------|
| (a) once in a year | (b) never |
| (c) twice in a year | (d) at regular intervals |

C. State whether the following statements are True or False

- To access any bank's website you need to enter the correct login and password.
- If the wrong credentials, such as login and password are entered, then you can access your bank account details.
- Always write your password somewhere so that you need not memorise it.
- A PDF file cannot be protected by using password.
- All the data elements in the biometric system must be classified as non-sensitive elements.
- Religion identity of an employee is highly sensitive data element.
- Company ID is a sensitive data element.
- Highly sensitive data elements can be accessed only through administrator login and password.
- Firewalls and antivirus programs protect the biometric equipment from unauthorised use.
- Employee working in biometric industry need not sign a confidentiality agreement.

D. Short answer questions

- What do you mean by data confidentiality among the workers of biometric industry?
- List certain sensitive and non-sensitive data elements of biometric data.
- Write the steps to protect a file with password.
- List any four precautions to be taken while creating a password.
- Define data security in biometric systems.
- What is PKI approach? Give examples of PKI.
- Define the term data handling in biometric system.
- Give the procedure for handling of data.
- Differentiate between random access and sequential access method of data.



Domestic Biometric Data Operator-Class 11- Unit 1 Session 1

A. Fill in the blanks

1. Computer is a _____ electronic machine.
2. The term computer is derived from the Latin word _____.
3. A computer can perform arithmetic and _____ operations.
4. A set of the instructions is called _____.
5. CPU stands for _____.
6. CPU consists of control unit and _____.
7. ALU stand for _____.
8. Keyboard and mouse are _____ devices of a computer system.
9. Monitor and printer are _____ devices of a computer system.
10. USB stands for _____.
11. UPS stand for _____.
12. The fastest access to the memory is _____.
13. The full form of RAM is _____.
14. The full form of ROM is _____.
15. Primary memory is memory that is accessed directly by the _____.
16. RAM is generally located on the _____.
17. Printers are mainly divided into two categories _____ and _____ printers.

B. Multiple choice questions

1. Which of the following is a valid type of ROM?
(a) PROM (b) EPROM
(c) EEPROM (d) All of these
2. Which of the following is not a type of memory?
(a) RAM (b) FEPROM
(c) EEPROM (d) ROM
3. Which of these is a type of memory used in computer system?
(a) PC (b) Laptop
(c) DRAM (d) Tablet
4. RAM in PC is used to _____.
(a) store the boot program (b) store applications
(c) load the operating system (d) Both (b) and (c)

5. _____ is a secondary storage device.
- (a) Keyboard (b) Mouse
(c) Pen drive (d) Printer
6. Which of the following is the fastest memory in a computer?
- (a) RAM (b) Registers
(c) HDD (d) ROM
7. In a _____ printer characters or letters are formed without the use of any mechanical impact.
- (a) page (b) line
(c) impact (d) non-impact
8. The devices that are used for storing program and data for long term are called _____ device.
- (a) volatile (b) non-volatile
(c) primary memory (d) CPU registers
9. The thickness of memory cards is given in _____.
- (a) millimeter (b) centimeter
(c) kilometer (d) None of these
10. Hard copy of the data can be obtained by using a device called _____.
- (a) keyboard (b) mouse
(c) pen drive (d) printer
11. Printers that make contact with paper are called _____ printers.
- (a) non-impact (b) impact
(c) global (d) local
12. Printers that do not make any contact with the paper while printing data are called _____ printer.
- (a) non-impact (b) impact
(c) global (d) local
13. Dot matrix printer is a _____ type of printer.
- (a) non-impact (b) impact
(c) global (d) local
14. Laser printer is a _____ type of printer.
- (a) non-impact (b) impact
(c) global (d) local
15. _____ is the faster printer.
- (a) Dot matrix (b) Inkjet
(c) Laser (d) Line
16. High quality printing can be achieved by using _____ printer.
- (a) dot matrix (b) inkjet
(c) laser (d) line

17. Which of the following printers' speed is measured in characters per second?
(a) Inkjet (b) Laser
(c) Dot matrix (d) Drum
18. Usually peripheral devices are connected to the computer system via _____ port.
(a) PCM (b) UCB
(c) USB (d) GPS
19. GPS stands for _____.
(a) Global Positioning System
(b) Global Partitioning System
(c) Google Positioning System
(d) Global Permanent System
20. To identify the geographical position and time information anywhere on the earth we use _____.
(a) GST (b) GMP
(c) GPS (d) GNU

C. State whether the following statements are True or False

1. UPS provides uninterruptible power supply.
2. Electrical generator provides uninterruptible power supply.
3. Electrical generator converts mechanical energy into electrical energy.
4. UPS needs battery for its operation.
5. Mouse and keyboard cannot be connected to the USB port.
6. Speakers of the computer systems are generally connected to the USB port.
7. Modern computer is a analog electronic device.
8. Tablet is a type of computer.
9. Memory of the computer system is measured in bytes.
10. Cache memory is slower and consumes lot of access time than main memory.
11. Cache memory is used to store application programs.
12. The instructions stored in ROM can be changed by the user.

D. Short answer questions

1. Draw the connectivity diagram of UPS and battery.
2. Explain the use of GPS in personal computer.
3. What is the use of USB port?
4. List the devices that can be connected to USB port.
5. Along with a suitable diagram explain the working of laser printer.

6. How are inkjet printers different from laser printers?
7. Explain the uses of line printer.
8. Describe the working of a dot matrix printer
9. List the different types of secondary memory storage devices that are commonly used.
10. List the uses of memory card and pen drive in different applications.
11. What do you mean by memory of a computer system?
12. What is cache memory?
13. What are the characteristics of main memory?
14. What are the major differences between RAM and ROM?

Domestic Biometric Data Operator-Class 11- Unit 1 Session 2

A. Fill in the blanks

1. The word data is taken from the Latin word _____.
2. In 1946 the term _____ was used first time with transmittable and storable computer information.
3. Alphanumeric data contains _____.
4. The data representing a large population is called _____ data.
5. The individual data is called _____ data.
6. Age, society, education, gender are considered as features of _____ data.
7. Government decisions or policies are mostly based upon _____ data.
8. The data captured by the electronic devices is called _____.
9. OTP stands for _____.
10. BHIM stands for _____.
11. The data that can only be described by using words and description is called _____ data.
12. Group discussion, interviews and surveys are used to collect _____ data.
13. The data that is expressed by numbers only is called as _____ data.

B. Multiple choice questions

1. Data may be _____.
(a) numbers (b) text
(c) alphanumeric (d) All of these
2. Quantitative data is expressed in _____.
(a) only numbers (b) only text
(c) only alphanumeric (d) Both (a) and (b)
3. Pie chart is used for _____.
(a) data interpretation (b) designing
(c) showing text (d) hiding data
4. OTP in credit card transaction is _____.
(a) Odd Transaction Password
(b) Owner Trading Passcode
(c) One Time Password
(d) One Time Pincode
5. Why is one time password safe?
(a) It is easy to generate.
(b) It cannot be shared.
(c) It is different for every access.
(d) It is a complex encrypted password.

6. Electronic data is _____
(a) digital form of data (b) hard copy of data
(c) only used for shopping (d) only used by apps
7. Height and weight of a person are examples of _____ data.
(a) qualitative (b) quantitative
(c) random (d) global
8. Face image and thumb image are examples of _____ data.
(a) qualitative (b) quantitative
(c) random (d) global
9. .DOC format is used with _____.
(a) text file (b) image file
(c) voice file (d) database file
10. .JPG format is used with _____.
(a) text file (b) image file
(c) voice file (d) database file
11. .MP3 format is used with _____.
(a) text file (b) image file
(c) video file (d) database file
12. .SQL format is used with _____.
(a) text file (b) image file
(c) video file (d) database file
13. Statistical data is also called _____ data.
(a) qualitative (b) quantitative
(c) random (d) global
14. All physical quantity data is _____.
(a) qualitative (b) quantitative
(c) random (d) global
15. Stock market data is an example of _____.
(a) demographic data (b) demographic data
(c) random (d) global

C. State whether the following statements are True and False

1. Data means facts or set of values.
2. Useful knowledge about data can be obtained without processing it.
3. Data cannot be measured and analysed.
4. Data can be visualised.
5. Quantitative and qualitative are the two types of data.
6. Demographic data is personal data.
7. Energy survey data and stock market data are the examples of demographic data.

8. Pie chart, bar graphs and line graph can be used to visualie data.
9. Useful conclusions cannot be drawn by using demographic data.
10. Data generated by electronic devices, such as mobile phone is called analog data.
11. The colour of skin and colour of eyes is qualitative data.
12. The crop yield and air pollution is the quantitative type of data.
13. .txt format is used for image file.
14. .wav format is used for voice file.
15. .mdb format is used for image file.
16. .gif format is used for image file.

D. Short answer questions

1. Explain the different types of text file formats using suitable examples.
2. What is data file format? Explain the format used for video files.
3. Along with suitable examples explain the different image file formats.
4. What are the different types of data? .
5. How is data processed?

Domestic Biometric Data Operator-Class 11- Unit 1 Session 3

A. Fill in the blanks

1. The word biometric is derived from the Latin word _____ and _____.
2. Greek word bio means _____ and metric means _____.
3. Biometric is used to identify _____ and _____ characteristics of a person
4. Authentication of a person can be performed by using _____ data.
5. Iris is actually an internal part of the _____ that controls the inflow of light to the eye.
6. The _____ style of signature of every individual person is different from the other.
7. Biometric system can be used as a (an) _____ system.
8. Quality of the biometric data refers to a clear and _____ free data capture of biometric data
9. Changes in the human face occurs due to an increase in the _____.
10. Every citizen gets a/an _____ Aadhaar number.
11. Signature and way of walking are _____ characteristics of a person.
12. Fingerprint and face image are _____ characteristics of a person.
13. Core, crossover and island are the parts of _____ image.
14. Fingerprint of every individual person is _____.
15. About 65 per cent of biometric systems make use of _____ data.
16. In palm biometric image we can observe _____ on the palm.

B. Multiple choice questions

1. Which of the following methods is the best form of authentication?
(a) Biometrics (b) Multiple factor
(c) Password-based (d) Token-based
2. Hand geometry identification can be performed by using _____.
(a) fingerprint image (b) palm image
(c) iris image (d) face image
3. Corona, crypts and rings are the different features of _____.
(a) fingerprint image (b) palm image
(c) iris image (d) face image
4. Face of the human can be used as _____ data.
(a) demographic (b) biometric
(c) local (d) global
5. Voice of a person is _____ data.
(a) physiological (b) non-physiological
(c) behavioural (d) non-behavioural

6. Pitch, tone and frequency are features of _____ data.
(a) signature (b) iris
(c) retina (d) voice
7. Pressure, speed and acceleration are features of _____ data.
8. Skin colour, shape and size are features of _____ data.
(a) signature (b) face
(c) retina (d) voice
9. About 11 per cent of biometric systems make use of _____ data for the purpose of identification.
(a) signature (b) face
(c) retina (d) voice
10. Gait recognition means _____.
(a) walking pattern recognition
(b) face recognition
(c) iris recognition
(d) fingerprint recognition
11. Which of the following are the elements of biometric recognition system?
(a) Data capture (b) Data Enrolment
(c) Data authentication (d) All of these
12. Which of the following is the limitation of biometric data?
(a) Biometric data cannot be captured
(b) Biometric data cannot be enrolled
(c) Collection of biometric data requires physical contact
(d) Data authentication is difficult
13. The biometric data of people associated with an organisation is called _____.
(a) domestic data (b) global data
(c) material data (d) None of these
14. The data stored on the Aadhaar server that is used for matching purposes is called _____.
(a) domestic data (b) global data
(c) material data (d) None of these

C. State whether the following statements are True or False

1. Domestic data is a global data.
2. Biometric system is an offline system.
3. Biometric system do not require any hardware and software.
4. Medical problems or accident injuries can create problem for behavioural data.
5. Quality of biometric data refers to clear and error free data.
6. Collection of biometric data does not require physical contact.
7. Face images get changed due to increase in age.
8. Data authentication is performed by using hardware.
9. Data capture is performed by using software only.
10. Voice of every individual person is different from the other person.

D. Short answer questions

1. Define the term biometric data.
 2. Define demographics data.
 3. What are the characteristics of successful biometric identification methods?
 4. What are the qualities of biometric data?
 5. State the types of biometric data.
 6. Explain the different parts of a fingerprint.
 7. Explain the different parts of a palm image.
 8. What are the different features associated with the face of a person?
 9. State the features of human eye.
 10. Draw the diagram of iris and state its different parts.
-
11. State the features associated with the signature of a person.
 12. List the voice features of a person.
 13. What is gait recognition?
 14. Differentiate between domestic and global data.

Domestic Biometric Data Operator-Class 11- Unit 1 Session 4

A. Fill in the blanks

1. Data collection is a process of _____ and _____.
 2. Data collection is _____ and _____ activity.
 3. Data collection is performed by private and _____ agencies.
 4. Data collection means the accurate _____ of data.
-
5. There are chances that handwritten data can be _____ or misinterpreted.
 6. Data is collected to get _____ for the questions raised within organisations.
 7. Popularity of the product or service can be measured by _____.
 8. Improvement in the existing services can be achieved through _____.
 9. When we fill a printed form, such data is called _____ data.
 10. The reliability of the handwritten data can be increased by _____.
 11. Data entered on the computer machine is called _____ data.
 12. Digital data is available in _____ form.
 13. The data that do not require any paper is _____ data.

B. Multiple choice questions

1. Which of the following are the advantages of digital data?
(a) Ease of accessibility (b) Environment friendly
(c) Security (d) All of these
2. Font face and colour can be easily changed in _____ data.
(a) handwritten (b) digital
(c) Both (a) and (b) (d) None of these
3. Virus can easily affect _____ data.
(a) handwritten (b) digital
(c) Both (a) and (b) (d) None of these

4. Use of paper is required in the creation of _____ data.
(a) handwritten (b) digital
(c) both (a) and (b) (d) None of these
5. Security protection for personal computers includes _____.
(a) internal components (b) locks and cables
(c) software (d) All of these
6. Secret words or numbers used for protection of devices is called _____.
(a) biometrics data (b) backup
(c) passwords (d) private words
7. In computer security, _____ means that computer system assets can be modified only by authorised parties.
(a) confidentiality (b) integrity
(c) availability (d) authenticity

8. MICR stands for _____.
(a) Magnetic Ink Control Recognition
(b) Magnetic Ink Character Recognition
(c) Magnetic Ink Character Receiver
(d) Magnetic Item Character Recognition
9. Banks process volumes of cheques quickly and accurately by using _____.
(a) OCR (b) OMR
(c) MICR (d) Scanner
10. OMR stands for _____.
(a) Optical Material Reader (b) Optical Media Reader
(c) Optical Magnetic Reader (d) Optical Mark Reader
11. PDF stands for _____.
(a) Post Data File (b) Purchase Data Format
(c) Post Data Format (d) Picture Data File
12. OCR means _____.
(a) Optical Character Recognition
(b) Open Character Recognition
(c) Optical Character Receiver
(d) Optical Character Recorder
13. Which of the following is an example of cloud services?
(a) Google drive (b) One drive
(c) Drop box (d) All of these
14. Digitised documents can be saved on _____.
(a) hard disk drive (b) virtual servers
(c) ROM (d) Both (a) and (b)

C. State whether the following statements are True or False

1. Digital documents can be saved in PDF format.
2. Digital documents cannot be saved in image format.
3. Handwritten documents can be scanned by using mobile devices.

4. Before digitising documents you need to remove paper clips and pins attached to the documents.
5. Digital documents cannot be saved on virtual servers.
6. Digital documents can be stored on secondary storage devices.
7. PDF is the most commonly used format for storing a document.
8. In competitive examinations OMR sheets are used to record answers.
9. Banks do not use MICR for processing cheques.
10. Handwritten data can easily get affected by computer virus.
11. Handwritten documents cannot be processed on computer system.

12. Digital documents require use of paper.
13. A large amount of money can be saved by storing the data on low-cost storage devices.

D. Short answer questions

1. What is data collection? Give examples where data collection is required.
2. State any four advantages of data collection.
3. Explain the importance of data collection.
4. Differentiate between handwritten data and digital data.
5. State any four advantages of digital data.
6. What do you understand by digitisation?
7. What are the benefits of digitising documents?
8. Describe security and data security?
9. Give the steps for conversion of handwritten data into digital data.
10. Draw the diagram and explain the working of MICR.
11. Draw the diagram and explain the working of OMR scanner.
12. Write a note on PDF format and state its advantages.
13. Give the steps for storing a document on cloud server.

Domestic Biometric Data Operator-Class 11- Unit 1 Session 5

A. Fill in the blanks

1. Writing of the data means _____ of the data.
2. Reading of the data means _____ of the data.
3. Data handling refers to the process of _____ data storing and retrieving.
4. Data handling should not _____ the data.
5. In hard disk drives data is stored _____.
6. In magnetic tape drive data is stored _____.
7. In optical disk drives data is accessed _____.
8. For long-term storage of the data _____ drives are preferred.
9. Before storing the data conversion of data is necessary if it is in _____ form.
10. Transfer of the files from computer memory to the storage device is performed by using _____ commands of operating system.
11. Before quitting any software application it is necessary to _____ the application.

B. Multiple choice questions

1. Protection of the data against unauthorised modification is called _____.
(a) data security (b) data disclosure
(c) data transfer (d) None of these
2. Chances of data loss are more if _____.
(a) it is modified frequently
(b) it is transferred frequently
(c) it has no security
(d) None of the above
3. PKI stands for _____.
(a) Public Key Infrastructure
(b) Public Key Internet
(c) Public Keyword Infrastructure
(d) Porous Key Infrastructure
4. PKI approach is related to _____.
(a) data modification (b) data destruction
(c) data disclosure (d) data security
5. In PKI approach the first key is called _____.
(a) private key (b) public key
(c) owner key (d) None of these
6. In PKI approach the key that is known to the owner of the data is called _____.
(a) private key (b) public key
(c) owner key (d) user key

7. Generally the length of the password should be minimum _____.
- (a) less than 8 characters
 - (b) equal to 8 characters
 - (c) more than 8 and less than 20 characters
 - (d) more than 20 characters
8. Every password must contain _____.
- (a) at least one digit
 - (b) one digit and one alphabet
 - (c) one digit, one alphabet and one special character
 - (d) only digits
9. Password must be changed _____.
- (a) once in a year
 - (b) never
 - (c) twice in a year
 - (d) at regular intervals

C. State whether the following statements are True or False

1. To access any bank's website you need to enter the correct login and password.
2. If the wrong credentials, such as login and password are entered, then you can access your bank account details.
3. Always write your password somewhere so that you need not memorise it.
4. A PDF file cannot be protected by using password.
5. All the data elements in the biometric system must be classified as non-sensitive elements.
6. Religion identity of an employee is highly sensitive data element.
7. Company ID is a sensitive data element.
8. Highly sensitive data elements can be accessed only through administrator login and password.
9. Firewalls and antivirus programs protect the biometric equipment from unauthorised use.
10. Employee working in biometric industry need not sign a confidentiality agreement.

D. Short answer questions

1. What do you mean by data confidentiality among the workers of biometric industry?
2. List certain sensitive and non-sensitive data elements of biometric data.
3. Write the steps to protect a file with password.
4. List any four precautions to be taken while creating a password.
5. Define data security in biometric systems.

6. What is PKI approach? Give examples of PKI.
7. Define the term data handling in biometric system.
8. Give the procedure for handling of data.
9. Differentiate between random access and sequential access method of data.



Procedures and Tools for Biometric Data



17110SCH02

INTRODUCTION

Biometrics is a biological characteristic of a person. The biometric process involves automated methods of verifying the identity of an individual. A standard biometric device consists of components, such as sensor, storage, match algorithm, and decision process. It is important to know about the various biometric processes, such as enrolment, authentication, matching, verification and identification. There are various types of biometric devices used for capturing the various types of biometric data. The process of capturing the biometric data often refers to the biometric data entry. As each biometric data has distinguished features and devices, the necessary guidelines and precautions should be followed by the operator in biometric data entry. The devices should be connected properly to the computer system. Biometric system comprises biometric devices, computer hardware and software. These devices should interact with each other to function as a system. Biometric interface is the method by which biometric system component communicates with another.

This unit covers the various biometric processes and terms associated with biometric technology. It also covers the biometric data entry for each kind of biometric data. The biometric data operator should also know the connectivity and interfacing of various biometric devices and the type of device required to capture the biometric data, which is covered in this unit.

SESSION 1: BIOMETRIC SYSTEM AND DEVICES

Suppose your teacher asks you to prepare a school ID card for all students of your class. To perform this job, you will require photographs, personal details and signature of every individual. For collecting all of these, you will need a camera, scanner and text processor. These devices are nothing but biometric devices. In this session you will understand the functioning of various biometric and input/output devices along with the biometric attendance machine.

Biometric System

A standard biometric system comprises five main components—sensor, feature extractor, matcher, storage and decision module as shown in Fig. 2.1.

Fig. 2.1 depicts that the sensor module is used to collect and digitise the biometric data. The sensor collects biometric data, such as fingerprint, palm or iris of the eye. The data collected is then converted into a digital format in preprocessing stage. The feature extractor checks the quality of the digitised image, extracts the feature set and generates the template. The database module is used to store the collected feature set stored in the template during the enrolment phase. A person's biographical information is used to identify the individual, such as name, employee number, PIN, address is also stored in the database. A matching module compares

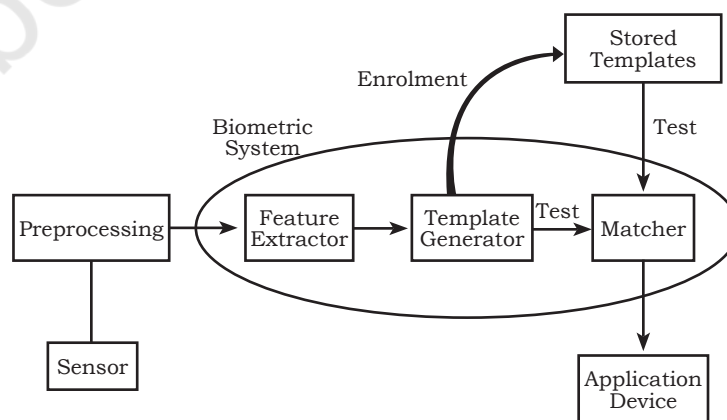
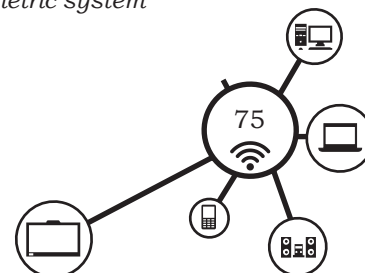


Fig. 2.1: Block diagram of biometric system



the feature set with templates stored in the database. A matching algorithm is used to compare the scanned data to the stored templates. After authenticating the individual, the device can grant access to the system.

Biometric Processes

There are various processes involved in biometric system, such as enrolment, template and matching.

Enrolment

Enrolment is the process of collecting biometric samples from a user. A biometric sample is biometric data acquired during submission. It is used to generate biometric templates. A biometric device is used to acquire biometric samples. These samples are then processed and stored for use in a biometric system. Enrolment is the first stage for biometric authentication because enrolment generates a template that will be used for matching. Normally, three samples of the same biometric are captured by the device and averages of them are produced as an enrolment template. Fig. 2.2 illustrates the enrolment process.

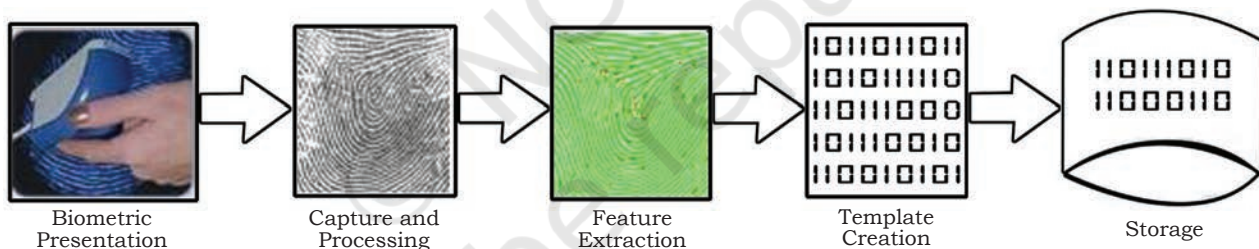
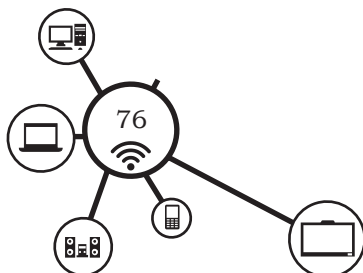


Fig. 2.2: Enrolment process

The first step in enrolment is biometric presentation or submission of biometric data to biometric system. For example, placing a finger on the scanner for submission of fingerprint data or looking into the iris camera to present the iris image. The fingerprint pressed by the user is captured by the biometric device, the captured data is processed by the device to extract the feature, the extracted feature is converted to machine readable form and then stored in the database. Feature extraction is the process of extracting the key features



of biometric sample to generate a template. Common physiological and behavioural characteristics used in feature extraction are given in Table 2.1.

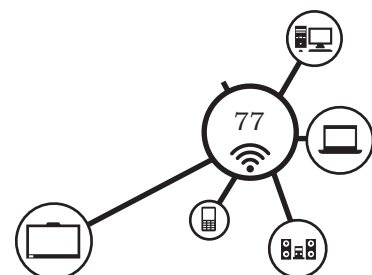
Enrolment should be done under the routine matching conditions. For example, for matching the voice biometric data in a noisy environment, the enrolment of voice may be done in the same environment so the captured voice can be matched with the template. Biometrics of a person change over a period of time. Many biometric systems update the changes by continuously averaging. The various acquisition devices and biometric sample associated with each biometric technology are given in Table 2.1.

Table 2.1: Biometric device, biometric sample and for various biometric technology

Biometric Technology	Biometric Device	Biometric Sample	Feature Extracted
Finger-scan	Fingerprint scanner, mouse, chip or reader embedded in keyboard	Fingerprint image	Location and direction of ridge endings and bifurcations on fingerprint
Voice-scan	Microphone, telephone	Voice recording	Frequency, cadence, and duration of vocal pattern
Facial-scan	Web camera, video camera	Facial image	Relative position and shape of nose, position of cheekbones
Iris-scan	Iris scanner	Iris image	Furrows and striations in iris
Retina-scan	Retina scanner	Retina image	Blood vessel patterns on retina
Hand-scan	Hand scanner	Hand image	Height and width of bones and joints in hands and fingers

Templates

A biometric template is a digital reference of distinct characteristics extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. Templates are only a record of distinguishing features, they are not an image or record of the actual fingerprint or voice. The information stored in the template is proprietary to biometric vendors. Biometric templates are not interoperable, means a template generated in vendor A's finger-scan system cannot be compared to a template generated in vendor B's finger-scan system.



NOTES

Matching

Matching is the comparison of template produced at the time of enrolment with the captured data at the time of access. A match attempt results in a score which is compared against a threshold. If the score exceeds the threshold, the result is a match; if the score falls below the threshold, the result is a non-match.

Threshold is a predefined number, which establishes the degree of correlation necessary for a comparison to match. If the score resulting from template comparison exceeds the threshold, the templates are a 'match'. There are three ways a match can fail.

- **Failure to enroll** is the failure of the technology to extract distinguishing features appropriate to that technology and hence not able to enroll the enrollee.
- **False match** occurs when a sample is incorrectly matched to a template in the database.
- **False non-match** occurs when a sample is incorrectly not matched to a truly matching template in the database

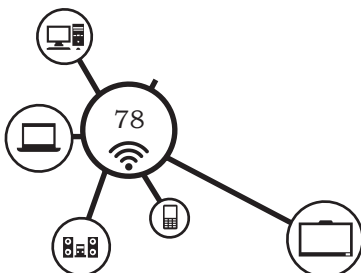
False match and false non-match describe the matching process between a live sample and a biometric template.

Biometric Authentication

Biometrics allow a person to be identified and authenticated based on the biometric data which is unique and specific. Biometric authentication works by comparing two sets of data, the data stored during the enrolment with the live captured data. If the two data are nearly identical, the biometric data is authenticated. The match between the two data sets has to be nearly identical. It is impossible for two biometric data to match 100 per cent.

Verification and Identification

Biometric authentication is used in two ways—to prove who you are and to prove who you are not. It is important to understand the significant difference between verification and identification.



Verification (1:1, matching, authentication)

Verification is the one-to-one process to confirm an individual's claimed identity by comparing a submitted biometric sample to a database of templates. It requires that an identity be claimed, after which the individual's enrolment template is located and compared with the verification template. For example, a user with three enrolled finger-scan templates may be able to place any of the three fingers to verify, and the system performs 1:1 matches against the user's enrolled templates until a match is found. The flowchart shown in Fig. 2.3 illustrates the verification process.

In Aadhaar based biometric attendance system the user first enters his or her Aadhaar number to claim identity and then presents the finger on the sensor. The biometric system first checks whether the Aadhaar number entered by the user is correct or not by checking in the database. If the Aadhaar number does not exist in database then the user is not authenticated itself in the first step. If the Aadhaar number is correct and found in the database then the biometric data is presented to the system and further matching is done with the enrolled template. If the captured data matches with the enrolled template then the person is authenticated as authorised, otherwise if the captured data is not matched somehow then the person is not identified by the system.

Identification (1:N, one-to-many)

It is a one-to-many process of determining a person's identity by performing matches against multiple biometric templates. If it matches with any of the templates then the identity of the enrollee is determined. In an identification application, the biometric device reads a sample and compares that sample against every template in the database. Identification applications require a highly robust and distinctive biometric, otherwise the error rates falsely matching and falsely non-matching users samples against templates cause security problems. There are two types of identification systems—positive and negative identification.

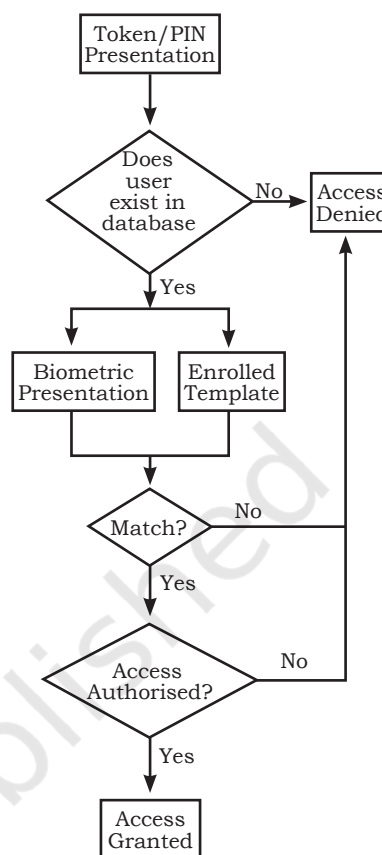
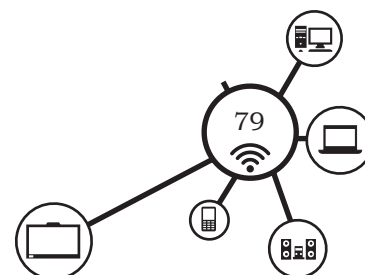


Fig. 2.3: Verification process



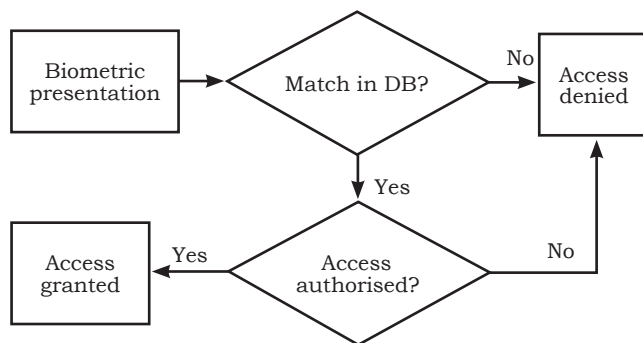


Fig. 2.4 (a): Positive identification

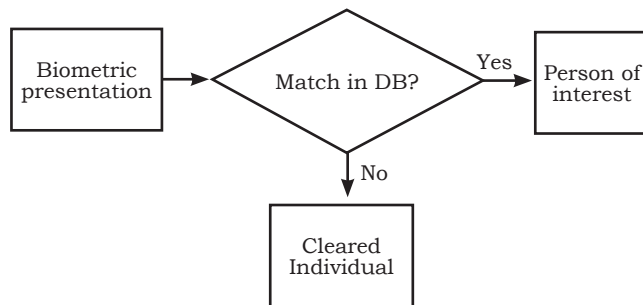


Fig. 2.4 (b): Negative identification

(a) Positive identification systems: are designed to find a match for a user in a database. Positive identification system identify a person based on the match of presented biometric data with the biometric data present in the database. A flowchart for positive identification system is shown in Fig. 2.4 (a).

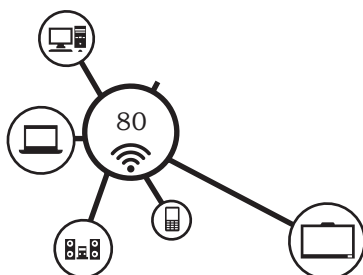
(b) Negative identification systems: search databases by comparing one template against many. It ensures that a person is not present in a database. This prevents enrolling twice in a system. A flowchart for positive identification system is shown in Fig. 2.4 (b).

Difference between Identification and Verification System

All biometric technologies are capable of verification. Identification systems are based on physiological biometrics finger-scan, facial-scan, iris-scan and retina-scan. Identification requires more processing power than verification, as identification systems execute large numbers of matches. In identification systems more comparisons are made because multiple users have similar physiological characteristics. So there are chances of more number of false matches. Identification systems take a longer time to process a request, while verification can take place in seconds or fractions of seconds. It is easy to interact with an identification system since no user ID is required.

Biometrics Technologies and Devices

Every biometric technology uses biometric devices and sensors. Devices and sensors are mechanical or electronic system used to enroll and capture raw biometric samples that can be digitised and converted to



a biometric template. A biometric scanner is an essential part of the biometrics to measure the biological data, such as fingerprint, iris, retina and facial characteristics. The fingerprints biometric technology uses fingerprint sensors to capture the fingerprint, face recognition uses web cam or digital camera to capture the facial image, iris biometric uses iris cameras to capture the iris image, the voice recognition uses microphone to capture voice. Each biometric technology has certain advantages and limitations. A single biometric technology cannot meet the requirement of all the applications. Some of the commonly used technologies along with their devices are explained below.

Fingerprint biometrics

A fingerprint is made of a number of ridges and valleys on the surface of finger that are unique to each human. The uniqueness of a fingerprint can be determined by the different patterns of ridges and furrows as well as the minutiae points.

A fingerprint scanner digitises these images into unique digital templates, which can then be used to match against existing records. Fingerprint biometrics is used in different applications, such as cellphones, laptops and USB flash drives. It is also used in judicial systems record to verify the identity of a person.

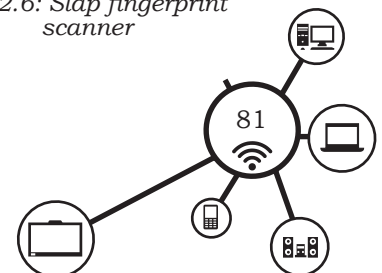
- (a) **Fingerprint Scanner** capture an individual's fingerprint images and translate the images into a digital code. It is made of hard optical sensor, which is resistant to scratches, impact, vibration and electrostatic shock. Fig. 2.5 shows a biometric fingerprint scanner.
- (b) **Slap Fingerprint Scanner** is used to capture all ten fingerprint images including four finger-slaps and thumbs of both the hands. At the time of registration of the fingerprints $4 + 4 + 2 =$ all 10 fingers are fully scanned and stored against the identity of the user. But at the time of verification any one or more of the fingers can be used for verification. Fig. 2.6 shows a slap fingerprint scanner.



Fig. 2.5: Fingerprint scanner



Fig. 2.6: Slap fingerprint scanner



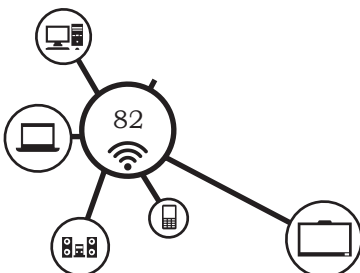
NOTES

There are three types of fingerprint scanners—optical, capacitive and ultrasound, based on the sensor used in the device.

- (i) Optical scanner uses a prism, light source, and light sensor to capture images of fingerprints. It uses prism to measure the distance between the tiny ridges and valleys which form a fingerprint image.
- (ii) Capacitive scanner works by measuring electrical signals sent from the finger to the scanner. Print ridges directly touch the scanner, sending electrical current, while the valleys between print ridges create air gaps. A capacitive scanner maps out these contact points and air gaps and gives an absolutely unique pattern. These are used in smartphones and laptops.
- (iii) Ultrasonic scanner uses high frequency sound wave to read the pattern of fingerprints. Ultrasonic sound waves reflect from the fingertip surface are measured by the sensor and a unique fingerprint pattern image is produced.

Face biometrics

The human face is the easiest characteristic used to identify a person in biometric system. Every individual around the globe has a distinctly unique face. Face recognition technology, is very popular and is used more widely because it does not require any extra hardware except camera and no physical contact is required between the user and device. Facial images are captured using webcam, mobile phone camera and digital SLRs. Digital facial images require resolution of about 60 pixels for one-to-one matching and 90 pixels for more accurate one-to-many matching. A person is identified by analysing the facial characteristics. These characteristics can be derived from either a still or video images. Every face has distinguishing landmarks, such as valleys and peaks. There are about 80 different nodal points on the face, which include distance between eyes, nose, mouths, ears, jaw, size of eyes, mouth, jawline



length, distance between eyes, cheekbone shape, nose width and others expressions. When the nodal points are measured, a numerical code is created, which is known as a faceprint. The faceprint is used in the database to compare the face to other 2D images to accurately identify the person. Fig. 2.7 shows the example of face-scan.

- (a) **Face Scanner** identifies a person by taking measurements of a human face. For example, the distance between the person's chin and pupillary of eyes, nose, ear and mouth. These types of scanners are secure, assuming they are smart enough to distinguish between a picture of a person and a real person. Fig. 2.8 shows a biometric face scanner.

Eye biometrics

The eye is one of the most reliable body parts for biometric authentication. Iris and retina are commonly used in eye biometrics. These are highly unique features that allow highly accurate biometric matching.

- (a) **Iris Recognition** is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irises of an individual's eye. It focusses on the unique pattern of iris of the eye to uniquely identify a person. The human iris, as shown in Fig. 2.9, is a thin circular structure in the eyes, which is responsible for controlling the diameter and size of the pupils. There are several colours for iris, such as brown, green, blue, grey, violet, which decides eye colour of individual. The iris also has its own patterns, which differs from person to person and this makes it unique for each individual.
- (b) **Iris Scanner** is a biometric device used for a real-time identification process with higher performance and greater accuracy. The iris scanner captures images of one or both of human irises to compare and match it with the existing iris pattern of an individual saved in the database. It uses pattern recognition

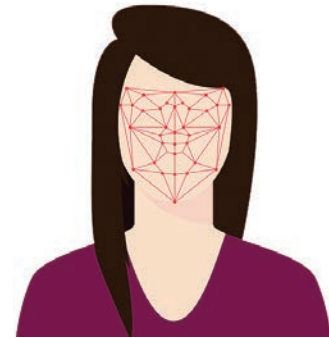


Fig. 2.7: Example of face recognition scan



Fig. 2.8: Face Scanner (webcam)

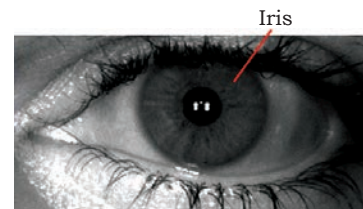


Fig. 2.9: Human iris

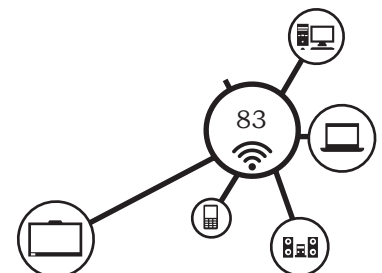




Fig. 2.10: Dual iris scanner

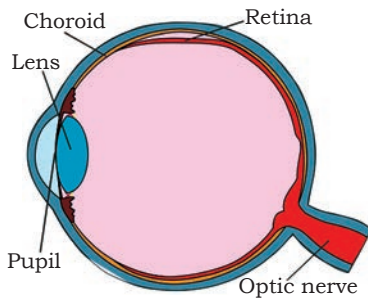


Fig. 2.11: Retina



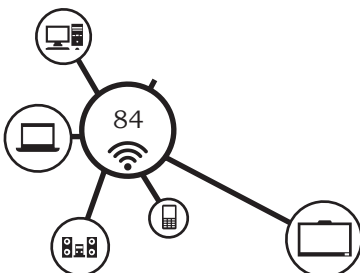
Fig. 2.12: Biometric retina scanner

techniques to identify and authenticate a person's identity. The high resolution images taken by the iris scanners are passed through a biometrics system with software to match the iris to the person. Iris and biometric retina scans are different. Retina scanners use similar scanning camera technology. The iris is the coloured portion of the eye. Special camera techniques create images of the iris, converts them into mathematical representations so that an individual can easily be identified. Most scanners are of high quality and will not be affected by the use of contact or glasses. Fig. 2.10 shows a biometric iris scanner.

- (c) **Retina Biometrics** include only the retina of the eye. The human retina is a thin tissue composed of neural cells that is located within the posterior part of the eye as shown in Fig. 2.11.

The network of blood vessels within the retina is so complicated that even identical twins have different comparable sample. Retina-based technologies are primarily used for access control in high security environments.

- (d) **Retina Scanner** is a biometrics security device that is designed to capture retina samples. Retinal scanners use infrared light to capture the retina's blood vessels in the retinal tissue inside the eye and their unique pattern. The samples captured undergo various processes, including identification, authentication and verification. The unique patterns of the retina cannot be duplicated. The false acceptance and rejection rates are much lower than the fingerprint scanners. Retina scanners are different from iris scanners and are quite expensive. It is very difficult to replicate or forge retinal patterns. Fig. 2.12. shows a biometric retina scanner.



Palm vein biometrics

Palm vein recognition is one of the recent and most secure biometric technology. Veins are blood vessels located inside the human body that carry blood to the heart. Vein recognition systems mainly focus on the veins of hands. The veins on human hand has own physical traits. The vein recognition system capture images of the vein patterns inside the fingers by applying light transmission to each finger. The method works by passing near-infrared light through fingers and a camera can record vein patterns. This pattern is recorded and stored in an encrypted format in a database, as a reference for future comparison. Vein recognition systems has higher level of accuracy and low cost on installation and equipment. It takes less time of about half second to verify each individual.

(a) **Palm vein scanner** is a palm-vein based authentication system. Palm vein scanner captures the image of an individual's vein pattern. The biometric vein pattern obtained is then verified against a pre-registered pattern of a vein to verify an individual. Fig. 2.13 shows a biometric palm vein scanner.



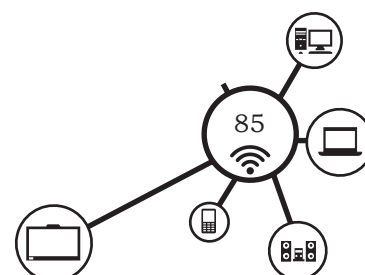
Fig. 2.13: Biometric palm vein scanner

Voice biometrics

Voice is one of the most commonly used biometrics today. Voice recognition systems validate an individual's claimed identity by using certain characteristics extracted from voice. This technology focuses on unique vocal features—voice tract and accent. These characteristics create the voice biometric to verify each person's identification using only their voice. Voice technologies measure a person's vocal tract and/or speech patterns to create a digital signature, which is matched against known records. Voice biometrics is also dependent on capture environment as facial biometrics. The background noise can interfere with the capture and matching process. Voice recognition systems are easy to install and it requires a minimal amount of equipment. This equipment includes microphones, telephone and/or even PC microphones. Fig. 2.14 shows biometric devices for voice recognition.



Fig. 2.14: Biometric devices for voice recognition



Practical Activity 1

Face recognition

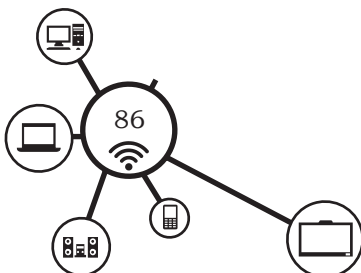
Material required

Face photos, writing material

Procedure

1. Conventionally people recognise the faces by observing key features of the faces, such as size of the face, shape of the face, skin colour, eyes, nose, lips and hair on the face.
2. You have been provided with four different faces as shown below. We can easily distinguish them based on the various features as given in the table.

	<p>Turban on head Long beard, moustache Dark complexion Wide nose</p>
	<p>Cap on head Long moustache Dark complexion</p>
	<p>Little hair on head Long moustache</p>
	<p>No hair on head Wearing spectacles Clean shaven face Smiling</p>



Digital Devices used in Biometrics

(a) **Handheld Scanner** is a small manual scanner, which is moved over a object to be scanned. It requires to keep your hand steady while scanning. Even a slight movement of hand can lead to distortion of the image. The barcode scanner is a common example of handheld scanner used in shopping stores. Handheld scanner is also called portable scanner as it can be easily carried one place to another. Fig. 2.15 shows a handheld scanner.



Fig. 2.15: Handheld Scanner

(b) **Digital Camera** is used to capture facial photograph in a digital format. It is connected to a laptop or desktop computer through the USB (Universal Serial Bus) port. The digital camera consists of an auto-focus lens and the mounting base. The lens is able to focus the person's face automatically. The mounting base helps to fix the camera on the laptop or desktop. It displays images immediately after capturing them. Fig. 2.16 shows different parts of a camera.



Fig. 2.16: Digital Camera

A digital camera has the following specifications:

- **Resolution** a photograph is made up of a large number of 'dots' or 'pixels'. Resolution depends upon the number of 'pixels'. Higher number of pixel means greater detail view and therefore better quality of photographs.
- **Aperture** is the size of the opening, which permits light to enter the camera and fall on the image sensor. The aperture size can be adjusted manually or automatically depending upon the type of camera. The adjustment will depend upon the amount of light falling on the person or the object being photographed.
- **Shutter Speed** determines the time duration for which the aperture is open.
- **Focal Length** is the distance between the lens and the surface of the image sensor. The focal length determines the magnification or 'zoom' of the image.

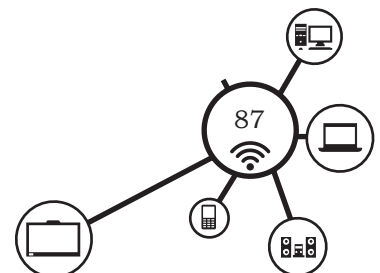




Fig. 2.17: Webcam



Fig. 2.18: Pixels in an Image

(c) **Webcam** is an external device and it captures images up to 30 frames per second. Webcam is very popularly used in biometric data applications, such as preparation of Aadhaar card and preparation of identity card. Fig. 2.17 shows a webcam.

Concept of Pixel and Resolution

The smallest unit of a digital image is called pixel. More number of pixels means higher resolution that creates a high quality image. The normal digital cameras available in the market have resolution around 20, 16 and 14.1 mega pixel, where 1 megapixel is equal to 1 million (1000000) pixels. Resolution is the number of pixels contained in an image. Resolution is expressed in terms of the number of pixels on horizontal axis and vertical axis. The sharpness of an image depends on the resolution. Fig. 2.18 shows pixels in an image.

Practical Activity 2

Identify and name the various parts of a digital camera

Material required

Digital camera, writing material

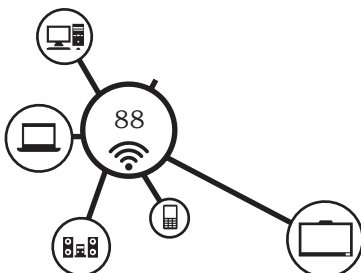
Procedure

1. Carefully observe the various parts of digital camera, such as camera lens, mirror, power switch, power lamp, battery slot, card slot, main dial, shutter button, focal plane mark, lens release button, lens mount index, flash and red eye reduction lamp
2. Draw and label the various parts of a digital camera in your notebook as shown in Fig. a below.



Fig. (a)

DOMESTIC BIOMETRIC DATA OPERATOR – CLASS XI



Integrated Biometric Machine

The biometric devices explained above are stand-alone devices and they work when connected to the system. The integrated biometric machines, such as integrated fingerprint and iris machines are used for biometric attendance. These machines work on the tablet with Android operating system and provide a user-friendly environment to the customers. The integrated biometric machines used in various organisation are explained below.

Punching machine or biometric attendance machine

Fingerprint attendance machine is a part of biometric revolution. A fingerprint attendance machine analyses several fingerprint patterns for matching purpose. Finger punching attendance machine has a sensor to capture digital reflection of fingerprint prototype. The captured reflection is called live scan. Finger punching attendance machine first captures the image of the fingers through the sensors and then matches the image with previously enrolled fingerprint templates. Biometric time and attendance systems are popular in the business world to track employees and their attendance. It is easy to use, install and track data regarding employees. The biggest advantage of these systems is that they prevent employees from clocking in for one another.

During the punch, the machine displays the employee name, ID and verifies the correct punch and thanks the person for the punch.

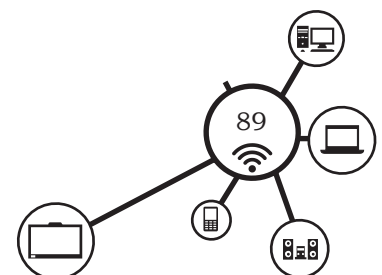
Fingerprint based biometric attendance device

This device is used to capture the fingerprints, authenticate and record the date and time of entry. These devices are used in office premises, industry, college and schools to monitor the attendance of human personnel (Fig. 2.19).

Basically the scanner in this device consists of a master data of fingerprints of all the human personals working in the organisation. Whenever a person scans



Fig. 2.19: Android based biometric attendance system



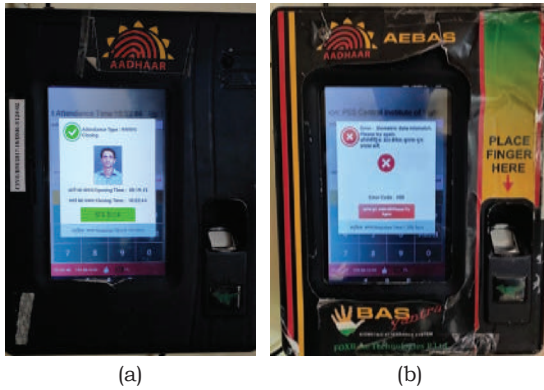


Fig. 2.20: Photographs of (a) matching and (b) non-matching



Fig. 2.21: Biometric LAN based fingerprint device



Fig. 2.22: Integrated fingerprint biometric machine

his or her fingers then that image is identified or verified among the images that are already stored on the devices. If the image is matched with any one of the images of master data then the corresponding ID is retrieved and displayed on the screen of the device. If it is not matched then the user is prompted to scan the image again. Also, accordingly the corresponding audio message is also generated by the device.

There are some other fingerprint devices also available that can be used for biometric identification. These devices are embedded devices that contain all related hardware and software like keyboard, scanner, motherboard, SMPS, and display. An image of such a device is given in Fig. 2.21.

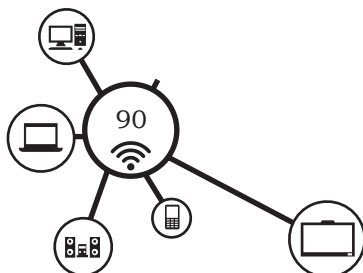
In early days most of these devices needed local area network (LAN) connection to send the data. But most of the modern devices are wireless devices and they do not require any wired connection. These devices can operate on mobile operating systems, such as Android or iOS.

Integrated fingerprint biometric device

In early days most of these devices needed local area network (LAN) connection to send the data. But most of the modern devices are wireless devices and they do not require any wired connection. These devices can operate on mobile operating systems, such as Android or iOS.

The typical specifications of integrated fingerprint biometric device are as following:

Parameters	Specification
Display	7 inch TFT LCD
Processor	1.3 GHz Quad Core, 64bit
RAM	2GB RAM
Memory	8GB with Expandable up to 32GB
OS	Android 8.1 GMS



Display Resolution	1024 × 600 Pixels
Audio Jack	Yes
Ports	Micro USB v2.0 Port - 1nos. (With OTG Support) or One Micro USB v2.0 Port and One Round Pin Charger Connector
Wi-Fi	802.11 b/g/n 2.4GHz
Bluetooth	Bluetooth Classic
SIM Slot	Dual SIM Card
GPS	GPS/AGPS
Camera	5MP Autofocus Rear Camera with LED
Baseband Version	MOLY.LR9.W1449.MD.LWTG.MP.V190, 2018/06/13
Battery	3500 mAh
Certification	ISO Compatible Fingerprint Templates and Images ANSI Compatible Fingerprint Templates and Images 500 DPI STQC/Aadhaar Approved Fingerprint Sensor CE, IEC60950, RoHS Certified Fingerprint Sensor
Connectivity	GPRS/EDGE Enabled, 2G, 3G, 4G, GPS
Acceptance and Rejection Rate	Lower FRR and FAR

NOTES

Fingerprint scanner

Parameters	Specification
Fingerprint Sensor	Optical (Scratch Free Sensor Surface)
Image Resolution	500 DPI / 256 Gray
Sensing Area	15 × 17 mm
FAP	FAP10

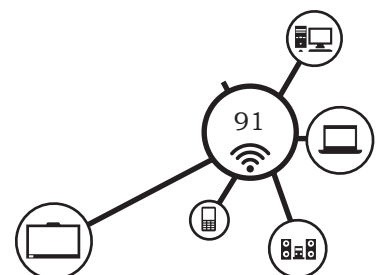




Fig. 2.23: Integrated iris scanner

Integrated IRIS scanner

Integrated Iris scanner working on tablet with Android Operating system provides a user-friendly iris recognition of users. It scans the iris and access card in one machine. Iris scanner is the safest identity recognition technique that scans the iris of an individual's eye. Integrated iris sensor renders high-level security and greater customer experience. Fig. 2.23 shows the integrated iris machine.

The specifications of integrated iris machine is given below.

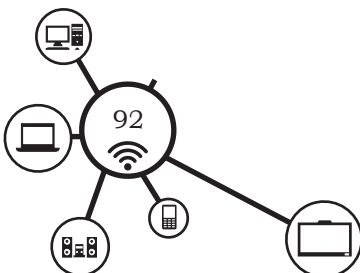
Processor	1.2 GHz Quad Core
Display	7 inch or higher; 1024x600 resolution
Memory	Internal memory 8 GB RAM 2 GB
Connectivity	Wi-Fi 802.11 b/g/n Bluetooth v4.0 Single SIM with 4G support (Bands - LTE 850 (5), LTE 1800 (3), LTE 2100 (1), LTE 2300 (40))
Audio	Microphone with High Amplitude Speakers
Camera	Rear Camera with auto focus and 5 MP resolution, LED flash
Location Technology	GPS
Battery	6000 mAH

Selection and Configuration of Biometric Devices

Before using any biometric device one needs to select an appropriate device.

1. Number of users of the device
2. Wired or wireless connectivity
3. Number of transactions to be stored offline
4. Device type embedded or android

Selection of the biometric device depends upon the number of users of the device. Many organisations may have less than 500 human resources. In such a case the device may be selected that can handle a data of 500 people. Generally, these machines comes with a user capacity of 500, 3000 and 5000. If there are more number of users then the memory capacity of the device must be



enhanced. In a large organisation, the organisation needs to maintain more number of machines instead of a single machine with a large number of user capacity.

While selecting the biometric device one needs to understand the availability of wired or wireless network connection. A wired connection means Internet connectivity. Wireless connection may include Wi-Fi Internet connection and GPRS (Global Packet Radio Service). Many times people prefer wireless connection over wired connection.

The device selection is also based on whether the device is stand alone or cloud-based device. Stand alone devices are connected to the local server through LAN or through Wi-Fi of organisation. On the other hand the cloud-based devices are connected with the cloud server through LAN or Wi-Fi or GPRS. These devices essentially require Internet connectivity to communicate with cloud server.

The device selection can also be based upon the number of transactions that can be stored in the device memory, when the device goes offline. For example, a typical device may store only about 52,000 attendance transactions. If the transactions cross this limit then it may not able to store further and the data may be lost.

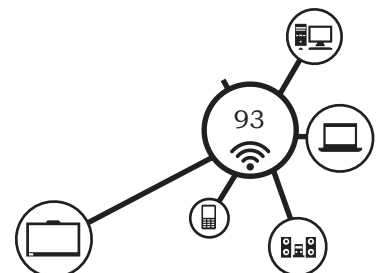
In modern android based devices this capacity can be up to 10 lakh attendance transactions and it can even be enhanced further by increasing the memory limit of memory card.



Fig. 2.24: LAN-based biometric device

Specification of LAN Based Biometric Device (BioSentry ETH 500/2000 User)

The specifications of a LAN based biometric device and android-based biometric device are given in Table 2.2. Observe that specifications include sensor specifications, human interface and working environment specifications. It also includes enrolment data limitations. These specifications are useful for selection of devices.



NOTES

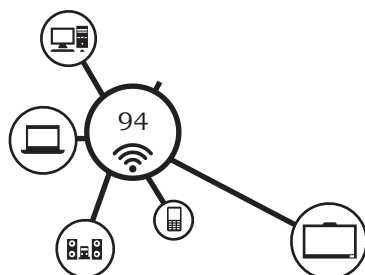
Table 2.2: Specifications of LAN-based Biometric Device

Description	Specification
Fingerprint Sensor	
Resolution	500 DPI with 14 × 22 mm Sensor array
Scanner	Optical (Sagem CBM Sensor)
Matching	1:N
Verification speed	<1.5 seconds
False Acceptance Rate (FAR)	0.0001%
False Rejection Rate (FRR)	0.001%
Image Quality	Distortion Free Images Resistance to Various Contaminants like sweat, dirt, wet finger
Human Interface	
Display	16 Characters 2 Lines Monochrome LCD Display, with Activity LEDs
Audio	Beeper with 5Khz frequency
Keyboard	13 Touch Keys
Connectivity	Connectivity over 10 base T Ethernet 10 MBPS
AC Input Storage	230 VAC 50 Hz
Enrolled Data	Upto 500 / 2000 person with two fingers each.
Transaction Data	Upto 51,000 records (non Volatile Flash memory)
Environment	
Temperature range	0°C to 60°C (Storage) 5°C to 47°C (Operating)
Humidity	Under 90%RH
Dimensions	150 mm x 200 mm × 80 mm
Weight	2.00 kg

Specifications of Android-based Biometric Device

Description	Specification
Processor	1.2 GHz Quad Core
Network Support	RJ 45 Ethernet 100/1000 MBPS
Display	7 inch; 800×600 resolution, with capacitive touchpad
Sound	3.5mm ear jack
Memory	4 GB with expandability up to 32GB RAM – 1GB

DOMESTIC BIOMETRIC DATA OPERATOR – CLASS XI



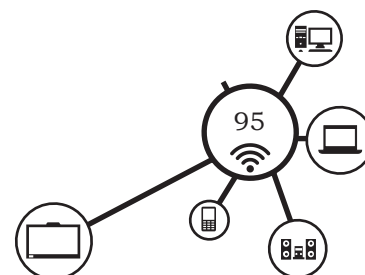
Connectivity	Wi-Fi 802.11 a/b/g/n (Optional) Micro USB v2.0 port – 1 Nos.(With OTG Support)
Camera	Front – 5MP with Auto Focus Feature
Audio	Microphone with High Amplitude Speaker (OPTIONAL)
Operating System	Android 4.2. xx above
Battery	6-8 hours
Biometric Sensor	SagemMorpho CBM E2, STQC Certified, 500 DPI, High Quality Optical.
Warranty	1 year (ex-factory).

Fingerprint Device Performance

Fingerprint device performance can be judged by using various parameters, such as interface, operating systems, framework, fingerprint sensor and sensor technology. The values of these parameters are shown in the Table 2.3.

Table 2.3: Parameters for Fingerprint Device Performance

Parameter	Values
Interface	USB 2.0 full speed
Operating Systems	Windows 7, Windows 10
Windows Biometric Framework (Windows 7 Plug and Play)	Yes
Fingerprint Sensor	AES2550 AuthenTec slide sensor
Sensor Technology	Trueprint® Subsurface RF Technology
Image Resolution	500 pixels per inch
Image Area	9.75mm × 0.41mm/ 192 × 8 pixels
Surface Coating	Scratch Resistant Withstands more than 10 million rubs Advanced 6-H hardness durability coating



Practical Activity 3

Scan fingerprint using biometric device

Material required

Biometric device, writing material

Procedure

1. Acquire live sample from candidate using sensors.



2. Extract prominent features from sample using processing unit.



3. Compare live sample with samples stored in database using algorithms.
4. Present the decision. Accept or reject the candidate.

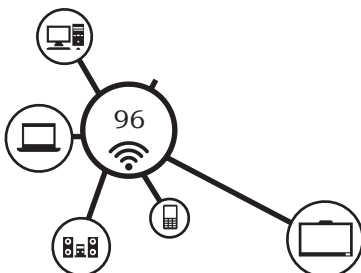
Practical Exercise

1. List different types of biometric devices and the corresponding data that can be collected by using them.
2. Go to Aadhaar card centre and observe how biometric devices are used to capture biometric data.

Check Your Progress

A. Fill in the blanks

1. A biometric device is a (an) _____ device.
2. Palm of the hand of a person is identified by using _____ device.
3. Iris of a person is identified by using _____ device.
4. BAT stands for _____.
5. The electronic device to register the digital image of the fingerprint pattern is known as _____.
6. Visible pattern is captured and then turned into electrical signal by using _____ sensor.



7. Optical sensor consists of array of _____.
8. Modern fingerprint sensors makes use of _____ or _____ optical imagers.
9. Photographic print images can be digitised by using _____ device.
10. In shopping stores, valuation of goods is normally performed by using _____ device.
11. A film scanner is used to scan _____.
12. The coloured ring of the eye muscle is called _____.
13. The smallest unit of the digital image is called _____.
14. Resolution of camera is expressed in terms of _____ on horizontal and vertical axis.
15. The sharpness of the image is determined by its _____.
16. Camera's with a resolution of 10 megapixel have _____ x _____ pixels.
17. Sensitivity of the digital camera is measured in terms of _____.

B. Multiple choice questions

1. A fingerprint device's performance is judged by using which of the following parameters?

(a) Audio	(b) Display
(c) Sensor technology	(d) Temperature range
2. Android-based biometric device has _____ connectivity.

(a) USB port	(b) Wi-Fi
(c) Both (a) and (b)	(d) wired
3. A typical false acceptance rate of biometric attendance system is _____.

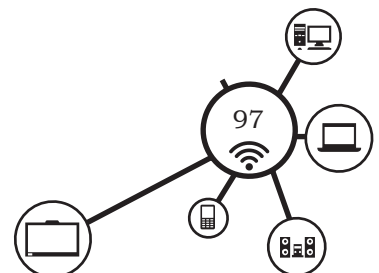
(a) 10%	(b) 50%
(c) 100 %	(d) .0001%
4. Which of the following is not a part of digital camera?

(a) Power button	(b) Lens
(c) Shutter button	(d) DSLR
5. On drones and bicycles the camera that can be attached is called _____.

(a) action camera	(b) 360 camera
(c) film camera	(d) DSLR
6. Full circle panoramic photos and videos can be obtained by using which of the following cameras?

(a) Action camera	(b) 360 camera
(c) Film camera	(d) DSLR
7. The image quality is highest in _____ camera.

(a) action	(b) 360
(c) film	(d) DSLR



NOTES

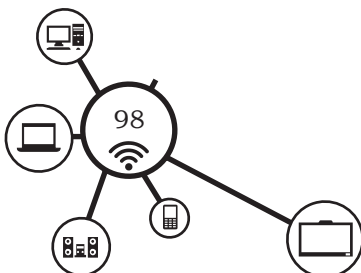
8. Red eye correction and white balanced feature is available in which of the following devices?
(a) Fingerprint sensor (b) Slap scanner
(c) Digital camera (d) Printer
9. The close look of the subject when they are physically far away can be obtained by using _____ feature.
(a) red eye correction (b) zoom
(c) image stabilisation (d) noise reduction
10. The document can be fed in case of horizontal or vertical slot in _____ scanner.
(a) sheet feed (b) hand held
(c) drum (d) photo

C. State whether the following statements are True or False

1. Fingerprint scanning system is being used in India since 1897.
2. A biometric device is a security identification and authentication device.
3. Face scanner identifies a person without measuring the person's face.
4. In an iris scanner an iris code is generated.
5. CCD detectors are not sensitive to low level of light.
6. Sensors using capacitive sensors are large in size.
7. DSLR means Digital Soft Lens Reflex.
8. Most of the digital cameras are water resistant.
9. Android-based biometric device makes use of an android operating system.
10. The minimum size of an image in fingerprint device is 192×8 pixels.

D. Short answer questions

1. Describe the process of fingerprint scanning.
2. State the parameters to judge the performance of a fingerprint device.
3. List any five specifications of biometric attendance device.
4. List the commonly used biometric devices.
5. What is a scanner? State their different types along with uses.
6. Explain the concept of pixel and resolution.
7. State any four features of a digital camera.
8. How can iris and fingerprint of a person be used for authentication?



SESSION 2: SETTING UP BIOMETRIC DEVICES

Suppose you are in a school computer lab. You will find many computer systems in a proper arrangement similarly biometric devices also need space as well as software for configuration. Biometric recognition devices need software and correct installation to run. This session will cover different types of biometric devices, such as iris scanner and fingerprint scanner.

Setting Up Various Components of Biometric System

Various biometric devices need to be connected to the computer system. After connecting in appropriate slot we need to install them on computer system by using the appropriate device drivers.

Steps for connecting and installing fingerprint scanner, web camera, iris scanner and GPS device have been illustrated below.

Connection of fingerprint scanner device

Step 1: Plug in the cable of the fingerprint device into the port as shown in Fig. 2.25 below.

Step 2: Connect one end of the data cable to the fingerprint scanner device as shown in Figs. 2.26 and 2.27.

Step 3: Observe that now this fingerprint scanner device is connected to the computer system as shown in Figs 2.28, 2.29 below. But it can be used only after its installation by using device driver.



Fig. 2.25: Plug-in cable of device into port



Fig. 2.26: Connecting data cable to scanner device



Fig. 2.27: Data cable of scanner device



Fig. 2.28: Connecting fingerprint scanner to computer through USB connector



Fig. 2.29: Fingerprint scanner connected and ready to capture biometric data

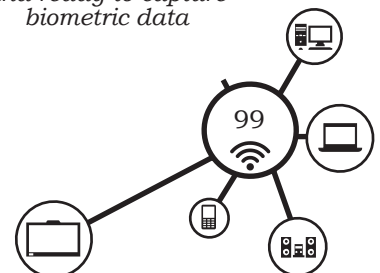




Fig. 2.30: Connecting web camera to computer system through USB connector

Connection of webcam to the computer system

Step 1: Plug-in the cable of the web camera device to the computer system through USB connector as shown in Fig. 2.30.

Step 2: Observe that now this web camera is connected to the computer system as shown in Fig. 2.31 below. Note that the web camera is plug and play device. It can be directly used once it is connected to the system.



Fig. 2.31: Web cam connected to computer and is ready to capture your photo



Fig. 2.32: Connecting iris eye scanner to computer system through USB connector

Connection of iris scanner to the computer system

Step 1: Plug in the cable of the iris scanner to the computer system into the USB port as shown in the Fig. 2.32.

Step 2: Observe that now this iris scanner is connected to the computer system as shown in Fig. 2.33. It can be used only after its installation by using device driver.



Fig. 2.33: Iris scanner connected to the computer and is ready to capture iris



Fig. 2.34: GPS Device

Connection of Global Positioning System (GPS) device to computer system

Step 1: Plug in the cable of the GPS device to the computer system through USB connector as shown in Fig. 2.35.

Step 2: Observe that now this GPS device is connected to the computer system as shown in Fig. 2.36. Note that the GPS device is plug and play device. Therefore, it can be directly used after connection.



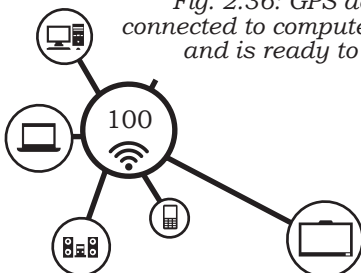
Fig. 2.35: Connecting GPS device to computer system



Fig. 2.36: GPS device connected to computer system and is ready to use

Installation of biometric devices

Installation of biometric devices consists of connecting the devices to the appropriate port and installation of their device driver software. Some devices are plug and play and they do not require installation of the device driver. In Aadhaar based biometric system,



you have to install the software Aadhaar Enrolment Client (AEC) along with the various biometric devices, such as fingerprint scanner, iris scanner, webcam, and 36 GPS device. After installing the AEC software and connecting the biometric devices, the connected devices will appear on the taskbar as shown in the Fig. 2.37. Observe that the biometric devices indicated by a red mark are not attached to the computer system. The printer does not show a red mark since it is attached to the computer.



Fig. 2.37: Active and deactivate biometric devices

Installation of device driver software

Since various companies are manufacturing the biometric devices, they supply its respective device driver along with the device. Install the device driver software of the respective biometric device supplied by the vendor. The installation of device driver software of iris scanner is illustrated below.

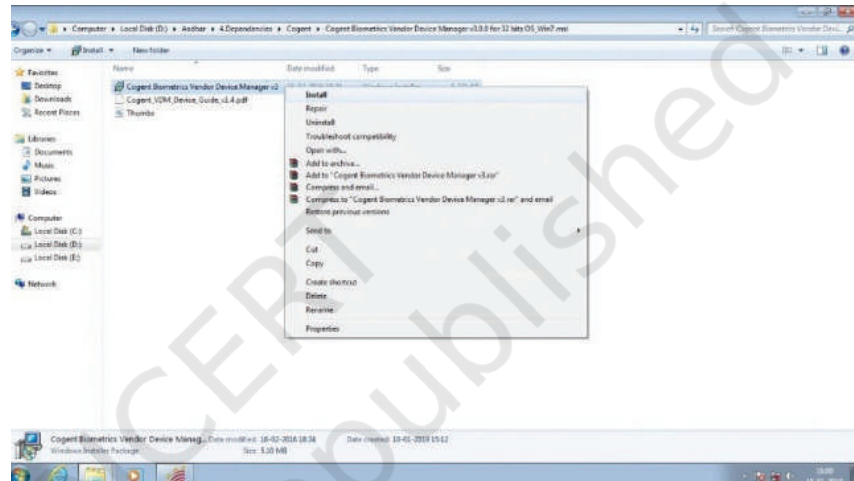


Fig. 2.38: Installing the device driver

Step 1: The device driver software is available on the company's website or it can be supplied in the media, such as DVD or USB drive. To install the software insert the driver media and search for the executable file. This example you will find the file Manager v2.4.0.msi to install the iris scanner.

Step 2: Run the executable file either by double-clicking on the file Manager v2.4.0.msi or by right clicking and selecting the install option as shown in Fig. 2.38.

Step 3. The Biometrics Vendor Device Manager Setup window will be displayed as shown in Fig. 2.39.

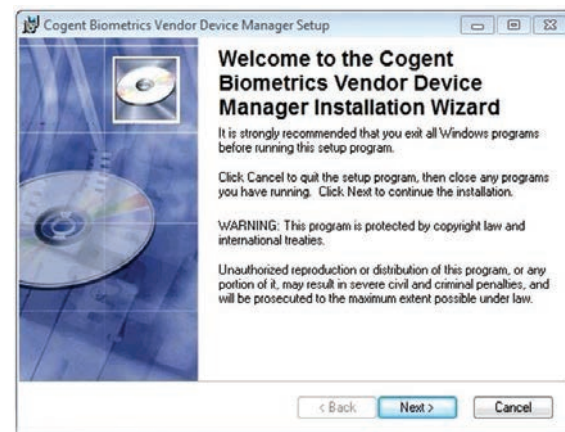
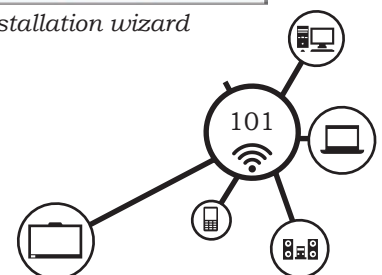


Fig. 2.39: Setup installation wizard



Step 4. Click on the Next button to proceed installation. The user information window will be displayed as shown in Fig. 2.40. Enter the user information, such as Name and organisation and click on the Next button.

Step 5: Select the location to install the driver software. By default it gets installed in Program Files. Click on Browse button to change the location if required.



Fig. 2.40: Entering user information

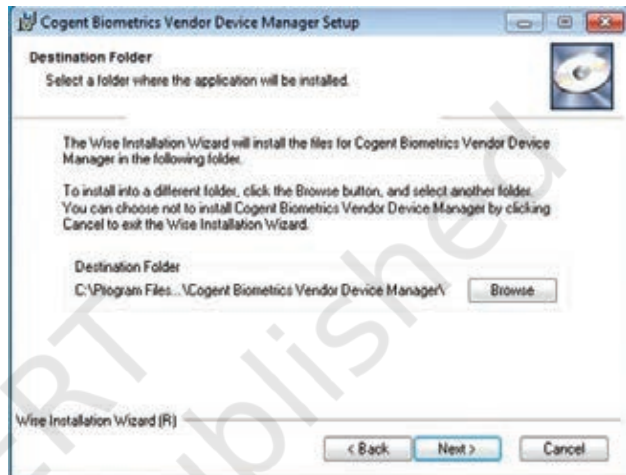


Fig. 2.41: Choosing destination folder

Step 6: Click on Next button to start the installation. The Ready to Install the Application window will be displayed as shown in Fig. 2.42.

Step 7: The files of device driver starts copying as shown in Fig. 2.43.

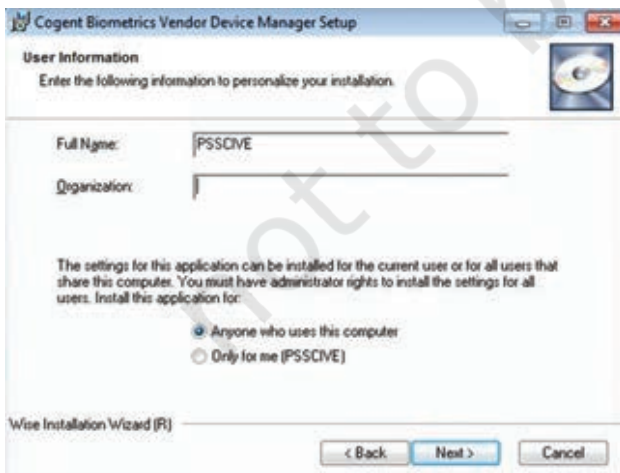


Fig. 2.42: Ready to install the application

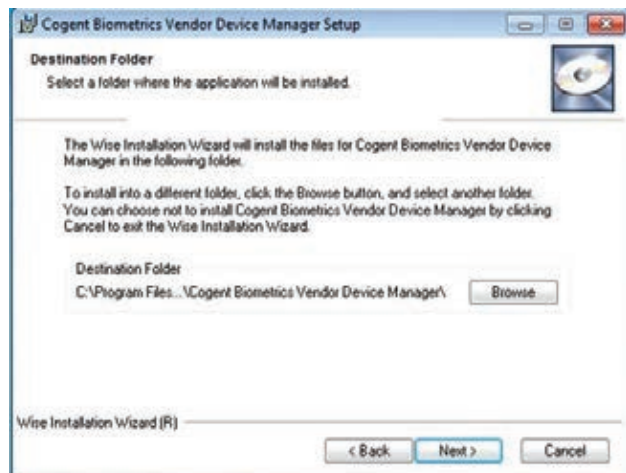
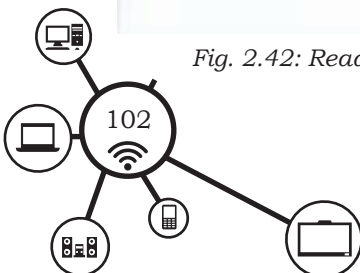


Fig. 2.43: Copying files and updating system



Step 8: Click on 'OK' and click on 'Finish' button to complete the installation.

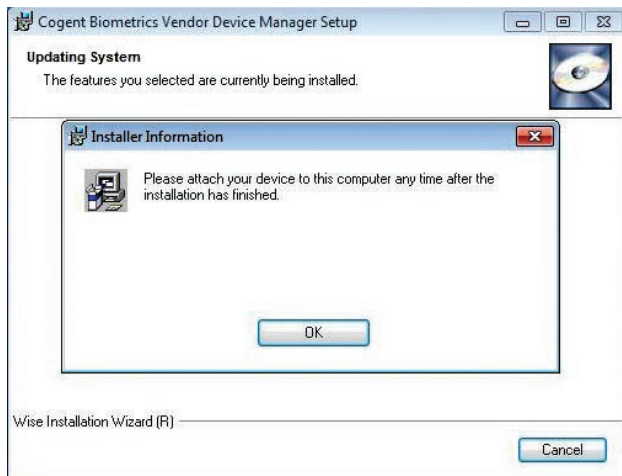


Fig. 2.44: Attach device to the system

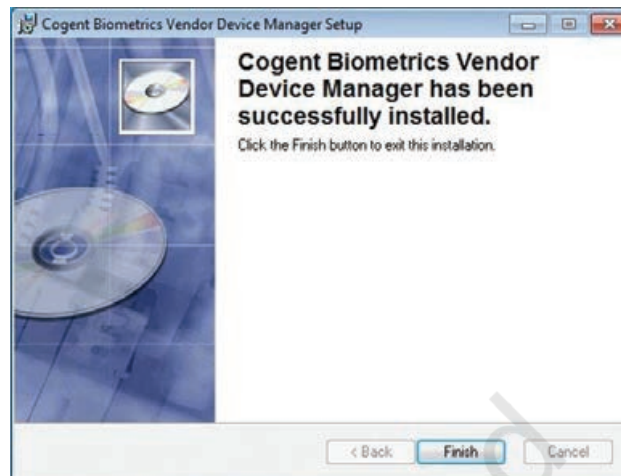


Fig. 2.45: Setup successful installation window

After installing the driver of these biometric devices, observe the taskbar of Aadhaar Enrolment Client (AEC) as shown in Fig. 2.46. Observe that the red mark will disappear for all those devices whose driver has been installed.



Fig. 2.46: Active biometric devices

Configuration of Scanners

To install the scanner also you need to attach the scanner to the appropriate port of the computer system and install its device driver. The device driver of the scanner normally available with scanner device itself or it can be downloaded from the website of that company. The following steps along with the screenshots of installation as shown in Figs 2.47 to 2.49 will illustrate the process of installation of scanner under Windows operating system.

Step 1: Click Start on the lower left corner of your computer screen as shown in Fig. 2.47.

Step 2: Select Devices and Printers from the popup list. A new window will open as shown in Fig. 2.48.

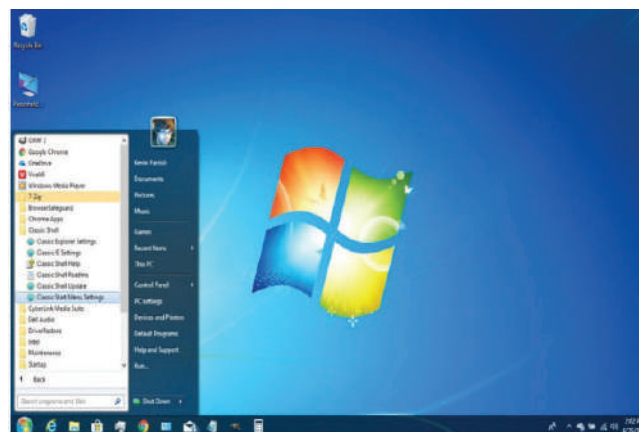
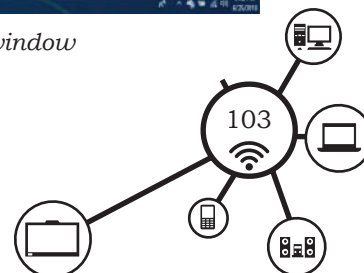


Fig. 2.47: Start window



- Step 3:** Right click on the scanner that you want to configure. A drop-down menu will appear.
- Step 4:** Select Printer Properties from the drop-down menu. A dialog box- Printer Properties will open. This is where you can configure ports, update drivers and customise your hardware options.
- Step 5:** Click the Ports tab from the list of tabs at the top of the box.
- Step 6:** Click on the Configure Port button.
- Step 7:** Configure the options according to your needs.
- Step 8:** Click OK to save your configuration choices.

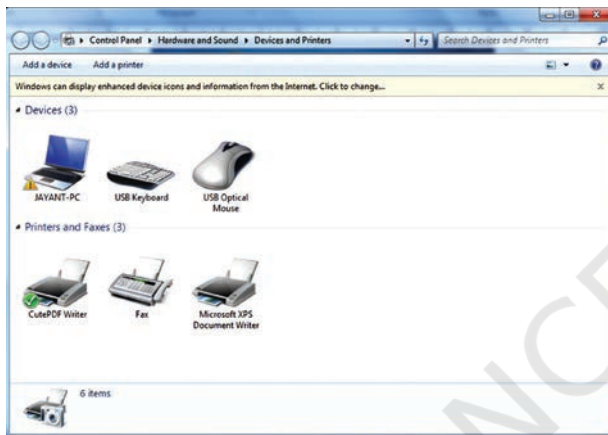


Fig. 2.48: Select devices and printers



Fig. 2.49: Select printer properties

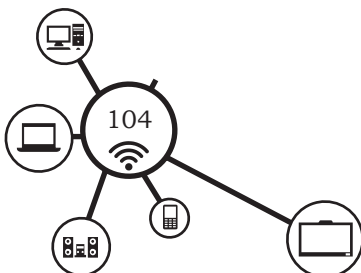
Installation of Biometric Attendance Device

There are various types of integrated devices for biometric attendance system. Here we will discuss basically two types of devices—one is LAN based and another is android based integrated biometric device. These devices are normally available in box packaging. Follow the steps given below, for proper installation of the device.

Steps of installation

Step 1: Unboxing of the device and identification of various accessories of the devices.

The following accessories are normally enclosed along with biometric device.



LAN based biometric device

- Biometric device
- Wall mounting bracket
- USB cable
- USB dongle
- Screw set
- Device driver media

Android based biometric device

- Biometric device
- Wall mounting bracket
- Power adaptor
- Screw set

Step 2: Wall mounting of device

1. Fit the bracket at an appropriate height so that one can easily scan their finger on the scanner of the device.
2. Also check the electrical connections and appropriate earthing as per the standards mentioned below.
 - Input Voltage must be 220–240 V AC
 - Voltage between earth and neutral point should be less than 5 V AC
 - Voltage between live and earth point should be 220–240 V AC
3. If the voltages are not as per the standard, then get the earthing done appropriately before connecting the device, otherwise there are chances that the device may get damaged.
4. In case at remote places there is no and input and AC power is not available then devices can be used with battery backup.
5. Fix the bracket on the wall and attach and screw the device.
6. Care should be taken about the location of the device so that it is not exposed to the rain, heat or sunlight. Normally these devices are placed at the entry gate.

NOTES

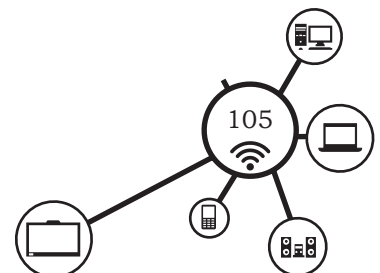




Fig. 2.51: Wall mounted biometric LAN based fingerprint device



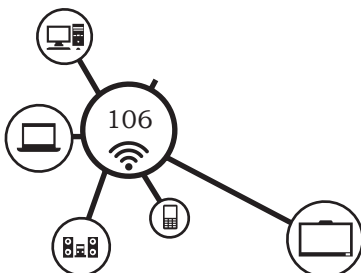
Fig. 2.52: Wall mounted android based fingerprint device

Step 3: Plugging and configuration of the device. Plug the device to the socket of the input power and press the power button ON. If the device is working then it will start and display date and time as shown in Figs 2.51 and 2.52.

(a) LAN based configuration

In case of LAN based device connect the LAN cable to LAN socket. Assign the network IP address, subnet mask and gateway address to the device by the prescribed process of the device as given in the user manual. The configuration of typical LAN based biometric device is illustrated below.

1. After pressing CLR button you will get a message on the device LCD to type password.
2. Type password from the keyboard or refer to the user manual.
3. After typing password press IN Button to get inside the device configuration.
4. You will see option of SET IP Address. To set IP address you have to again press IN button.
5. Now Type IP address as desired and to save press IN button. For example, the IP address can be 192.168.0.56
6. To exit the IP Address Setting Press OUT Button and simultaneously Press Clear Button.
7. Now to Set Subnet Mask of device, Press OUT Key Simultaneously, press 2 key from numeric pad.
8. Then, you will get an option of Set Subnet Mask, now to set subnet mask press IN button and enter the desired subnet mask. For example, the subnet mask to be entered can be 255.255.255.0.
9. To save subnet mask press IN Button
10. To get out of Subnet Mask Setting press OUT Button and simultaneously press Clear Button.
11. Now if you want to check what is Subnet Mask and IP address of device, you can go to display



settings option by pressing OUT Key and scrolling by pressing simultaneously '2' key from numeric pad.

The above process of configuring the device can also be done by using configuration utility given by the company on computer connected to network.

For the data flow upstream and downstream the recommended port must be open in the network. For example, the recommended UDP ports can be 2002, 2003 and 2005.

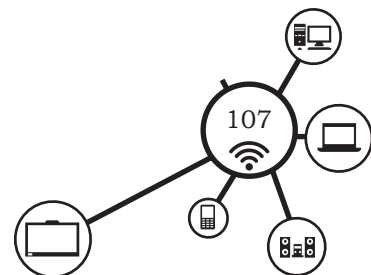
Here the setting up of a typical LAN-based punching device has been explained. Similar steps need to be followed for devices of other brands.

(b) Android based configuration

Follow the following steps to configure android based biometric device.

- Step 1.** Go to the settings of the device and enable the Wi-Fi connectivity. In some cases for accessing the setting you need to follow a certain procedure. For this procedure refer to the user manual.
- Step 2.** In case of Wi-Fi network is not available then insert the SIM inside the sim socket of the device. Enable the SIM network. Check for Internet connectivity from SIM.
- Step 3.** There is no necessary of setting up network configuration as Internet connectivity is available from the network (Wi-Fi or SIM).
- Step 4.** Android based biometric devices make use of cloud services. For such services we need to have some additional settings, such as 'Cloud Server IP address' and 'Port number'. For example, cloud server IP address can be '115.124.109.34' and TCP Port Number '2006'.

Every cloud based biometric Android device has a specific serial number and it has to be registered with the cloud server. Normally the company providing such devices are taking care of these registrations.



Identification and Verification of Biometric Data

Biometric devices are used for identification and verification of a person. This identification and verification can be done by using some biometric data of a person, such as fingerprint, iris, palm image or face image.

In identification, the fingerprint of the person is matched against the selected stored fingerprint in the database. In verification the input fingerprint is verified among the all fingerprints stored in the database. If the database is very large then, in such a case verification is time consuming process and it may require several hours. But in identification the comparison is made only between input image and selected image. Therefore it requires very less time.

For example, in case of Aadhaar the database is very huge containing the biometric data of more than 80 lakh people. Therefore, normally while using the Aadhaar database only identification is done entering Aadhaar number. Verification in Aadhaar may require more time.

Practical Exercise

1. Set up and install a scanner and web cam on your computer.

Check Your Progress

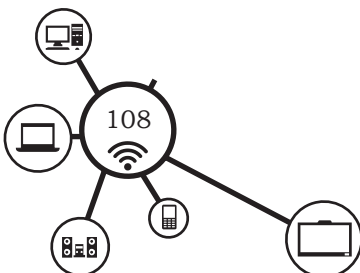
A. Fill in the blanks

1. Before using any biometric device one needs to _____ device.
2. A biometric device is a security identification and _____ device.
3. Fingerprint scanner device can be connected to the _____ port of the computer system.
4. Fingerprint scanner device needs _____ for its installation.
5. Face scanners identify a person by taking measurements of _____.

DOMESTIC BIOMETRIC DATA OPERATOR – CLASS XI

(a) Face Domestic Biometric Data Operator–Class XI

2021-22

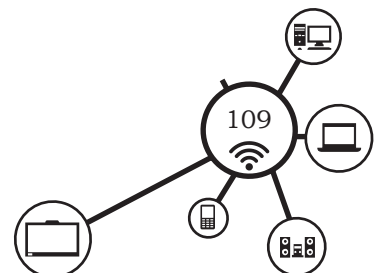


NOTES

6. Web camera is a _____ device.
7. Plug and play devices automatically get _____.
8. Iris scanner is connected to the _____ port of the computer system.
9. Biometric retina or iris scanner identifies a person by scanning the iris or retina of their _____.
10. A fingerprint sensor is an electronic device used to register a digital image of the _____ pattern.
11. Configuration of the scanner can be done by using _____.
12. Configuration of the biometric devices can be done by using _____ provided by the vendor.
13. While installing fingerprint scanner device _____ must be appropriately adjusted.
14. The voltage between earth and neutral point should be less than _____ volts.
15. In case AC power is not available then devices can be used by using _____.
16. The typical IP address of the device contain _____ numbers.
17. The subnet mask of the device contain _____ numbers.
18. For the data flow upstream and downstream the recommended ports must be _____ in the network.
19. Android based devices require a _____ network.

B. Multiple choice questions

1. In case Wi-Fi network is not available then we should use _____ network.
(a) SIM (b) data
(c) LAN (d) Intranet
2. Android based biometric devices makes use of _____ services.
(a) LAN (b) Cloud
(c) Intranet (d) SIM network
3. In identification the input image is compared with _____.
(a) online image (b) stored image
(c) selected image (d) offline image
4. In verification, the database input image is compared with _____.
(a) online image (b) stored image
(c) selected image (d) offline image

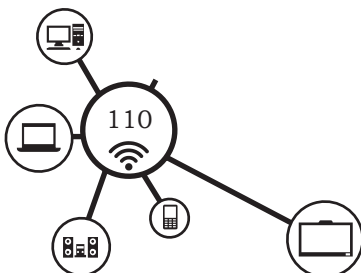


NOTES

5. Which of the following is not a biometric technique?
(a) Retina (b) Badge
(c) Face (d) Palm
6. What is the most common type of biometric device used in organisations?
(a) Face recognition (b) Fingerprint scanners
(c) Signature recognition (d) Voice recognition
7. What makes biometrics the strongest authentication methods?
(a) Fingerprints, voice patterns and faces are all unique
(b) It is difficult to copy or spoof biometric data
(c) Biometric data is analog and not digital
(d) Biometrics are typically used as part of a two-factor authentication system
8. The input voltage and live and earth point should be _____.
(a) 0-100 V (b) 220-240 V
(c) 110 V (d) 300 V
9. The bracket of the fingerprint device must be fitted at _____ height.
(a) 6 feet and above (b) 4 to 5 feet
(c) ground level (d) the top
10. Setting up of biometric devices require connectivity and _____.
(a) fixing (b) wall mounting
(c) installation (d) fitting

C. State whether the following statements are True or False

1. For identification of Aadhaar biometric data we need to enter Aadhaar card number.
2. A typical IP address is written as 255.255.255.
3. A typical subnet mask is normally expressed as 255.255.255.0.
4. Plug and play devices get automatically installed on the computer system.
5. The location of the biometric device must be exposed to the rain, heat or sunlight.
6. Before connecting any biometric device, proper electrical earthing must be performed.
7. Device drivers of the biometric devices can be obtained through Internet.
8. GPS means Global Posting System.
9. Active and deactivate devices are shown in the taskbar of operating System.
10. Web camera cannot be connected to the USB port of the computer system.
11. Iris scanner requires no device driver for its installation.



D. Short answer questions

1. Write the steps for installation of fingerprint device.
2. Write the steps for setting of web camera on your computer system.
3. What is a GPS device? How can it be installed on the computer system?
4. What do you mean by device driver? Explain how to obtain device driver for biometric devices.
5. Write the steps for configuration of biometric device by using computer system installed on your computer.
6. Write the steps for android-based fingerprint configuration.
7. Write steps to set up android-based fingerprint scanner.
8. Write steps for setting up iris scanner.
9. What are guidelines for setting up a digital camera?
10. Explain biometric data exceptions.
11. Discuss errors and errors handling process.
12. Differentiate between identification and verification of biometric data.

SESSION 3: BIOMETRIC DATA ENTRY

Once the biometric devices are connected and installed, they are ready to capture data. Capturing data by using biometric devices is called biometric data entry. In this session, you will understand how to collect data of fingerprints, palm images, iris images and facial images.

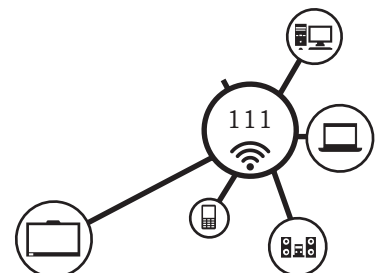
Biometric Data Entry for Biometric Attendance System

Steps for collecting fingerprint data includes the

- (i) Registration of data
- (ii) Enrolment of data

Registration and enrolment

After configuration of the biometric device, the device gets ready to accept the data. First of all the master data is created for an organisation. A typical format of the master data is shown in Fig. 2.53.

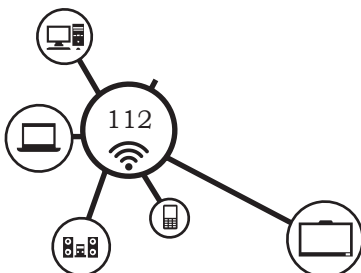


Employee ID	Name	Type	Designation	Department	Religion	Gender	Joining Date	Birth Data	Email ID
19610035	Rishik Rai	On-Rolled Confirm	Team Leader	Food & Beverage	Hindu	M	2/2/2018	2/3/1998	rishik_1998@gmail.com
19610036	Ankush Kumar	On-Rolled Confirm	Team Leader	Food & Beverage	Hindu	M	15/07/2017	9/12/1999	ankushk@gmail.com
19610037	Akash Jain	On-Rolled Confirm	Team Leader	Food & Beverage	Jain	M	9/12/2015	30/05/1998	akashjain@gmail.com
19610038	Priyanaka Singh	On-Rolled Confirm	Team Leader	Food & Beverage	Punjabi	F	10/1/2018	17/10/1995	priya1999@gmail.com

Fig. 2.53: Master data

Observe that the master data contains various fields as mentioned below.

- **Company ID:** is a unique number assigned to the organisation. This number can be a three-digit number.
- **Employee ID:** is a unique number assigned to each employee of the organisation. This can be a nine digit number in which the first three digits are for company ID and the rest upto six digits are assigned to the individual employee.
- **Employee Name:** is the name of individual employee and it is in the format of First Name and Last Name.
- **Type:** is the type of employee. It can be either confirmed, temporary, contractual or on probation.
- **Designation:** is the official designation of the employee. It can be Manager, General Manager, Head of the Department and Vice President.
- **Religion:** is the religion of the employee, such as Hindu, Muslim, Jain, Christian. Normally this field is used for holiday management.
- **Nationality:** indicates the nationality of the employee.
- **Gender:** is the gender of the employee, such as Male, Female
- **Joining Date:** is the date of joining of employee. It is necessary to maintain and calculate the length of service.
- **Birth Date:** is the date of bright of the employee.
- **Blood Group:** is the blood group of the employee.
- **AlphaNumeric ID:** is the alphanumeric ID. It is the combination of alphabets and number.
- **Email ID:** is the email ID of an employee.



- **Visa Exp Date:** is the date of visa expiry. It is required by the employee during a foreign tour for training.
- **Passport Exp Date:** is date of passport expiry. It is required by the employee during a foreign tour for training.
- **Subdept:** is necessary to define department with subtitles.
- **Contractor Name:** is the name of the contractor of employee.
- **Grade:** is the grade of the designation of employee, such as Grade A, B, C, D
- **Mobile Number:** is the authenticated mobile number of employee used for various authentication purpose.

Steps for master data creation

Step 1: As per the above format, fill the data in the Excel sheet by using your computer. Save the file on computer.

Step 2: Login to the company account provided by biometric service provider. For example, a typical login can be as shown below in Fig. 2.54.

URL: <https://presence.attendanceportal.com>

Username: etam492

Password: @Etam123

Step 3: After login go to the desired path where the created master file in Excel can be uploaded. For example, a typical path can be as shown below.

Select upload option. In upload select Employee Registration and then click to upload. Choose the file and upload it.

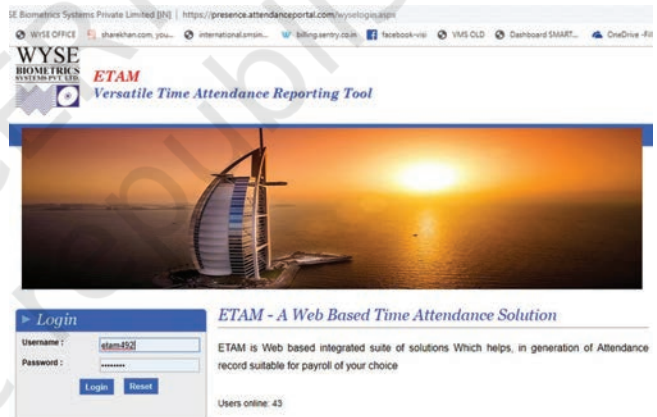


Fig. 2.54: Typical login page

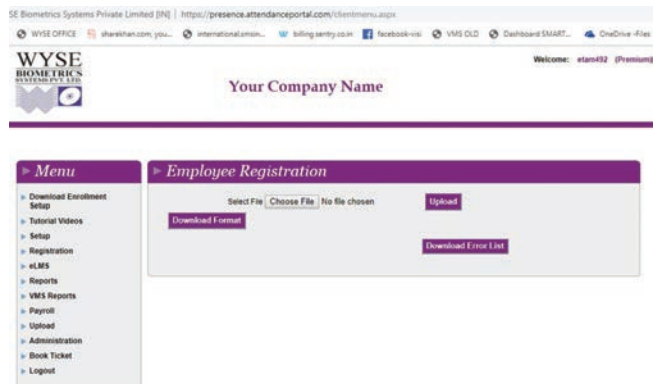
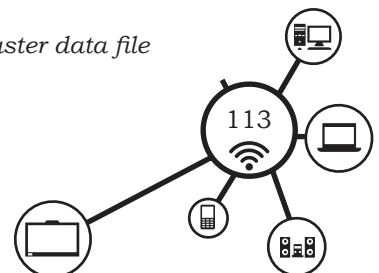


Fig. 2.55: Uploading master data file



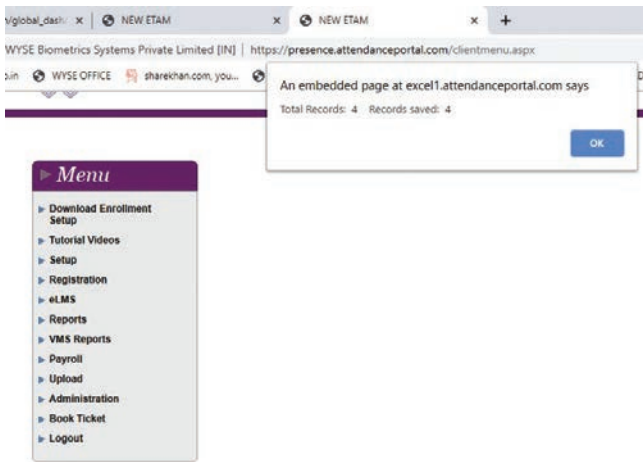


Fig. 2.56: Indication of successfully uploading records

Step 4: If all the records are filled correctly then a successful message will be displayed indicating that all the records are saved on server.

If some records have certain issues then those records will not be saved and such message will be prompted to the user. In such a case user need to correct all the faulty records and file can be uploaded by using the above procedure.

Enrolment

After successfully uploading the master data file one needs to enroll all of the employees of the company so that the fingerprint data of all the employees is made available for the purpose of comparison. Steps for enrolment are as given below.

Step 1: First download the setup by using 'Download Enrollment Setup' option in the main menu.

Another way to do the same is to execute a Setup DVD or CD provided by the vendor.

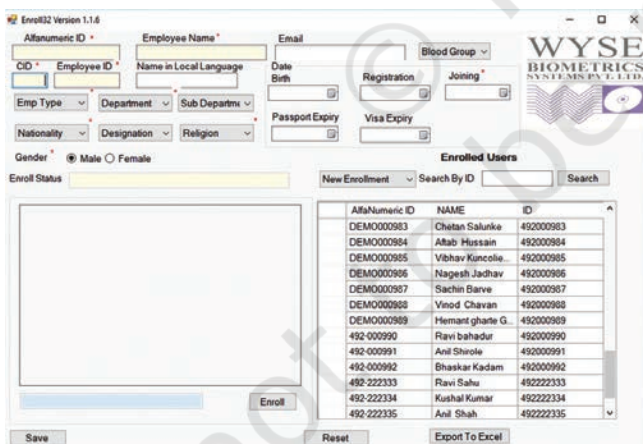


Fig. 2.57: Screen after login

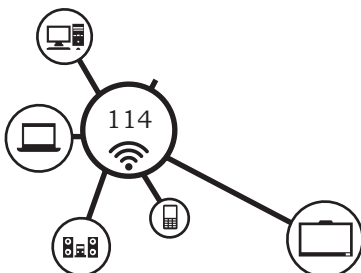
Step 2: Install the program by using the setup file.

Step 3: After installation, the shortcut icon of the Enrolment program appears on the desktop.

Step 4: After clicking on the Enrolment icon the login name appears. Enter the appropriate login and password.

Step 5: After successful login an screen appears as shown in Fig. 2.57.

Step 6: Now select the employee from the employee list and obtain their fingerprint image by



using fingerprint scanner. Note that your computer must be connected with fingerprint scanner as shown in Fig. 2.58.

After obtaining fingerprint, click on the Save button to save the fingerprint data of the employee.

It is recommended to obtain the thumb impression of both the hands. Normally, a software has a provision to obtain thumb impression multiple times. When the thumb impression is used for the purpose of identification, then the punching ratio gets improved and rejection ratio is minimum.

Step 6: Go on repeating Step 5 until the fingerprint data of all employees is recorded. By using the same menu it is also possible to add a new record if the record is not available in the master file. The data will be saved at the cloud server.

Step 7: Now one need to transfer the data to the biometric device. Biometric device can be selected by using the login as shown in Step 2 for master data creation.

After login go to **Administration** option. Select **Control Centre** option. Select appropriate Biometric device. Note that this biometric device must be online during the data transfer process. Select the employee from the master file and then transfer the data to the device by clicking double forward (>>) button.

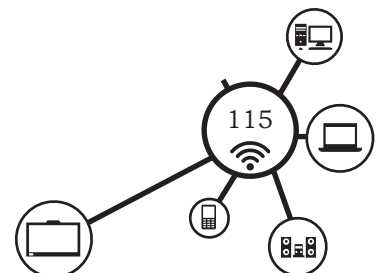
Step 8: Once the data transfer has been completed the biometric device is ready for punching. An employee can punch into the biometric device for in and out.

Biometric Data Entry for Aadhaar Card

In case of Aadhaar card, we require the fingerprints of all the fingers of left hand and right hand of a person. The images of these fingerprints can be scanned through a platen. Platen is a transparent glass surface of the fingerprint scanning device on which the fingers are placed.



Fig. 2.58: Fingerprint scanner connected to the computer



The steps for collection of such data is explained below.

Steps for Collection of Fingerprint Data

In preparation of Aadhaar card, the fingerprint of all the five fingers of left hand and five fingers of right hand, i.e., 10 fingers of two hands are required to be captured. There are certain procedures which need to be followed if the person has more or less than 10 fingers. The images of these fingerprints can be scanned through a platen. The steps for collection of such data is explained below.



Fig. 2.59 (a): Capturing left hand fingerprint data



Fig. 2.59 (b): Fingers to be scanned



Fig. 2.59 (c): Digitised output of captured left hand fingerprint data



Fig. 2.60 (a): Capturing right hand fingerprint data



Fig. 2.60 (b): Fingers to be scanned

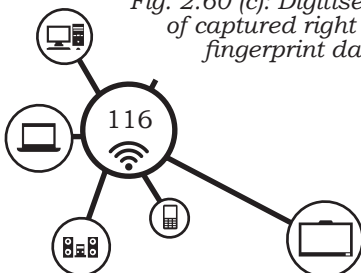


Fig. 2.60 (c): Digitised output of captured right hand fingerprint data

Step 1: First to capture the fingerprints left hand, put left hand fingers of enrollee, excluding thumb on scanner platen and apply light some pressure to have good contact with the surface as shown in the Fig. 2.59 (a). The fingers to be scanned are illustrated in Fig. 2.59 (b). The software interface captures these images and digitise it. The digitised output of captured fingerprint is shown in Fig. 2.59 (c).

Step 2: Secondly, to capture the fingerprints of the right hand, put right hand fingers of enrollee, excluding thumb on scanner platen and apply light pressure to have good contact with the surface as shown in Fig. 2.60 (a). The fingers to be scanned are illustrated in the Fig. 2.60 (b). The software interface captures these images and digitise it. The digitised output of captured fingerprint is shown in Fig. 2.60 (c).

Step 3. Next to capture the thumbprints, put the thumbs of both the hands on the platen and apply light pressure to have good contact with



the surface as shown in Fig. 2.61 (a). The fingers to be scanned are illustrated in Fig. 2.61 (b). The software interface captures the thumb images and digitise it. The digitised output of captured thumb is shown in Fig. 2.61 (c).



Fig. 2.61 (a): Capturing thumb impression



Fig. 2.61 (b): Thumbs to be scanned

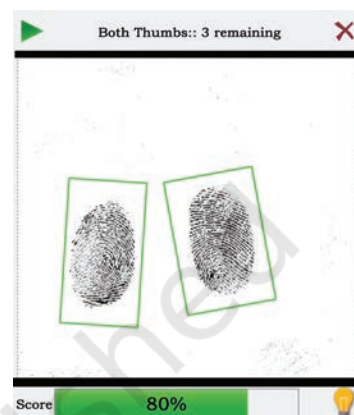


Fig. 2.61 (c): Digitised output of captured thumb impression

The application software automatically captures the fingerprint when the fingers are placed on the platen. It does not require any click of the mouse or pressing of any button. When the scanner indicates successful grab of the image, the application software captures the image of the fingerprint. Unless the scanner shows successful indication for each finger the image is not captured by the software. If the fingerprint does not get captured automatically then the software allows forced or manual capture by clicking Force Capture button. This is possible after at least one failed attempt during automatic capture. Finally, check the images of the fingerprints visually in the application software for quality and typical problems.

Guidelines for fingerprint scanning

1. If the image of fingerprints is not proper in spite of repeated attempts, there may be a problem in putting the fingers on the platen or fingers are too dusty to capture the image. The solution for this is to wash the hands. The proper way of placing the fingers on the platen is shown in Fig. 2.62.
2. Ensure that the fingers do not touch the edge of the platen. There should be space between the fingers to capture the fingerprint image properly. No portion of the fingers should touch the edge of the platen as shown Fig. 2.63.
3. While giving the fingerprint impression, apply some pressure on the platen to increase the area of contact to obtain the requisite image quality.



Fig. 2.62: Correct way of placing fingers on the fingerprint scanner platen

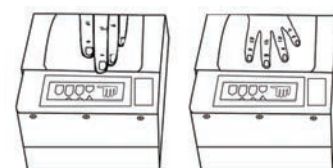
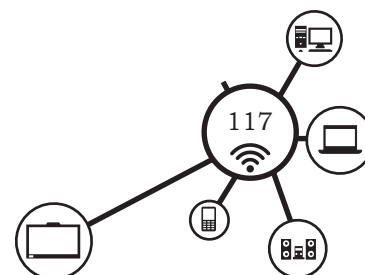


Fig. 2.63: Correct position of fingers on the platen



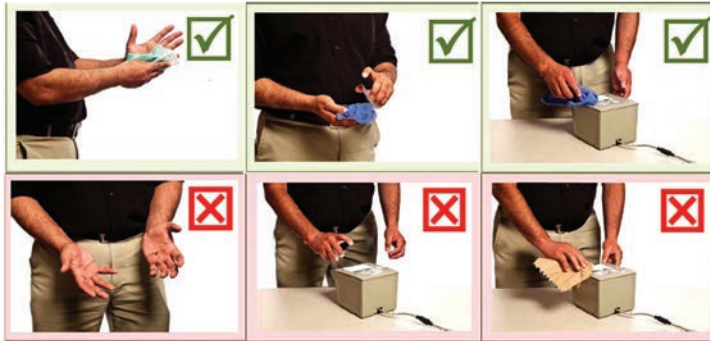
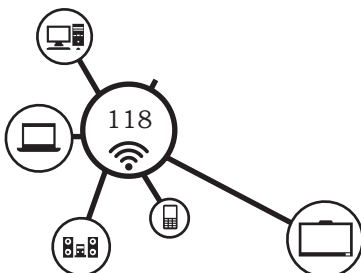


Fig. 2.64: Cleaning the fingerprint scanner

4. In case of Henna on the hands, follow the normal procedure to capture the fingerprint image. In case of worn out ridges rub the hands to get the proper image of fingerprint.
5. Place the fingers flat till the top joint of the finger is placed well on the scanner. There should be no direct light shining on the platen. Use the indicators on the fingerprint device for positioning of fingers. The fingers should be placed in right direction on the device.
6. Periodically clean the platen by using a lint free cloth. The procedure for cleaning the device is illustrated in Fig. 2.64.
7. Periodically check the devices for scratches on the platen. Also check for out of focus or partial images of fingerprints getting captured.
8. Capture the fingerprints in standing position of enrollee as fingerprints are best captured in standing position. In case of additional finger(s), ignore the additional finger and capture the main five fingers of each hand during the time of fingerprint image capture.

Steps for Collection of Iris Data

There are two types of iris capturing device viz., single and double iris capturing device which captures single iris image of single eye and two iris image of two eyes, respectively. Single iris scanner scans one eye at a time. This is mainly used in biometric attendance system. The iris capturing device is connected with laptop/desktop computer through USB port. They gets power from the laptop/desktop computer through USB port. No separate power supply is required to run this device.



To capture iris images, hold the iris scanner in hand close to your eyes as shown in the Fig. 2.65 (a). The software interface captures the iris images and digitise it. The digitised output of captured iris is shown in Fig. 2.65 (b).

Guidelines for Iris Scanning

In case of squint eyed, if the capture of both eyes at a time is not possible, then recapture for second eye. Eyes should be opened widely to capture a good quality image of iris. Iris capture device uses auto focus and auto-capture functions and hence it does not require any focussing or capturing adjustment.

Steps for collection of facial data

Photographs of the face are commonly used in various types of identification cards and are widely accepted as a biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. A face needs to be well lit, using controlled light sources, for automated face authentication systems to work well. Even a smile can alter the features sufficiently and affect the system. Hence, neutral facial expression is required for correct verification. Enrolment Operator has to ensure the proper position of an enrollee to capture the facial image using a digital camera or webcam. The typical position of an enrollee is shown in Fig. 2.66. Observe that an enrollee's face is facing the webcam attached to the computer.

Step 1: Sit in front of web camera in such as way that a complete face image is visible to the camera as shown in the Fig. 2.66. The background must be clear. Check the enrollee's position such that the photograph should be taken with the resident directly facing the camera. No head rotation or tilt is acceptable.

Step 2: Adjust the camera as per the enrollee's position for the right distance and posture as shown in Fig. 2.67.

Step 3: Check the enrollee's expression. Ensure that enrollee has a neutral expression. For example, the enrollee should not be smiling, mouth



Fig. 2.65 (a): Capturing eyes using iris

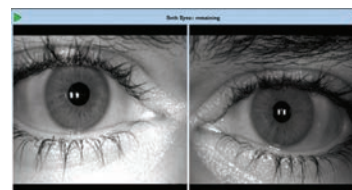


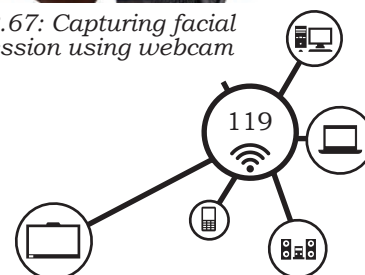
Fig. 2.65 (b): Digitised output of captured eye



Fig. 2.66: Position of the enrolment operator and enrollee



Fig. 2.67: Capturing facial expression using webcam



should be closed and both the eyes must be open, while taking the photograph.

Step 4: Check the shadow or reflection such that there should be sufficient light to get a proper image of the face. Ensure that there is no shadow on the enrollee's face and no reflection on eyes. Place the additional light source in front of the enrollee so that there are no shadows under the eye.

Step 5: Check the visibility of iris and pupil through eyeglasses. If the enrollee is wearing glasses, the photograph must be taken with the glasses on. Ensure that the iris and the pupil are clearly visible and that enrollee is not wearing dark or coloured sunglasses.

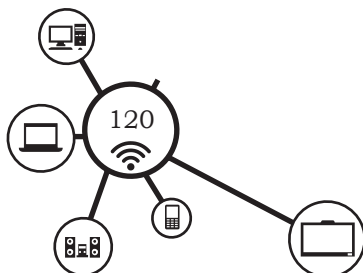
Step 6: The software interface of Aadhaar card captures the face image and the digitised output is shown on the screen as shown in Fig. 2.68.



Fig. 2.68: Digitised output of facial expression

Guidelines for Capturing Facial Image

1. Set the digital camera with auto focus technology so that it does not require any focussing adjustment.
2. Ensure that the output image is not blurred because of jerks or movements of the camera. The image should neither be too dark nor too bright.
3. Ensure there is sufficient lighting in the room to capture the photograph.
4. Do not use flashlight to capture a photograph.
5. Place the background preferably white behind the resident against an opaque wall or partition.
6. Ensure that the entire face of the resident is visible while taking the photograph. Adjust the position of the camera to get full coverage of residents face.
7. Use of accessories that cover any region of the face is not permitted. However, accessories like eye patches due to medical conditions are allowed.



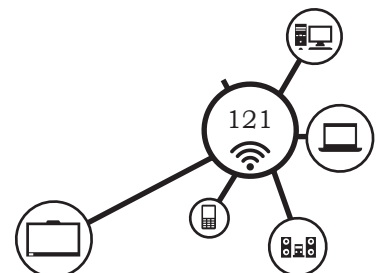
8. Ensure that the lady volunteer should help a lady resident for preparing to capture the facial image.
9. In case the child sitting on its parent's lap, ensure that the parent's face is not captured along with the child's face.
10. The image should not contain any kind of radial distortion, i.e. distortion of a straight line.
11. Ensure that the enrollee has a neutral expression, i.e. non-smiling, closed mouth and eyes open.
12. Ensure that there is equally distributed lighting and that there are no shadows on the resident's face and eyes.
13. The eyeglasses of resident should be clear and transparent so that both the iris and the pupil are clearly visible. If enrollee is wearing tinted glasses then the direct and background lighting sources should be tuned accordingly.

Different situations may arise while taking the facial images of different types of persons. You need to find the solutions to deal with such situations. Following are some exemplar situations that illustrate for taking the photographs of different persons.

Scenario 1: Capturing the photograph of a person wearing a turban



Fig. 2.69: Capturing the photograph of a person wearing a turban



Scenario 2: Burkha clad lady - facial image capture

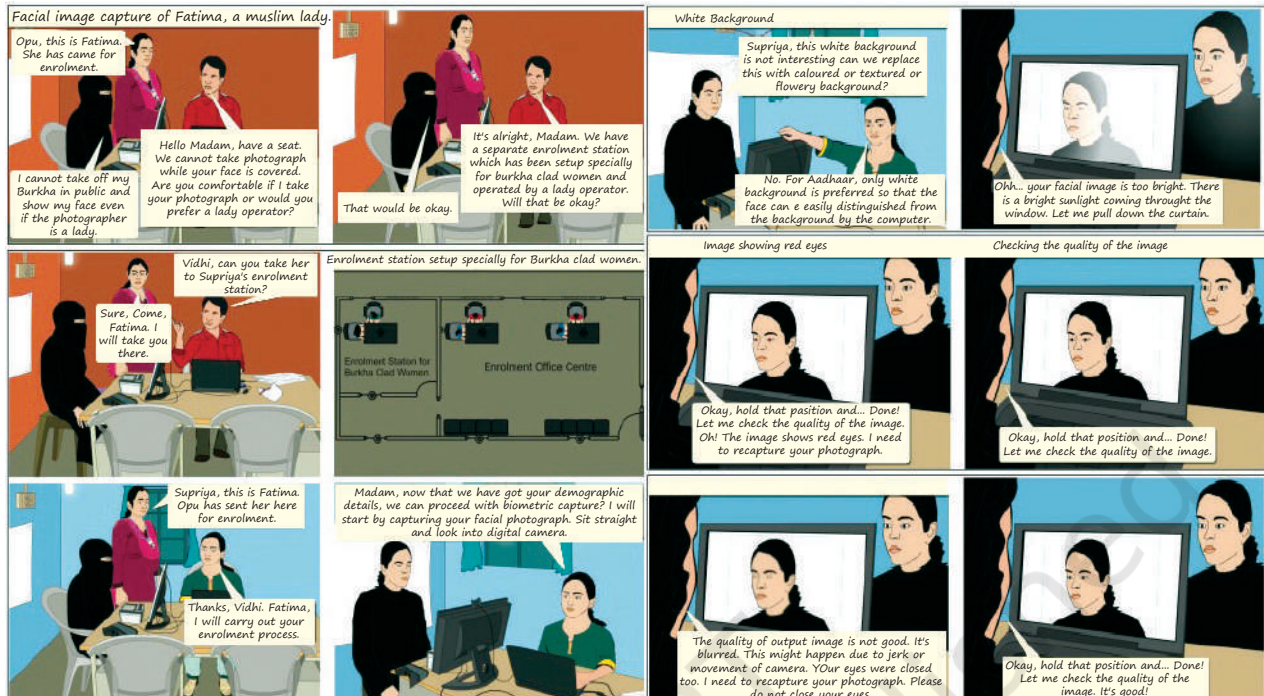
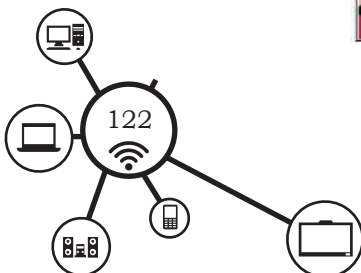


Fig. 2.70: Capturing the photograph of a lady wearing burkha

Scenario 3: Capturing the photograph of a 5-year-old



Fig. 2.71: Capturing the photograph of a child



Registration and Enrolment

After capturing the data we need to enroll the data by using Aadhaar enrolment client set up as given in the following steps.

Step 1: Double Click on 'Aadhaar Enrolment Client' Setup as shown in Fig. 2.72.

Step 2: Login with Authorised Operator's Credentials as shown in Fig. 2.73.

Step 3: Home Page of Aadhaar Enrolment Client will appear as shown in Fig. 2.74.



Aadhaar Enrolment Client

Fig. 2.72: AEC Shortcut



Fig. 2.73: Aadhaar Enrolment Client login window

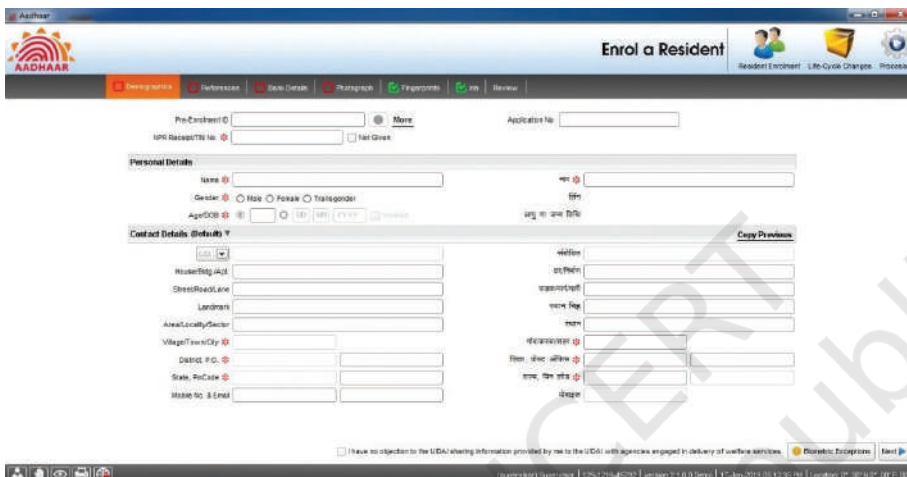


Fig. 2.74: Demographic data entry form in Aadhaar Enrolment Client

Step 4: Fill the enrollee's details under Demographic Tab such as Name, Gender, Age/DoB as shown in Fig. 2.75.

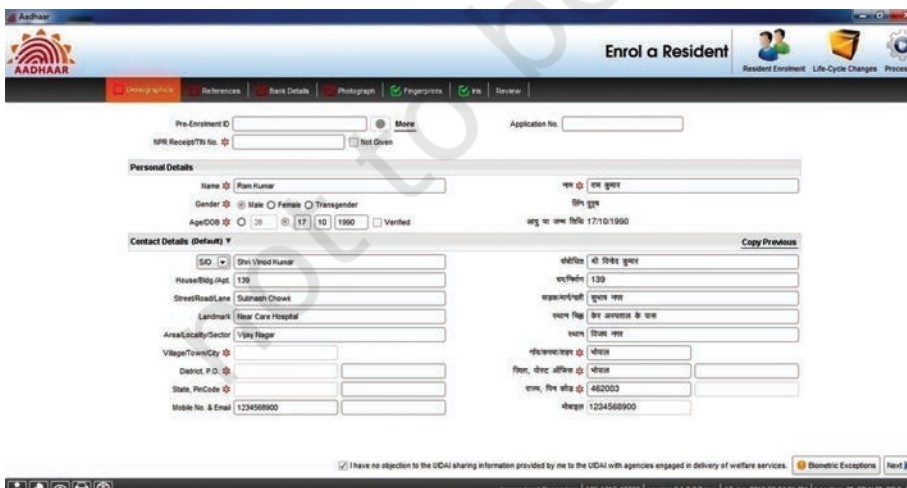
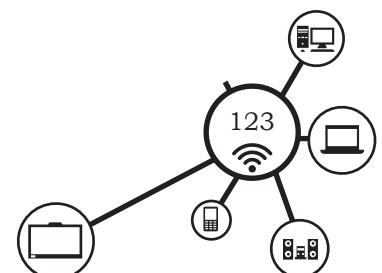


Fig. 2.75: Demographic filled data in Aadhaar Enrolment Client



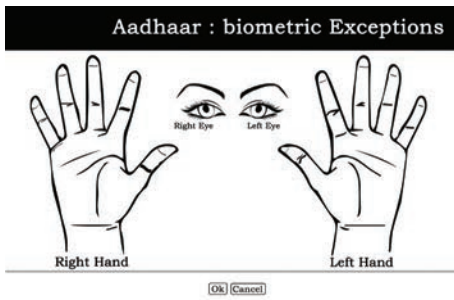


Fig. 2.76 : General preview of biometric data exceptions

Step 5: After filling enrollee's details, Accept 'Declaration' and Click on Biometric Exceptions button as shown in Fig. 2.76. Then click on Ok button.

Step 6: Fill additional details of enrollee in 'References Tab', such as proof of date of birth, identity and address verification documents, relative details as shown in Fig. 2.77.

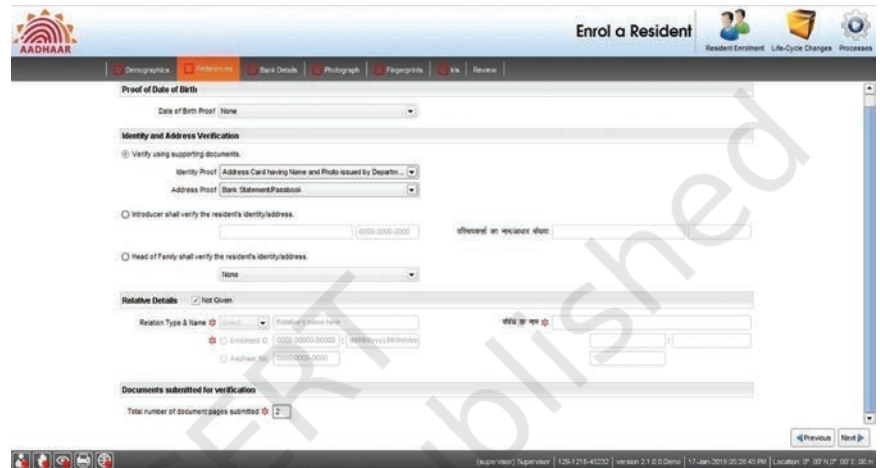


Fig. 2.77: References tab of data entry form of Aadhaar Enrolment Client

Step 7: Fill 'Bank Details' of enrollee as shown in Fig. 2.78.

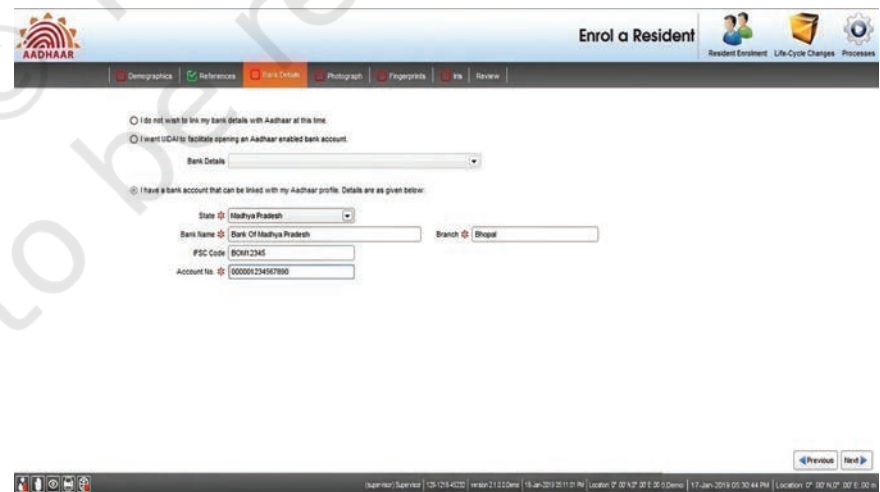
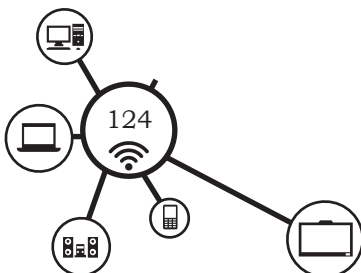


Fig. 2.78: Bank details tab of data entry form of Aadhaar Enrolment Client

Step 8: To upload the data, click on 'Processes' and Select 'Import Pre-Enrolment Data'.



The preview will appear on the screen as shown in Fig. 2.79.

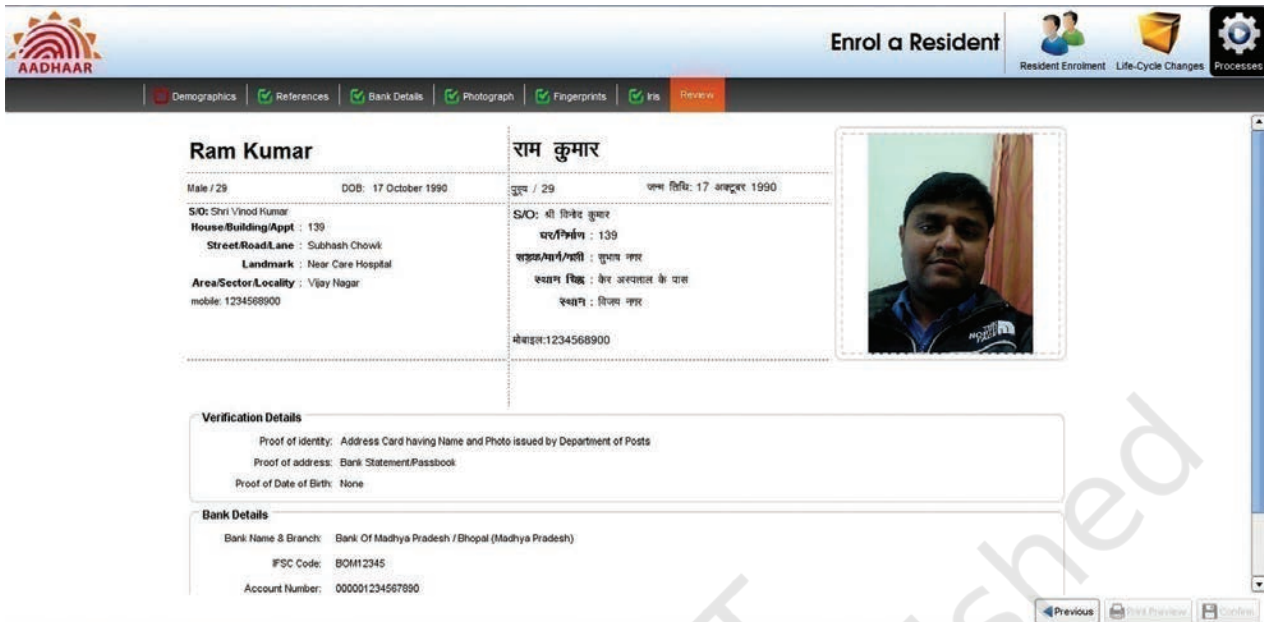


Fig. 2.79: Preview of details entered in AEC

Step 9: To print the data click on 'Processes' and Select **Export Enrolment Data** option. Select appropriate location on the disk for exporting the biometric data as shown in Fig. 2.80.

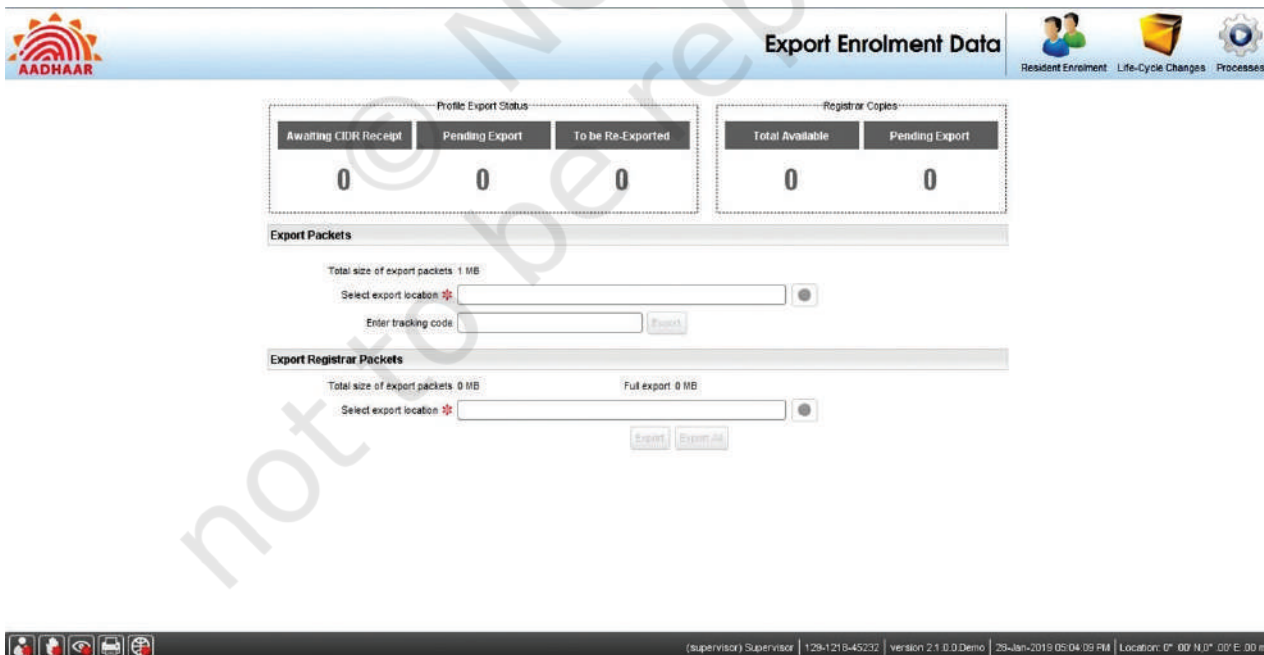
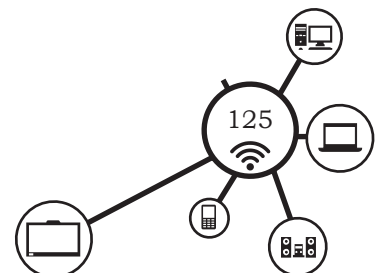


Fig. 2.80: Export enrolment data



the fingers are not placed properly then an error messages will be displayed as shown in Fig. 2.83.

If the fingers are not placed in the correct order then also an error message will occur. The correct order of placing the fingers for scanning is first left and then right. If the enrolle first puts right hand fingers then an error encountered will be shown as in Fig. 2.84.

While scanning the eyes using iris scanner, if scanned data accuracy is below 50 per cent then an error gets encountered as shown in Fig. 2.85.

Errors and Error Handling—FAR, FRR and ERR

Errors and errors handling process in biometric matching is probabilistic, and the placing of that threshold is critical. There may be chances that the system accepts the match against wrong reference or system rejects to accept the correct reference.

False Acceptance Rates (FAR) or false positive means a sample is matched against the wrong reference. FAR occurs when the system accepts a non-enrolled user's fingerprint.

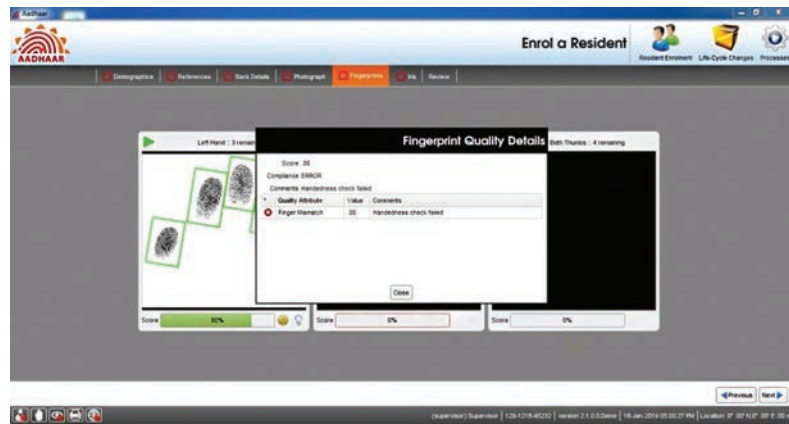


Fig. 2.83: Error encountered in wrong placement of fingers

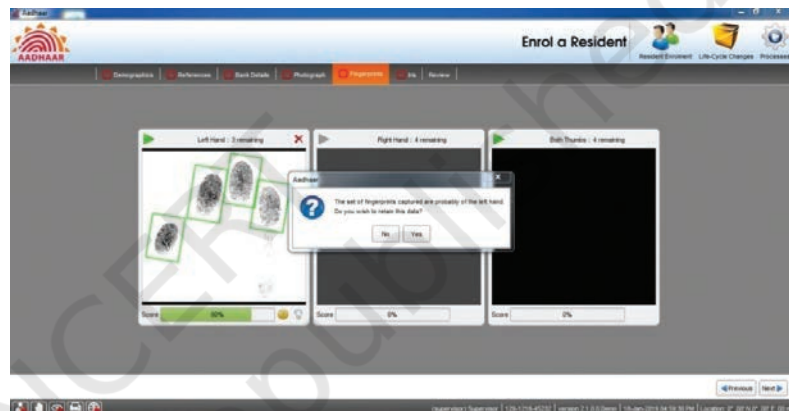


Fig. 2.84: Error encountered while placing the fingers in wrong order

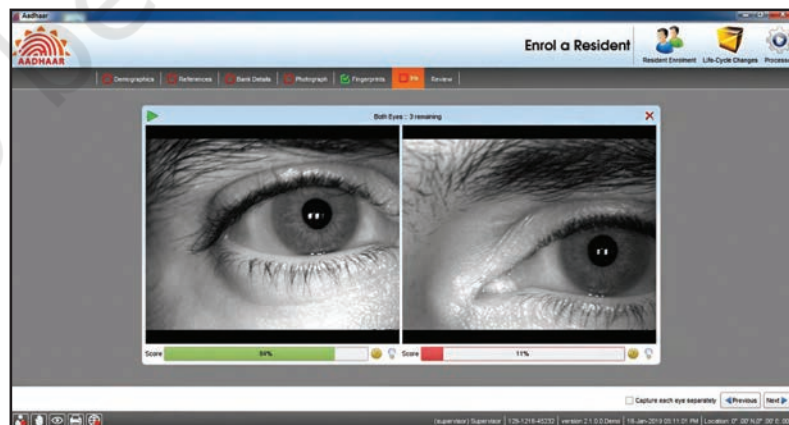
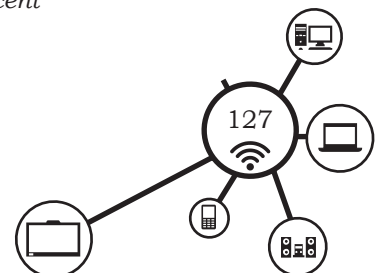


Fig. 2.85: Error encountered while scanning the eyes where data accuracy is below 50 per cent



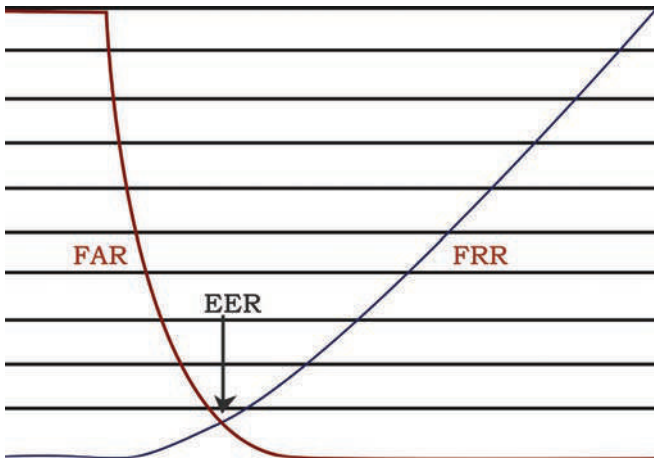


Fig. 2.86: FAR, FRR, EER

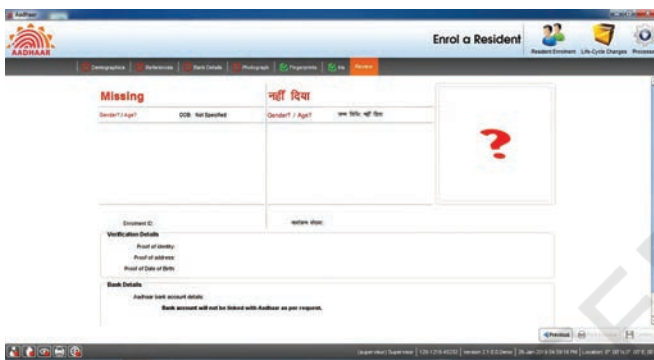


Fig. 2.87: Missing data form

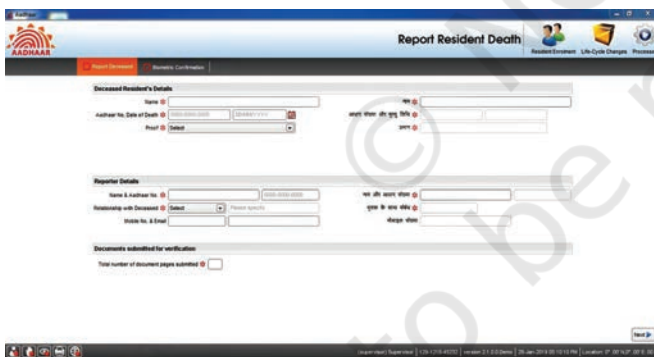


Fig. 2.88: Report deceased form

False Rejection Rates (FRR) or false negative is a failure to match a sample against the correct reference. FRR occurs when the system reject an enrolled user's fingerprint.

A high threshold means a low FAR but a higher FRR. A low threshold means a low FRR but a higher FAR. The point where those are balanced is the Equal Error Rate (EER). This is not used to set how the thresholds should be applied but it provides a way of comparing between approaches. A higher EER means a less accurate overall performance.

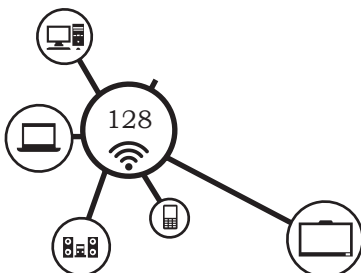
If data entry forms miss out certain information, then the missing error appears on the screen as shown in Fig. 2.87.

There are two other error rates. Failure to Acquire (FTA) is where the image acquired by the device is, for whatever reason, not of sufficient quality to create a template. Failure to Enroll (FTE) is similar, but the failure is in creating an original reference. FTE is the probability that a given user will be unable to enroll the user in a biometric system due to insufficiently distinctive biometric sample(s).

Biometric Data Exceptions

Biometric data has exceptions because of the following reasons.

1. Environment and usage can affect measurements
2. Systems are not 100% accurate
3. Require integration and/or additional hardware
4. Cannot be reset once compromised



Biometric exceptions occur when a user is unable to give complete set of biometrics as required by the system. For example, in preparation of Aadhaar card the UIDAI system requires to capture all kind of biometric data, such as fingerprint, thumb, palm, iris and face. The exception can of different types, such as missing finger (s), missing eye due to which the user is not able to give the complete biometric data to the system. The exceptions may occur because of injury, amputation of fingers, amputation of hands, problems with the eye. Also the fingerprint quality can be affected by henna or Rough fingers or calloused hands.

Handling exceptions

Exceptions have to be handled with care. Special care has to be taken to make them comfortable throughout the entire process. Given below are the ways to handle exceptions.

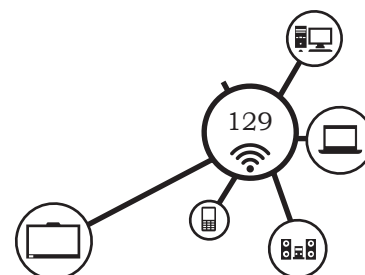
Capturing the Biometric Exceptions in the Enrolment Client

In the Aadhaar enrolment process, capture all exceptions at one go, by clicking the Biometric Exceptions Capture button.

- First, check the user's fingers and eyes for fitness. If the user has an extra finger(s), ignore to capture the extra finger. The extra finger will not be captured as a biometric exception.
- While capturing the photograph of the exception, keep the palms facing to the camera, keep face and both the hands in the frame.
- Click on any part of the image to indicate non-availability of data for that part.
- Capture exceptions as photographs, on the photograph screen.
- Obtain supervisor verification for biometric exception.

Handling Face Image Exceptions

There are various kinds of problems while capturing facial image, such as poor light conditions, inability to



NOTES

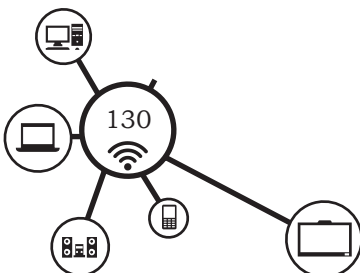
crop the image because of turban or head scarf and the user is unable to keep the face or body still and vertical. Such problems should be handled carefully.

- To handle the poor light conditions, do not use flash. Improve the light in the surroundings or move to a location with better light. Use the generator backup to improve lighting, in case of insufficient lighting due to low voltage. Place the backdrop against an opaque wall or partition.
- If accessories are worn due to religious reasons, choose the manual capture option.
- If the user is unable to keep the face or body still and vertical, then guide and assist the user for that. In case of ladies provide assistance by a lady operator

Handling Fingerprint Exceptions

Let us now see how to handle the problems occurred while capturing fingerprints. The possible problems and solutions are given below.

- **Missing fingers** capture the biometric exception in the enrolment client. If the user has an extra finger(s), ignore the extra finger to capture as a biometric exception.
- **Fingerprint captured is not of the right quality** if fingerprint images captured are not of the standard then it is better to wash the hands with a wet sponge or towel. Also apply little pressure on the platen to capture the images of better quality.
- **Inability to flatten the fingers** if the user is unable to flatten the fingers then assist in capturing fingerprints.
- **Worn out ridges of hands blackened through henna or some other substance** if the user's fingerprint ridges are worn then attempt a manual capture and capture fingerprints of fingers which are not blackened or without worn out ridges. Do not capture the fingerprints with henna on hands. The henna should be washed out before the fingerprint capture.



Handling eye exceptions

- **Squint or Disoriented Eye** If it is not possible to capture both eyes at a time, the single eye iris scan device may be used to capture one of the irises correctly by using dual eye device.
- **Inability to open the eyes properly** If the user is unable to open the eyes properly, guide and help the enrollee to open the eyes.

Handling Generic Exceptions

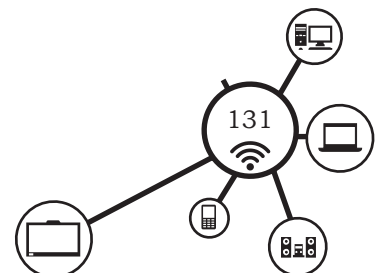
The enrollee may not be able to keep herself or himself in the correct posture photograph due to old age or sickness. In such cases the arrange to capture biometric data by moving the equipment close to the enrollee.

Check Your Progress

A. Fill in the blanks

1. Capturing data by using biometric devices is called _____.
2. The initial creation of data for all employees of the organisation is known as _____.
3. In biometric data the employee is identified by _____.
4. The holiday management of the individual employee is based on _____ data.
5. Length of the service of the employee can be determined by using _____ data.
6. Master data file can be uploaded only by _____.
7. When individual fingerprint data of all employees is created, then it is called _____.
8. Uploading of master data file to the server is also known as _____.
9. In Aadhaar card data enrolment first of all _____ data is collected.
10. For Aadhaar enrolment we require _____ software.
11. For Aadhaar enrolment one needs to fill _____ form.
12. Proper enrolment of the data is called _____.
13. In Aadhaar enrolment if the fingers are not placed on the scanner in the right sequence then _____ occurs.
14. The iris data will not be accepted by Aadhaar system if its data accuracy is below _____.
15. In biometric system FAR must be _____.

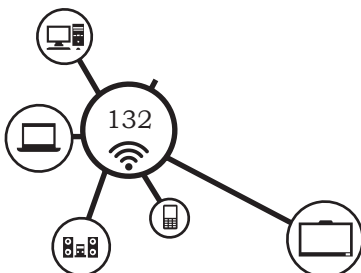
NOTES



NOTES

B. Multiple choice questions

1. Data duplication in biometric data can be checked by _____ method.
(a) score based (b) target based
(c) Both (a) and (b) (d) None of these
2. Biometric data has exceptions due to which of the following reasons?
(a) Environment and usage can affect measurements
(b) Systems are not 100% accurate
(c) Require integration of additional hardware
(d) All of the above
3. When the biometric device is unable to capture the image because of any reason, then it is called _____.
(a) failure to capture (b) failure to acquire
(c) failure to enroll (d) failure to register
4. FTE means _____.
(a) failure to enroll (b) false to enroll
(c) fault to enroll (d) fault to exam
5. In biometric systems FAR stands for _____.
(a) file allocate rate (b) file accept rate
(c) false accept rate (d) None of these
6. A false negative is a failure to match a sample against correct reference and it is called _____.
(a) FAR (b) FRR
(c) EER (d) FTE
7. A high threshold means a low FAR, but FRR will be _____.
(a) high (b) low
(c) medium (d) extremely low
8. A low means a low FRR, but FAR will be _____.
(a) high (b) low
(c) medium (d) extremely low
9. The point where FAR and FRR are balanced is known as _____.
(a) EER (b) FTA
(c) FTE (d) FRR
10. When FAR approaches to zero it may cause _____.
(a) a very low FRR (b) very high FRR
(c) FRR equal to zero (d) None of these
11. For the access to the site of national security the threshold must be set to _____.
(a) low (b) extremely low
(c) medium (d) high
12. Data validation is a process of ensuring _____ data.
(a) raw (b) mismatch
(c) quality (d) poor

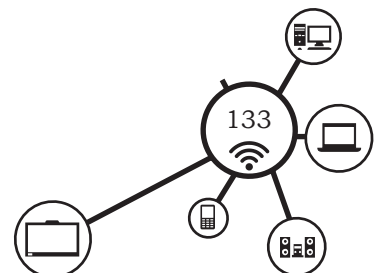


C. State whether the following statements are True or False

1. In Aadhaar enrolment the correct order of placing the fingers for scanning is first of the right hand then left.
2. For new enrolment in Aadhaar we need to fill our information on Aadhaar enrolment form.
3. The uploading of the data in Aadhaar enrolment is performed through export enrolment data.
4. Bank details of resident can be entered in Aadhaar enrolment.
5. Printing of the Aadhaar data can be performed through export enrolment data.
6. Enrolment of the data of the resident is performed by using Aadhaar enrolment client.
7. To capture the iris data the iris scanner should not be close to the eyes.
8. To capture the face image the background must be clear.
9. Head rotation or tilt is acceptable while capturing face data.
10. Smiling is not allowed while capturing the face image of an enrollee.

D. Short answer questions

1. Give the steps for registration and enrolment of biometric data in biometric attendance system.
2. List various fields that are required while collecting the data of an employee. Mark them as sensitive, very sensitive and non-sensitive elements.
3. State the reasons why some data elements should be marked as sensitive and very sensitive.
4. What do you mean by master data?
5. What do you understand by the term enrolment of data?
6. Give the steps for data enrolment in Aadhaar card.
7. Identify important documents to be attached with Aadhaar enrolment form.
8. What is data validation? How is it performed in the data enrolment of Aadhaar card?
9. Write the procedure for collecting biometric data.
10. Write the steps to capture face biometric data.
11. What are different types of errors that may occur in data enrolment?
12. Define the terms FAR, FRR, ERR.
13. Define the term FTA and FTE.
14. How can the death of a resident can be reported in Aadhaar?
15. What is biometric data exceptions? Give reasons for it.



16. What is data duplication in biometric data?
17. State the percentage of duplication in Aadhaar biometric data.

Practical Exercise

1. Perform registration and enrolment for student attendance system of your class and measure FAR and FRR of your attendance system.

SESSION 4: INTERFACING OF BIOMETRIC DEVICES

Biometric interface is the system by which one biometric system element communicates with another. These elements may be devices, software or entire system. The exchange of information—in general is that of biometric data.

Interfaces are essential for biometric system architecture and design that provide the basis for interoperability. Fig. 2.89 shows one such biometric interface. Observe that it contains biometric devices, networking with other devices, such as workstation, server and output devices as shown in Fig. 2.89.

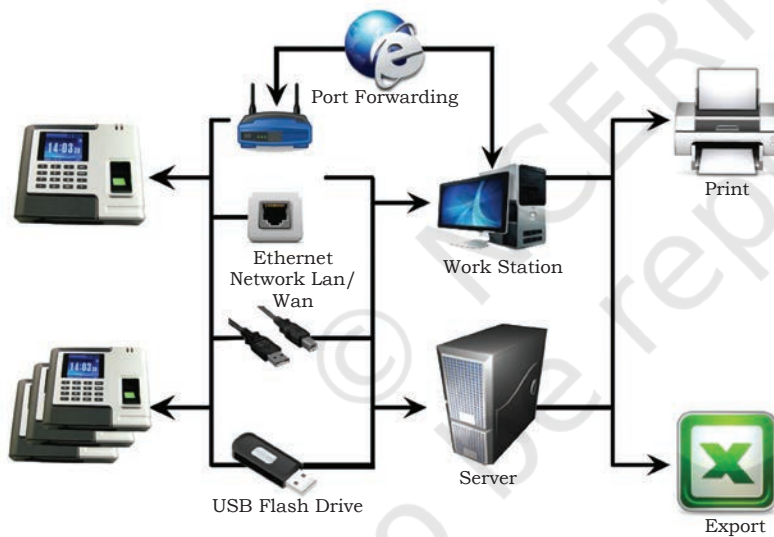
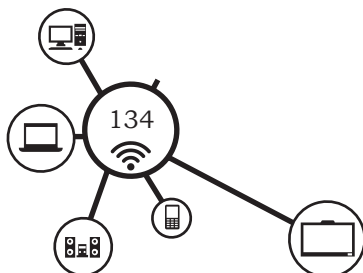


Fig. 2.89: Biometric systems

Biometric systems are composed of subsystems and components, the configuration and interrelationship of which describe the system architecture. For functioning of system, all components have to interact with each other across intra-system interfaces. The system itself may be a part of a larger 'system of systems' in which inter-system interfaces also exists. In a biometric or biometrically enabled system, the interface involves the



exchange of biometric data or the invocation of biometric services. Fig. 2.90 shows interfacing of various devices used for preparation of Aadhaar card.

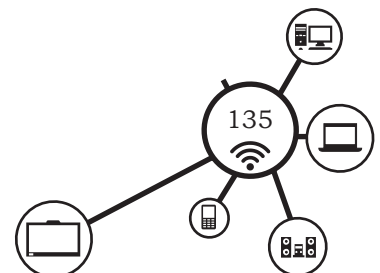
Biometrics Human-Machine Interface

It is the part of biometrics system which interacts with the end user and communicates with the host computer. The end user's attitude to the BHMI is critical to his or her attitude to the whole biometrics system. Fig. 2.91 shows the diagram of Biometric Human-Machine interface (BHMI) and user are at the end of both sides. So a biometrics system is not reasonably a good one if it does not have a good human-machine interface. To demonstrate the importance of the human-machine interface for a biometrics system, let's take a brief look at the history of the human-computer interfaces against that of the computer industry. In the early stage of the computer, the common human-computer interfaces were tedious punched card files, dull command-line interfaces on a black and white screen and the users of the computer must be experts to know how to manipulate them. Nowadays, however, a dummy that is not trained much can easily use the computer to surf the Internet. Today's computers use windowing systems that have fancy elements, such as windows, menus, buttons, scrollbars, combo boxes and sophisticated input devices like mice, joysticks, trackballs, microphones and writing pads, etc. These rapid developments in the human-computer interface field contribute much to the popularity of the computer. Similarly, the development of a user-friendly human machine interface is important to the popularity and marketing of a successful biometrics product.

On the other hand, the BHMI communicates with the host computer through some kind of communication protocols. The BHMI provided to the host computer



Fig. 2.90: Various devices used for preparation of Aadhaar card



must meet the requirements set by the host computer or the designer. These requirements include the speed, the quality of the sample. Consequently, the two goals that the BHMI designers try to achieve are:

- (i) Producing a high-quality output for subsequent biometrics processing like verification and identification. For example, the human-machine interface of an iris biometrics system must provide a high-resolution and sharp iris image for recognition procedure.
- (ii) Providing user-friendly and easy-to-use operating interfaces for the end users while not making the end users feel uncomfortable. This goal is not so easy to achieve because people are easily sensitive about their organs. For example, intensive light will be intrusive to the end users during iris image capturing.

BHMI structure

Fig. 2.91 shows a general structure of the human-machine interface of a biometrics system. Generally, the end user presents his or her biometrics source, i.e., a finger in a fingerprint system, an eye in an iris system. Then the capturing device gets a sample of the biometrics characteristic. Usually, this sample will not be sent to the computer immediately because it is not suitable to be processed at the moment.

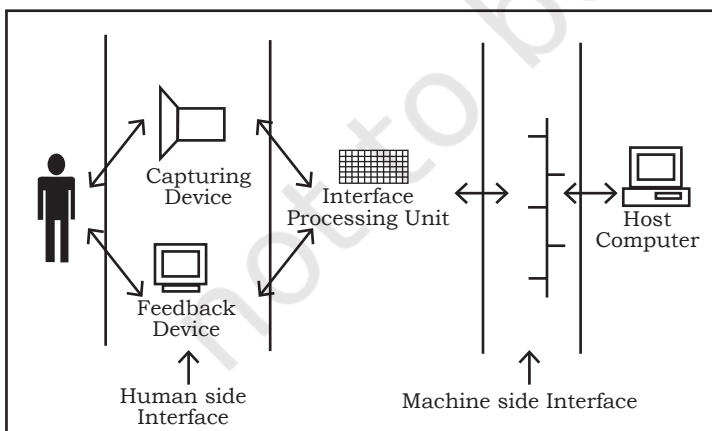
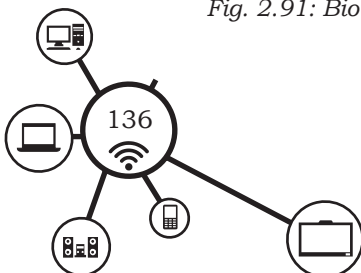


Fig. 2.91: Biometric Human Machine Interfaces

For example, the initial image captured in an iris system will probably not have the iris located in the centre of the picture without the interaction of the end user. So the feedback device is needed in most of the biometrics systems. The end user can make corresponding adjustments aided by the feedback presented on the feedback device. This is just like the end user adjusts his or her eye's location so as to make the



iris image in the centre of the picture in an iris system. The sample is sent to the computer when it is good enough for processing. The system may sense this automatically or the end user decides this by pushing a button or other inputting methods.

Biometric interfaces exist at a variety of levels—from low-level internal interfaces to high level interfaces.

Practical Activity 6

Demonstration of Aadhaar Card Biometric System

Material required

Computer, web cam, scanner, iris scanner, fingerprint scanner

Procedure

1. Connect all biometric devices to the computer as shown in Fig. a.
2. Start interface software on the computer system and check if all devices are working properly.
3. Observe interfacing menes appearing on screen.
4. Read and understand the error messages displayed on screen.



Fig. a

Practical Activity 7

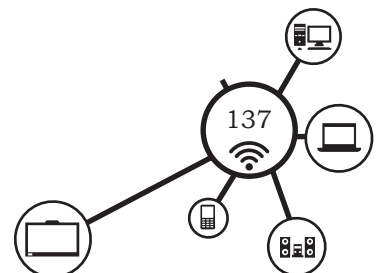
Installation of Aadhaar Enrolment Client Interface

Material required

Computer, Aadhaar Enrolment Client Software

Procedure

1. To install the Aadhaar Enrolment Client interface, we need to have its installation file. For example, in this case the name of executable installation file for Aadhaar Enrolment Client is **gSetup_Aadhaar_Enrolment_Client_v2.2.0.0.exe**.
2. Follow the steps below to install the Aadhaar Enrolment Client.
 - Double-click on the gSetup_Aadhaar_Enrolment_Client_v2.2.0.0.exe file located directly under AadhaarEnrolmentClient folder.
3. To install the Aadhaar Enrolment Client you should have administrator privilege.



NOTES

- The **Aadhaar Installer** screen appears as shown in Figs a and b.

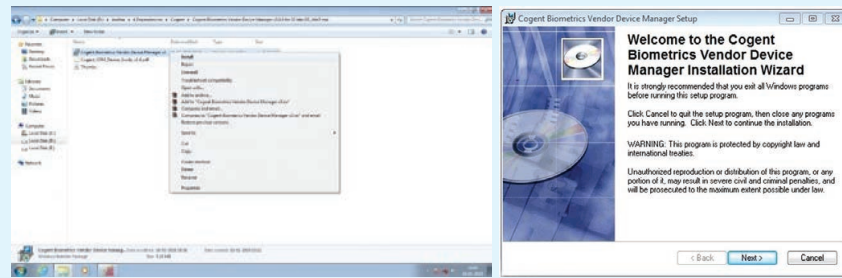


Fig. a and b

- Click on the **Next** button to start the installation. The License Agreement page appears as shown in the Figure above.
- Click the **I Agree** button. The Choose Installation Location screen appears.
- Click on the **Next** button to start the installation. The License Agreement page appears as shown in the Figure above.
- Click the **I Agree** button. The Choose Installation Location screen appears as shown in the Figs c and d.

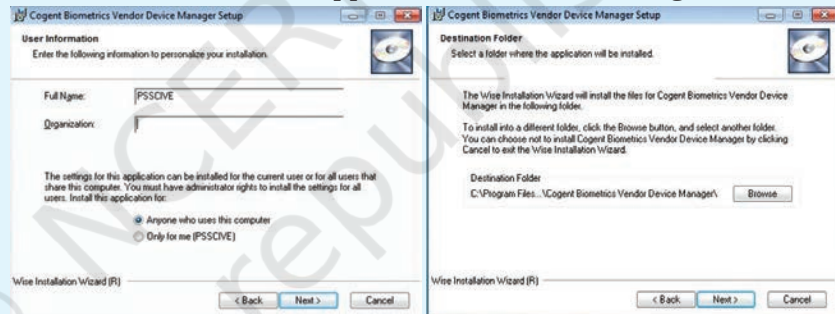


Fig. c and d

- Select the installation location by clicking on the Browse button. By default the installation location is selected as **C:\Program Files**. Click the **Next** button to start the installation. The installer installs all the components automatically, and prompts after successful installation.
- Click Finish to complete the installation.
- After successful installation, the Aadhaar Enrolment Client icon appears on the desktop as shown in the Fig. e.

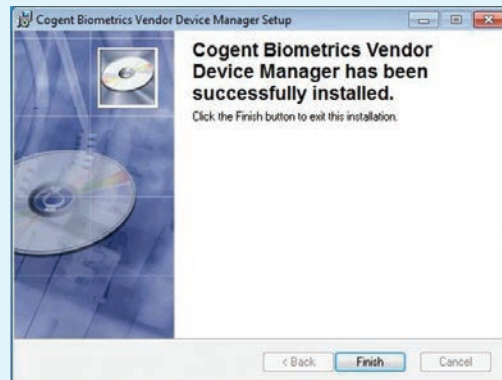
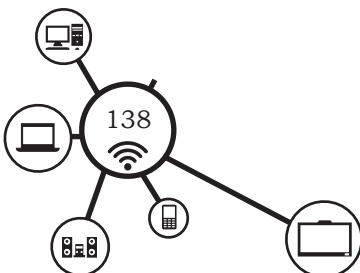


Fig. e



Practical Exercise

1. Draw interface connectivity diagram for biometric attendance system. Illustrate the procedure required for interfacing.
2. Draw interface connectivity diagram for preparation of school ID card. Illustrate the procedure required for interfacing.

NOTES

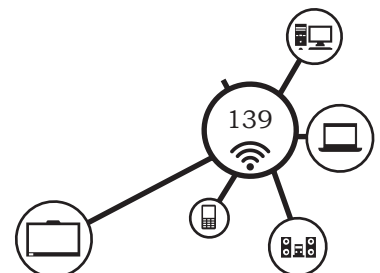
Check Your Progress

A. Fill in the blanks

1. The system by which one biometric system element communicates with another is called _____.
2. Biometric interface contains _____ and _____ of the system.
3. By using biometric interface _____ is exchanged between the devices.
4. Biometric interface provides the basis for _____.
5. Biometric interface is one of the _____ interfaces.
6. BHIM means _____.
7. At both the end sides of interface there are _____.
8. In early days the human computer interaction takes place through _____.

B. Multiple choice questions

1. In case of disk operating system the human machine interaction was performed through _____.
(a) punch cards
(b) command line interfaces
(c) window interfaces
(d) writing pads
2. In modern computers the human machine interface is performed through _____.
(a) punch cards
(b) command line interfaces
(c) windows and menus interface
(d) None of the above
3. The popularity of the computer is increased because of _____.
(a) rapid development in human computer interface
(b) advancement in hardware technology
(c) advancement in software technology
(d) reduction in the cost



NOTES

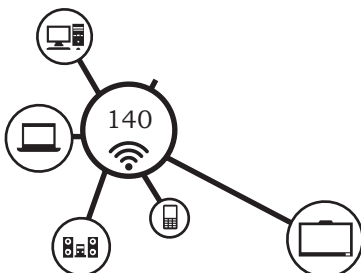
4. All the devices in the biometric interface communicate with each other by using _____.
 - (a) wires
 - (b) network services
 - (c) communication protocol
 - (d) through air
5. The following goal must be achieved by biometric interface _____.
 - (a) producing high quality output for verification
 - (b) consuming less electricity for operation
 - (c) using minimum software
 - (d) using minimum hardware resources
6. Providing user friendliness to the end user is difficult to achieve in biometric interfaces because _____.
 - (a) people do not cooperate
 - (b) people are not ready to give their data
 - (c) hardware and software do not provide user friendliness
 - (d) people are sensitive about their organs

C. State whether the following statements are True or False

1. Usually the sample obtained by the capturing device cannot be stored in the computer immediately because it is not in suitable form.
2. Most of the time the iris image is located at the centre of the picture.
3. Feedback devices are not needed in biometric systems.
4. Biometric interfaces exist only at one level.
5. For enrolment of Aadhaar data we need Aadhaar enrolment client interface.
6. In biometric system the biometric data is exchanged.

D. Short answer questions

1. What is biometric interface?
2. Explain the functioning of Biometrics Human-Machine Interface.
3. Give the steps for installation of Aadhaar enrolment client interface.
4. Give the salient features of Aadhaar enrolment client interface.



Domestic Biometric Data Operator-Class 11- Unit 2 Session 1

A. Fill in the blanks

1. A biometric device is a (an) _____ device.
2. Palm of the hand of a person is identified by using _____ device.
3. Iris of a person is identified by using _____ device.
4. BAT stands for _____.
5. The electronic device to register the digital image of the fingerprint pattern is known as _____.
6. Visible pattern is captured and then turned into electrical signal by using _____ sensor.
7. Optical sensor consists of array of _____.
8. Modern fingerprint sensors makes use of _____ or _____ optical imagers.
9. Photographic print images can be digitised by using _____ device.
10. In shopping stores, valuation of goods is normally performed by using _____ device.
11. A film scanner is used to scan _____.
12. The coloured ring of the eye muscle is called _____.
13. The smallest unit of the digital image is called _____.
14. Resolution of camera is expressed in terms of _____ on horizontal and vertical axis.
15. The sharpness of the image is determined by its _____.
16. Camera's with a resolution of 10 megapixel have _____ x _____ pixels.
17. Sensitivity of the digital camera is measured in terms of _____.

B. Multiple choice questions

1. A fingerprint device's performance is judged by using which of the following parameters?
(a) Audio (b) Display
(c) Sensor technology (d) Temperature range
2. Android-based biometric device has _____ connectivity.
(a) USB port (b) Wi-Fi
(c) Both (a) and (b) (d) wired
3. A typical false acceptance rate of biometric attendance system is _____.
(a) 10% (b) 50%
(c) 100 % (d) .0001%
4. Which of the following is not a part of digital camera?
(a) Power button (b) Lens
(c) Shutter button (d) DSLR

5. On drones and bicycles the camera that can be attached is called _____.
- (a) action camera (b) 360 camera
(c) film camera (d) DSLR
6. Full circle panoramic photos and videos can be obtained by using which of the following cameras?
- (a) Action camera (b) 360 camera
(c) Film camera (d) DSLR
7. The image quality is highest in _____ camera.
- (a) action (b) 360
(c) film (d) DSLR
8. Red eye correction and white balanced feature is available in which of the following devices?
- (a) Fingerprint sensor (b) Slap scanner
(c) Digital camera (d) Printer
9. The close look of the subject when they are physically far away can be obtained by using _____ feature.
- (a) red eye correction (b) zoom
(c) image stabilisation (d) noise reduction
10. The document can be fed in case of horizontal or vertical slot in _____ scanner.
- (a) sheet feed (b) hand held
(c) drum (d) photo

C. State whether the following statements are True or False

1. Fingerprint scanning system is being used in India since 1897.
2. A biometric device is a security identification and authentication device.
3. Face scanner identifies a person without measuring the person's face.
4. In an iris scanner an iris code is generated.
5. CCD detectors are not sensitive to low level of light.
6. Sensors using capacitive sensors are large in size.
7. DSLR means Digital Soft Lens Reflex.
8. Most of the digital cameras are water resistant.
9. Android-based biometric device makes use of an android operating system.
10. The minimum size of an image in fingerprint device is 192×8 pixels.

D. Short answer questions

1. Describe the process of fingerprint scanning.
2. State the parameters to judge the performance of a fingerprint device.
3. List any five specifications of biometric attendance device.
4. List the commonly used biometric devices.
5. What is a scanner? State their different types along with uses.
6. Explain the concept of pixel and resolution.
7. State any four features of a digital camera.
8. How can iris and fingerprint of a person be used for authentication?

Domestic Biometric Data Operator-Class 11- Unit 2 Session 2

A. Fill in the blanks

1. Before using any biometric device one needs to _____ device.
2. A biometric device is a security identification and _____ device.
3. Fingerprint scanner device can be connected to the _____ port of the computer system.
4. Fingerprint scanner device needs _____ for its installation.
5. Face scanners identify a person by taking measurements of _____.
6. Web camera is a _____ device.
7. Plug and play devices automatically get _____.
8. Iris scanner is connected to the _____ port of the computer system.
9. Biometric retina or iris scanner identifies a person by scanning the iris or retina of their _____.
10. A fingerprint sensor is an electronic device used to register a digital image of the _____ pattern.
11. Configuration of the scanner can be done by using _____.
12. Configuration of the biometric devices can be done by using _____ provided by the vendor.
13. While installing fingerprint scanner device _____ must be appropriately adjusted.
14. The voltage between earth and neutral point should be less than _____ volts.
15. In case AC power is not available then devices can be used by using _____.
16. The typical IP address of the device contain _____ numbers.

17. The subnet mask of the device contain _____ numbers.
18. For the data flow upstream and downstream the recommended ports must be _____ in the network.
19. Android based devices require a _____ network.

B. Multiple choice questions

1. In case Wi-Fi network is not available then we should use _____ network.
- (a) SIM (b) data
(c) LAN (d) Intranet
2. Android based biometric devices makes use of _____ services.
- (a) LAN (b) Cloud
(c) Intranet (d) SIM network
3. In identification the input image is compared with _____.
- (a) online image (b) stored image
(c) selected image (d) offline image
4. In verification, the database input image is compared with _____.
- (a) online image (b) stored image
(c) selected image (d) offline image

5. Which of the following is not a biometric technique?
- (a) Retina (b) Badge
(c) Face (d) Palm
6. What is the most common type of biometric device used in organisations?
- (a) Face recognition (b) Fingerprint scanners
(c) Signature recognition (d) Voice recognition
7. What makes biometrics the strongest authentication methods?
- (a) Fingerprints, voice patterns and faces are all unique
(b) It is difficult to copy or spoof biometric data
(c) Biometric data is analog and not digital
(d) Biometrics are typically used as part of a two-factor authentication system
8. The input voltage and live and earth point should be _____.
- (a) 0-100 V (b) 220-240 V
(c) 110 V (d) 300 V
9. The bracket of the fingerprint device must be fitted at _____ height.
- (a) 6 feet and above (b) 4 to 5 feet
(c) ground level (d) the top
10. Setting up of biometric devices require connectivity and _____.
- (a) fixing (b) wall mounting
(c) installation (d) fitting

C. State whether the following statements are True or False

1. For identification of Aadhaar biometric data we need to enter Aadhaar card number.
2. A typical IP address is written as 255.255.255.
3. A typical subnet mask is normally expressed as 255.255.255.0.
4. Plug and play devices get automatically installed on the computer system.
5. The location of the biometric device must be exposed to the rain, heat or sunlight.
6. Before connecting any biometric device, proper electrical earthing must be performed.
7. Device drivers of the biometric devices can be obtained through Internet.
8. GPS means Global Positioning System.
9. Active and deactivate devices are shown in the taskbar of operating System.
10. Web camera cannot be connected to the USB port of the computer system.
11. Iris scanner requires no device driver for its installation.

D. Short answer questions

1. Write the steps for installation of fingerprint device.
2. Write the steps for setting of web camera on your computer system.
3. What is a GPS device? How can it be installed on the computer system?
4. What do you mean by device driver? Explain how to obtain device driver for biometric devices.
5. Write the steps for configuration of biometric device by using computer system installed on your computer.
6. Write the steps for android-based fingerprint configuration.
7. Write steps to set up android-based fingerprint scanner.
8. Write steps for setting up iris scanner.
9. What are guidelines for setting up a digital camera?
10. Explain biometric data exceptions.
11. Discuss errors and errors handling process.
12. Differentiate between identification and verification of biometric data.

Domestic Biometric Data Operator-Class 11- Unit 2 Session 3

A. Fill in the blanks

1. Capturing data by using biometric devices is called _____.
2. The initial creation of data for all employees of the organisation is known as _____.
3. In biometric data the employee is identified by _____.
4. The holiday management of the individual employee is based on _____ data.
5. Length of the service of the employee can be determined by using _____ data.
6. Master data file can be uploaded only by _____.
7. When individual fingerprint data of all employees is created, then it is called _____.
8. Uploading of master data file to the server is also known as _____.
9. In Aadhaar card data enrolment first of all _____ data is collected.
10. For Aadhaar enrolment we require _____ software.
11. For Aadhaar enrolment one needs to fill _____ form.
12. Proper enrolment of the data is called _____.
13. In Aadhaar enrolment if the fingers are not placed on the scanner in the right sequence then _____ occurs.
14. The iris data will not be accepted by Aadhaar system if its data accuracy is below _____.
15. In biometric system FAR must be _____.

B. Multiple choice questions

1. Data duplication in biometric data can be checked by _____ method.
(a) score based (b) target based
(c) Both (a) and (b) (d) None of these
2. Biometric data has exceptions due to which of the following reasons?
(a) Environment and usage can affect measurements
(b) Systems are not 100% accurate
(c) Require integration of additional hardware
(d) All of the above
3. When the biometric device is unable to capture the image because of any reason, then it is called _____.
(a) failure to capture (b) failure to acquire
(c) failure to enroll (d) failure to register
4. FTE means _____.
(a) failure to enroll (b) false to enroll
(c) fault to enroll (d) fault to exam
5. In biometric systems FAR stands for _____.
(a) file allocate rate (b) file accept rate
(c) false accept rate (d) None of these

6. A false negative is a failure to match a sample against correct reference and it is called _____.
 (a) FAR (b) FRR
 (c) EER (d) FTE
7. A high threshold means a low FAR, but FRR will be _____.
 (a) high (b) low
 (c) medium (d) extremely low
8. A low means a low FRR, but FAR will be _____.
 (a) high (b) low
 (c) medium (d) extremely low
9. The point where FAR and FRR are balanced is known as _____.
 (a) EER (b) FTA
 (c) FTE (d) FRR
10. When FAR approaches to zero it may cause _____.
 (a) a very low FRR (b) very high FRR
 (c) FRR equal to zero (d) None of these
11. For the access to the site of national security the threshold must be set to _____.
 (a) low (b) extremely low
 (c) medium (d) high
12. Data validation is a process of ensuring _____ data.
 (a) raw (b) mismatch
 (c) quality (d) poor

C. State whether the following statements are True or False

1. In Aadhaar enrolment the correct order of placing the fingers for scanning is first of the right hand then left.
2. For new enrolment in Aadhaar we need to fill our information on Aadhaar enrolment form.
3. The uploading of the data in Aadhaar enrolment is performed through export enrolment data.
4. Bank details of resident can be entered in Aadhaar enrolment.
5. Printing of the Aadhaar data can be performed through export enrolment data.
6. Enrolment of the data of the resident is performed by using Aadhaar enrolment client.
7. To capture the iris data the iris scanner should not be close to the eyes.
8. To capture the face image the background must be clear.
9. Head rotation or tilt is acceptable while capturing face data.
10. Smiling is not allowed while capturing the face image of an enrollee.

D. Short answer questions

1. Give the steps for registration and enrolment of biometric data in biometric attendance system.

2. List various fields that are required while collecting the data of an employee. Mark them as sensitive, very sensitive and non-sensitive elements.
 3. State the reasons why some data elements should be marked as sensitive and very sensitive.
 4. What do you mean by master data?
 5. What do you understand by the term enrolment of data?
 6. Give the steps for data enrolment in Aadhaar card.
 7. Identify important documents to be attached with Aadhaar enrolment form.
 8. What is data validation? How is it performed in the data enrolment of Aadhaar card?
 9. Write the procedure for collecting biometric data.
 10. Write the steps to capture face biometric data.
 11. What are different types of errors that may occur in data enrolment?
 12. Define the terms FAR, FRR, ERR.
 13. Define the term FTA and FTE.
 14. How can the death of a resident can be reported in Aadhaar?
 15. What is biometric data exceptions? Give reasons for it.
16. What is data duplication in biometric data?
 17. State the percentage of duplication in Aadhaar biometric data.

Domestic Biometric Data Operator-Class 11- Unit 2 Session 4

A. Fill in the blanks

1. The system by which one biometric system element communicates with another is called _____.
2. Biometric interface contains _____ and _____ of the system.
3. By using biometric interface _____ is exchanged between the devices.
4. Biometric interface provides the basis for _____.
5. Biometric interface is one of the _____ interfaces.
6. BHIM means _____.
7. At both the end sides of interface there are _____.
8. In early days the human computer interaction takes place through _____.

B. Multiple choice questions

1. In case of disk operating system the human machine interaction was performed through _____.
 - (a) punch cards
 - (b) command line interfaces
 - (c) window interfaces
 - (d) writing pads

2. In modern computers the human machine interface is performed through _____.
- (a) punch cards
 - (b) command line interfaces
 - (c) windows and menus interface
 - (d) None of the above
3. The popularity of the computer is increased because of _____.
- (a) rapid development in human computer interface
 - (b) advancement in hardware technology
 - (c) advancement in software technology
 - (d) reduction in the cost
4. All the devices in the biometric interface communicate with each other by using _____.
- (a) wires
 - (b) network services
 - (c) communication protocol
 - (d) through air
5. The following goal must be achieved by biometric interface _____.
- (a) producing high quality output for verification
 - (b) consuming less electricity for operation
 - (c) using minimum software
 - (d) using minimum hardware resources
6. Providing user friendliness to the end user is difficult to achieve in biometric interfaces because _____.
- (a) people do not cooperate
 - (b) people are not ready to give their data
 - (c) hardware and software do not provide user friendliness
 - (d) people are sensitive about their organs

C. State whether the following statements are True or False

1. Usually the sample obtained by the capturing device cannot be stored in the computer immediately because it is not in suitable form.
2. Most of the time the iris image is located at the centre of the picture.
3. Feedback devices are not needed in biometric systems.
4. Biometric interfaces exist only at one level.
5. For enrolment of Aadhaar data we need Aadhaar enrolment client interface.
6. In biometric system the biometric data is exchanged.

D. Short answer questions

1. What is biometric interface?
2. Explain the functioning of Biometrics Human-Machine Interface.
3. Give the steps for installation of Aadhaar enrolment client interface.
4. Give the salient features of Aadhaar enrolment client interface.



Operating System and System Maintenance



17110SCH03

INTRODUCTION

Biometric systems work on computing device, such as laptop, iPad, tablet or smartphone, and requires an essential software to work which is known as operating system. Biometric devices are connected with computing devices or is an integrated self-contained unit. An integrated biometric attendance system uses Android operating system while Windows or Linux operating system can be used in a computer. The biometric devices take input from the user and the data is processed in the server. The server also needs an operating system to process the biometric data. When any device or software is operated over a period of time its maintenance and updating is also essential as failure or wear and tear of any component in the biometrics system can cause a problem in operations.

In this unit, you will understand the need and importance of operating system, its features, functions, and also updating and maintenance.

SESSION 1: OPERATING SYSTEM

Suppose your father gifts you a bicycle for your birthday and you are excited to ride it. But as soon as you sit on it, you are unable to balance. Simply owning the cycle cannot help you ride it. Similarly, using an operating system is like riding a bicycle. One cannot use a computer without understanding the functioning of an operating system. In this session, you are going to understand the concept of operating system and embedded operating system. You will also understand the various jobs that can be performed by the operating system. For biometric data collection, we require a different interface. One such interface has also been discussed in this session.

Operating System

An operating system (OS) is a system software that manages computer hardware resources and provides services for programs. OS is an interface between the user and the computer hardware. It allows you to communicate with the computer hardware. It is impossible to use computing hardware without OS. Fig. 3.1 shows an operating system interface. The hardware is placed at the center, the operating system is at the upper level, the User interface is on the next level and the applications are at the outer most level. The User can interact with hardware only through applications.

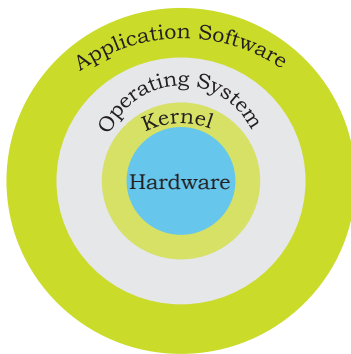


Fig. 3.1: Operating system interface

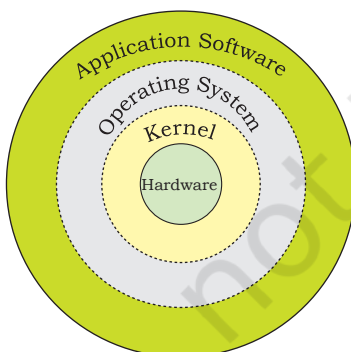
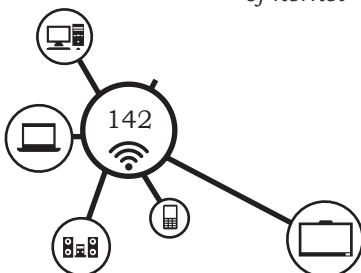


Fig. 3.2: Operating system interface showing placement of kernel

Structure of operating system

The kernel and shell are the main parts of an operating system. Any command given by the user first goes to the shell. The shell interprets it and sends it to the kernel. The kernel processes the request and displays the result on the screen. Fig. 3.2 shows that the kernel is close to the hardware while shell can interact with the kernel and the user.

- **Kernel:** is a bridge between the shell and hardware. It is the core of the operating system as every operation is performed by it. It is responsible for running programs and providing secure access to the hardware.



- **Shell:** acts as an interpreter to convert the commands from the user to a machine code. Shells present in different types of operating systems are of two types—command line shells and graphical shells. The command line shells provide a command line interface while graphical line shells provide a graphical user interface.

Types of operating systems

Operating systems are classified as Desktop OS and Server or Network OS. Windows and Linux OS comes for both the Desktop as well as Server OS. Desktop OS is used for single computer while Network OS is installed in server. OS are open source or proprietary. Linux is the open source while Windows is proprietary OS. Desktop OS, such as Windows, Linux, Unix are used for computer while Android and iOS are used in mobile devices, such as tablet and smartphone. OS are classified into different types depending on processing—(i) Single user, (ii) Multiuser, (iii) Multitasking, (iv) Multiprocessing and (v) Embedded.

- **Single user OS:** is used by a single user in a single computer for performing a single task. MS-DOS is an example of single user OS. It is not in use now. Fig. 3.3 shows a user using single user OS.
- **Single user multitasking OS:** allows execution of more than one task or process at a time. A user can perform multiple tasks, such as working on the document, printing and listening music at a time. For this, the processor time is divided amongst different tasks. Windows, Linux and Mac OS, are the examples of multitasking OS. Fig. 3.4 shows a single user multitasking OS.
- **Multiuser OS:** allows to be used by multiple users at a time. It is used in networking where data and applications are accessed by multiple



Fig. 3.3: Single user OS

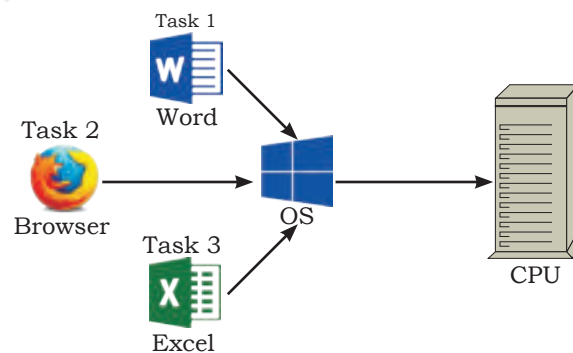
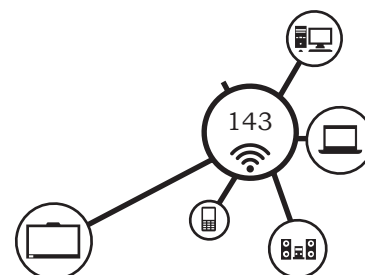


Fig. 3.4: Single user multitasking OS



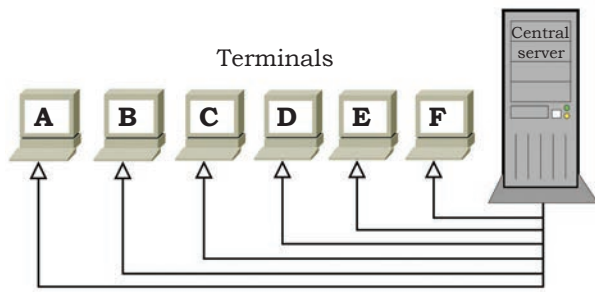


Fig. 3.5: Multiuser OS

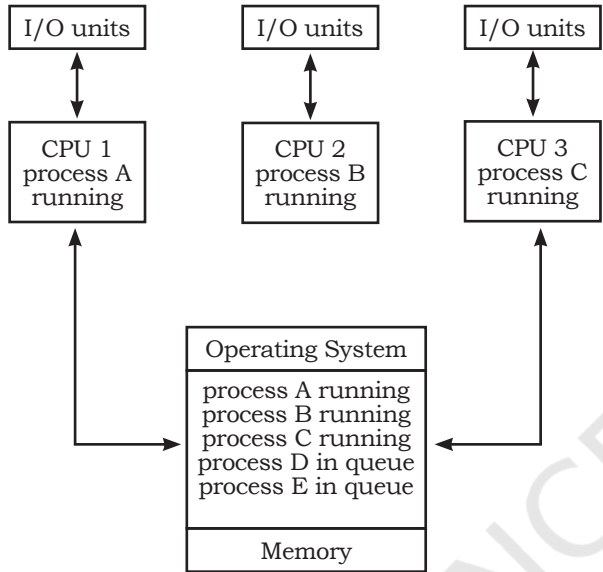


Fig. 3.6: Multiprocessing OS

users at the same time. The server OS, such as Windows server, Linux server and Unix server are examples of multiuser OS. Fig. 3.5 shows the such multiuser OS.

- **Multiprocessing OS:** has two or more processors running in parallel. It is also called parallel processing. It is used for complex applications, where processing of multiple processes is required. Windows, Linux and UNIX OS supports for multiprocessing. Fig. 3.6 shows multiprocessing OS. In Fig. 3.6 there are three processors–A,B,C. OS manages three different processes running on different processors. Other processes D, and E are kept in que by OS. This is because there is no processor available for their execution. This is how OS manages multiple processes in the computer system.
- **Embedded OS:** is embedded in a device in the ROM. They are specific to a device and are less resource intensive. They are used in appliances like microwaves, washing machines, traffic control systems, Fig. 3.7 shows the embedded OS and standard OS.

Embedded OS

Standard OS

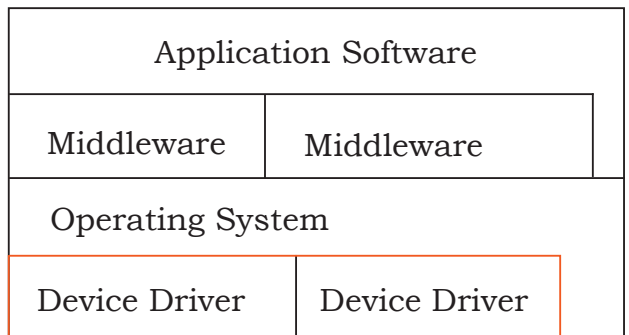
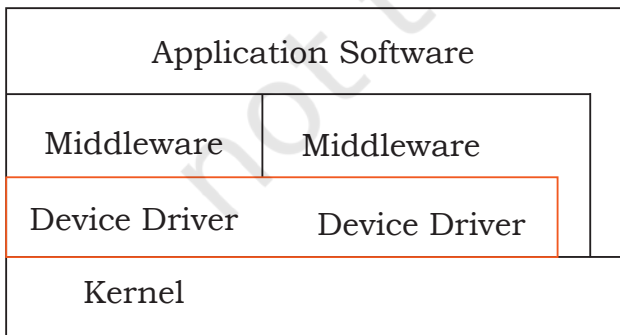
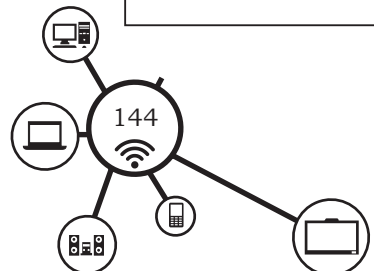


Fig. 3.7: Embedded OS and Standard OS



Embedded System

An embedded system has software embedded in computer hardware as shown in Fig. 3.8. It is dedicated to a specific part of an application or product of a larger system. An embedded system has three main components—embedded system hardware, embedded system software and operating system.

Airplanes, smartphones, gaming machine, cameras, tablets, printers, electronic medical diagnosis machines, modern cars all use embedded systems for their performance improvement. Fig. 3.9 shows a block diagram of biometric embedded system. It contains sensors, programming software, hardware, storage and output interface.

Functions of the Operating System

An operating system controls and manages the various resources, such as CPU, memory, and input/output devices for optimum use of computer system. Operating system performs some basic task, such as recognising the input from keyboard or mouse, sending output to the display units, keeping track of files and directories on the hard disk, and controlling the peripheral devices, such as printer, scanner. The tasks performed by the operating system are briefly explained below.

- **Input/output management:** in a computer, transfer of information from or to the CPU and main memory is considered as Input/Output (I/O). Input and Output devices are used to perform I/O operations. Users should access all devices in a uniform manner. In order to use these devices optimally, they should be managed properly by the system. An operating system manages all I/O devices used in the biometric system. OS maintain security of the devices and optimise the performance

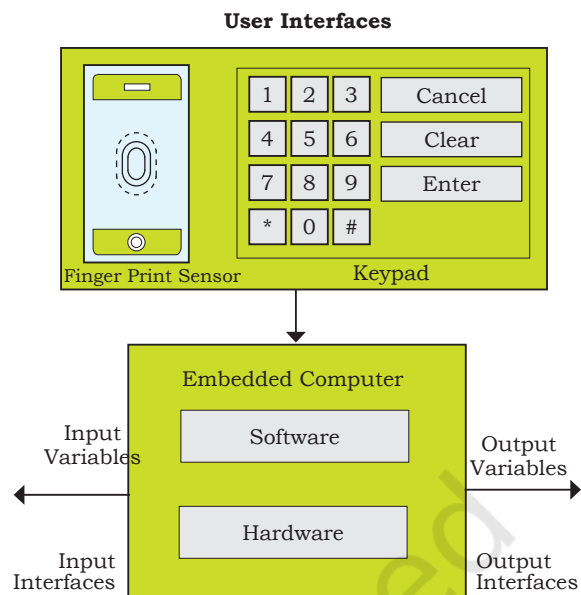


Fig. 3.8: Embedded system

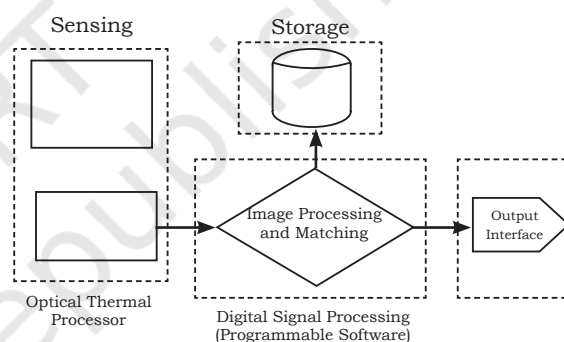
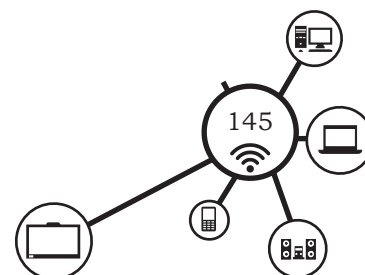


Fig. 3.9: Biometric embedded system



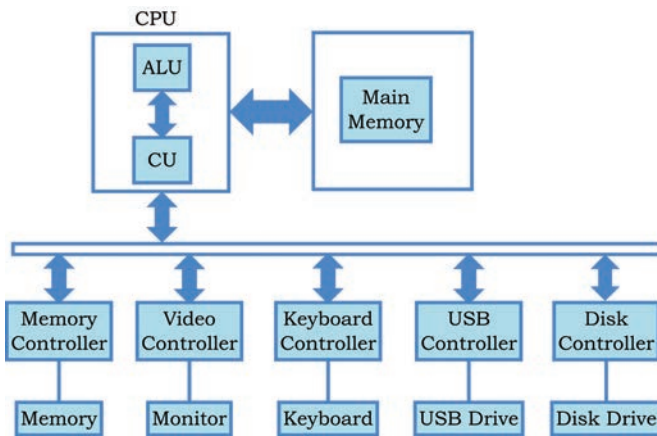


Fig. 3.10: Input output management

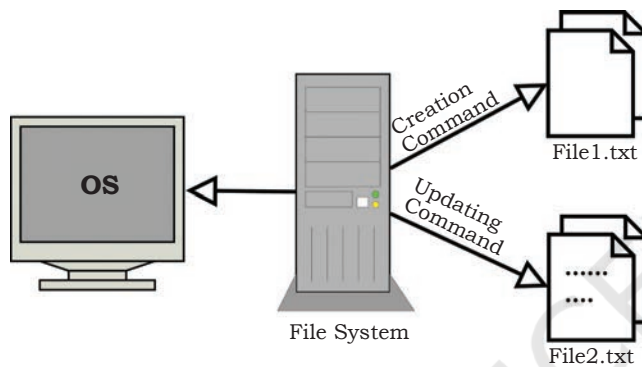


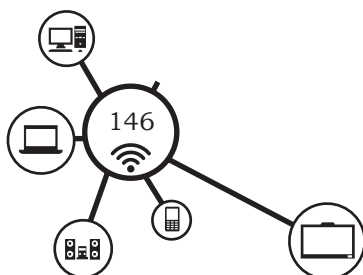
Fig. 3.11: Data management

of the I/O system. Iris scanner, fingerprint scanner, face-capturing cameras can also be controlled by using operating system installed on the computer.

Fig. 3.10 shows that I/O instruction is issued to an I/O device and the program executes in 'busy-waiting' (idle) mode till the I/O is completed. During the busy-wait period the processor is continually interrogating to check if the device has completed I/O.

- **Data management:** the data is organised into logical groups that are called files. By using operating system, we can create a file and such file can be stored, read and can be written by using the commands of operating system. Creation, updating, modification and removal or deletion of a file can be achieved through an operating system. Fig. 3.11 shows data management of operating system.

- **Memory management:** is one of the important task performed by the OS. Memory management is important in multitasking where the OS requires switching of memory from one process to another. Every single program requires some memory space for its execution, which is provided by the memory management unit (MMU). Every computer has a primary memory and secondary memory. Primary memory or RAM of a computer system can be managed by using operating system. It is basically a large array of words with each word having its own address. When the user asks the CPU for access of such memory locations, then it can be achieved through operating system. OS



loads the data into RAM and executes the data or program from memory. After completing the execution of program the memory space is made free and is made available for other programs. Fig. 3.12 gives an outlook of memory management of the operating system.

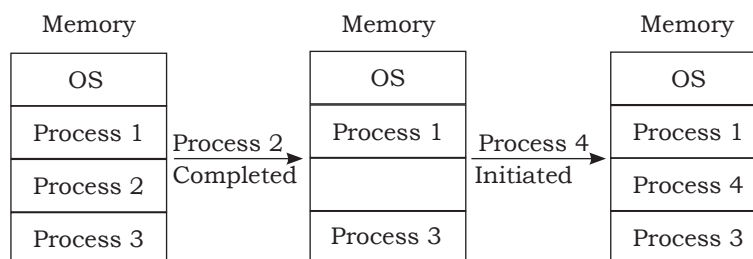


Fig. 3.12: Memory management

- Process management:** every job to be performed by the computer system is scheduled in the form of processes. These processes are managed by the operating system. A process is a program in a state of execution. A process can be created, executed and stopped. A process changes its state during execution as shown in Fig. 3.13.

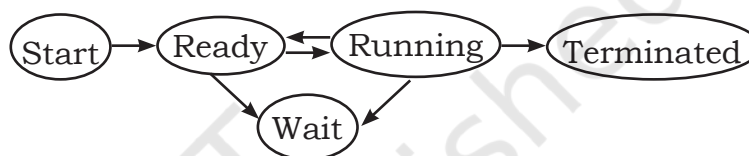


Fig. 3.13: Different states of process in process management

Stages of the process

- Start** is the initial state when a new process is first started or created.
- Ready** when the process is waiting to be assigned to a processor, it is in the ready state.
- Running** when the processor is executing the process, it is in the running state.
- Waiting** when the process is waiting for some resources or operation then it is in the waiting state.
- Terminate or exit** once the process finishes its execution, it is terminated by the operating system and removed from main memory.
- Device management** is responsible for managing all the devices including the storage device and input output devices. The OS keep track of the status of all the internal or external devices as they are free or busy. If a device requested by a process is free at a specific time, the OS allocates that device to the process. It allocates the devices, such as I/O devices for I/O operations and other

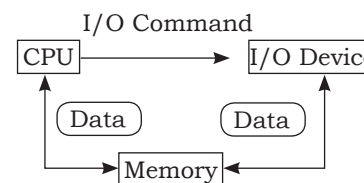
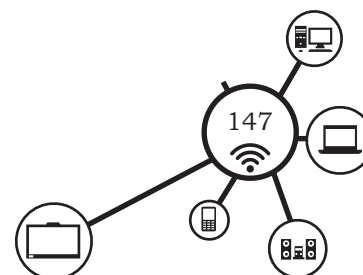


Fig. 3.14: Device management



peripherals as and when required by the processes. Once the processes gets completed then devices are made free so that they can be allocated to the other processes whenever required. An OS manages the devices in a computer system with the help of device controllers and device drivers. Fig. 3.14 shows the process flow of device management in operating system.

- **File management** operating system manages all files of the computer system. File management is the process of manipulating files and keeping track of all files in computer system. It includes the process of creating, modifying and deleting

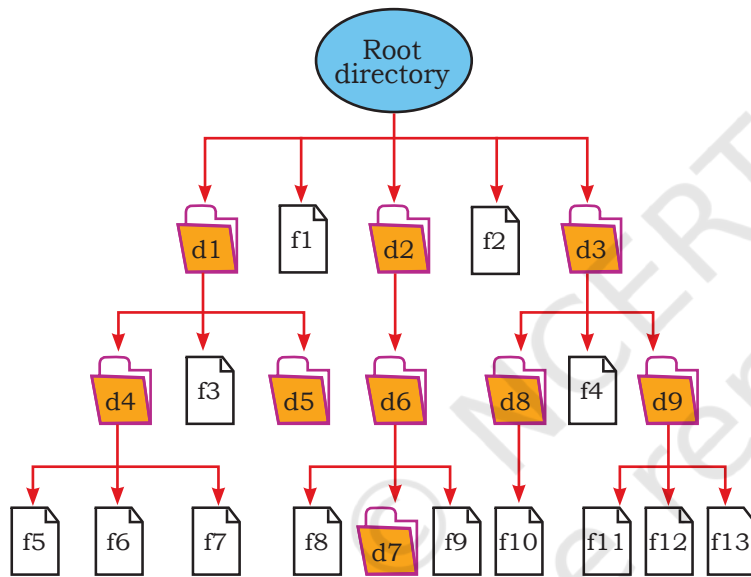
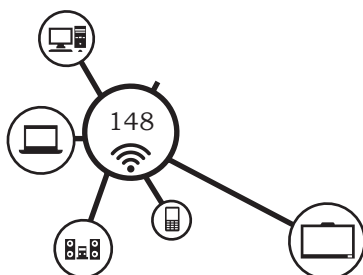


Fig. 3.15: File Management

the files. OS manages opening and closing of files whenever required. It finds and allocates the file required for the process. When the process is executed it closes the file and remove the file allocation. Fig. 3.15 shows the general hierarchy of the storage in an operating system. The root directory is present at the highest level in the hierarchical structure. It includes all subdirectories in which the files are stored. Subdirectory is a directory present inside another directory in the file storage system.

Fig. 3.15, d1, d2,d9, indicates the directions at different levels. F1, F2 F13 indicates files at different levels.

- **User interface** is close to the user. It allows users to easily access and communicate with the applications and the hardware. The users can interact with the computer by Command Line Interface (CLI) and Graphical User Interface (GUI).
- **Command Line Interface (CLI)** is also known as command line interpreter. It allows to interact user by using commands issued by the



user on the command prompt. The CLI accepts the text based commands on the command line or terminal and executes them. In CLI the correct syntax of commands has to be used, hence the commands need to be remembered by the user. CLI was used by the OS of the early days. DOS and Unix operating systems are the examples of CLI. Although the modern OS are GUI based but it also has command prompt. For example, the CLI of Ubuntu Linux is shown in Fig. 3.16. Have the command prompt indicated by and sign. The name of the terminal appears before the command prompt as shown in Fig. 3.16.

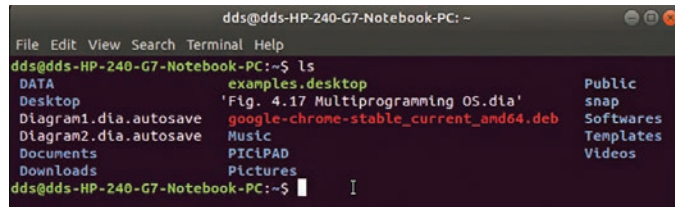


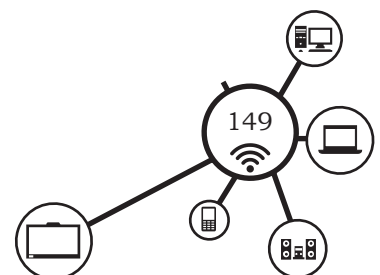
Fig. 3.16: Command Line Interface of Ubuntu Linux OS

- **Graphical User Interface (GUI)** is a modern operating system, such as Windows, Linux and Mac all uses GUI. GUI is easy to operate and user-friendly. GUI use graphics to display the various commands. The interface consists of icons, menus, windows and pointers. The user need not to learn the commands, instead, the user can give instructions by moving the pointer on the screen using a mouse and pressing the mouse button. Fig. 3.17 shows the GUI of Ubuntu Linux OS.



Fig. 3.17: Graphical User Interface of Ubuntu Linux OS

- **Time sharing management** in network environment the number of users can use the same computer system in parallel. In time sharing management the each user is allocated certain amount of time to access to the hardware of the computer system. This access time is moved from one user to another user rapidly, so that every user feels that the computer hardware is available for all the time to them. As the number of user increases the response time decrease. Time sharing manages



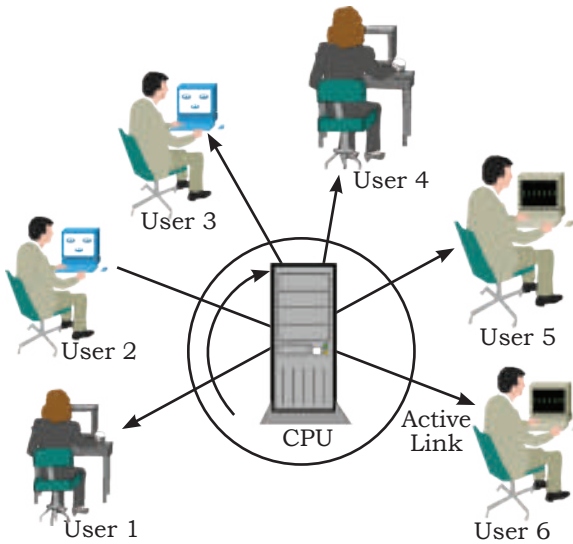


Fig. 3.18: Time sharing management

the CPU time. This time sharing management between the number of users of the computer hardware is performed by the operating systems. Fig. 3.18 shows time sharing management of operating system.

Advanced Features of Operating System

Apart from the above mentioned tasks modern operating system performs many other tasks, such as security management, deadlock prevention and virtual storage.

- **Security management** in security management the security of one user is protected from other users. The security management helps to secure and protect the computer system internally as well as externally. Internal security is the protection of activities of one process from the activities of another process. External security refers to security of data, programs and various resources of the computer system against unauthorised access. External security is necessary specially when the computer is on a network or connected to Internet.
- **Deadlock prevention** the situation where the resource shared by two or more processes cannot continue, because the resource required by a process is held by another, is called deadlock. Fig. 3.19 shows deadlock prevention. For example,

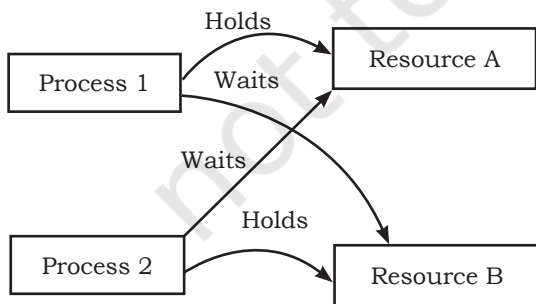
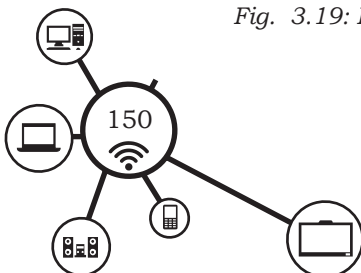


Fig. 3.19: Deadlock prevention

the resource A is allocated to process 1 and resource B is allocated to process 2, and later process 1 requests resource B, which is held up by process 2, similarly the process 2 requests resource A which is held up by process 1. All such processes are halted and waiting to free up the resources. Thus, the deadlock occurs. OS ensures that this condition does not hold and deadlock is prevented. OS allocates



the resources so that deadlock can be avoided. If deadlock cannot be avoided, OS tries to recover it.

- **Virtual storage management**

sometimes a program is much larger in size than the storage capacity of a computer system. In multiprogramming, many programs are located in the memory along with the OS. In such a case operating system makes use of secondary memory, which is termed as virtual memory. Such virtual storage management can be achieved through operating system. Fig. 3.20 shows that the physical memory gets fully utilised by certain applications. Hence, some portion of secondary memory is used as virtual memory.

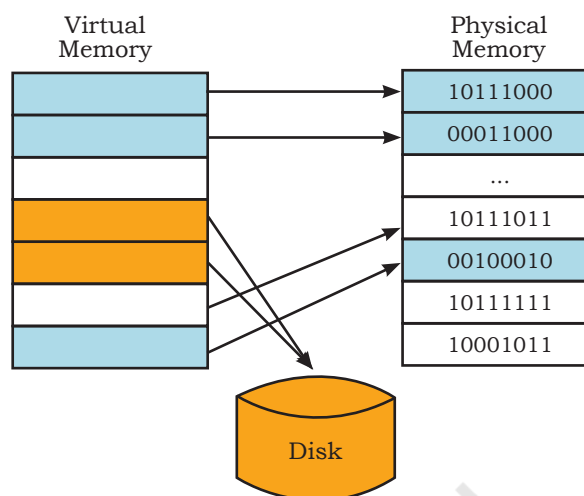


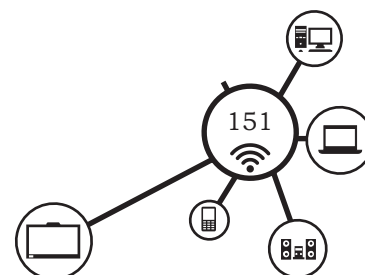
Fig. 3.20: Virtual storage management

Examples of Operating System

Operating systems are normally preloaded on the computer that you purchase. But it is possible that you can upgrade or you can install the operating system on computer hardware. There are three most common types of operating system—Microsoft Windows, Mac OS and Linux. For mobile devices, such as phones, and tablet computer, the commonly used operating systems are Apple iOS and Google Android.

- **Microsoft Windows** is a graphical user interface (GUI) operating system. In this GUI system all the programs or commands of operating system are available in the form of icons, buttons and menus. Everything within the operating system is clearly displayed on the screen by making a combination of graphics and text. Whenever we want to execute any command or program, the corresponding icon needs to be clicked.

There are various versions of Microsoft Windows OS available. Most recent version of Microsoft Windows OS is Windows 10, which is released in 2015. The



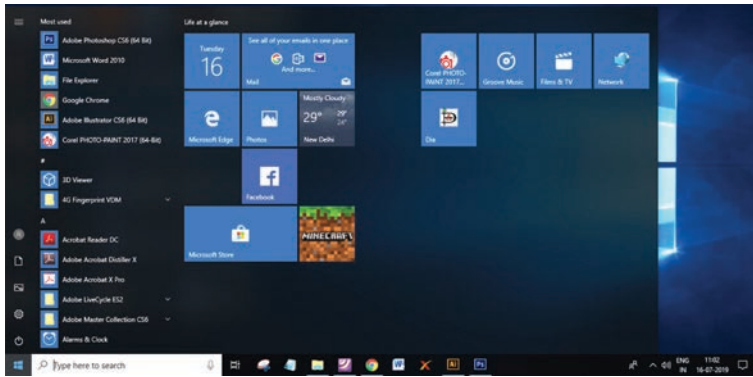


Fig 3.21: Windows 10 desktop

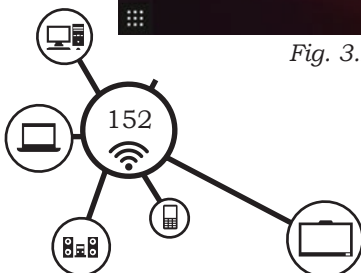
earlier versions are Windows 8 released in 2010 and Windows 7 released in 2009. Microsoft Windows is one of the most popular single user operating system. Fig. 3.21 shows typical desktop of Microsoft Windows 10 operating system.

- Linux** is a family of open source operating systems. It means that this OS can be modified and distributed by anyone around the world. OS, such as Windows and Mac OS are proprietary. It means that they can be modified only by the company that owns it. Whenever you want to use proprietary software on your computer system you need to purchase it by paying the cost so that you can get a user license. Linux is a freeware, you need not pay any cost and you can use it for free on your computer system. There are various distributions of Linux, such as Ubuntu, Debian, Fedora, Redhat, Mandriva, each having various versions. For example, the latest version of the Ubuntu Linux is 20.10. Ubuntu releases are given code names using an adjective and an animal with the same first letter. For example, Ubuntu 15.10 (Wily Werewolf), Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 16.10 (Yakkety Yak), Ubuntu 17.04 (Zesty Zapus), Ubuntu 17.10 (Artful Aardvark), Ubuntu 18.04 LTS (Bionic Beaver), Ubuntu 18.10 (Cosmic Cuttlefish) and Ubuntu 19.04 (Disco Dingo). A desktop image that runs Linux is shown in Fig. 3.22.



Fig. 3.22: Ubuntu Linux desktop

Linux is also available in the form of GUI. Every program in the Linux OS is displayed in the form of icon, button or graphics. By clicking on the icon or button



we can execute that appropriate program. There are many distributions of Linux and accordingly they have named Linux differently. For example we have Ubuntu, Linux mint, Fedora, Suse, Red Hat as the different distribution names of the Linux.

- **Mac OS** is an operating system that is created by apple. It is preloaded OS on Macintosh computer or Macs. An image of Mac OS screen is shown in Fig. 3.23.

This operating system has a graphical user interface (GUI). But the GUI of Mac OS is different from that of Microsoft Windows. All the commands and programs available in Mac OS are displayed in the form of icons or buttons. By clicking appropriate buttons, we can execute that program.

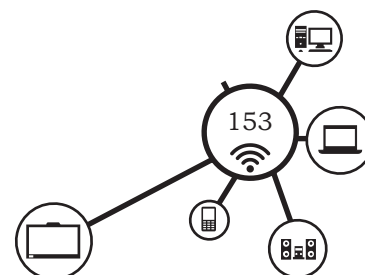


Fig. 3.23: Mac OS screen

There are various versions of Mac OS. Most recent version of Mac OS is OS X, which is pronounced as OS 10. The latest version released on 24 September 2018 is MAC OS 10.14 and is named as Mojave (Liberty). The earlier versions of Mac OS OS X 10.11: El Capitan (Gala) realised in 30 September 2015, OS X 10.10: Yosemite (Syrah) - 16 October 2014, OS X 10.9 Mavericks (Cabernet) - 22 October 2013, OS X 10.8 Mountain Lion (Zinfandel) - 25 July 2012, OS X 10.7 Lion (Barolo) - 20 July 2011.

OS for Mobile Devices

Earlier OS that were having discussed are designed for desktop and laptop computers. But these OS are not suitable for mobile devices such as smart phones and tablet computers. The most commonly used OS for mobile devices are Apple iOS and Google android.



and 1.1, every other Android version has been named. Latest version of Google Android is Android 9.0 named as Android Pie was released in 2018. The previous versions are Android 8.0 named as Android Oreo was released in 2017, Android 7.0 named as Android Nougat was released in 2016, Android 6.0 named as Android Marshmallow was released in 2015 and Android 5.0 named as Android Lollipop was released in 2015.

NOTES

Practical Activity 1

List the system elements of various operating systems

Material required

Computer with various operating systems Windows, Linux, iPad with iOS, tablet mobile phone with android operating systems

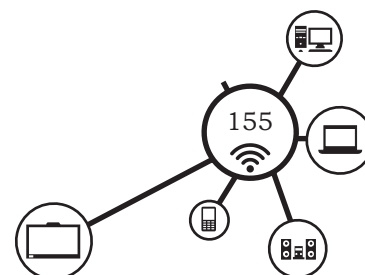
Procedure

For Windows

1. Start the desktop computer which has Windows 10 operating system and observe its user interface.
2. Identify and list the various apps that appear on the desktop.
3. List the common user interface elements of the Windows 10 as given below
 - Microsoft store
 - Maps
 - Calendar
 - Weather or News
 - Calculator
 - Skype

For Linux Ubuntu

1. Start the desktop computer which has Ubuntu Linux operating system and observe its user interface.
2. Identify and list the various apps that appear on the desktop.
3. List the common user interface elements of the Windows 10 as given below
 - Panels
 - Menu
 - System tray
 - Launcher
 - Dashboards
 - File manager
 - Terminal emulator
 - Text editor
 - Display manager



NOTES

iOS

1. Start the iPad or tablet and observe its user interface.
2. Identify and list the various icons on the initial screen.
3. List the various default apps of iOS as given below.
 - Contact
 - YouTube
 - Play store
 - Email

Android

1. Take an android tablet or smartphone and observe its user interface.
2. Identify and list the various apps on the initial screen.
3. List the various default apps of android OS as given below.
 - Play store
 - Calendar
 - Gmail
 - Messaging
 - Gallery
 - File Manager

Practical Activity 2

Perform common tasks in various operating systems

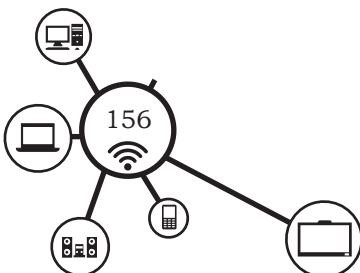
Material required

Computer with various operating systems Windows, Linux, iPad with iOS, tablet, mobile phone with android operating systems

Procedure

Windows OS: Create a document in Microsoft Word

1. Start the computer with Microsoft Windows operating system.
2. After loading the Microsoft windows, locate the icons or apps for Microsoft Office > Microsoft Word.
3. Open the application in Microsoft Word by clicking on it.
4. Create a document in MS Word.
5. Enter text in the document.
6. Apply the required formatting feature.
7. Save the document on the disk.
8. Exit the application Microsoft Word.
9. Similarly, open the other installed applications, such as MS Excel, MS Power Point.
10. Perform the relevant task on it, save your work on the disk and exit the application.
11. Take the print of the document printed by using the installed printer.



Linux OS: perform the above task in Ubuntu Linux operating system.

Android OS: similarly perform the following task in android operating system.

1. Open the Google play store.
2. Download a scanner app from the Google play store.
3. Open the app.
4. Scan some documents using this app and send or share the scanned documents to your friends via email or WhatsApp.

Operating System Interface for Biometric Data Collection

The biometric data collection required for an application, such as Aadhaar card, we require the interface program to get installed on our existing computer system. Fig. 3.26 shows one such sample program 'Aadhaar Enrolment Client'.

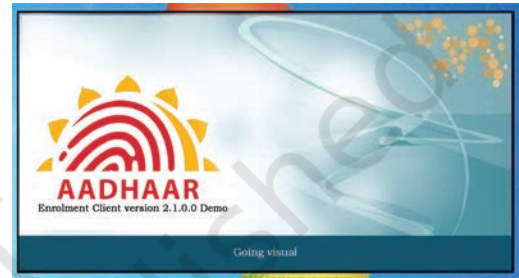
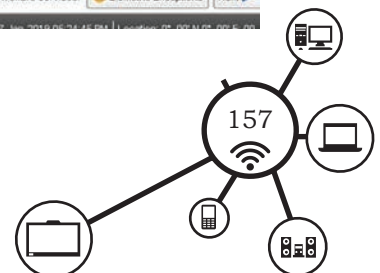


Fig. 3.26: Aadhaar Enrolment Client Window Software

Once we click on the **Aadhaar Enrolment Client** icon, the enrolment window will open as shown in Fig. 3.27.

The data entry form shown in Fig. 3.27 is used to enter the various types of biometric data, such as face, fingerprints and iris images.

Fig. 3.27: Aadhaar Enrolment Window



Check Your Progress

A. Fill in the blanks

1. The software that manages computer memory, processor and its hardware is called _____.
2. Operating system is a (an) _____ between and user and computer hardware.
3. We cannot use computer hardware without _____.
4. When hardware and software are added together to perform a specific function it is called _____ system.
5. Aeroplane, smartphone and gaming machines are examples of _____ system.
6. Input, output and device management is performed by _____.
7. File creation, updating and modification is referred to as _____.
8. Loading of the data or program in memory and executing program from the memory is called _____.
9. Allocation of the CPU to the different processes is known _____.
10. Allocation of the files to different processes is called _____.
11. When a number of users use the same computer system in parallel then it is _____ management.
12. In time sharing management every user is allocated a small amount of CPU time and it is known as _____ time.
13. In multiuser operating system the security of one user is protected from the other user and it is referred to as _____ management.
14. When two or more processes cannot continue because they want to share the same resource then this situation is called _____.

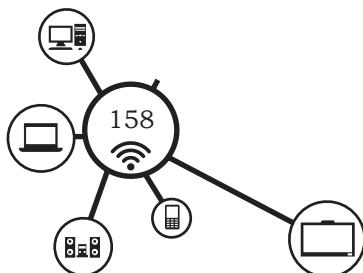
B. Multiple choice questions

1. Microsoft Windows is _____ operating system.

(a) single user	(b) multi user
(c) open source	(d) time sharing
2. Which of the following does not support more than one program at a time?

(a) DOS	(b) Linux
(c) Windows	(d) Mac
3. Linux is a _____ operating system.

(a) open source	(b) proprietary
(c) Unix	(c) mobile



4. Which one of the following is not a multitasking operating system?

(a) Windows	(b) MS DOS
(c) Unix	(d) Linux
5. The primary purpose of an operating system is to _____.
 - (a) make the most efficient use of computer hardware
 - (b) allow people to use the computer
 - (c) keep the programmer engaged
 - (d) make the computer easier to use
6. Virtual memory means _____ memory.
 - (a) primary
 - (b) secondary
 - (c) Both (a) and (b)
 - (d) None of the above
7. The latest version of Microsoft Windows operating system is _____.

(a) Windows 98	(b) Windows 8
(c) Windows 10	(d) Windows 15
8. Operating system developed by the Apple corporation is _____.

(a) Window	(b) Linux
(c) Mac	(d) Android
9. Which of the following is an open source operating system?

(a) Window	(b) Linux
(c) Mac	(d) Android
10. Which of the following is an operating system for mobile device?

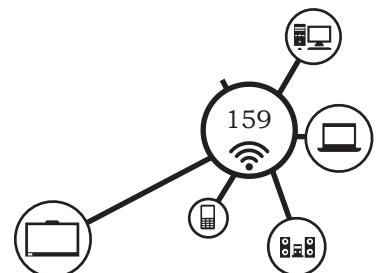
(a) Window	(b) Linux
(c) Mac	(d) Android
11. Android 8.0 is named as _____.

(a) Android Oreo	(b) Android Marshmallow
(c) Android Lollipop	(d) Android Nougada
12. In 2018 Apple released _____.

(a) iOS 11	(b) iOS 12
(c) iOS 13	(d) iOS 14

C. State whether the following statements True or False

1. Operating system is an application software.
2. Operating system allows to communicate with computer hardware.
3. Modern cars are not examples of embedded system.
4. Input/output device management can be performed by using operating system.



NOTES

5. Data and file management cannot be performed by using operating system.
6. In process management threads are managed by the operating system.
7. Only single user can access a computer system in time sharing management.
8. Virtual storage management can be achieved through operating system.
9. Microsoft Windows has a graphical user interface.
10. Mac operating system was developed by Microsoft.
11. Windows and Mac operating systems are proprietary software.
12. Ubuntu, Red hat and Fedora are different distributions of Linux operating system.
13. Mobile devices, such as tablets and mobile phones do not have an operating system.

D. Short answer questions

1. What is a mobile operating system? State the features of a mobile operating system.
2. Differentiate between single user and multiuser operating systems.
3. List the features of Windows operating system.
4. State the features of Linux operating system.
5. State the different types of tasks that can be performed using an operating system.
6. What are the advanced features of an operating system?
7. What are the different types of operating systems?

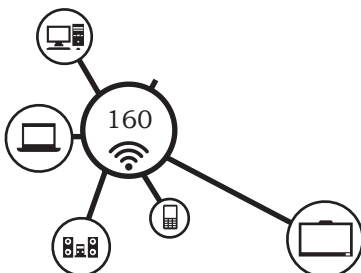
SESSION 2: MAINTENANCE OF BIOMETRIC SYSTEM

Biometric systems require regular maintenance, else there are chances that the system will not work or the data in the system might get lost. In this session, we are going to study the concept of system maintenance and virus and malware software, importance of taking backup of data. Various antivirus software have also been discussed in this session.

Biometric System Maintenance

Any working system is evaluated by its intended performance. The results obtained from the evaluation process help to determine whether the system is effective and efficient. The process of monitoring, evaluating and

DOMESTIC BIOMETRIC DATA OPERATOR – CLASS XI



modifying the existing systems to make the required or desirable improvements may be termed as system maintenance. System maintenance is an ongoing activity, which covers a wide variety of activities, including removing program and design errors, updating documentation and user support.

Accurate setup, configuration and working of the hardware, software and network components are important in a biometric system. Failure of any component in the biometrics system can compromise the security of assets, operations, the safety of personnel and the accuracy of reporting systems. Biometric system maintenance involves the maintenance of biometric devices, networks, cameras and related systems, operating system and applications that support are controlled by the biometrics solution.

Virus, Antivirus and Malware Software

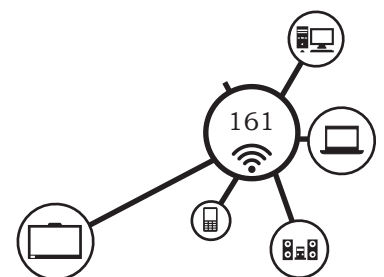
Malware

It is the short form for malicious software. It can harm a computer system, interfere with users' data, or make the computer perform actions without the users' knowledge or permission. The use of a computer involves various threats. Malicious software or Malware or malicious codes cause serious harm to computers and networks in many ways. Some examples of such effects are listed below.

- Decreased efficiency of the computer, such as improper function, or re-starts again and again.
- Destruction or malfunction of software
- Inability to install other software
- Weakened computer hardware
- Damage of computer networks
- Data theft and destruction
- Reduction of the storage capacity of the hard disk by storing unnecessary documents and files

Some examples of malware:

- Spyware (spies on you)
- Adware (pop up adverts all the time)
- Root kits (allows a hacker full access to your computer)



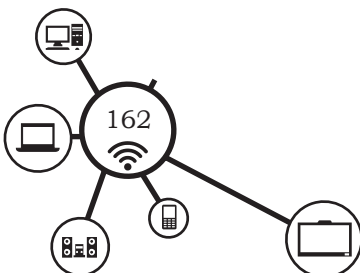
NOTES

A few types of harmful software and how it can cause damage have been discussed below.

- **Computer virus** is a piece of software that can 'infect' a computer, that is, it will install itself and copy itself to other computers, without the users' knowledge or permission. Computer viruses gain entry into the computer through a computer program and spread rapidly within the computer causing enough harm. Viruses can enter a computer through networks, a USB flash drive, external devices like memory chips, or through e-mail. Viruses enter the system as executable files. In other words, the viruses always remain active within the computer. Most computer viruses come with some kind of 'payload' — the malware that does something to your computer. For example, the virus might install some spyware, it might search your computer for credit card information, or it might install software that gives someone remote control of your computer.
- **Computer worms** also act similar to computer viruses. Worms, however, are capable of acting and spreading alone using e-mail attachments, false websites and instant messages.

Spyware

- **Trojan horse** is a harmful software based on the Greek trojan horse constructed using wood. It presents itself as harmless and enters the system without the knowledge of the user. Trojan horse spyware makes the user uncomfortable by unnecessary opening up windows, producing different desktops, deleting documents and stealing data. Further, it allows other harmful software to gain entry. Trojan enters computer with e-mail attachments. However, unlike computer viruses and worms, the trojan horse does not spread by itself.

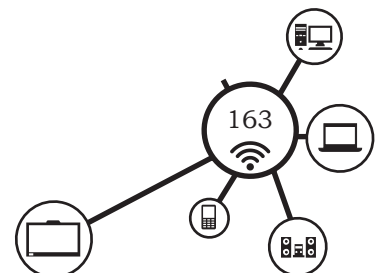


- **Adware** is displaying unnecessary notices on the computer screen. Using these advertisements, adware collects commercial information. Adware is not harmful as other computer viruses but disturbs the by displaying ads on the browsers.
- **Bots** are derived from the word 'robots'. Bots is a harmful software that functions on its own communicating with other networks. Bots are used to collect personal information through Internet messages and conversations.
- **Hijacker** is capable of misdirecting a user to a different website through the Internet, to collect information regarding trade, commerce and advertisements. Hijacker, is similar to adware.
- **Phishing** is the art of deceiving users to collect information about bank accounts or electronic accounts. E-mail is used for the purpose. Such mail is sent through a popular organisation or a friend together with a link for access. With a click on the link, or by filling forms, valuable information and cash deposits related to the unsuspecting user gets stolen.
- **Spam** is unauthorised e-mail. Most often, spam mails are advertisements about products or a mail from any unknown person. The mailbox can get filled with such mails and make the user uncomfortable. Also, spam may collect e-mail addresses that can be used unlawfully for frauds.

Safeguarding Computer and Network from Harmful Software

There are some simple things you can do to help prevent a virus infecting your computer:

1. Always install the latest version of anti-virus software and keep it up-to-date.
2. Install anti-malware software that stops software installing without your knowledge.



NOTES

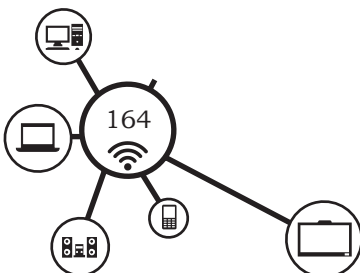
3. Never download and install software from unsecure source.
4. Do not open e-mail attachments without scanning them.
5. Do not click suspicious links in websites.
6. Be careful with the use of a USB memory. Check USBs for possible viruses using antivirus software.
7. Do not trust cracked versions of software from file-sharing sites. These have viruses and other malware added to them—a Trojan horse.

If the computer is connected to the Internet

1. access secure websites. Check URL for verification.
2. select only secure websites for the download of software or other material. Before downloading, check it by using antivirus software.
3. be careful when opening e-mails. Where necessary use antivirus software before downloading attachments.
4. do not click on suspicious links in e-mail. Avoid opening suspicious e-mails.
5. avoid suspicious advertisements or messages.
6. do not enter personal information without checking on security.
7. use firewall, virus guards, e-mail filters to avoid the risk.

Some secure, popular antivirus software to be installed on a computer are as follows.

1. Avast Antivirus
2. AVG Antivirus
3. K7 Antivirus
4. Digital Defender Antivirus
5. Kaspersky Antivirus
6. Panda Cloud Antivirus (B)
7. Microsoft Security Essentials
8. Norton Antivirus
9. Bit Defender Antivirus
10. McAfee Antivirus
10. Quick Heal Antivirus



Practical Activity 3

Updating of windows defender and scanning using Windows defender

Material required

Computer with Windows 10 operating system

Procedure

1. Open Windows Defender program either using **Start menu** search as shown in Fig. a or clicking its icon in system tray, and then check the current version and installed date of definition.

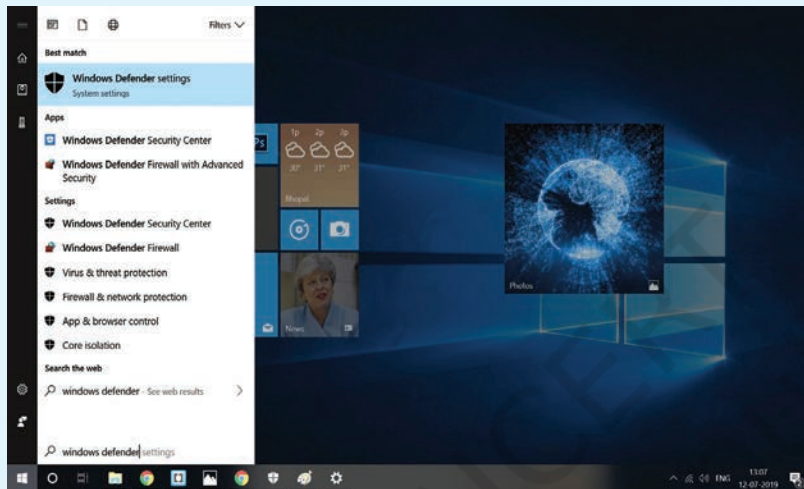


Fig. a

2. The Windows Defender will open as shown in Fig. b.

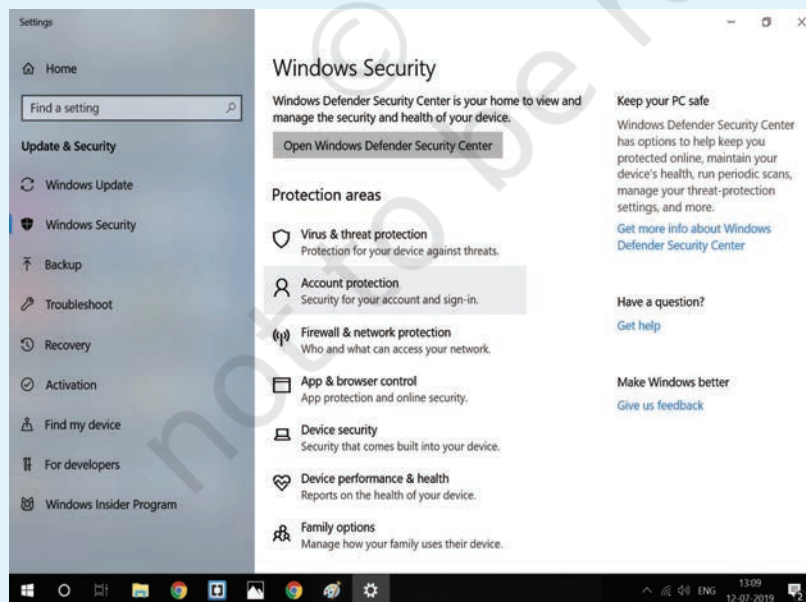
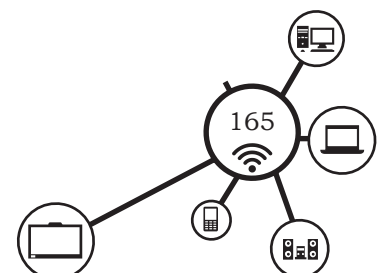


Fig. b

NOTES



NOTES

- Click on Virus and threat protection, a window will open as shown in Fig. c.

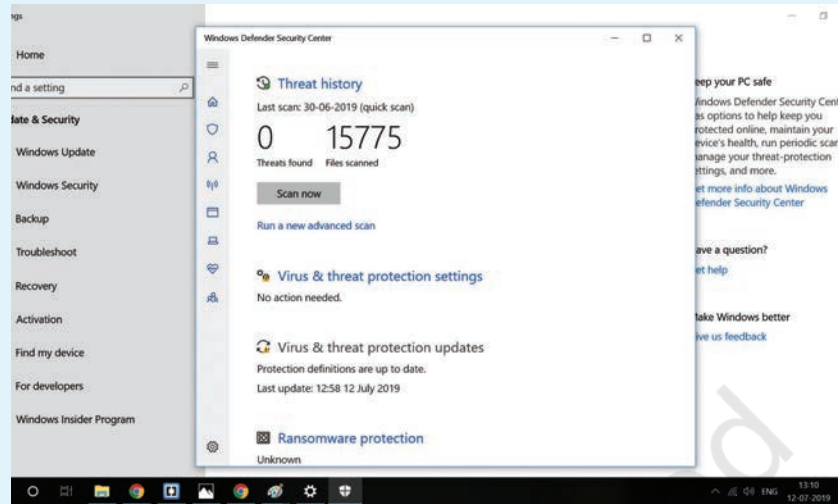


Fig. c

- Click on Virus and threat protection updates.
- Click on Check for updates as shown in Fig. d. This window will also show the Threat definition version and last updated date.

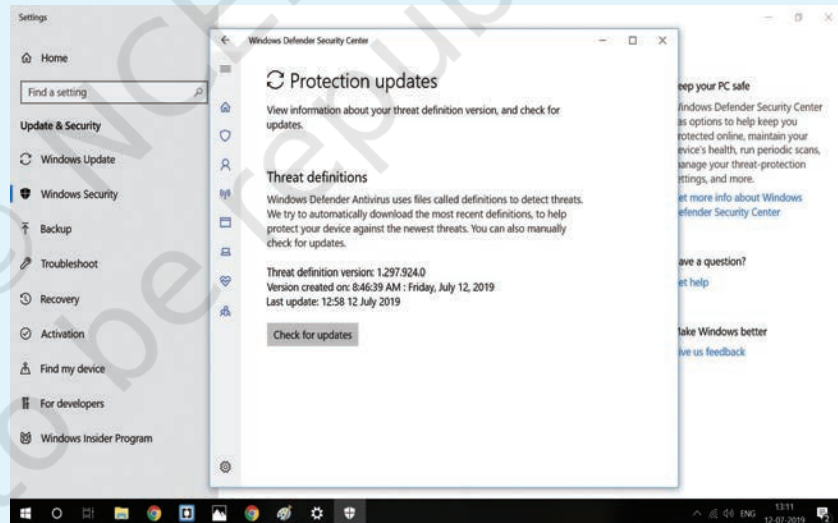
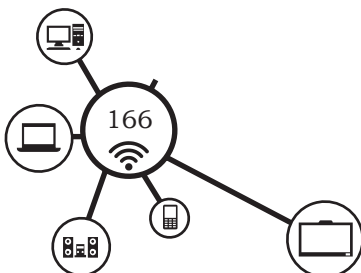


Fig. d

- It will check for updating Windows defender. If your computer is connected to the Internet, it will automatically download the most recent definitions. The updated version of Windows defender is now ready to scan the disk.
- To scan the hard disk drive of your computer, open the Windows defender.



- Select and click on Virus and threat protection tab as shown in Fig. e.

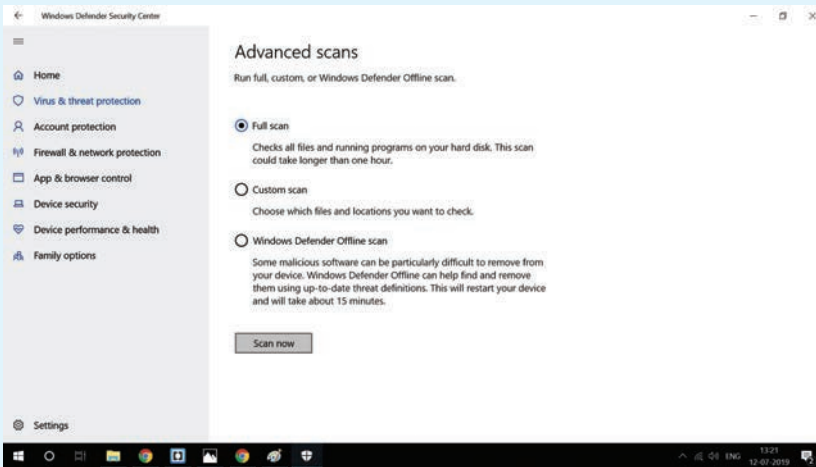


Fig. e

- Click on the **Scan now** button to quick scan the hard disk of your computer.
- Click on Run a new advanced scan to explore the advanced options.
Select the appropriate option Full scan, Custom scan or Offline scan and then click on Scan now as shown in Fig. f.

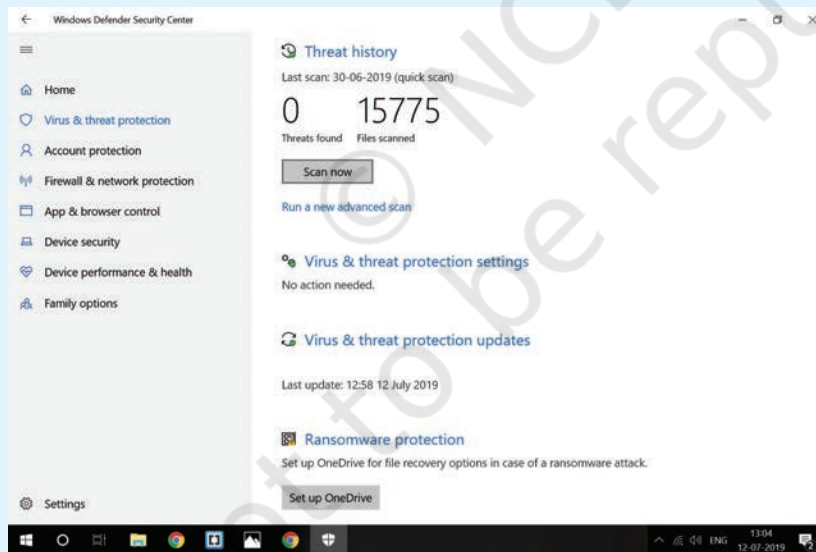
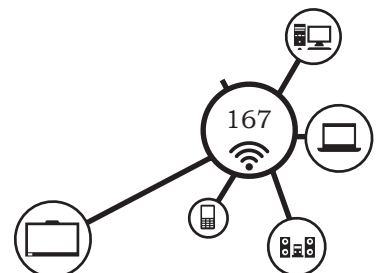


Fig. f



Maintenance of the System

Regular maintenance of the system involves:

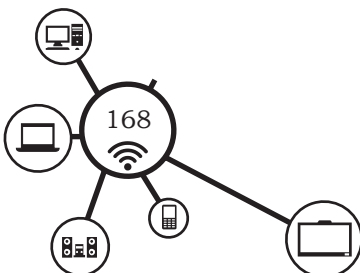
- **Setup and clean up** successful setup of a biometrics system hinges first and foremost on accurate registration of unique identifiers, for example, fingerprint or iris scans—that are entered into a database. If the registration process is faulty, the system will deliver false positives or erratically deny access. Administration of the database also needs to be meticulous—much like other access control technologies, if someone leaves the company or their status changes, the database must be updated and ‘cleaned’. This is crucial as biometrics databases usually have a limit to the number of registrations they can efficiently process. Exceed this and the system slows down, stalls and begins to fail, affecting operational and productivity efficiencies and increasing risk.

In excessive use of biometric system, such as 3000 to 4000 transactions per day there is a chance of wear and tear. All the physical components that make up the system need to be regularly assessed for mechanical or other failure. If the biometrics reader gets grimy or is damaged — through use or exposure to harsh environments or the elements, such as rain, dust, heat. It can literally collapse the entire system. Biometrics secured access is also of little use if the door granting access has faulty locking units. In addition, network access and reliability, including quality of service, need to be regularly reviewed to ensure the biometrics system and all the processes it enables access, time and attendance can operate and respond efficiently.

Maintenance Optimises Performance

Regular maintenance of biometric system on an average for every three months can reduce the occurrences of faults or extends the life of the biometric system. It also helps to optimise the performance of the system so that you need not have its repair and maintenance at its crucial level at the end by service provider.

It is better to have maintenance contract with some agency. It includes doing the necessary diagnostics on all



systems, critically assessing the network, the database, environmental factors and the impact of other devices on the biometrics and related systems.

Cleaning biometric hardware

It is often observed while making fingerprint entry in biometric attendance system; the finger rests during the scanning process and could not properly capture a fingerprint image. The regular use of biometric hardware devices especially fingerprints reader leaves residues or other foreign materials on the surface. The biometric hardware devices are like most other electronic equipment, which requires maintenance.

Wear and Tear in Fingerprint Biometric Devices

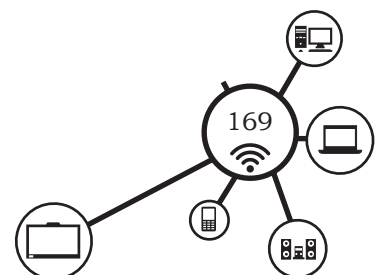
Due to regular use of biometric devices the hardware will undergo wear and tear as the end users place their fingers or palms on the device for recognition. The fingerprint readers have shorter life spans due to the fact that an end user must make physical contact with the fingerprint sensor in order for the device to capture a print and identify through a biometric software interface. Within environments where staff is prone to having dirty, greasy, or grimy fingers due to their job responsibilities, it is recommended to clean hands before using either of the fingerprint readers. The dirty residue, oils or other materials on the surface of a fingerprint reader result in false acceptance of data.

Cleaning easy scan fingerprint reader

To clean the fingerprint reader, dampen a lint-free cloth or cotton swab with alcohol or acetone. Gently rub the cloth across the sensor surface in a left and right direction. Move slowly down the sensor to cover the entire surface area. Repeat this process 2–3 times. Visually observe that no residual solution remains on the sensor. Abrasive materials are not recommended for cleaning the fingerprint reader.

Cleaning the fingerprint reader

The scanning surface of the fingerprint scanner is coated with a thin film of silicone. This silicone layer helps the



dirty but cleaning frequency dropped significantly and the contactless sensor meant a longer life for the hardware. Here is the breakdown of how to clean each vascular reader:

Finger Vein (FV) scanner maintenance

- Before performing the FV Scanner maintenance, remove the USB cable. Keeping the cable connected with the USB connector during maintenance may cause failures.
- For FV Scanner maintenance, be careful not to allow water to come in contact with the inside of FV Scanner. This may cause malfunctioning.
- Do not clean the device using organic solvents, such as gasoline and alcohol. This may cause malfunctioning.

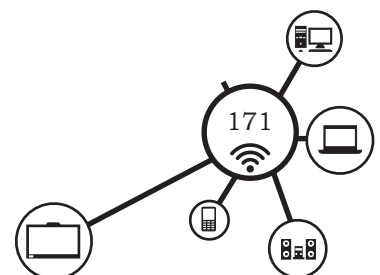
Maintenance of the external part of the FV Scanner should be about once a month or whenever required according the condition of the scanner. Clean the external part of the scanner by rubbing it with a soft piece of cloth. If dirt is not removed by doing this, soap the surface to be cleaned with detergent and clean using a tightly wrung out piece of damp cloth. If dirt remains, immerse the piece of cloth into water and cleaning detergent, wring tightly and apply to remove the dirt.

Scanning area maintenance method

- Use a soft piece of cloth to clean the scanning area.
- Lift up and remove the front part of the device where the finger is placed.
- Clean the scanning area using a soft piece of cloth. In case of big and obvious dirt particles, remove these before cleaning.
- Place the support back into its position once the cleaning is finished.

Palm Vein (PV) scanner maintenance

Before performing the PV Scanner maintenance, remove the USB cable. Keeping the cable connected with the USB connector during maintenance may cause failures.



NOTES

- For PV scanner maintenance, be careful not to allow water to come in contact with the inside of the PV Scanner. This may cause malfunctioning.
- Do not clean the device using organic solvents, such as gasoline and alcohol. This may cause malfunctioning.

Maintenance of the external part of the PV scanner is required according to the condition of the scanner. Clean the external part of the scanner by rubbing it with a soft piece of cloth. If dirt is not removed by doing this, soap the surface to be cleaned with natural detergent and clean using a tightly wrung out piece of damp cloth. If dirt remains, immerse the piece of cloth into water and cleaning detergent, wring tightly and apply to remove the dirt.

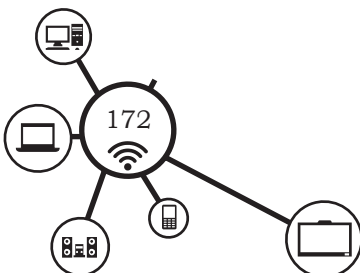
Sensor maintenance

is regular and systematic cleaning of the enrolment stations to avoid 'ghost fingerprint' effect, especially in the case of consultation processes taking place in heavily used check points.

Software Maintenance

Software maintenance actually consists of preventive, adaptive and corrective maintenance.

- **Perfective maintenance** enhancing and modifying the biometric system to respond to changing user requirements and organisational needs, improving biometric system efficiency.
- **Adaptive maintenance** changing the application to adjust it to a new hardware or software environment for biometric system. Adaptive maintenance may involve, for example, moving an application from a mainframe to a client or server environment in biometric system, or converting it from a file to a database environment.
- **Corrective maintenance** correcting an error discovered during operations in biometric system.



Procedure

A software maintenance procedure consists of three steps:

1. Understanding the biometric software to be modified and identifying the biometric device targeted for maintenance.
2. Modifying the appropriate biometric components of the application system without adversely affecting the rest of the biometric system.
3. Testing and thus validating the modified biometric components, as well as the entire biometric system.

Disk Defragmenter

Basically biometric devices are connected through a computer system. After long use of computer system there will be a need of disk fragmentation of hard disk for optimal use of hard drive to save biometric data file. The disk defragmenter is another tool that comes with Windows and is used for many different solutions. The main function of the disk defragmenter is to reassemble fragmented files. Whenever a file is modified in any way, the computer stores the file in broken pieces across the hard drive rather than putting the whole file in one spot. This can lead to system malfunction and poor performance because your computer must search for all the pieces of a specific file before it can display it. The disk defragmenter searches for all pieces of every file on your hard drive and reassembles the files into a specific location. This increases the speed at which files are displayed and results in less delay when opening files or programs. Fig. 3.29 (a) shows the disk before defragmentation and Fig. 3.29 (b) shows the disk after defragmentation.

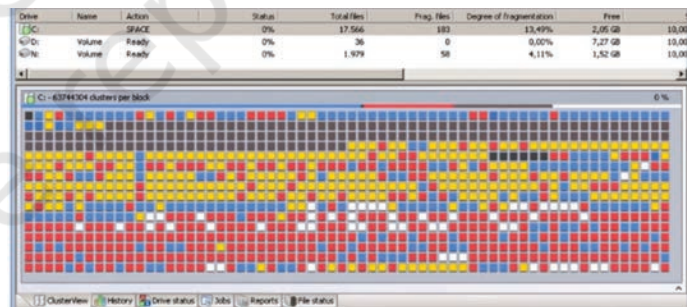


Fig. 3.29 (a): Disk before fragmentation

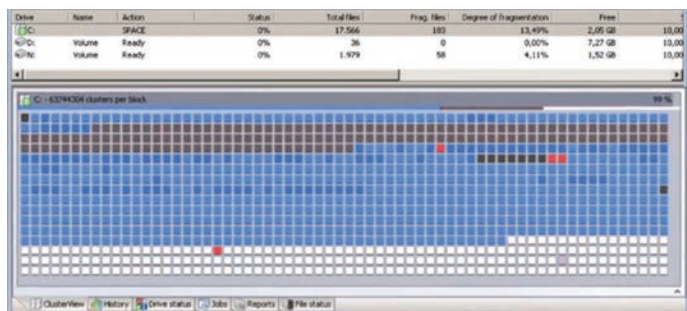
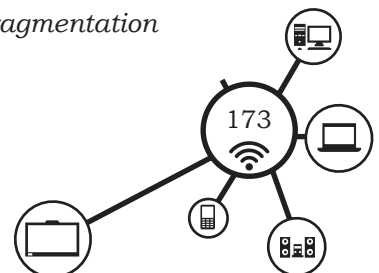


Fig. 3.29 (b): Disk after fragmentation



Practical Activity 4

To defragment hard disk

Material required

Computer

Procedure

1. Click on the window button. In the search box, type disk defragmenter, and then, click disk defragmenter.
2. Select the disk to defragment.
3. Click 'Analyse disk' to determine whether the disk needs to be defragmentation.
4. Once Windows is finished analysing the disk, check the percentage of fragmentation on the disk in the Last Run column. If the number is above 10%, defragment the disk.
5. Click defragment disk.
6. Disk defragmenter might take from several minutes to finish, depending on the size and degree of fragmentation of hard disk.

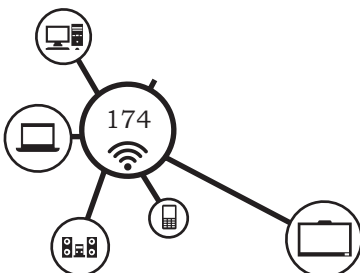
Checking for Updates for Applications

Always check for updates of important applications as mentioned below.

1. Browsers—Google Chrome, Safari, Opera and Firefox
2. Documents—OpenOffice, Adobe Reader, SumatraPDF, Foxit Reader, CutePDF, LibreOffice, PDF Creator
3. Security—Quick Heal, Microsoft Security Essentials, Avast, AVG, Norton, McAfee, Malware Bytes, Ad-Aware, Spybot, Super AntiSpyware
4. Online Storage or Backup—Carbonite, Dropbox, Google Drive, Mozy, Microsoft SkyDrive, Biometric data backup and storage.
5. Create system recovery disks and, if applicable, a file backup plan and create system recovery disks.

Practical Exercise

1. Give the steps to perform disk defragmentation.
2. Give the steps for taking back up of important data on your computer system.



Check Your Progress

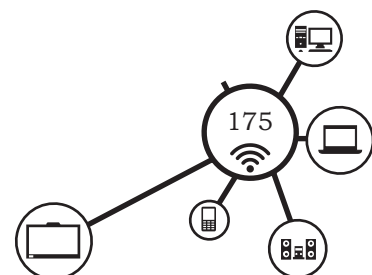
NOTES

A. Fill in the blanks

1. The process of monitoring, evaluating and modifying the existing system to deliver the desirable performance is called _____.
2. Biometric system maintenance involves maintenance of _____ and _____.
3. The efficiency of computer system gets decreased because of _____ software
4. A piece of software that can infect a computer system is called _____.
5. The computer virus that spreads using email attachment or instant messages is known as _____.
6. The harmful software that is based on the Greek horse is called _____.
7. The software that opens unnecessary windows and produces different desktops is called _____.
8. When unnecessary advertisement are displayed on the screen then this software is called _____.
9. The harmful software that communicates on its own with other networks is called _____.
10. Personal information through Internet messages is collected by the software is known as _____.

B. Multiple choice questions

1. Misdirection of the user to a different website is called _____.
(a) spam (b) phishing
(c) hijacking (d) Trojan horse
2. When the user information about their bank accounts is collected through email then such activities is called _____.
(a) spam (b) phishing
(c) hijacking (d) Trojan horse
3. When the advertisement about the product or a mail from unknown person is received in the mailbox then it is called _____.
(a) spam (b) spyware
(c) adware (d) malware
4. When unnecessary notices are displayed on the screen such as commercial advertisement then it _____.
(a) both (b) phishing
(c) virus (d) adware



NOTES

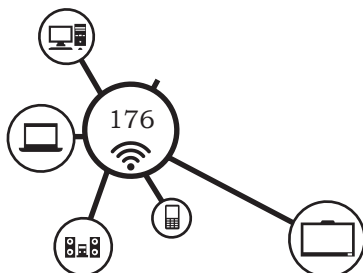
5. If you receive an e-mail with an attachment file then _____.
(a) do not open the attachment without scanning
(b) open the attachment immediately
(c) open the attachment after some time
(d) never open the attachment
6. The most commonly affected device by the computer viruses is the _____.
(a) keyboard (b) mouse
(c) pen drive (d) hard disk drive
7. While accessing the website on Internet always prefer _____.
(a) http (b) https
(c) httpc (d) httpm
8. Computer virus is a _____.
(a) hardware (b) sensor
(c) arch (d) software
9. Windows defender is a _____.
(a) spyware (b) antivirus program
(c) malware (d) application software

C. State whether the following statements are True or False

1. You can download and install software from unsecure sources.
2. One should not click on suspicious links.
3. Use trusted and cracked versions of software.
4. Do not enter personal information without security check.
5. A biometric system with multiple transactions per day do not have wear and tear.
6. Rain, dust and heat can damage a biometric system.
7. Regular maintenance of the biometric system is not necessary.
8. Abrasive material is recommended for cleaning a scanner.
9. Biometric software maintenance must be performed at regular intervals.
10. Optimal use of hard disk is possible by using disk defragmenter.

D. Short answer questions

1. What do you understand by maintenance and updating of a software?
2. Give the steps to defragment a hard disk drive.
3. How are the biometric systems maintained?
4. How can hardware biometric devices be maintained?
5. List the steps for maintenance of fingerprint scanner.



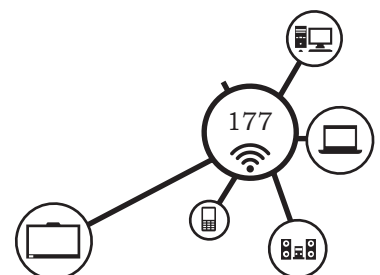
6. List any four tips to safeguard your computer while using the Internet.
7. What is computer virus? State the different types of viruses.
8. What is antivirus? State the different types of antivirus software.
9. Give the steps for updating of antivirus and cleaning of the computer system using antivirus.

SESSION 3: UPDATING OF BIOMETRIC SYSTEM

In earlier days, computers were big in size and had low speed. But modern computers are small in size with enhanced speed. We need to replace old technology with the new one. One has to check the compatibility of the existing hardware with the new hardware and updated versions of new devices. In the same way software as well operating system comes with new versions. The updates of operating system may be installed whenever available.

The updating technology requirements of biometric systems are poorly understood and neglected. Most biometric systems have basic needs, such as cleaning of the lenses or plates, sensor recalibration when the components or the environment changes, software updates to keep pace with hardware changes, and so on. Evolution of large-scale systems while in use requires careful pretesting to verify the ability to migrate from the old technology to the new and have both coexist in the system simultaneously. Some system components may change without maintaining backward compatibility. Technologies will change significantly over the expected lifespan of a system, and biometric components may need to be updated. In general, biometric systems may be similar to other computer-based systems in that useful lifetimes cannot be expected to surpass 5 to 7 years without becoming obsolete.

Unlike some computer-based systems, however, biometric systems are likely to have a critical hardware component, making upgrades and replacements more logistically challenging than, say, pushing software updates to a networked information system.



NOTES

For example, consider the simple case of a single fingerprint sensor, deployed to provide data security rather than convenience by controlling access to a laptop.

In normal operation, this application will be limited to repeated private interactions between the owner and machine for the machine's full life. However, a sensor can fail from simply wearing out, from Physical damage due to rough usage, from a dirty environment, or from intentional damage by an unauthorised user who obtains control of the machine. The fingerprint acquisition and/or fingerprint matching software, or the file with the enrolled biometric template—a software issue—can also be corrupted.

Quality control, especially in large-scale systems, is critically important. When engineering a biometric system, planning how to ensure continued high-quality performance is key. At the same time, mechanisms are needed to detect and accommodate degraded performance, should it occur.

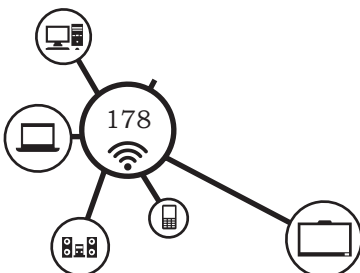
Components of Biometric System

A biometric system is a complex system comprising various components, such as (i) Computer system, (ii) Biometric devices (iii) Biometric technology and (iv) Biometric software. Updating of biometric system involves updating of its components.

Need of Upgradation

All electronic devices have a limited span of life. There is a depreciation of about 20 to 30% in case of electronic devices. Hence the electronic devices becomes absolute in a span of 3 to 5 years. Therefore it is necessary to upgrade the electronic devices in the span of 3 to 5 years.

In biometric system, biometric devices are used extensively. For example, a punching device is used by several people throughout the day. All these devices are continuously working 24 x 7, once they are installed. Many times we find that the environment conditions of these devices are not good. Sometimes they are exposed



to the sunlight and rain also. All such things causes wear and tear of the biometric devices. Hence it becomes necessary to upgrade the biometric devices in a span of 3 to 5 years.

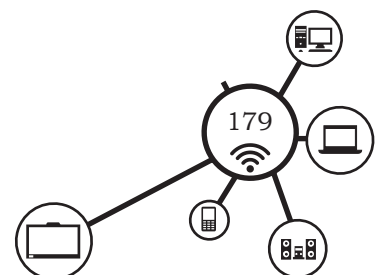
Biometric technology is enhancing in a rapid pace. A lot of new modification are added in hardware and the biometric algorithms. Hence, it is necessary to upgrade the biometric system at regular intervals so that the user can have an access to the advanced technology.

Updating of Biometric Hardware

Biometric hardware comprises computer system and various biometric devices, such as punching machine or biometric attendance system, iris scanner, camera and fingerprint or palm scanner. If we observe the development of these devices over a period of last 20 years, then we easily find that these devices and their functionality is changing at rapid pace. For example, in early days people make use of LAN-based biometric devices. But now most of the devices are cloud-based devices and they do not require any wired connection.

Cloud-based devices makes use of android operating system. Most of the cloud-based devices are platform independent devices and hence they can be used on any platform. Also observe that the data of these devices is stored on the cloud server. Therefore, a large amount of data can easily stored and accessed by using these devices. Companies can easily maintain these devices by using Internet technology, i.e., online maintenance of these devices is possible. If we observe the various performing parameters then we can easily differentiate between the modern biometric devices and old biometric devices. Modern biometric devices has a very high verification speed. Almost instantly authentication is done without any time gap. In early days these machines requires certain amount of time which is about 2 to 3 seconds for the purpose of authentication.

The size of the devices is reduced drastically. Modern devices are compact in size and can be easily installed on the wall. These devices consist of high quality optical sensors. The resolution quality is more than 500 dots per inch.



The error rates in the modern biometric devices are reduced. These devices can also work on battery. Due to the advancement in the battery technology it is possible to have several hours backup for these devices. The restriction on the number of users of these devices is almost removed because of large availability of the storage space on server.

Table 3.1: Comparison of specifications or parameters of old and modern biometric devices.

Device	Specifications or parameters	Old device	Modern device
Computer system	Processor	2.44 GHz	4.2GHz
	Primary Memory	512 MB	8 GB
	Secondary storage	500 GB	1TB
	Cost	30,000	55,000
Printer	Type	Laser printer	Multi-function printer
	Speed	1 to 20 ppm	55 ppm
	Printing quality	Low	High
	Cost	6,000	15,000
Fingerprint sensor	Optical scanner	Simple scanner sensor	Optical scratch free sensor
	Operating system	Windows 2000, Windows Server 2003/2007/2008, Linux	Windows 7,8,10, Windows Vista, Windows 2000, Windows Server 2003/2007/2008 Linux, Windows ME, Windows 98 SE SDK, Libraries and Drivers support across all above
	RAM	512 MB	1GB or Higher
	Hard Disk	16GB	80GB or Higher
Camera	Resolution	320x240	2240x1680
	Zoom	3x optical zoom	20x optical zoom
	Type	SLR	DSLRs
	Sensor size	332 sq. mm	858 sq. mm
	Focus	Manual	Auto/Manual

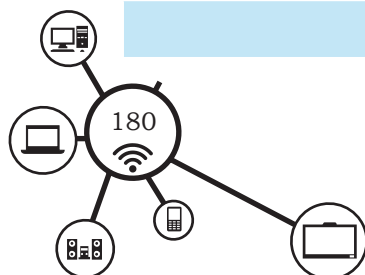
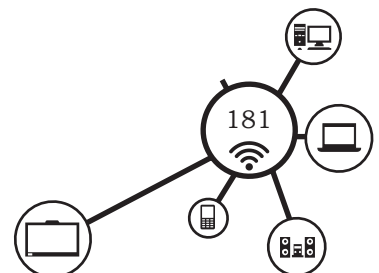


	Image stabilisation	No	Yes
Iris scanner	Resolution	640 x 480 pixels	800 x 1280 pixels
	Operating system	Windows 2000, Windows Server 2003/2007	Windows 32/64-Bit, Android, Linux, Embedded RTOS
Palm scanner	Optical sensor	Optical fingerprint sensor	Optical Scratch free sensor
	Operating system	Windows 2000, Windows Server 2003/2007/2008, Linux	Windows 7,8,10, Windows Vista, Windows 2000, Windows Server 2003/2007/2008 Linux, Windows ME, Windows 98 SE SDK, Libraries and Drivers support across all above
	RAM	512 MB	1GB or Higher
	Sensor	Ambient Light Sensor	Ambient Light Sensor, Accelerometer, Gyroscope, Proximity Sensor Supported

Biometric technology comprises the following technologies:

1. Face recognition technology
2. Pattern recognition technology
3. Networking technology
4. Character and signature recognition technology

Many new algorithms are developed and added so that the performance of biometric system gets enhanced. Biometric algorithms comprises various algorithms such as face recognition algorithm and pattern recognition algorithms. Face recognition technologies suffers from various parameters such as bad lighting conditions and change in the pose of the face. But soft computing technologies, such as fuzzy logic and neural network are enhancing the performance of face recognition algorithms in biometric system. These biometric algorithms are used for authentication purpose, i.e., matching of the face with the stored data faces and matching of the fingerprint or iris with the stored images is performed by these algorithms.



NOTES

In networking technology many new concepts such as cloud computing, is added. This technology has changed the way biometric devices can be accessed and their performance is enhanced. The uploading and downloading speed of the data are increased to a new peak level because of advancement in networking technology.

Recognition of character and signature recognition is widely used in modern biometric systems. Modern algorithms for character recognition can recognise the characters written in Indian languages as well, i.e., character written in regional languages such as Marathi, Hindi, Tamil, Malayalam can also be recognised by the recently developed algorithms. In future it is possible that all handwritten data can be recognised by a system automatically.

Updating of Biometric Software

Software technology comprises various programs through which one can make access to the biometric hardware. Also with biometric software, we can generate various reports that are needed for organisation. Reports, such as daily attendance, weekly attendance, monthly attendance, salary sheet, shift-wise report, total working hours of employee can be easily generated with biometric software. Biometric software also allows us to perform many other task.

For example, when the government wants to disburse the subsidy to the farmer then the authentication of the farmers can be done by using Aadhaar card software. Whenever a new person wants to open a bank account the authentication can be easily done by entering his or her Aadhaar number in the computer system of the bank. The authentication of the user can be verified by using the Aadhaar server software. Thus, we observe that because of the development of the software in biometric systems, many tasks can be easily performed as illustrated in Fig. 3.30.

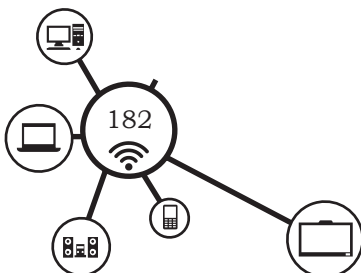




Fig. 3.30: Use of Aadhaar in various schemes

There are many new enhancements in the client side software of biometric systems. The features of the modern biometric software are enlisted in Table 2.4.

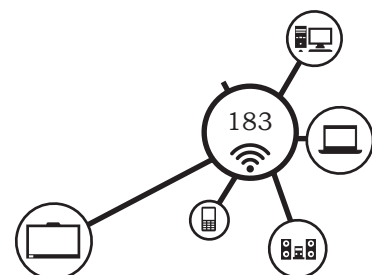
Table 2.4: Features and values of software

Feature name of software	Feature value
Operating system platform	Multi-Modal Hybrid Biometric Platform™
Software technology used	Multimodal biometric authentication systems
Connectivity of operating system	Windows 7/8/10, Linux, Android
Internet access	Wired and wireless

Check Your Progress

A. Fill in the blanks

1. Replacing old systems with modern systems is called _____.
2. Updating is necessary because all electronic devices have _____.
3. In case of electronic devices there is a depreciation of _____ annually.
4. Using biometric devices extensively causes _____.
5. Modern biometric systems use _____ operating system.
6. Number of users of any biometric system can be virtually _____.



NOTES

B. Multiple choice questions

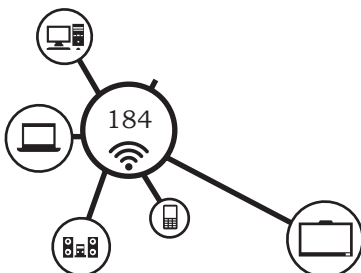
- Which is the latest processor used in modern computer system?
(a) i7 8th generation (b) i7 8th generation
(c) i5 8th generation (d) i3 7th generation
- In early days the primary memory used was in _____.
(a) MB (b) GB (c) TB (d) KB
- The secondary storage device capacity used in modern computer is about several _____.
(a) GB (b) KB (c) TB (d) MB
- The resolution of the camera is enhanced to _____ megapixel.
(a) 1600 × 1200 (b) 1800 × 1800
(c) 1600 × 1200 (d) 1200 × 1600
- The sensitivity of the iris scanner is _____.
(a) high (b) low (c) medium (d) very low
- The connectivity of palm scanner is _____.
(a) 600ppi, 1100ppi (b) 500ppi, 1000ppi
(c) 400ppi, 700ppi (d) 600ppi, 600ppi
- The error rates in fingerprint sensor are _____.
(a) four optical sensors (b) one optical sensors
(c) three optical sensors (d) two optical sensors
- Cost of the modern printer is _____.
(a) low (b) high (c) very low (d) very high

C. State whether the following statements are True or False

- Face recognition technology makes use of fuzzy logic and neural network.
- Modern pattern recognition technology cannot recognise Indian language characters.
- Uploading and downloading speed of the network is decreased nowadays.
- By using biometric software we cannot generate the salary sheet.
- By using Aadhaar card, authentication of the farmers can be done.
- Shift-wise report can be generated in biometric software.
- Upgradation of biometric devices is not possible.
- Biometrics software cannot be updated.
- Upgradation of biometric system ensures quality control.

D. Short answer question

- What do you mean by updating of biometric system?
- Why is updating important?
- How can biometric devices be upgraded?
- State the features of upgradation in biometric technology.
- State the features of upgradation in biometric software.



4. Which one of the following is not a multitasking operating system?
(a) Windows (b) MS DOS
(c) Unix (d) Linux
5. The primary purpose of an operating system is to _____.
(a) make the most efficient use of computer hardware
(b) allow people to use the computer
(c) keep the programmer engaged
(d) make the computer easier to use
6. Virtual memory means _____ memory.
(a) primary
(b) secondary
(c) Both (a) and (b)
(d) None of the above
7. The latest version of Microsoft Windows operating system is _____.
(a) Windows 98 (b) Windows 8
(c) Windows 10 (d) Windows 15
8. Operating system developed by the Apple corporation is _____.
(a) Window (b) Linux
(c) Mac (d) Android
9. Which of the following is an open source operating system?
(a) Window (b) Linux
(c) Mac (d) Android
10. Which of the following is an operating system for mobile device?
(a) Window (b) Linux
(c) Mac (d) Android
11. Android 8.0 is named as _____.
(a) Android Oreo (b) Android Marshmallow
(c) Android Lollipop (d) Android Nougada
12. In 2018 Apple released _____.
(a) iOS 11 (b) iOS 12
(c) iOS 13 (d) iOS 14

C. State whether the following statements True or False

1. Operating system is an application software.
2. Operating system allows to communicate with computer hardware.
3. Modern cars are not examples of embedded system.
4. Input/output device management can be performed by using operating system.

5. Data and file management cannot be performed by using operating system.
6. In process management threads are managed by the operating system.
7. Only single user can access a computer system in time sharing management.
8. Virtual storage management can be achieved through operating system.
9. Microsoft Windows has a graphical user interface.
10. Mac operating system was developed by Microsoft.
11. Windows and Mac operating systems are proprietary software.
12. Ubuntu, Red hat and Fedora are different distributions of Linux operating system.
13. Mobile devices, such as tablets and mobile phones do not have an operating system.

D. Short answer questions

1. What is a mobile operating system? State the features of a mobile operating system.
2. Differentiate between single user and multiuser operating systems.
3. List the features of Windows operating system.
4. State the features of Linux operating system.
5. State the different types of tasks that can be performed using an operating system.
6. What are the advanced features of an operating system?
7. What are the different types of operating systems?

Domestic Biometric Data Operator-Class 11- Unit 3 Session 2

A. Fill in the blanks

1. The process of monitoring, evaluating and modifying the existing system to deliver the desirable performance is called _____.
2. Biometric system maintenance involves maintenance of _____ and _____.
3. The efficiency of computer system gets decreased because of _____ software
4. A piece of software that can infect a computer system is called _____.
5. The computer virus that spreads using email attachment or instant messages is known as _____.
6. The harmful software that is based on the Greek horse is called _____.
7. The software that opens unnecessary windows and produces different desktops is called _____.
8. When unnecessary advertisement are displayed on the screen then this software is called _____.
9. The harmful software that communicates on its own with other networks is called _____.
10. Personal information through Internet messages is collected by the software is known as _____.

B. Multiple choice questions

1. Misdirection of the user to a different website is called _____.
(a) spam (b) phishing
(c) hijacking (d) Trojan horse
2. When the user information about their bank accounts is collected through email then such activities is called _____.
(a) spam (b) phishing
(c) hijacking (d) Trojan horse
3. When the advertisement about the product or a mail from unknown person is received in the mailbox then it is called _____.
(a) spam (b) spyware
(c) adware (d) malware
4. When unnecessary notices are displayed on the screen such as commercial advertisement then it _____.
(a) both (b) phishing
(c) virus (d) adware

5. If you receive an e-mail with an attachment file then _____.
- (a) do not open the attachment without scanning
 - (b) open the attachment immediately
 - (c) open the attachment after some time
 - (d) never open the attachment
6. The most commonly affected device by the computer viruses is the _____.
- (a) keyboard
 - (b) mouse
 - (c) pen drive
 - (d) hard disk drive
7. While accessing the website on Internet always prefer _____.
- (a) http
 - (b) https
 - (c) httpc
 - (d) httpm
8. Computer virus is a _____.
- (a) hardware
 - (b) sensor
 - (c) arch
 - (d) software
9. Windows defender is a _____.
- (a) spyware
 - (b) antivirus program
 - (c) malware
 - (d) application software

C. State whether the following statements are True or False

1. You can download and install software from unsecure sources.
2. One should not click on suspicious links.
3. Use trusted and cracked versions of software.
4. Do not enter personal information without security check.
5. A biometric system with multiple transactions per day do not have wear and tear.
6. Rain, dust and heat can damage a biometric system.
7. Regular maintenance of the biometric system is not necessary.
8. Abrasive material is recommended for cleaning a scanner.
9. Biometric software maintenance must be performed at regular intervals.
10. Optimal use of hard disk is possible by using disk defragmenter.

D. Short answer questions

1. What do you understand by maintenance and updating of a software?
2. Give the steps to defragment a hard disk drive.
3. How are the biometric systems maintained?
4. How can hardware biometric devices be maintained?
5. List the steps for maintenance of fingerprint scanner.

6. List any four tips to safeguard your computer while using the Internet.
7. What is computer virus? State the different types of viruses.
8. What is antivirus? State the different types of antivirus software.
9. Give the steps for updating of antivirus and cleaning of the computer system using antivirus.

Domestic Biometric Data Operator-Class 11- Unit 3 Session 3

A. Fill in the blanks

1. Replacing old systems with modern systems is called _____.
2. Updating is necessary because all electronic devices have _____.
3. In case of electronic devices there is a depreciation of _____ annually.
4. Using biometric devices extensively causes _____.
5. Modern biometric systems use _____ operating system.
6. Number of users of any biometric system can be virtually _____.

B. Multiple choice questions

1. Which is the latest processor used in modern computer system?

(a) i7 8 th generation	(b) i7 8 th generation
(c) i5 8 th generation	(d) i3 7 th generation
2. In early days the primary memory used was in _____.

(a) MB	(b) GB	(c) TB	(d) KB
--------	--------	--------	--------
3. The secondary storage device capacity used in modern computer is about several _____.

(a) GB	(b) KB	(c) TB	(d) MB
--------	--------	--------	--------
4. The resolution of the camera is enhanced to _____ megapixel.

(a) 1600 × 1200	(b) 1800 × 1800
(c) 1600 × 1200	(d) 1200 × 1600
5. The sensitivity of the iris scanner is _____.

(a) high	(b) low	(c) medium	(d) very low
----------	---------	------------	--------------
6. The connectivity of palm scanner is _____.

(a) 600ppi, 1100ppi	(b) 500ppi, 1000ppi
(c) 400ppi, 700ppi	(d) 600ppi, 600ppi
7. The error rates in fingerprint sensor are _____.

(a) four optical sensors	(b) one optical sensors
(c) three optical sensors	(d) two optical sensors
8. Cost of the modern printer is _____.

(a) low	(b) high	(c) very low	(d) very high
---------	----------	--------------	---------------

C. State whether the following statements are True or False

1. Face recognition technology makes use of fuzzy logic and neural network.
2. Modern pattern recognition technology cannot recognise Indian language characters.
3. Uploading and downloading speed of the network is decreased nowadays.
4. By using biometric software we cannot generate the salary sheet.
5. By using Aadhaar card, authentication of the farmers can be done.
6. Shift-wise report can be generated in biometric software.
7. Upgradation of biometric devices is not possible.
8. Biometrics software cannot be updated.
9. Upgradation of biometric system ensures quality control.

D. Short answer question

1. What do you mean by updating of biometric system?
2. Why is updating important?
3. How can biometric devices be upgraded?
4. State the features of upgradation in biometric technology.
5. State the features of upgradation in biometric software.



Computer Networks, Internet and Standards of Biometric Data



17110SCH04

INTRODUCTION

In biometrics system the individual's identity is authenticated based on unique personal characteristics. Authentication is an essential component of network security. The use of networks is growing at an exponential rate. With the advancement and cost-effectiveness of network technology it becomes easy for biometrics to control identification and authentication for all internal networks. Biometrics are significantly used in commercial networks accessed by the general public to reduce fraud. The biometric attendance system mostly works on Internet technology. The biometric data presented by the user is stored on the server or cloud. In Aadhaar enrolment also the enrollee's data gets stored in the cloud server. In the modern era any application uses network-based infrastructure or cloud-based infrastructure to store the biometric data. Therefore, it is essential to understand the network technology and Internet for biometric systems.

Many biometric-based identity documents, such as electronic passports, ID cards and visas are used at international level as the people travel across the world.

These documents should follow the biometric standards to ensure interoperability, reliability, security and scalability. With international standards, it is possible to use the biometric system in wide range of applications.

Biometric systems deal with the human biological data. The technology should deal with the ethical and legal aspects of usage and protection of personal biometric data.

In this unit we will understand the basic concept of computer network, network technology, Internet and its application, national and international standards of biometric data and IT practices to protect the biometric data.

SESSION 1: COMPUTER NETWORKS

As you talk to different people in your area, around the world, discussing common issues, you are in a network. It is a network of people talking to each other. Fig. 4.1 shows a network of friends.

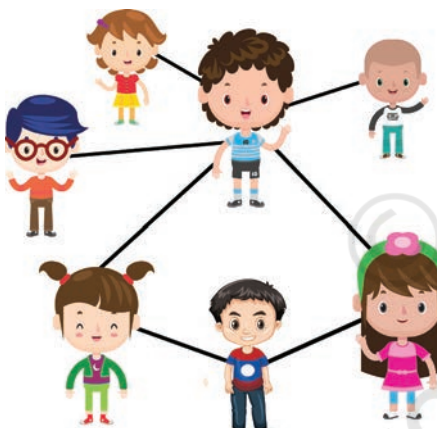
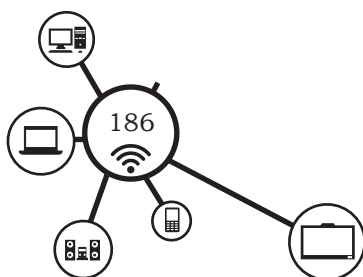


Fig. 4.1: Chain or group of friends

We use social networking sites, such as Facebook. In Facebook, one can connect with their friends by creating an account on Facebook, share images and videos with them too. Similarly, computer is also connected by a network made up of wires or frequencies through air that is wireless. It allows the computers to communicate with each other. When the computers in this network are connected to Internet then all the computers of this network can communicate with the other computers connected to the Internet across the globe. Even a single computer connected to Internet can communicate with other computers, which are connected to the Internet.

Need and Importance of Networking in Biometric System

The biometric attendance system is commonly used in every organisation to record the attendance of employees. We have seen that the biometric attendance system normally works on wireless network. It takes the input from the user only when it is connected to Internet through Wi-Fi network. This is because any



input provided to the biometric devices gets stored in the server, which provides services to clients. Biometric system architecture allows the use of networking. This is quite useful in large scale biometrics implementation. There could be a combination of biometric modalities to be used with another. It is possible to network these biometric modalities. All these are networked together and connected to a central server. In some application it may require utmost security. Biometric systems consist of many devices interlinked together due to which biometric devices can communicate with each other and can share the biometric templates within few seconds.

Network Processing Loads

This is the concept of properly balancing the network load. It ensures the workload of all the devices connected to network is proportionately equal to avoid the delays.

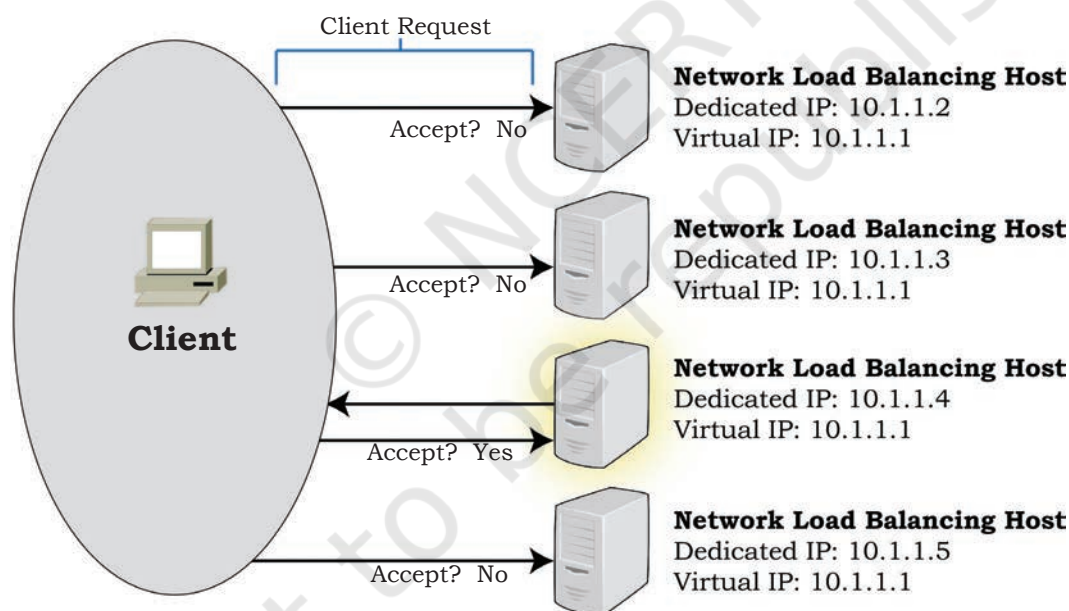
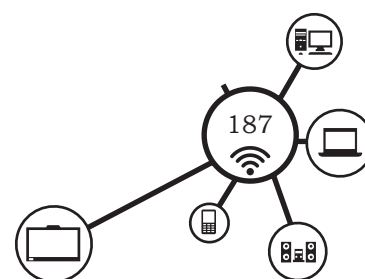


Fig. 4.2: Network processing loads

When the biometric devices are connected with one another, the transaction processing load for the verification and identification based applications can be shared with distributed network resources. For example, in international airport, the identity of the passengers is tracked by the facial and iris recognition. For the large number of passengers many such devices



are required which are placed on different locations throughout the airports. These biometric devices are networked together.

Another advantage with networking is that if there is a system failure in one segment, the other modalities will be able to quickly make up for any downtime in just a matter of a few minutes. Fig. 4.2 shows that when a client sends a request to the system and when there are various terminals networked in the system, there is at least one terminal, which can respond to the client if others are bust or not working.

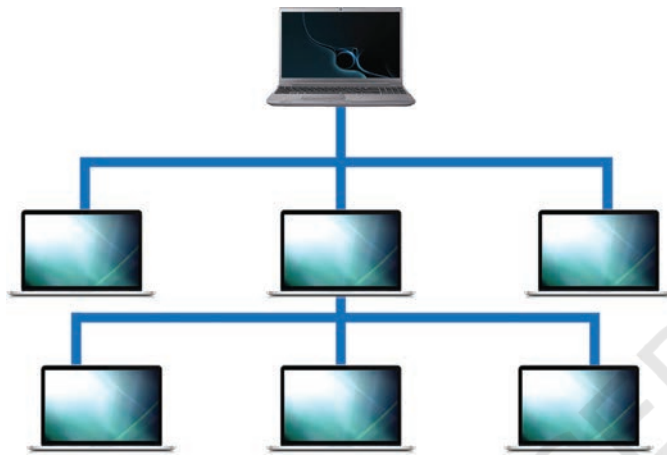


Fig. 4.3: Simple computer network

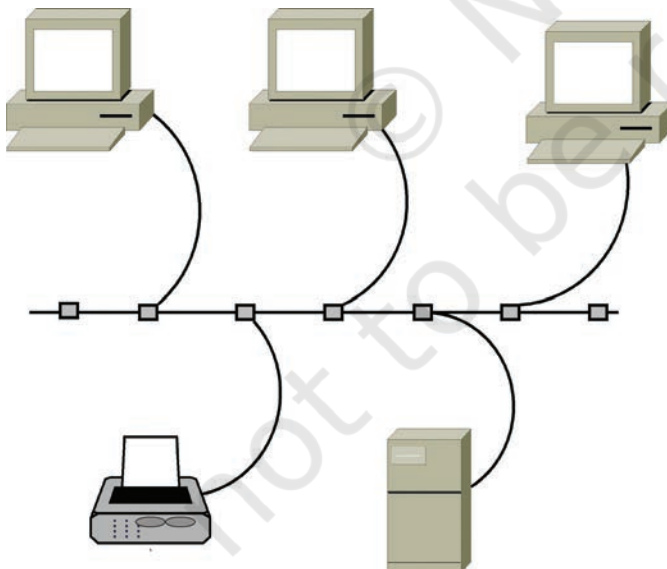


Fig. 4.4: Local Area Network (LAN)

Computer Networks

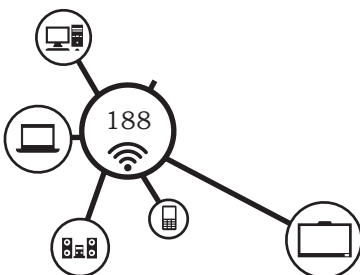
A computer network consist of computers, printers, scanners and other hardware interconnected by communication channels. The network is used for sharing of resources, such as printer, scanner or storage devices and services, such as mail and web services. The computers on a network may be linked through cables or wirelessly. Fig. 4.3 shows a simple computer network.

Types of networks

The network infrastructure is created in the organisation as per the requirement, and accordingly the computer network is classified as local, wide and metropolitan area network.

LAN (Local Area Network)

Most of the organisations create a simple network of computers within the building or campus by connecting computers and peripherals to serve the purpose of sharing computing infrastructure within the organisation. This type of network is called local area network (LAN) (Fig. 4.4).



LAN operate in a limited geographical area, such as schools, colleges, offices, etc. Computers and other network devices are connected in the network by using a wired media. It also uses a wireless connection.

Wide Area Network (WAN)

When an organization needed to provide a network in different locations across large geographical areas then WAN is created. WAN connect LAN's between different locations. For example, computers or devices in a branch office could connect to the computer networks at the head office through telephone lines or satellites. Apart from distance, the other feature that distinguishes a WAN from a LAN is that the WAN would make use of a range of communication technology, such as telephone, microwave and satellite links. WANs are also used in biometric systems to communicate with the remote server as in the case of Aadhaar, biometric data is saved and retrieved from server through biometric device. Fig. 4.5 shows the WAN network.

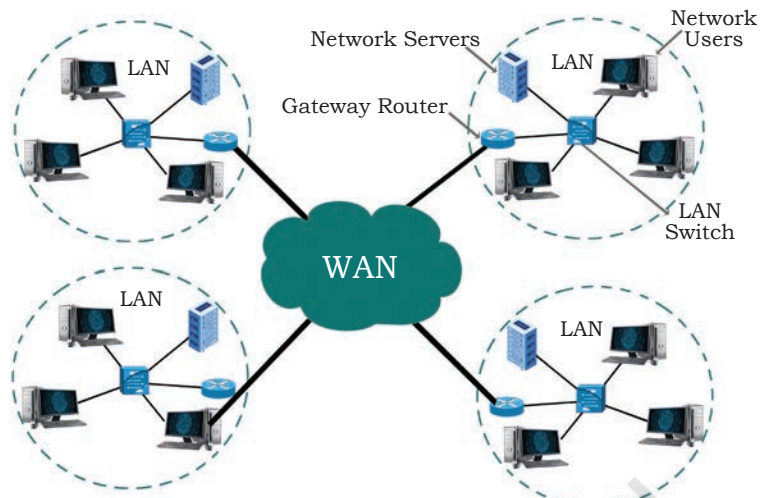


Fig. 4.5: Wide Area Network (WAN)

Metropolitan Area Network (MAN)

A MAN is a network that connects two or more LAN or CAN (Campus Area Network) together but does not extend beyond the boundaries of metropolitan area. Multiple routers, switches and hubs are connected to create a MAN. MAN is operated by a government body or corporation. Fig. 4.6 shows the MAN.

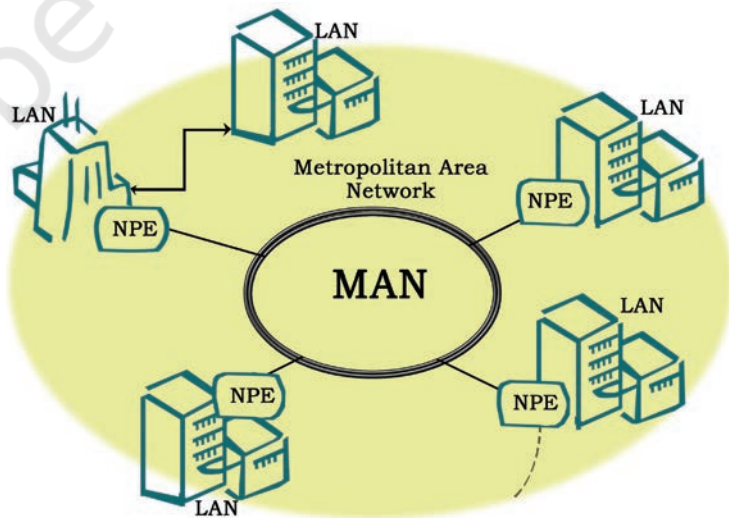
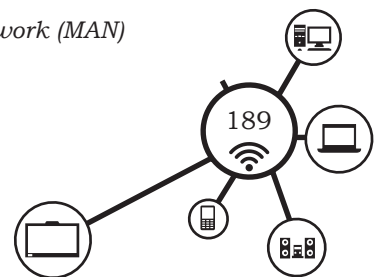


Fig. 4.6: Metropolitan Area Network (MAN)



Practical Activity 1

Draw the diagrams of different types of network—simple computer network and biometric system network

Material required

Writing material

Procedure

1. Visit the various computer network infrastructure.
2. Observe the computer network carefully.
3. Draw the diagram of each network on paper as shown in Fig. a.

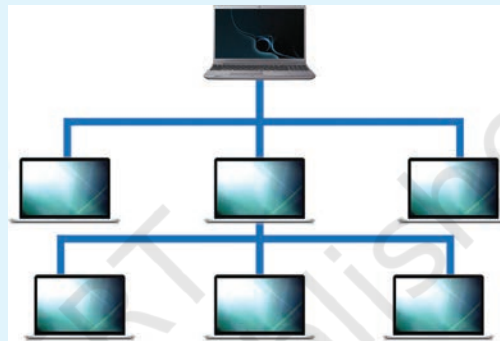


Fig. a. Simple computer network and biometric system network

Biometric Networking Topologies

Biometric operator must have a broad understanding of the various networking topologies that are used in biometric system. However, it is important to know some key concepts of network in general.

Data Packets

Data Packet is one of the most fundamental unit in the world of networking. For example, every time a biometric template is sent to a central server for storage and verification or identification processing, it is done via the data packet as shown in Fig. 4.7.

Communication process in network involves the sending and receiving of data packets. In biometric system, the biometric devices can communicate between each other or with server. The biometric data is image data and hence its size is large. So the biometric template is broken down into bits, known as 'Data Packets.' These

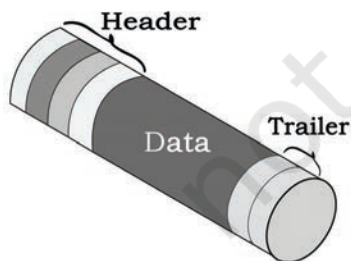
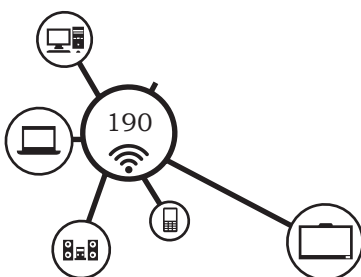


Fig. 4.7: Data packet



data packets then travel across the network and are then reassembled back again into their original format after arriving at their point of destination. The server then processes the data.

A data packet consists of a header, packet and trailer as shown in Fig. 4.8. The header specifies the final destination of the biometric template. The trailer possesses the ability to ensure that the data packet gets to the right destination during the intended time frame.

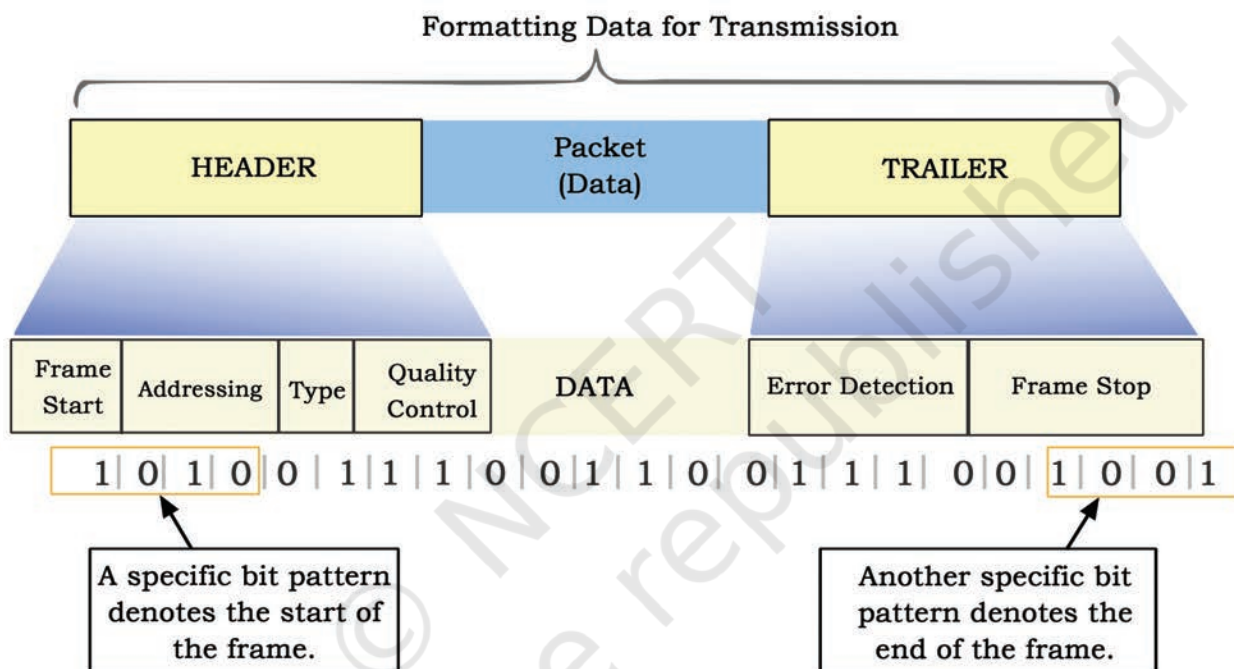


Fig. 4.8: Formatting data for transmission

Data Packet Switching

Data packet switching is an important aspect of biometric network design. For example, when more than three biometric devices are connected to the server, different network routes may be used to reach the destination. This is done to optimise the flow of data packets in biometric network system.

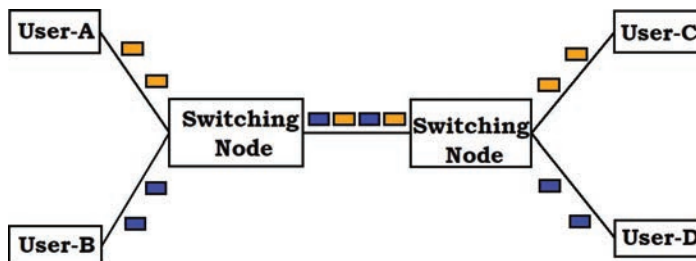
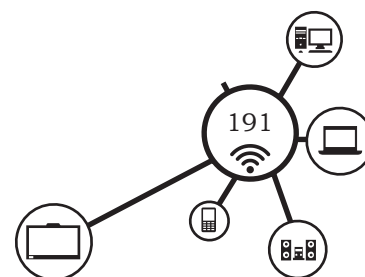


Fig. 4.9: Formatting data for transmission



Networking Models

There are basically two network models—peer-to-peer and client/server. The computer network can have the combination of both peer-to-peer and client/server models. For example, you may be using a centralised mail server and/or access files from other machines in the network.

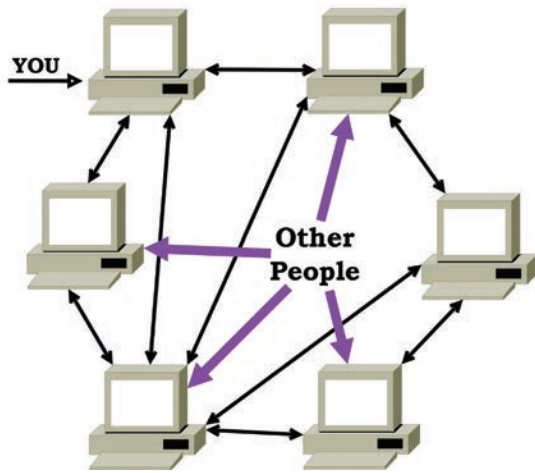


Fig. 4.10: Peer-to-Peer (P2P) Model

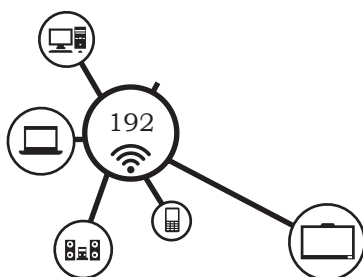
Peer-to-peer (P2P) model

In a peer-to-peer biometric network, the clients are all networked to one another without having the need of main hosts. The computers communicate with each other by using a protocol. The biometric devices known as 'Peers.' Fig. 4.10. shows an example of a peer to peer network.

For example, if the processing of verification and/or identification transactions become too much for one peer to handle, then the workload can be transmitted across to the other peers since they are all networked together.

Client/server model

Client/server network consists of one central server and several client computers connected to the server. The server is a powerful computer with high processing speed and high storage capacity, while the clients are less powerful with either personal computers or workstations. In client/server networking of biometric system all biometric devices are interlinked with another and the overall system is connected to a central server. The server is known as the 'Host,' and the connected biometric devices are called 'Clients.' The clients transmit the biometric templates and other relevant information to the host. The host then conducts the verification and/or identification at database level. The transmission of the biometric templates to the host is known as 'Network Requests.' The client asks the host to confirm the identity of the individual and to send the result of this transaction back to the client.



For example, in a large organisation where thousands of employees are working, one fingerprint scanner cannot do all of the work of confirming the identity of each and every employee. The scanners are installed all over the organisation and all networked together to the central server. Fig. 4.11 shows that the computers, printer and scanner are connected to the central server.

Intranet

Intranet provides access to the web applications within the organisation. The websites created for Internet

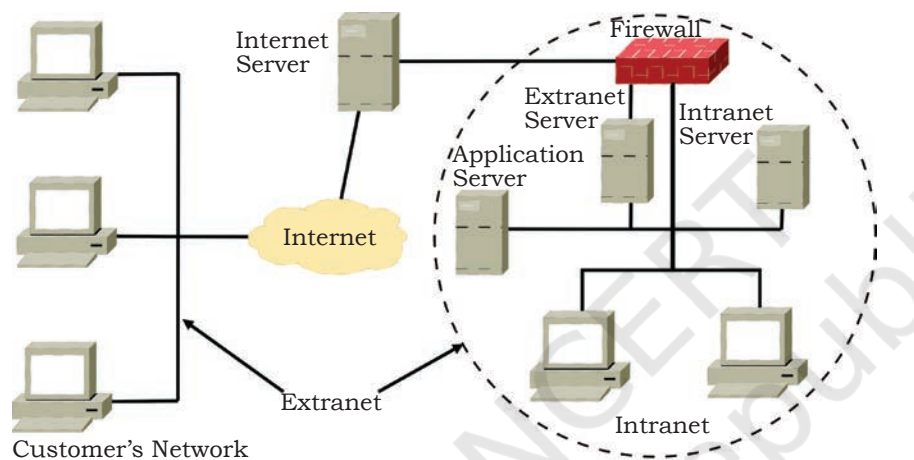
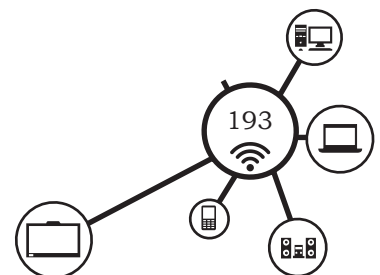


Fig. 4.11: Intranet

provide global access, while internal web application is set up to be used by the employee of the organisation. This internal web application is called Intranet. Web pages on the Intranet are not accessible to an employee who tries to access them from outside the company's network. Fig. 4.11 shows the typical Intranet infrastructure.

Extranet

Extranet is a part of the company's network that can be made available to use securely by an employee through outside. For example, an organisation may allow a vendor to view or access their resources, such as their internal website for updating a product catalogue, or training material. However, this is highly restricted to Internet users that are public. Some organisations allow



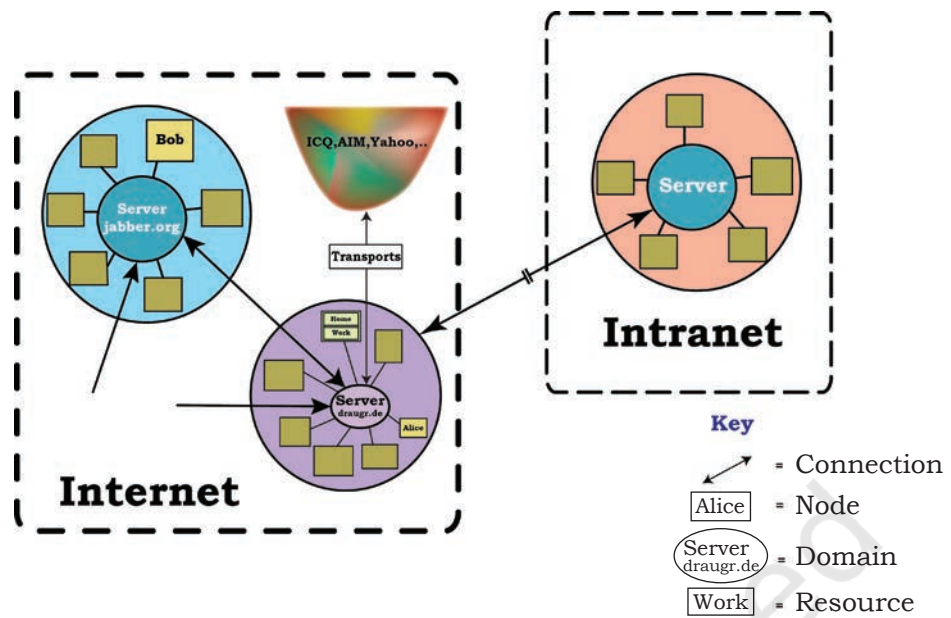


Fig. 4.12: Extranet

provision to access through virtual private network (VPN). Fig. 4.12 shows the extranet infrastructure.

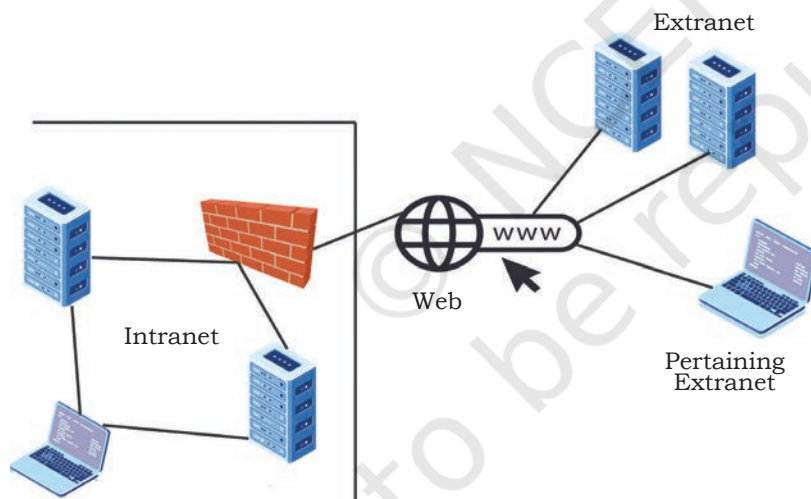


Fig. 4.13: Internet

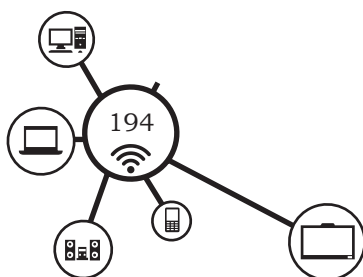
Internet

Internet is a global system of interconnected networks and uses TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite. Internet consists of billions of computing devices and is the largest network in the world. Internet is used for various purposes, such as browsing, e-mail, chatting, social networking and

online shopping, etc. Fig. 4.13 shows the diagram of Internet.

Network Devices

The physical devices called nodes, which help computers to communicate with each other are called network devices. These devices are used for connecting two different network models. In a network, the devices,



which receive or generate data are called hosts and the intermediate devices are called nodes. There are different types of networking devices, which are listed as follows

- Network Interface Card (NIC)
- Repeaters
- Network Bridge
- Network Hubs
- Network Switches
- Routers
- Network Gateways
- Modem
- Access Point
- Wi-Fi Router

Network interface card (NIC)

It is the essential hardware required to connect the computer to a network. NIC is an expansion card either ISA or PCI, or can be on-board integrated on a chipset. NIC has an appropriate connector to connect the cable to it. The MAC address is a globally unique hardware number present on the NIC and is specified by the NIC manufacturer. Fig. 4.14 shows the typical NIC card.

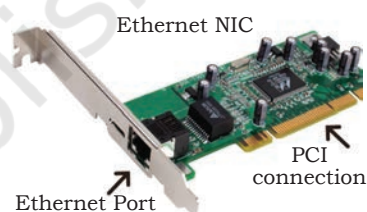


Fig. 4.14: Network Interface Card (NIC)

Repeaters

Repeaters is a two port device. In a long distance network, when the signal becomes weak, a repeater is used to regenerate the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. The signal can be transmitted over the same network. Repeaters can be both wired and wireless, if it is wireless then we call it a range extender. Fig. 4.15 shows how repeater is used in connecting the network.

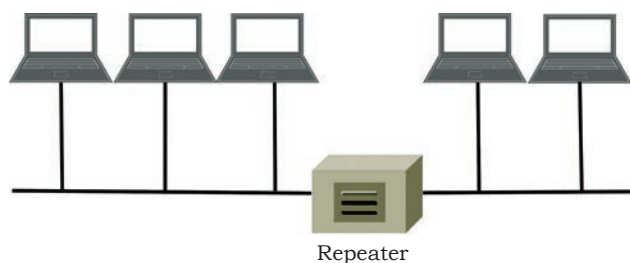
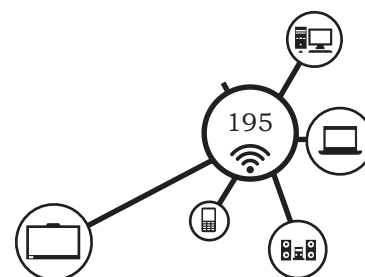


Fig. 4.15: Repeater in joining the network

Network bridge

A network bridge is a repeater, which joins two physical segment of a same network. It filters content by reading



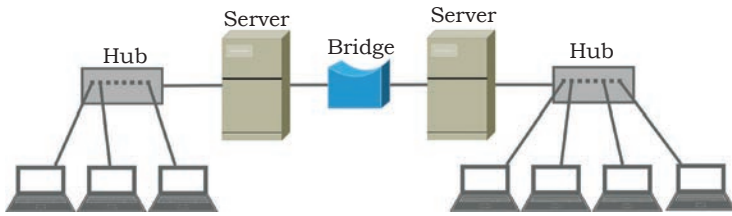


Fig. 4.16: Bridge connecting the physical segment of a network

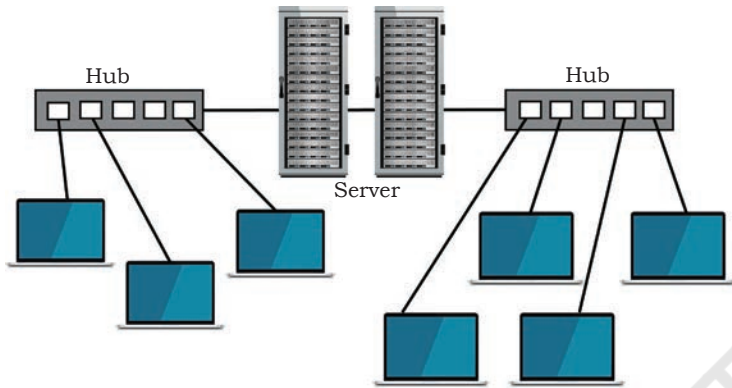


Fig. 4.17: Computers connected to hub in a network

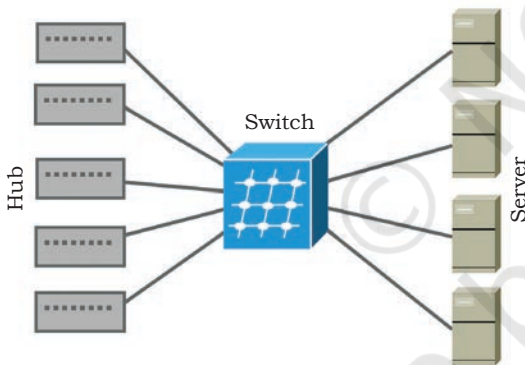


Fig. 4.18: Connectivity of computers and devices with the switches

the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device. Fig. 4.16 shows a connecting the physical segment of a network.

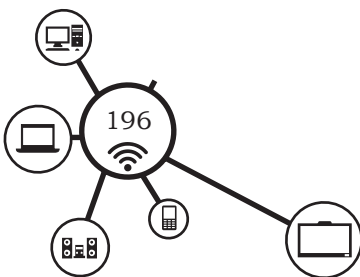
Network hubs

It is used to connect multiple nodes in the network. In a hub, the data received in one port, replicates to all of its port except the receiving port. The entire node attached to this hub, receives the same data. Fig. 4.17 shows how computers are connected to hub.

Network switches

It is the combination of a network hub and a network bridge. A switch can perform packet forwarding and bridging at the same time. Switches are similar to hub but manage traffic based on MAC address and are efficient in large networks. Switches are considered intelligent as they build a table of MAC addresses of devices connected to it and when each packet is received, they are analysed and forwarded to the device with matching MAC address. Fig. 4.18 shows connectivity of computers and devices with the switches.

Switches are of two types — managed and unmanaged. The Unmanaged switches are used for networking at homes or small offices where administrative configuration is not required. The managed switches are used in enterprise networks and ISP's, which are required to be configured by the network administrator before it is used in a network.



Routers

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Layer 3 or Network Layer device. Routers are used for connecting various networks (LAN or WAN). A router transmits data from incoming network to another network. A router maintains a routing table of various networks. For biometric device, router should support port forwarding after which one should ensure that the router has access to it. Based on the destination address, the router determines to which network the incoming packet should be transmitted. Fig. 4.19 shows how the router is used to connect heterogeneous networks.

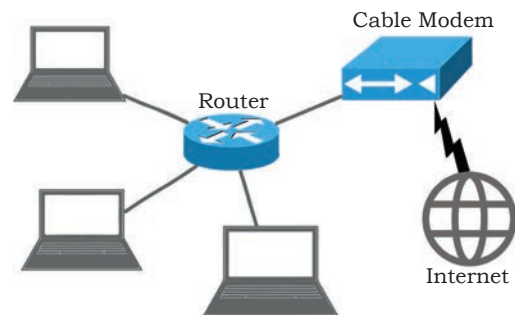


Fig. 4.19: Router to connect heterogeneous networks

Network gateways

A gateway is a passage to connect two networks together that may work upon different networking models. They take data from one system, interpret it and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router. Fig. 4.20 shows Gateway.

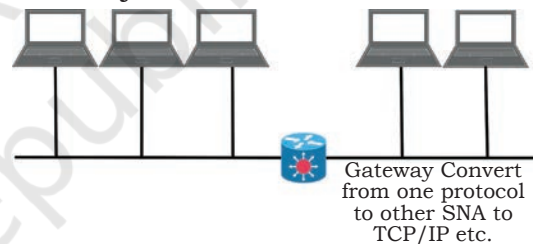


Fig. 4.20: Gateway

Modems

Modems, also called as modulator and de-modulator, are the device that modulates one or more carrier waves to encode data and demodulates the carrier wave to decode that data. The modems provide the cheapest way to send and receive data, like the telephone lines. Modem is used in dial-up network Internet connection at home. Fig. 4.21 shows a modem.



Fig. 4.21: Modem

Access points

Wireless access points, which are commonly known as access points, are the devices that allow wireless (or Wi-Fi) devices to connect with a wired network. It is a device which converts the wired signal to a wireless form so as to access by smartphone, laptops and tablets.

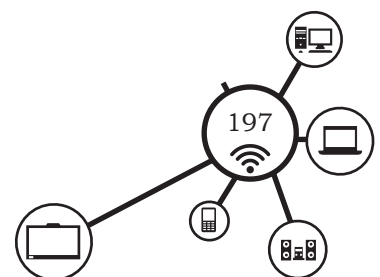




Fig. 4.22: Wi-Fi router

Wi-Fi routers

Wi-Fi routers are used at homes, offices, etc., for high speed broadband connection. It is the combination of a router, an access point, a gateway and a modem. Wi-Fi routers can perform routing, switching, giving a gateway to the data and granting access to the wireless devices. A Wi-Fi router is shown in Fig. 4.22.

Practical Activity 2

Demonstrate the working of network devices

Material required

Network devices, computer

Procedure

1. Visit a computer network centre and observe the various network devices installed in the network.
2. Identify and name the various network devices.
3. Observe the working of various network devices in the network.

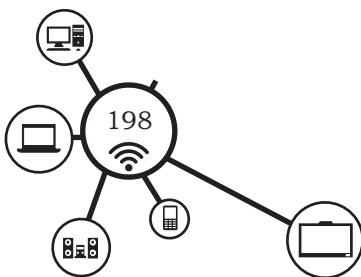
Network Protocol

Protocols are a set of rules or standards that allow network devices to communicate and exchange information. The biometric devices connected in network also have to use network protocols to transmit the information through data packets. Some examples of protocols at the network layer are NetBEUI, IPX/SPX, TCP/IP, AppleTalk.

The NetBEUI protocol is used to connect and communicate between computers with Microsoft Windows. AppleTalk protocol is used to connect and communicate among computers with MAC OS. However, when connecting computers with different operating systems you need to use the TCP/IP protocol.

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is a combination of two protocols. TCP stands for Transmission Control Protocol, and IP stands for Internet Protocol. Biometric systems most commonly



use TCP/IP protocol. It is the most widely used protocol for data transfer over Internet. TCP offers connection-based services. Most operating systems support TCP/IP. TCP/IP consists of four distinct network layers:

Link layer

This layer consists of the communication tools used in the biometric network. The data packets containing biometric templates travel from one link to the next till they reach the server.

Internet protocol

This is responsible for the internal communications between the various network links that make up the entire network segments between the biometric devices and the server.

Transport layer

This is primarily responsible for overall communication between the biometric devices and server.

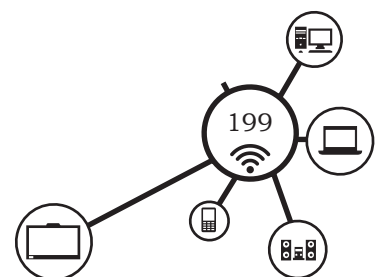
Application layer

This is responsible for the processing services, such as the verification and/or identification transaction processing.

TCP/IP is the most widely used protocol in LAN, WAN and Internet because is open standard can be used in different operating systems, runs on any network framework, such as ethernet, token ring, dial-up connections, follow routable and a common addressing scheme.

IP Address

Every computing device, such as computer, tablet, smartphone, that communicates on the Internet, is assigned a unique identifying number called IP (Internet Protocol) address. Currently there are two standards of IP-address — IPv4 and IPv6. IPv4 (version 4), has the format of four numbers between 0 and 255 separated by a period. These IP addresses are assigned by an Internet Service Provider (ISP). The ISP charges a fee for the service. Example of IP address are:



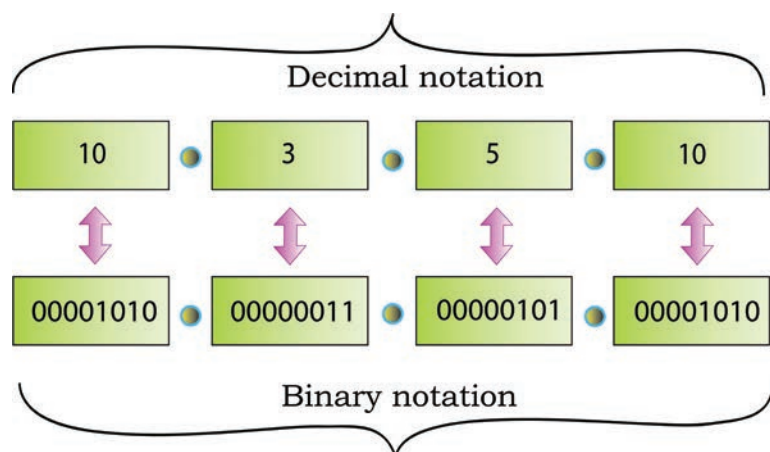


Fig. 4.23: Sample IP address

- 172.64.85.42
- 193.213.78.154

The IPv4 standard has a limit of 4,294,967,296 possible addresses. The IPv6 standard is eight groups of four hexadecimal digits, such as 2001:0db8:85a3:0042:1000:8a2e:0370:7334. The IPv6 standard has a limit of 3.4×10^{38} possible addresses. IP addresses are stored in text files and

displayed in human-readable notations, such as 10.3.5.10 as shown in Fig. 4.23.

Classful Network

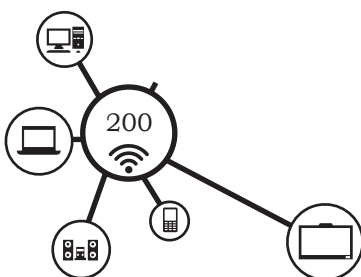
Classful network is an addressing schedule originally introduced in 1981 and used for several years until the introduction of Classless Inter-Domain Routing (CIDR) method. In this method, the 32-bit address space is divided into five address classes, namely A, B, C, D and E. Each class defines a fixed network size and number of hosts within networks.

Following table summarises the classes of IPv4 addressing:

Class	Range	Subnet	No. of Networks	No. of Hosts/ N
A	0.0.0.0 – 126.255.255.255	255.0.0.0	126	16777214
B	128.0.0.0 – 191.255.255.255	255.255.0.0	16384	65532
C	192.0.0.0-223.255.255.255	255.255.255.0	2097152	254
D	224.0.0.0 – 239.255.255.255	Multicast		
E	240.0.0.0 – 255.255.255.255	Reserved for future use		

Examples of Class A , B, & C type IP address are:

Class A	Class B	Class C
5.2.2.1	129.1.2.3	200.12.3.4
12.1.1.14	160.2.3.34	202.13.14.15
72.34.23.23	190.2.3.4	220.3.2.3



Practical Activity 3



Fig. (a)

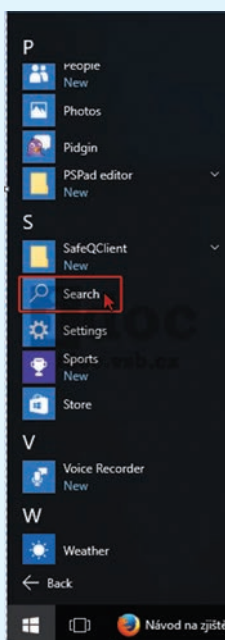


Fig. (b)

Check IP address of computer connected in network.

Material required

Computer system connected in network, writing material

Procedure

To find the IP address on Windows 10 using GUI:

1. Visit the computer network lab and start the computer connected in network.
2. Click on Start button and choose All apps.
3. Click on the command prompt or press WinKey+R to enter command (Figs a and b).
4. Type **ipconfig/all** and press **Enter**. Find your **Ethernet adapter Ethernet**, locate row **IPv4 Address** and **IPv6 Address**. (Fig. c)

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\abc123>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-70D5JUQ
Primary Dns Suffix . . . . . : vsb.cz
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : vsb.cz

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : vsb.cz
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address. . . . . : 58-94-6B-5B-72-80
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

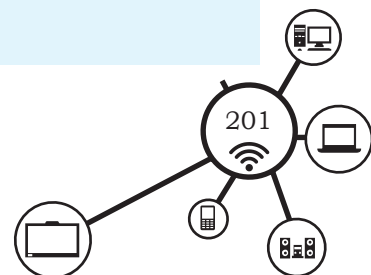
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : vsb.cz
Description . . . . . : Broadcom NetXtreme 57xx Gigabit Controller
Physical Address. . . . . : F0-4D-A2-B9-C5-63
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address. . . . . : 2001:718:1001:158:286a:2516:6819:a6e4(Preferred)
Temporary IPv6 Address. . . . . : 2001:718:1001:158:3808:1bf1:5d53:9ad0(Preferred)
Link-local IPv6 Address . . . . . : fe80::286a:2516:6819:a6e4%4(Preferred)
IPv4 Address. . . . . : 158.196.158.56(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, October 14, 2015 10:21:52 AM
```

Fig. (c)

1. Find internal (network) IP address

1. Start the computer with Ubuntu Linux.
2. Open the **Activities overview** and start typing **Network**.
3. Click on **Network** to open the panel.



NOTES

4. Choose which connection, **Wi-Fi** or **Wired**, from the left pane.
5. The IP address for a wired connection will be displayed on the right. Click the details button to see the IP address for the wireless network in the details panel.
6. It will display the internal (network) IP address as shown in Fig. d.



Fig. d

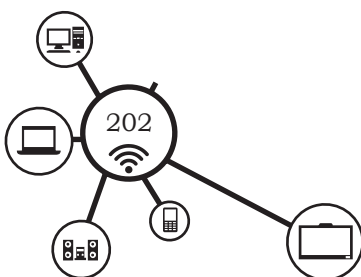
2. Find external (Internet) IP address

1. To find the external or Internet IP address, open the site whatismyipaddress.com.
2. The site will display external IP address of your computer.
3. Thus you can find local or remote IP addresses.

Wireless Networking

Wireless networking is the wireless technology to establish a wire-free connection or communication between two or more devices. In wired technology data is encoded as electric current and signals travel through wires, while in wireless technology data is encoded on electromagnetic waves that travel through air. Today, we are using wireless communication in laptop, iPad, and smartphones to access the Internet. The wireless technologies have made these devices more functional.

The wireless networks have two main components — the wireless access points that include the transmitter along with the area it can cover, and the wireless clients like mobile handsets, laptops with Ethernet cards, etc. The access point receives data frames from the



computers attached to it wirelessly, checks the frames and transmits them to their destination. The speed of wireless connection is determined by the distance of the wireless client device from the access point, the obstruction-free path interference, and the number of users using the network at a given time. Following are the most common wireless technology.

Wi-Fi

Wi-Fi is a technology that takes an Internet signal and converts it into radio waves. These radio waves are picked up by wireless adapter. The devices in the radius of approximately 50–60 feet can catch the signal. Wi-Fi routers are used for broadband connections at home.

Mobile network

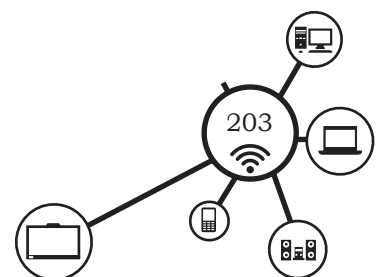
Mobile phone technologies have evolved different communication standards for their networks. GSM is used by AT&T and T-Mobile and CDMA is used by other major carriers. It is possible for a mobile phone using one type of network to switch to the other type of network by switching out the SIM card, which controls your access to the mobile network. With the release of 4G networks, it has become easy and fast to access Internet over a smartphone and other cellular devices. Currently wireless carriers began to offer 4G data speeds, giving the cellular networks the same speed that customers were used to get via their home connection.

Bluetooth

Bluetooth technology is used to connect the different components wirelessly. Bluetooth has a range of approximately 300 feet and consumes little power. The printer, wireless keyboard and mouse can be connected to computer through Bluetooth.

Biometric Attendance System (BAS)

Biometric attendance system is used in most of the organisations. Biometric attendance machine captures fingers or iris for identity verification. Biometric time attendance machines also counts employees' work schedule, based on the report. Biometric attendance



NOTES

systems ensure the accuracy of attendance and is useful in the organisations with large number of employees.

Internal Structure of Biometric Attendance System (BAS)

1. The Biometric Attendance System (BAS) supports TCP/IP protocols for communication. It also supports Wi-Fi, GPRS and GPS.
2. The BAS can store 8000 to 10000 unique biometric fingerprints records and up to 1,00,000 total transactions in their storage.
3. BAS works over push data technology and also supports both static and dynamic IP address.
4. Biometric attendance system has a 800 MHz 32-bit microprocessor.

Practical Activity 4

Establish connectivity of biometric attendance system

Material required

Biometric attendance system, computers connected in LAN

Procedure

Step 1. Connectivity of Biometric Attendance System (BAS):

The Biometric Attendance System (BAS) is connected to the computer system either in a LAN via Ethernet port or through a USB port. We can also connect the Pendrive directly to the BAS using its USB port also. It uses Wi-Fi as well as GPRS with an auto switch mechanism. The desktop application can be used over Wi-Fi, Ethernet or Data Card connectivity option. The possible connectivity of the BAS to the PC or the USB drive is shown in Fig. a.

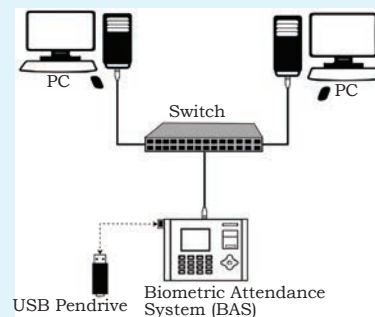
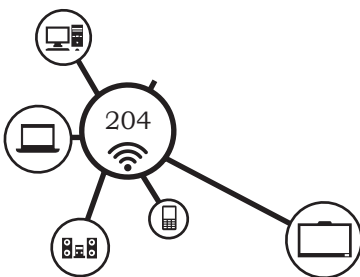


Fig. a



Step 2. BAS Connectivity either with PC in LAN or with USB Pendrive.

- If the PC and the BAS machine both are connected in LAN using Ethernet port, then such a network is shown in Fig. b.
- If the PC and the BAS machine both are connected directly via USB Cable using USB port, then such a network is shown in Fig. c.

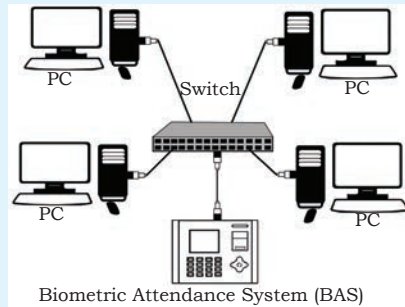


Fig. b

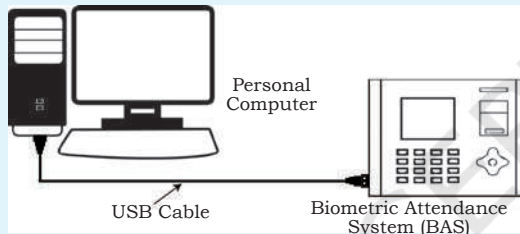


Fig. c

Step 3. Connectivity and Configuration of the BAS to the PC

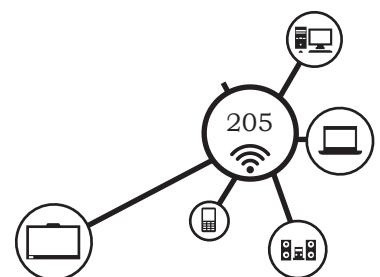
- After having the physical connection of BAS in LAN as explained above, the BAS has to be configured in the network to function as a node.
- To connect the BAS machine to the PC in LAN, it is necessary to assign the IP address of same series. Assign the IP address 192.168.1.5 and 192.168.1.201 to BAS machine.

Step 4. To configure manual IP address to the PC do the following

- First right click on the network icon on lower right corner of taskbar area (Fig. d).
- When this icon is right-clicked the option to Open 'Network and Internet' settings will appear below. Click on 'Open Network and Internet'. (Fig. e)



Fig. d



NOTES



Fig. e

Once 'Network and Internet Settings' appears, go ahead to click on 'Change adapter settings' on top of right corner under 'Related settings'.

Step 5. Here you can see Ethernet adapters installed on your computer. You can change the network settings by right clicking on the connection and then selecting the option Properties, as shown in the Fig. f and g.



Fig. f

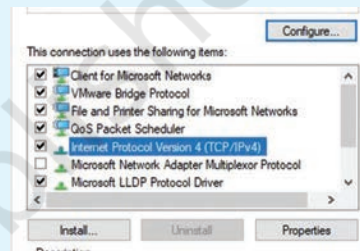


Fig. g

Step 6. In the Network Connection Properties window, put a tick (✓) on Internet Protocol Version 4 (TCP/IPv4) and click on 'Properties'.

Step 7. If you have DHCP server configured, you can configure the computer to get IP address and other network information automatically by selecting 'Obtain an IP address automatically'.

Step 8. To assign static IP address or do manual network configuration, click on the 'Use the following IP addresses', as shown in Fig. i and j.



Fig. i

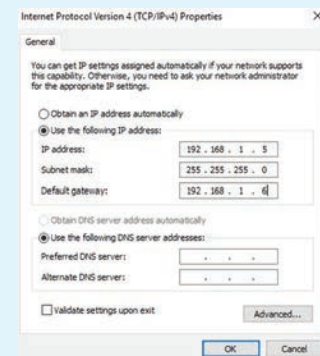
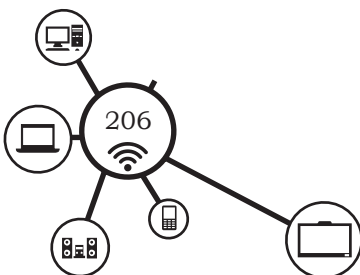


Fig. j



Step 9. Now login in eSSL desktop, based application using default login credentials as shown in Fig. k.



Fig. k

Step 10. To configure IP address to BAS, click on 'Utilities Tab' and select 'Device Management' as shown in Fig. l.

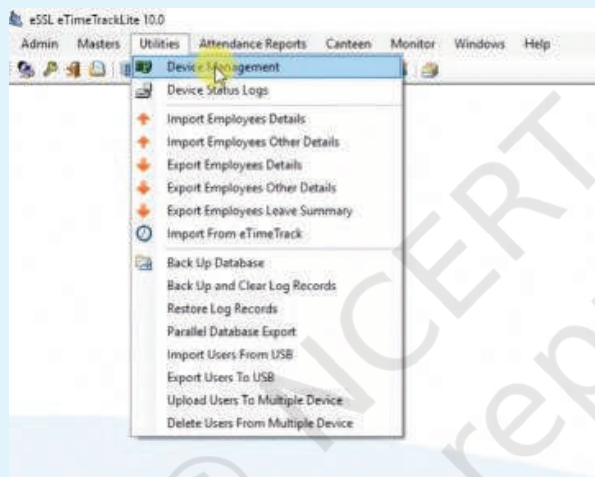


Fig. l

Step 11. The TD and USB options are displayed under Device Name, where TD works on LAN (Ethernet) port and USB on USB port as shown in Fig. m.

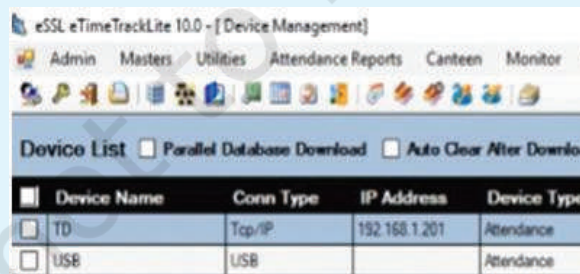
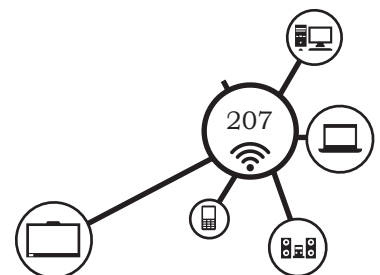


Fig. m

To assign or edit IP address, right click on TD and select 'Edit' option as shown in Fig. n.



NOTES

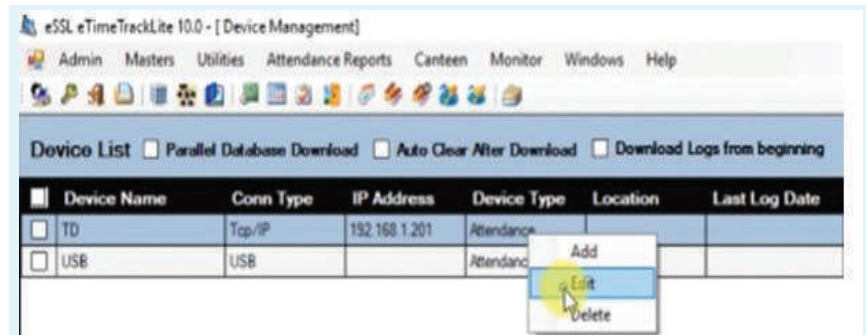


Fig. n

Assign the IP address and click on 'Save' button as shown in Fig. o.

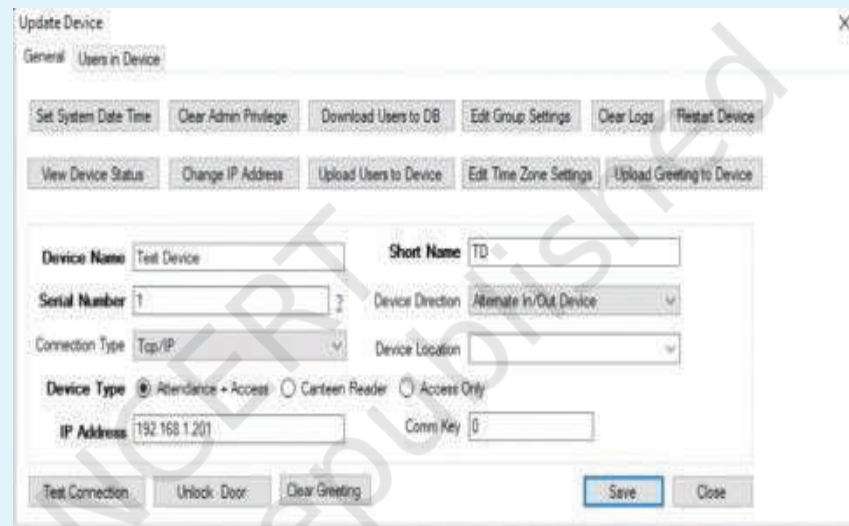


Fig. o

Testing of BAS Using Ping command

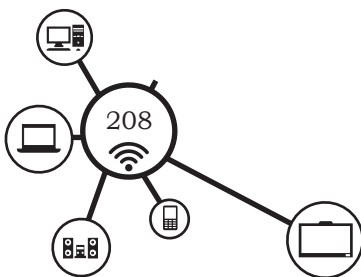
Ping is a utility used to test network connectivity. The ping utility is commonly used to check for network errors and network connectivity. After assigning the IP address of same series to the PC and BAS, check whether it is communicating to each other or not. To confirm that both devices are in same network, run a command **ping <BAS_Machine_IP>** to the terminal of a PC.

Practical Activity 5

Test BAS using Ping command

Material required

Biometric attendance system, computers connected in LAN



Procedure

1. Open the command line terminal window of PC using run command as shown in Fig. a.

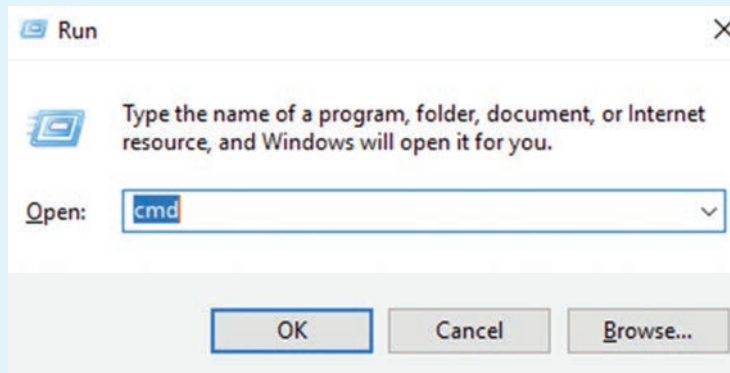


Fig. a

2. Click on 'OK' button.
3. At the command prompt type ping <BAS_Machine_IP> -t, i.e. 192.168.1.201, as shown in Fig. b.

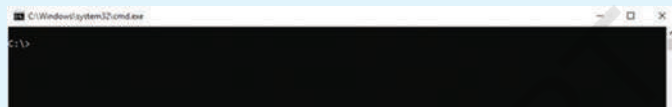


Fig. b

4. Press Enter key. The time between these two transmissions is calculated to generate an average response or latency time as shown in Fig. c.

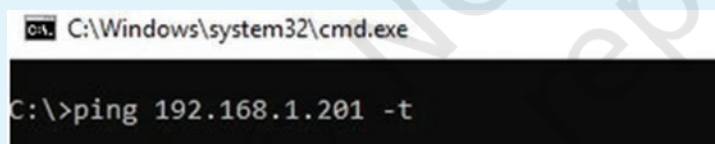


Fig. c

Thus we have tested the proper network connectivity between BAS machine and PC Fig. d.

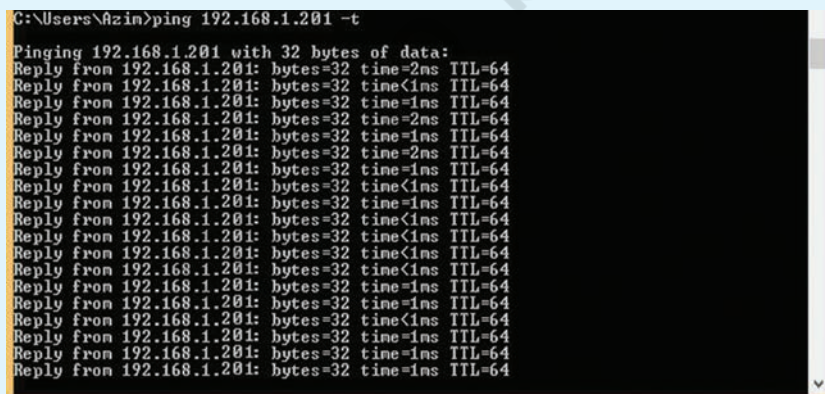
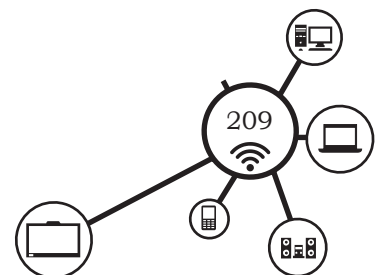


Fig. d



NOTES

Practical Activity 6

Draw the diagram of client server networking. Identify and name the various tools used in networking from the given pictures.

Materials required

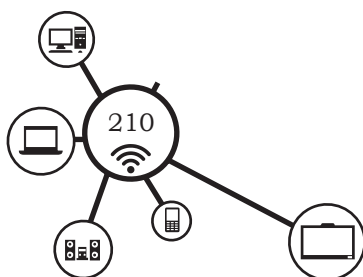
Pen, Pencil, Paper, Pictures of various networking tools

Procedure








1. Visit the computer laboratory where client server network is installed
2. Observe the network carefully and draw the diagram of client server network.

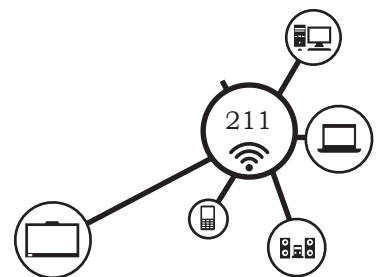
Basic Tools for Networking

Name of the tool	Picture of tool
Crimping Tools	
UTP Cable	
Coaxial Cable	
Cable Ties	



NOTES

Screws	
Pliers	
Soldering Iron	
Desoldering	
LAN Tester	
Wireless Hub	
Bluetooth Device	



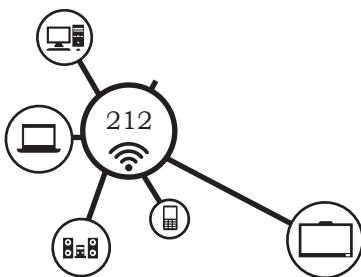
NOTES

Telephone	
Cable Modem	

Check Your Progress

A. Fill in the blanks

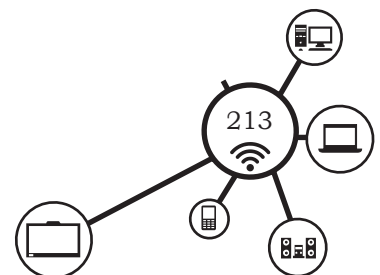
1. Collection of computers and other hardware components interconnected by communication channel is called _____.
2. Computer network allows sharing of _____ and _____.
3. Computers can be connected through _____ or _____.
4. Resources in computer network include devices, such as _____.
5. Printer sharing is possible through _____.
6. There are _____ types of computer networks.
7. LAN stands for _____.
8. Computers networked within a limit of geographical area are called _____.
9. WAN means _____.
10. LANs at different locations, when connected together are called _____.
11. MAN stands for _____.
12. LANs beyond the boundaries of a city, when connected together are called _____.
13. P2P networking model stands for _____ model.
14. When each computer can act both as a server and client, then that networking model is called _____ model.
15. HTTP stands for _____.
16. IP address means _____ address.
17. When there is one server and many clients, then such networking model is called _____ model.
18. In Aadhaar card biometric data the _____ networking model is used.



19. Internal network of an organisation is called _____.
20. The network that is not accessible to the public is known _____.
21. The network that is accessible to the public is known _____.

B. Multiple choice questions

1. The computer network that is used outside the Intranet is known as _____.
 (a) Internet (b) Extranet
 (c) Cable (d) Router
2. The global system of interconnected networks that use TCP/IP protocol is known as _____.
 (a) Internet (b) WAN
 (c) Intranet (d) LAN
3. The largest network of the computers in the world is _____.
 (a) Internet (b) Extranet
 (c) MAN (d) LAN
4. Which of the following are network devices?
 (a) Repeater (b) Modem
 (c) Router (d) All of these
5. _____ is used to regenerate the signal when it becomes weak.
 (a) Network hub (b) Network switch
 (c) Repeater (d) Router
6. To join the two physical segments of the same network _____ is used.
 (a) Network bridge (b) Network switch
 (c) Repeater (d) Router
7. Multiple nodes in the network are connected by using the _____.
 (a) Network hub (b) Wi-Fi
 (c) LAN (d) router
8. The combination of network hub and network bridge can be performed by using _____.
 (a) Bluetooth (b) network switch
 (c) gateway (d) modem
9. The device that routes the data packets based on their IP addresses is _____.
 (a) UTP cable (b) telephone
 (c) repeater (d) router
10. Two networks working on different networking models can be connected together by using a _____.
 (a) network gateways (b) desktop
 (c) Internet (d) Wi-Fi



NOTES

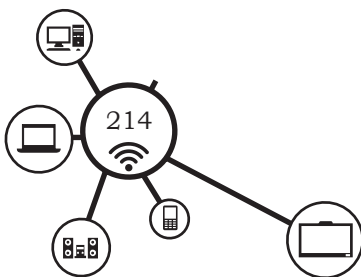
11. Modem means _____.
(a) modulator demodulator (b) modulator
(c) de-modulator (d) router
12. The cheapest way to send and receive the data through the telephone lines can be performed by using a _____.
(a) modulator demodulator (b) modulator
(c) de-modulator (d) modem
13. Wireless access point is also known as _____.
(a) spot (b) soft spot
(c) hot spot (d) Wi-Fi spot
14. The device that is a combination of router and an access point is _____.
(a) modem (b) hot spot
(c) Wi-Fi router (d) repeater
15. The set of standards that allow network devices to communicate an exchange information is called _____.
(a) Wi-Fi router (b) protocol
(c) repeater (d) modem

C. State whether the following statements are True or False

1. Protocols are the set of rules for communication.
2. In a computer network, all computers need not use the same protocol for communication.
3. Protocols may include signaling, authentication, error detection and correction.
4. TCP/IP stands for Transmission Control Protocol/Internet Protocol.
5. TCP/IP is not a core protocol of Internet.
6. IP is the primary protocol used for relaying data across the network boundaries.
7. Ipv4 uses 64 bit addressing scheme.
8. Ipv4 provides 232 possible addresses.
9. IANA means Internet Assigned Numbers Authority.
10. Ipv6 uses 64 bit address.
11. Ipv6 address consists of 8 groups of four hexadecimal digits.
12. Most of the operating systems support Ipv4 and Ipv6.

D. Short answer questions

1. What is a computer network?
2. List the advantages of a computer network.
3. What are the different types of computer networks?
4. Write the features of LAN.



5. Write the features of WAN.
6. State the networking models used in computer networks.
7. Give the diagrams of networking models.
8. What is Intranet?
9. What is Internet?
10. Explain the function of the following network devices—
 - (a) repeaters
 - (b) router
 - (c) modem
11. What is network protocol? Explain TCP/IP network protocol.

SESSION 2: INTERNET AND ITS APPLICATION

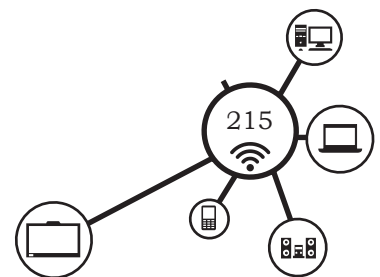
Each one of you must have heard about the Internet and most of you would be using it on your smartphone. We connect to the Internet from home, school, or a cyber café. Once connected to Internet we can go around the world, communicate with others, order our food, clothes and everything. In this session we will learn the basic concept of Internet, and the the various application of Internet in our daily life.

Introduction to Internet

Internet is the largest computer network in the world, connecting billions of computers and other computing devices. It is possible to access any information on the Internet as well as communicate with anyone. Internet is the information super highway and fastest available way to share information with the world community. Internet allows computers on different kinds of networks to interact with each other. Any two computers, having different software and hardware, can exchange information over the Internet. The exchange of information may be among connected computers located anywhere, like military and research institutions, different and organisations, banks, educational institutions, public libraries, commercial sectors.



Fig. 4.24: Internet



How Internet Works

Internet is a network of interconnected networks and is designed to operate without a central control. It consists of clients, servers and Internet Service Provider (ISP). The architecture of Internet is hierarchical in nature.

Clients

They are the end users. These are computer or any computing device connected to the Internet to access web pages from the server. They use browsers, such as Mozilla Firefox, Internet Explorer, Google Chrome, to access the web pages.

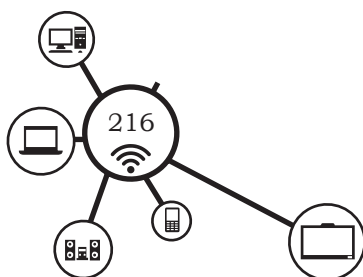
Internet Service Provider (ISP)

The next level is the local Internet Service Provider (ISP). There are two levels of ISP — local and regional. Local ISP is connected to Regional ISP.

- (i) Local ISP is the local telephone company, such as Bharat Sanchar Nigam Ltd. (BSNL), Mahanagar Telephone Nigam Ltd. (MTNL), and Airtel. The client can call local ISP using a modem.
- (ii) Regional ISP is at next level, which connects the local ISP's located in various cities via routers. A router can interconnect networks having different technologies, different media and physical addressing schemes. If the packet received by the concerned regional ISP is for a client connected to that regional ISP, then the packet is delivered, otherwise, packet is sent to the backbone.

Backbone

The backbone networks are connected to Regional ISP's with a large number of routers through high speed fiber-optics. The backbones are connected to Network Access Point (NAP), so that packets travel across different backbones. The packet traverses different backbones until it reaches the backbone of regional ISP for which



it is destined. The Internet hierarchy is shown in Fig. 4.25.

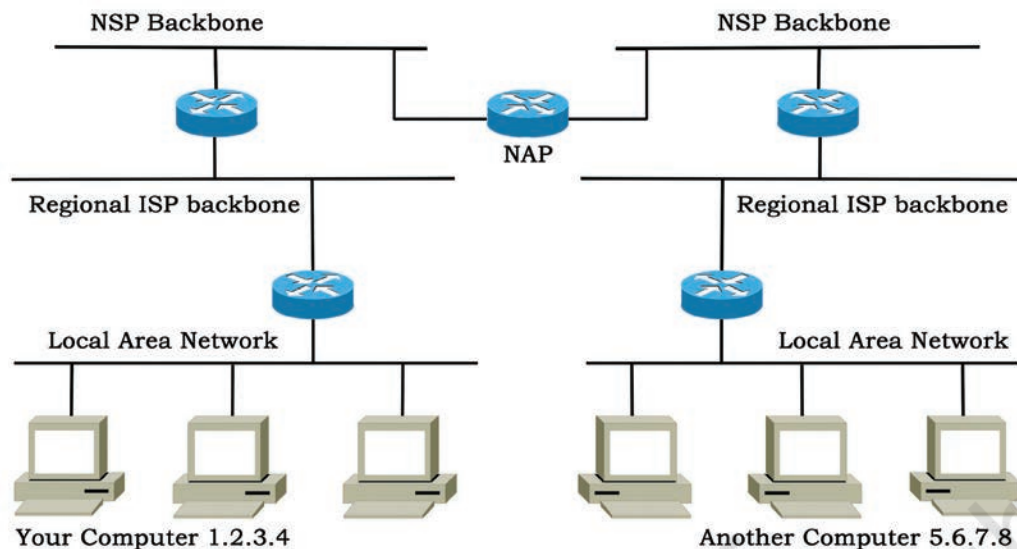


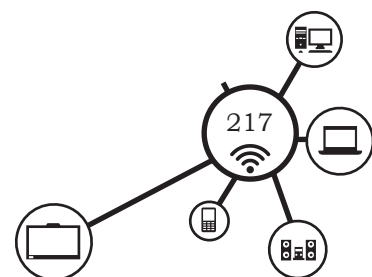
Fig. 4.25: Internet hierarchy

When the client requests a webpage to access through the browser, the browser sends a request to ISP server asking the requested web page. The ISP server looks the requested web page in the database and finds the exact host server containing the requested website or web page. The host server sends the requested page to the ISP server. The ISP sends the page to browser, thus you can see the requested information.

Internet Connection

There are various types of Internet connections provided by ISPs. Bandwidth and cost are the two factors to decide to take Internet connection to use. The speed of Internet access depends on the bandwidth. ISPs offer various services to connect with the Internet, such as Dial-up connection, DSL, Cable modem and Integrated Services Digital Network (ISDN) connections.

Most of the dial-up and ISDN connections are now replaced by high speed broadband Internet connection, as many ISPs, such as BSNL, Airtel are offering high speed broadband connections in low cost. Its speed is ranging from 4 MBPS to 40 MBPS (Megabytes per second).



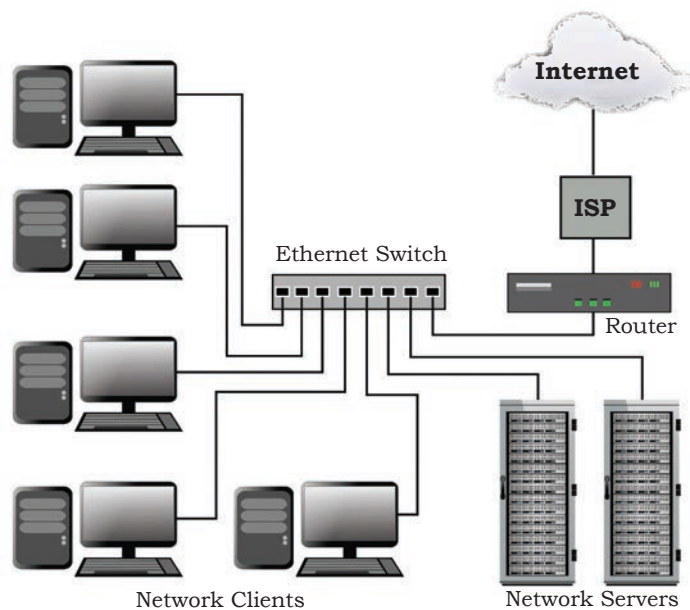


Fig. 4.26: A typical LAN Internet connection

Internet connection through LAN

Many organisations are using LAN to share the resources. Internet connection can be made available to the computers connected in LAN if the LAN is provided an Internet connection. A network router is used to provide the interface between the LAN and the Internet. The Internet connection to LAN is provided by an ISP. The clients on the network are sharing the Internet connection bandwidth, hence the connections become

slow in network. The LAN Internet infrastructure is shown in Fig. 4.26.

Downloading and Uploading

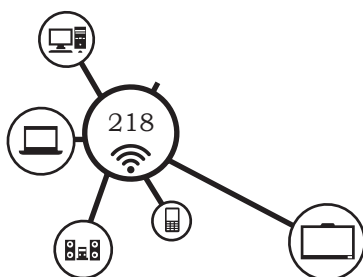
The transfer of information between server and client takes place in two ways — downloading and uploading.

The process of retrieving information from the server computers to client computers is called **downloading**.

The process of providing information from client computers to server computers is called **uploading**.

The various types of servers are used in the Internet world. Some names of the server computers are web server, mail server, print server and DNS server

- **Web server** – used for storing web pages and providing these to the client computers.
- **Mail server** – used for electronic mail and providing them to the client computers.
- **Print server** – used to manage the printing services of client computers.
- **DNS Server** – used for translating URL to IP addresses.



Practical Activity 7

Draw the logical diagram of Internet

Material required

Computer with Internet connectivity, writing material

Procedure

1. Visit any computer laboratory or organisation where Internet is working.
2. Carefully observe the Internet connections.
3. Draw the logical diagram of Internet and explain its components.
4. Observe the computer and explore browsers. List such three browsers.
5. Open a browser, such as Google Chrome and visit any website in the browser.
6. Open a browser, such as Internet Explorer and visit any website in the browser.

Protocols

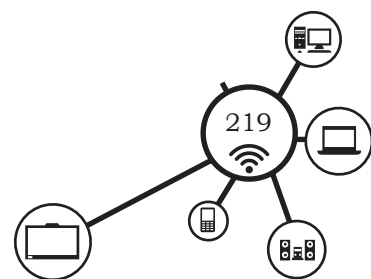
The Internet is controlled by protocols. A protocol can be seen on a system of law operated in computer networks. Following are some of the protocols used in the Internet.

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol or HTTP is the connection-less text based application protocol used to communicate with web browsers and web servers with each other. It means the connection is disconnected after fetching the requested page. A new connection is made for each request. When you type the URL on the address bar of browser, the following process takes place.

1. If the URL contains a domain name, the browser first connects to a domain name server and retrieves the corresponding IP address for the web server.
2. The web browser connects to the web server and sends an HTTP request for the desired web page.
3. The web server receives the request and checks for the desired page. If the page exists, the web server sends it. If the server cannot find the requested page, it will send an HTTP 404 error message.

NOTES



NOTES

4. The web browser receives the page back and the connection is closed.
5. The browser then passes through the page and looks for other elements, such as images applets.
6. For each element, the browser makes additional connections and HTTP requests to the server for each element.
7. When the browser has finished loading all images. The page will be completely loaded in the browser window.

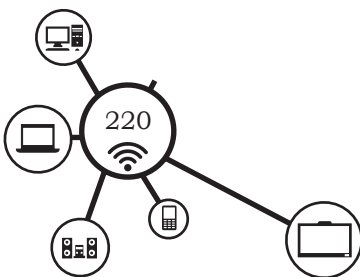
Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is used for electronic mail. SMTP is connection oriented text-based protocol. When you open your mail client to read your e-mail, typically the following happens:

1. The e-mail client software, such as Microsoft Outlook opens a connection to its default mail server. The mail server's IP address or domain name is typically setup when the mail client is installed.
2. The mail server will always transmit the first message to identify itself.
3. The client will send an SMTP HELO command to which the server will respond with a 250 OK message.
4. The appropriate SMTP commands will be sent to the server depending on whether the client is checking mail sending mail.
5. This request/response transaction will continue until the client sends an SMTP QUIT command. Then the connection will be closed.

Transmission Control Protocol (TCP)

TCP is a connection-oriented, reliable, byte stream service. Connection-oriented means the applications first establish a connection and then exhibit the exchange of data. TCP is reliable as it sends acknowledgment to the sender to confirm the delivery.



Internet Protocol (IP)

IP is an unreliable, connection-less protocol. IP's job is to send and route packets to other computers. It does not care whether a packet gets to its destination or not. IP packets are independent entities and may arrive out of order or not at all. It is TCP's job to make sure packets arrive and are in the correct order.

File Transfer Protocol (FTP)

e-mail client software have a limited capacity of sending a file of upto 25 MB in size) as an attachment. The files exceeding the size of 25 MB cannot be sent as e-mail attachments. FTP is used to transfer large files of one computer to another computer over the Internet. This protocol is operated on TCP/IP and used to upload files on the Internet as well as to download files from Internet.

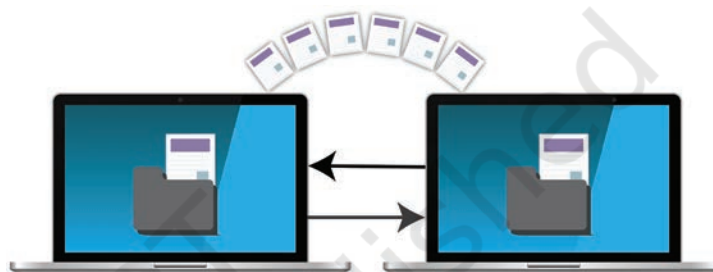


Fig. 4.27: File transfer system

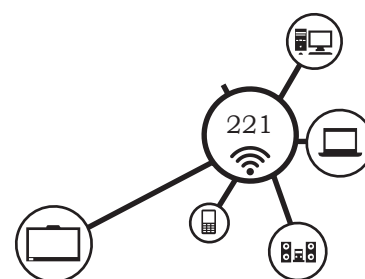
Important Terms Used in Internet

World Wide Web (WWW)

World Wide Web is a service provided by Internet and it is a large collection of electronic documents saved in computers all around the world connected to the Internet. Sir Tim Berners Lee is considered the father of world wide web.

Website

A website consists of several webpages. The web page consists of text, images, videos and other multimedia and hyperlinks. The hyperlinks provide links to other web pages or websites. Using hyperlinks makes browsing websites easy. To access a website, we need to enter the website address on the address bar of the web browser and then press the Enter key. The first page of the website which contains the basic information about the website is called the Home Page. The other pages of the website can be accessed through the hyperlinks



included in it. Fig. 4.28 shows the home page of the website of NCERT.



Fig. 4.28: Home page of NCERT website

- **Website address or URL:** Internet has a having lot of information which is available different websites. The system used to uniquely identify various resources in websites is the Uniform Resource Locator (URL). The URL must have HTTP protocol to domain name. To browse the website or webpage, you have to type the URL in the address bar of the browser or click on the link of the web page. Given below are some URLs related to the field of education.

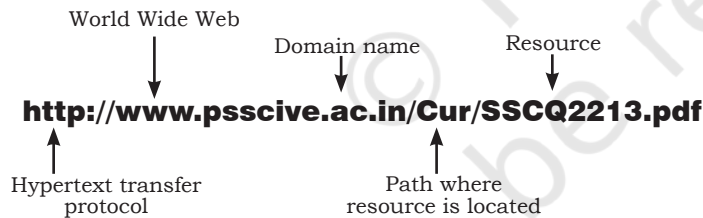


Fig. 4.29: Uniform Resource Locator

<https://www.mhrd.gov.in>

- Ministry of Human Resource Development

<https://www.nios.ac.in>

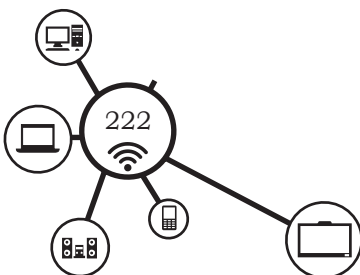
- National Institute of Open Schooling

<https://www.ignou.ac.in>

- Indira Gandhi National Open University

Consider the following example of URL.

<http://psscive.ac.in/Cur/SSCQ2213.pdf>



Web browser

A Web Browser is an application software used to access the World Wide Web. There are several web browsers developed by different companies. Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera are some of the popular web browsers. They may differ in look and feel, but does the same work of displaying web pages. Modern websites are designed to support most of these web browsers.

To work with most of the browsers, you need to be familiar with some basic concepts.

Address bar

All the browsers have an address bar where the user enters the web address or URL. For website of web page, type website address in the address bar and then press Enter key. The address bar is shown in Fig. 4.31.

Navigation buttons

These are buttons on the browser to go back or forward of the current web page. When you go on navigating the web pages, you can press the back button to go to the previous page. If you move to the previous page the forward button gets activated through which you can move forward.

When using the Back and Forward buttons, the browser may use its web cache to display the page. The web cache stores recently-viewed web pages so that they need not be downloaded again. It speeds up your web browsing, but sometimes you want to see the most up-to-date information on the page. In this situation you can use the Refresh or Reload button to load the page again.

Search bar

The browsers have a search bar for performing web searches. Many browsers have combined the address



Fig. 4.30: Web browsers

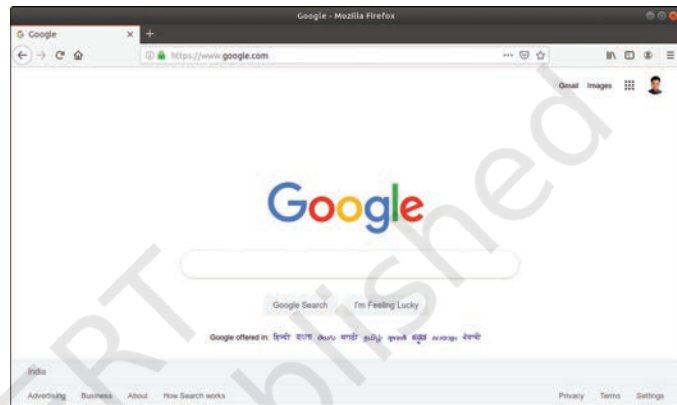
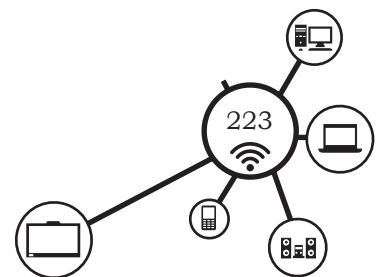


Fig. 4.31: Browser showing the address bar, search bar and navigation buttons



NOTES

bar and the search bar into a single bar to type web addresses or search terms.

Links

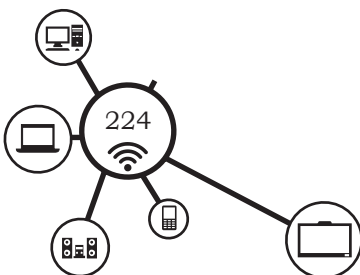
In websites you will find the links given to various pages or images. The text links appear in blue colour and are underlined. The link will open a web page in a new window. It may lead to another web page, document, video, or any other type of file.

Search Engines

Search engines are the websites used to search the information on the Internet. It is not always possible to know the website address of all the websites. Search engines make it possible to search the required information based on the search criteria. Search engines are designed for the Internet users to find any information easily. After typing the keywords in the search box of the search engine and clicking the search button, you will get a number of websites matching your requested information. You can obtain the necessary information by clicking one or several hyperlinks.



Fig. 4.32: Search engines



Some examples of search engines are as listed below.

- <https://www.google.com>
- <https://www.yahoo.com>
- <https://www.msn.com/>
- <https://www.ask.com/>

Domain Name

It is difficult to remember the IP address of every web server. A domain name is a human-friendly name for a device on the Internet. Domain name gives an identity to all the websites, which exist on the Internet. For example, the domain name <psscive.ac.in> has the IP address 164.100.60.91. Following are the names used to represent the fields, which the domains belong to.

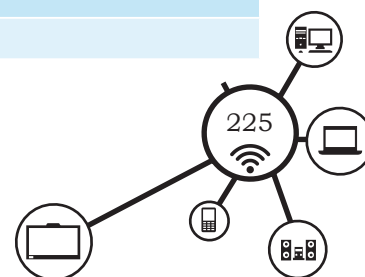
Domain	Meaning	Example
.com	Commercial (for-profit) websites	https://www.youtube.com
.org	Non profitable organisations	https://www.wikipedia.org
.gov	Government organisations	https://www.indianrail.gov.in
.edu	Educational institutions	https://www.educause.edu
.net	Network-related domains	https://www.media.net

The following country domains are used to represent the country related to the domain.

Domain	Meaning	Example
.in	India	https://www.mygov.in
.au	Australia	https://www.studyinaustralia.gov.au
.us	United States	https://weather.us
.uk	United Kingdom	https://www.gov.uk
.ca	Canada	https://www.cdw.ca
.nz	New Zealand	https://www.govt.nz

The last part of the domain name is called the top level domain.

URL	Domain	Top Level Domain
https://www.google.com	google.com	.com
https://www.mhrd.gov.in	Mhrd.gov.in	.in



https://researchgate.net	researchgate.net	.net
https://www.amazon.in	Amazon.in	.in
https://www.facebook.com	Facebook.com	.com
https://www.wikipedia.org	wikipedia.org	.org

Practical Activity 8

Browsing and searching on the Internet

Material required

Computer with Internet connectivity, writing material

Procedure

1. Identify the browser and start the browser on your computer.
2. Search the various types of browsers.
3. Identify and name the various parts of a browser.
4. Browse the various websites and identify the top level domain.
5. Browse the various search engines and search on the topic from the search box.
6. Search the websites that belong to India.
7. Identify the name of the country it belongs to from the URL of a website.

Application of Internet in Social Networking

The Internet can also be used to connect and interact with people around the world with the help of social networking sites. It is about connecting with friends, family and people you have never met before. There are many different ways to communicate online, including social networking, chat, VoIP and blogging. Social networking has become one of the main ways people keep in touch. Some of the most popular social networking sites are Facebook, Twitter, LinkedIn, etc.

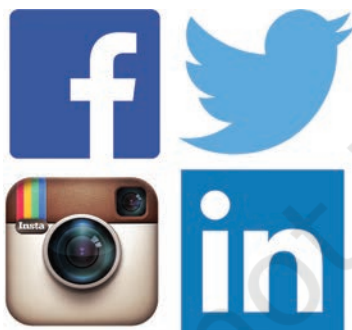
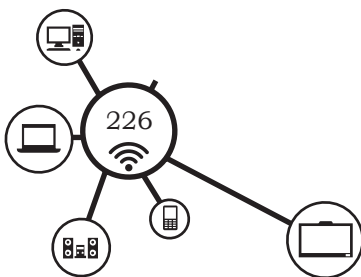


Fig. 4.33: Social networking

- Facebook is used by around one billion people around the world to interact with your family or friends that live far away. You can also share your photos and videos on Facebook to be viewed by public or your close friends.



- Twitter allows you to share brief messages called 'tweets' with the entire world, or with just your circle of friends. By following people with similar interests, you can discover new things that you would not have found otherwise.
- LinkedIn is a site that you can use for business networking. It allows you to connect with other people in your field and find out about new job opportunities.

Electronic Mail

Electronic mail or e-mail enables exchanging messages as electronic mails or files between two or more people.

e-mail is a way to send and receive messages across the Internet. There are several organisations, which provide e-mail service free of charge through the Internet. Hence, the cost is only for the use of the Internet. This is the cheapest and fastest communication method in the world. Any person in the world can create an electronic mail account with the help of Internet and this can also be used to find this person on the Internet. e-mail messages received are stored in the mailbox.

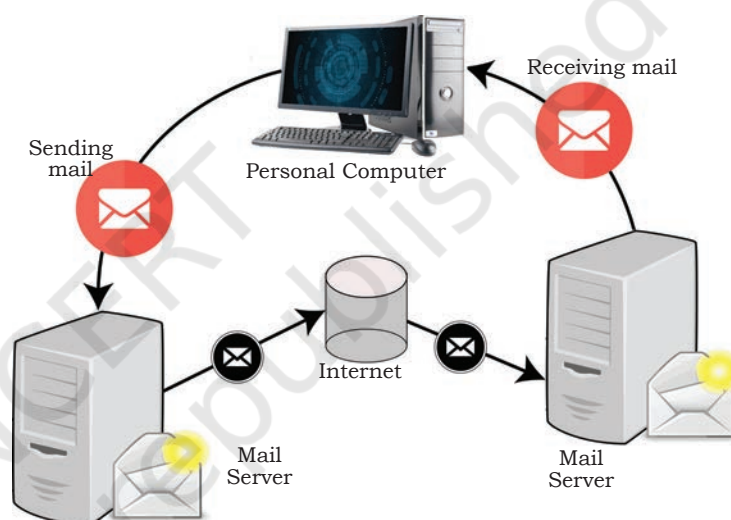


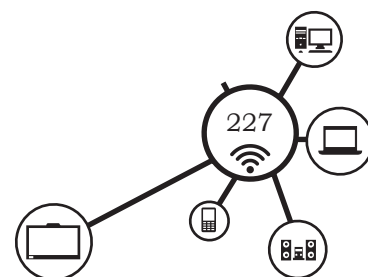
Fig. 4.34: Exchange of e-mails on the Internet

e-mail address

You must have an e-mail address to use e-mail. e-mail addresses can be web based or hosted internally like Outlook Express. Anyone of you can create an e-mail account through websites of e-mail providers such as Gmail, Yahoo, Hotmail, Rediffmail, etc. An electronic mail address consists of user name, @ sign and domain name. For example, dds@yahoo.com, xyz@hotmail.com, abc@gmail.com and ab.cd@rediffmail.com

e-mail etiquettes

When using e-mail there are several rules that you should follow.



NOTES

These are as follow:

- Avoid typing the complete message in capital letters. This is referred as shouting.
- Always include the subject in the subject line. It gives an information about the content.
- Do not use a very small or very much large font size, coloured text and background in the message body.
- When sending a message to a number of users at the same time use Bcc-rather than Cc, as it helps in protecting their e-mail addresses being passed on.
- Do not open and or forward junk mail and chain letters.
- Do not give out any personal information, such as phone numbers, passwords, bank account details in emails.
- Keep e-mail communications private. It is illegal to post the content of a private e-mail in a public domain.
- Send the e-mail attachments in compress (zip) form. This allows to send larger documents quickly and consumes less space in inbox.

Creating an e-mail Account

It is essential for the sender as well the receiver to have e-mail accounts. You can create your e-mail account under any domain you like. There are various websites, such as yahoo, google offering free e-mail services. The following activity will illustrate how to create an e-mail account in Gmail.

Practical Activity 9

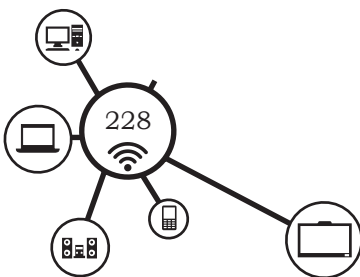
Creating an e-mail account in Gmail

Material required

Computer with Internet connectivity

Procedure

1. Open up the Internet browser and type the address as www.gmail.com in the address bar. The Gmail creation web page will open as shown in Figure a.



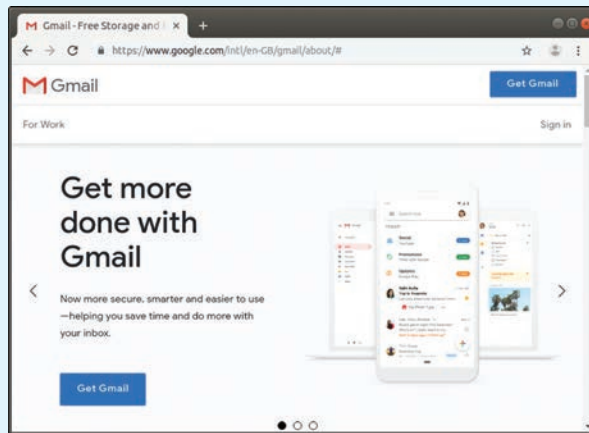
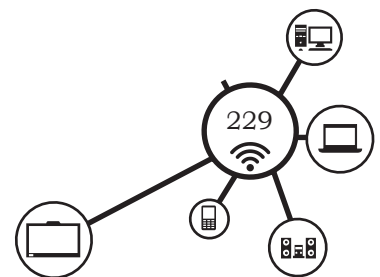


Fig. a

2. Observe that there is an option 'Get Gmail' located in the upper right and lower left corner of the web page. Click on any one option to proceed with the creation of e-mail account.
3. Then click on the 'Sign up' option.
4. Then click on the 'Create account' and select the option 'For myself' to create your personal e-mail account as shown in Fig. b.

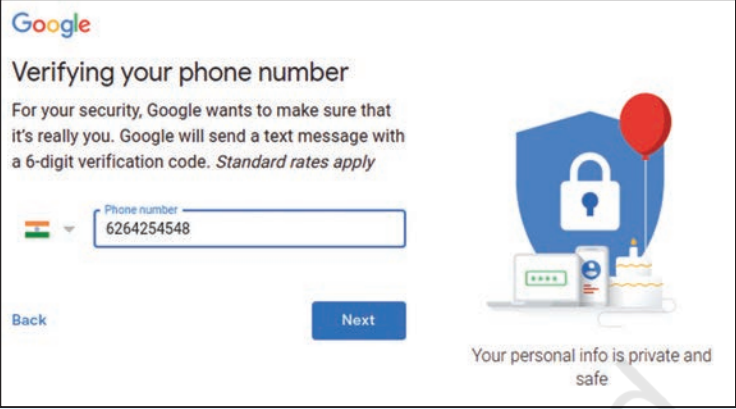
Fig. b

5. Fill the requested details—Firstname, Lastname, Username and Password. Then click on the Next button.
6. If the username provided is already used by others then the e-mail will not be created with this name. You can select any of the suggested usernames or provide other username of your choice. For example, in our case since the username 'falgun' is already used we have use another user name 'mailtofalgun' instead of picking the suggested one. Then click on Next button.



NOTES

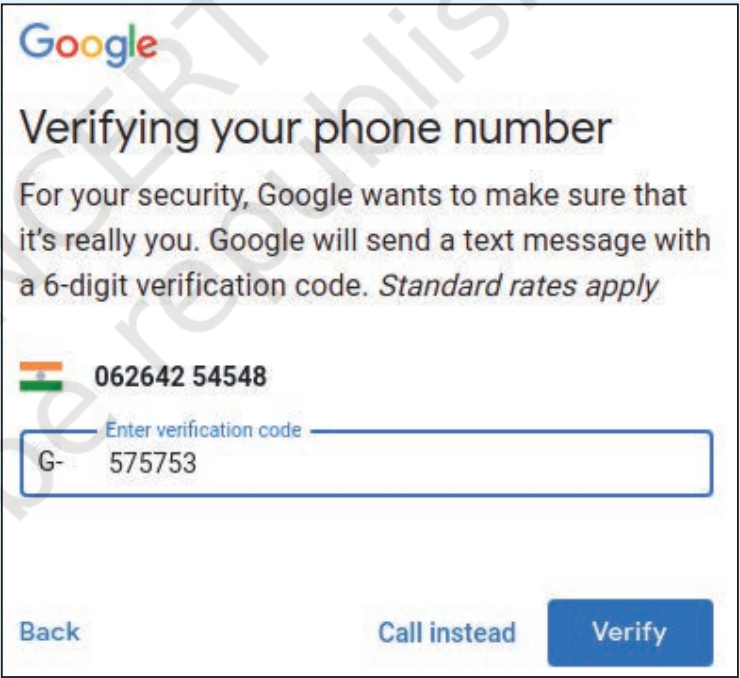
7. Then you need to provide your phone number to verify yourself. Provide the phone number as shown in Fig. c, and click on Next button.



The screenshot shows the Google interface for verifying a phone number. At the top is the Google logo. Below it, the heading reads "Verifying your phone number". A message states: "For your security, Google wants to make sure that it's really you. Google will send a text message with a 6-digit verification code. *Standard rates apply*". On the right, there is an illustration of a shield with a padlock, a red balloon, a laptop, and a birthday cake. Below the message, there is a dropdown menu for the country (India) and a text input field containing the phone number "6264254548". At the bottom left is a "Back" link, and at the bottom right is a blue "Next" button. A footer message says "Your personal info is private and safe".

Fig. c

8. A 6-digit verification code will come as a message on your mobile. Enter the verification code as shown in Fig. d below and click on Verify button to verify yourself.



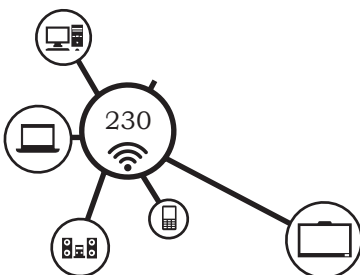
The screenshot shows the second step of Google's phone verification. It features the Google logo and the heading "Verifying your phone number". The same security message is present. Below, the country is set to India and the phone number "062642 54548" is displayed. A text input field is labeled "Enter verification code" and contains "G- 575753". At the bottom, there are three buttons: "Back", "Call instead", and a blue "Verify" button.

Fig. d

9. Your e-mail id will be created.

Sending an e-mail

A message can be sent through e-mail just like a postal mail. To send e-mail, the sender and receiver must have an e-mail address and Internet connectivity. So if



you have an e-mail address and want to send e-mail to others who are also having e-mail address, the following activity will illustrate the sending and receiving of e-mail.

NOTES

Practical Activity 10

Sending e-mail message

Material required

Computer with Internet connectivity, e-mail address of sender and receiver

Procedure

1. Open your e-mail account by providing the correct e-mail ID and password.
2. Click on Compose Message to create a new e-mail message.
3. This opens the New Message window as shown in figure a. A message window will open, which will allow you to enter the e-mail ID of the recipient.
4. Enter the receiver's e-mail address in To (sales@wyse.co.in) as shown in Fig. a.

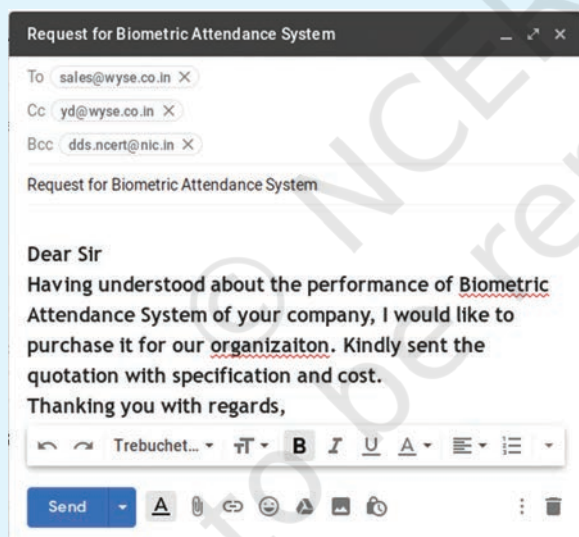
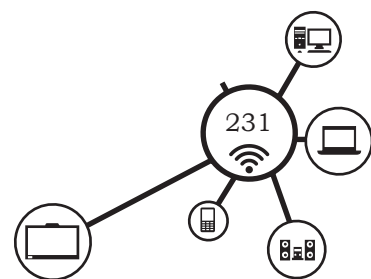


Fig. a

5. Make sure that the e-mail address is typed carefully and accurately with correct spelling and punctuation. One typing error will mean that the message will not be sent to the correct person.
6. If you wish to send a copy of the message to another person, add their names to the Cc: box. Type the e-mail address of others (yd@wyse.co.in) who should receive the copies of the e-mail in Cc (Carbon copy)



7. You can also copy and send the message to another person using Bcc (Blind Carbon Copy). Type the e-mail addresses of those who should receive the mail without the awareness of those receivers typed under To and Cc in Bcc (Blind carbon copy). Those who receive Bcc copies can view all the receivers of the mail. However, the receivers typed under To and Cc cannot view the receivers of Bcc copies (dds.ncert@nic.in). This prevents the Bcc e-mail addresses from being passed on to other people.
8. The person who receives Bcc copy (dds.ncert@nic.in), can see all the e-mail addresses (sales@wyse.co.in) and (yd@wyse.co.in) that this letter is sent to. Persons under To and Cc i.e., (yd@wyse.co.in) and (sales@wyse.co.in) cannot see the e mail address of Bcc.
9. Type the title or relevant subject related to the mail in Subject. The subject line of a message helps to know about the message. This allows them to read the most urgent messages first.
10. Enter the content of the message into the main box. Use a greeting at the start of the message and a salutation at the end.
11. Attach the other file or files which should be sent with the e-mail by clicking the attachment button with the paper clip icon. (Letter.pdf)
12. Send the e-mail by clicking 'Send' button. The e-mail will then be sent to the mailbox of each account in the To:, Cc: and Bcc: boxes.

Receiving and Replying to an e-mail

The e-mails sent by others to you are received in the Inbox of your e-mail account. The e-mails are categorised inside an e-mail account for easy use. There are other mailboxes also for other purpose as explained below and shown in Fig. 4.35.

Inbox – to store mails received

Drafts – to store mails that are composed to be sent but could not be completed

Sent – to store mails sent

Trash/Deleted – to store mails for a certain period that are deleted

Spam/Junk – to store mails that are unwanted

Unwanted emails stored in a separate folder without disturbing the Inbox are known as spam.

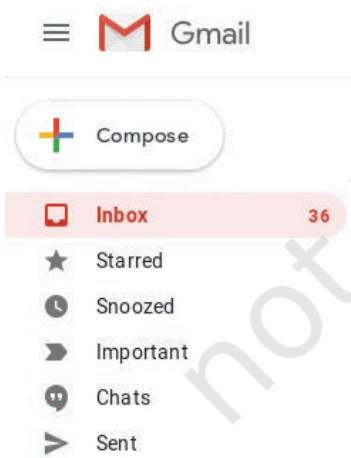
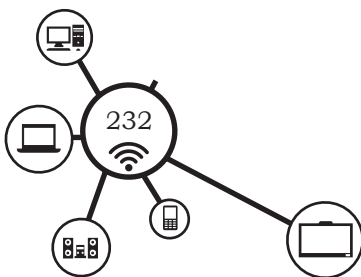


Fig. 4.35: Mailbox



Practical Exercise

Receiving and replying to an e-mail

Material required

Computer with Internet connectivity

Procedure

1. Click on the Inbox for your e-mail account.
2. The new e-mails received will appear in bold.
3. Clicking on the message will open it in a message window.
4. To reply to a message from the original sender click on Reply.
5. To reply to all address placed in the To: box and Cc: box, click on Reply all.
6. To send the message to another person without adding the contents use Forward as shown in Fig. a.

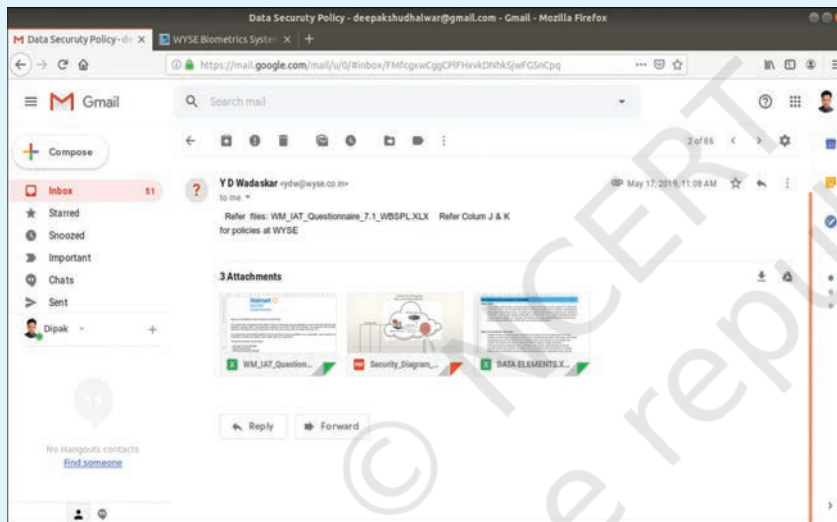
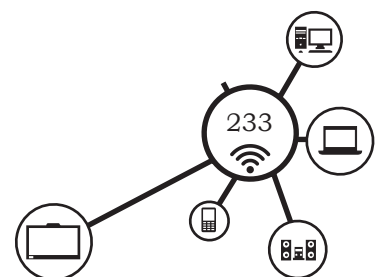


Fig. a

Check Your Progress

A. Fill in the blanks

1. The _____ is the largest network in the world.
2. Internet is run by a non-profitable organisation called _____.
3. Every website address starts with _____.
4. WWW stands for _____.
5. URL means _____.

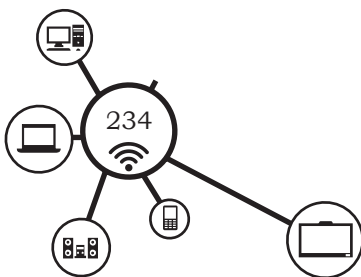


NOTES

- The domain name .gov indicates that it is a _____ website.
- Every computer connected to the Internet is identified by its _____ address.
- IP address contains _____ numbers.
- ISP stands for _____.
- IP addresses are stored in _____.
- Testing of the network can be performed by using _____ command.
- Domain name gives _____ to all the websites on the Internet.
- Commercial websites are indicated by _____ in the domain name.

B. Multiple choice questions

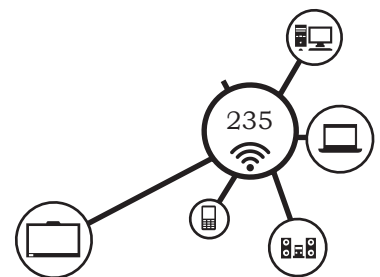
- Normally all Indian websites are indicated by _____ in the domain name.
(a) .au (b) .us
(c) .in (d) .uk
- Which of these is a protocol used in the Internet?
(a) TCP/IP (b) HTTP
(c) FTP (d) All of these
- FTP stands for _____.
(a) File transfer protocol (b) File transfer practice
(c) File to punch (d) Former transfer protocol
- The main usage of FTP protocol is _____.
(a) electronic mail exchange
(b) file exchange
(c) informing and controlling messages
(d) HTML document exchange
- The main usage of HTTP protocol is _____.
(a) controlling IP addresses
(b) file exchange
(c) electronic mail exchange
(d) HTML document exchange
- The main usage of TCP/IP protocol is _____.
(a) controlling the exchange of IP addresses
(b) file exchange
(c) electronic mail exchange
(d) HTML document exchange
- Electronic mail exchange can be achieved by using _____ protocol.
(a) FTP (b) SMTP
(c) HTTP (d) TCP/IP



8. SMTP stands for _____.
 - (a) Simple mail transfer protocol
 - (b) Simple mail transfer process
 - (c) Super mail transfer protocol
 - (d) Super mail to process
9. Error messages are informed and controlled by using _____ protocol.
 - (a) FTP
 - (b) SMTP
 - (c) ICMP
 - (d) TCP/IP
10. The computer that distributes the resources is called _____.
 - (a) Client
 - (b) Server
 - (c) Down-loader
 - (d) Up-loader
11. The process of retrieving information from the server computer to the client computer is _____.
 - (a) uploading
 - (b) downloading
 - (c) managing
 - (d) printing
12. The process of providing information from the client computer to the server computer is _____.
 - (a) uploading
 - (b) downloading
 - (c) managing
 - (d) printing
13. DNS server is used _____.
 - (a) to manage printing services
 - (b) to manage electronic mails
 - (c) for storing of webpages
 - (d) for translating URL to IP addresses

C. State whether the following statements are True or False

1. Web server is used for storing of web pages and providing these to the client computers.
2. DNS server is used to manage electronic mails.
3. FTP means file transfer practice.
4. Mozilla Firefox is a web browser.
5. Sir Tim Berners Lee is considered as the father of world wide web.
6. Safari is a text editing software.
7. Computers connected to the Internet cannot be controlled remotely.
8. Using remote access functionality, sometimes hackers can steal important data without the owner's knowledge.
9. Checking of examination result online is an example of file sharing.
10. Any information on the Internet cannot be found using search engine.
11. Google is an example of search engine.
12. Unique identity of a website cannot be reflected by its domain name.



NOTES

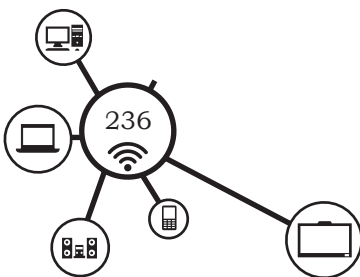
13. By using electronic mail we can exchange our messages or files to two or more people.
14. Cost of the use of Internet is very high.
15. E-mail can be sent from one country to any other country in the world.

D. Short answer questions

1. What is electronic mail? State its advantages.
2. Give the steps for sending and receiving e-mail.
3. What do you mean by search engine? Give the steps for obtaining useful information using search engine.
4. Explain the role of DNS server.
5. What is FTP? How is FTP used for sharing of files?
6. Illustrate the concept of remote access in Internet.
7. What is a web browser? State any four commonly used web browsers.
8. What is a website? Give examples.
9. Explain the role of the following servers—
(i) web server (ii) mail server (iii) print server (iv) DNS server
10. What do you mean by uploading and downloading on Internet?
11. Explain how Internet works.
12. What is domain name? Explain the different domain name extensions and their meaning.
13. Give the steps for connecting biometric attendance system to the Internet.
14. Give the steps to check your computer's IP address.

SESSION 3: STANDARDS OF BIOMETRIC DATA

In recent years, biometric recognition has become essential for personal identity. It becomes necessary to develop biometric standards to ensure reliability, security, interoperability, usability and scalability. In the current age we are using various national and international biometric-based identity documents, including electronic passports, ID cards and visas, which leads to develop international standards. Government authorities are not likely to accept proprietary or non-standardised documents. With the availability



of international standards, it is possible to use the biometric system in a wide range of applications.

Need and Importance of Developing Biometric Standards

Biometrics are used for national security purposes since September 11, 2001. National Institute of Standards and Technology (NIST) has proposed to form an international standards body to increase the deployment biometrics standards for a variety of applications.

Biometric technologies are supposed to be highly secure identification and personal verification solutions. A comprehensive standards is necessary to ensure the systems and applications are interoperable, scalable, usable, reliable and secure. The development of industry standards make the biometric technology easier and more reliable to deploy and maintain. It ensures uniformity of certain processes to enable communication and data exchange between systems. The American National Standards Institute (ANSI) approves the creation of all national and international standards.

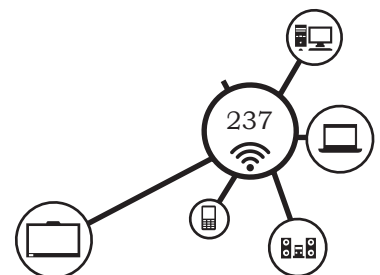
Biometric Standards Developing Organisations

At the international level, ISO/IEC Joint Technical Committee 1 (JTC 1)/Subcommittee 37 (SC 37) was established in June 2002 for international biometric standards by INCITS M1 (International Committee for Information Technology Standards), M1 technical committee on biometrics. This body coordinates the development of biometric standards.

International Telecommunication Union (ITU-T) and the International Civil Aviation Organization (ICAO) are the other international standard bodies. Specific work is also being carried out by specialised international groups including OASIS and the Open Group.

There are several national and international bodies working in the development of biometric standards. To simplify the analysis, the standards developing groups are classified into three broad categories:

- 1. Government appointed Standards Development organisations (SDO):** are ISO/IEC, ITU-T, CEN, ANSI. They try to develop standards in accordance



NOTES

with their respective government appointed mandates to achieve the overall economic benefit that results from standardisation or to fulfill specific legislative mandates.

2. Industry consortia: including BioAPI Consortium, Biometric Consortium and OASIS develop standards that support the objectives of their membership, intended to aligns and complement with the overall goal of enhancing standardisation.

3. Other organisations: such as ICAO and ILO develop very specific standards related to particular applications within their domain.

The several international standards organisations are mandated to work on IT standards are listed below.

International Organisation for Standardisation (ISO)

ISO is the world's largest developer of standards. It is composed of government or industry representatives from the national standards bodies of 148 countries.

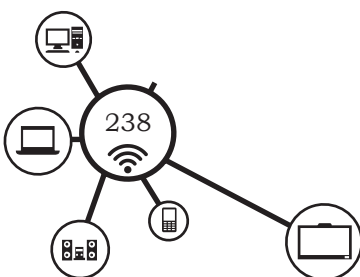
International Electrotechnical Commission (IEC)

The IEC was one of the first international standard bodies founded in 1906, mandated to prepare and publish international standards for all electrical, electronic and related technologies.

ISO/IEC Joint Technical Committee 1 (JTC 1)

In 1987, (ISO) and IEC formed the Joint Technical Committee 1 (JTC 1) on Information Technology (IT) to develop and promote IT standardisation and thereby meet the global demands of businesses and users. The ISO/IEC JTC 1 created a series of SubCommittees (SCs).

- SC 17 is focussed on the application of biometrics to smart cards and travel documents.
- SC 27 is focussed on security issues surrounding biometrics and the evaluation of the security implications of biometrics.



- SC 37 has the primary responsibility for international biometrics standards.

SC 37 has several subordinate Work Groups (WGs) that address different aspects of biometric standards development. These include:

WG 1 – Standards for Biometric Vocabulary

WG 2 – Standards for Technical interfaces

WG 3 – Standards for Data Exchange Formats

WG 4 – Standards for Biometric Profiles

WG 5 – Standards for Performance Testing and Reporting

WG 6 – Standards for Cross jurisdictional and Societal Aspects

INCITS (International Committee for Information Technology Standards)

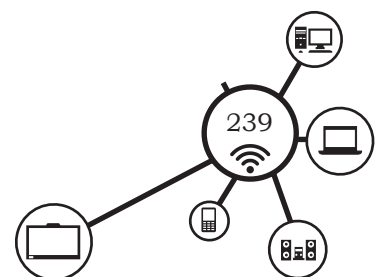
INCITS is the US standardisation body in the field of information and communications technologies. It includes the storage, organisation, processing, display, management and retrieval of information. INCITS has a number of Technical Committees (TCs) that lead standards development efforts in various areas. The Technical Committee that focusses on the development of biometric standards is known as M1.

INCITS Technical Committee M1 Biometrics

INCITS M1 is the US Technical Advisory Group (TAG) to ISO/IEC JTC 1 SC 37 – Biometrics. M1 was established to ensure a high priority, focussed and comprehensive approach for the rapid development and approval of national and international standards for biometric data interchange and interoperability.

OASIS (Organization for the Advancement of Structured Information Standards)

OASIS is a non-profit, international consortium that produces a large number of web standards in supporting areas for e-business, such as security and biometrics. The OASIS XML Common Biometric Format (XCBF) is a common set of secure XML encoding provides security to biometric data.



The Open Group

The Open Group is an international consortium has been involved in biometric standardisation through its Security Forum, which participated in the development of the BioAPI, and encourages the development of secure methods of personal authentication.

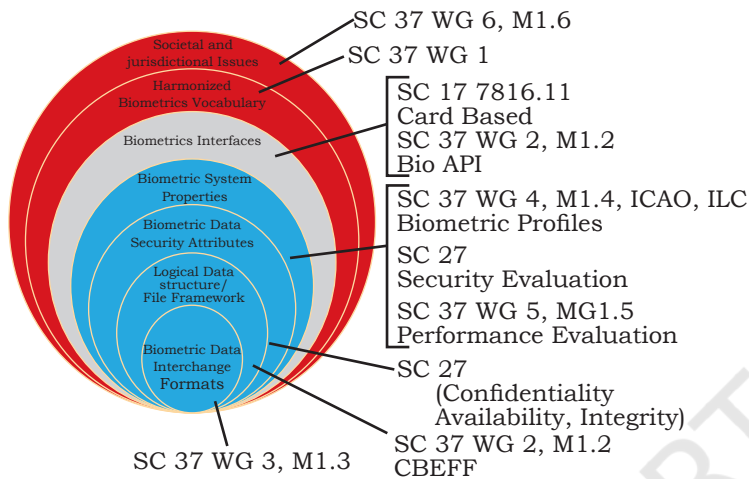


Fig. 4.36: Structure of Biometric Standards

Structure of Biometric Standards

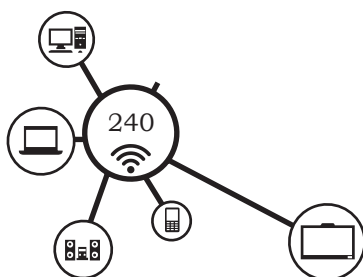
In order to understand how the different types of biometric standards fit together, it is useful to know the overall structure of biometric standards. The structure shown in Fig. 4.36 is commonly called 'Onion Diagram'.

Fig. 4.36 shows the biometric standards as a series of layers, starting with the heart of the onion and the inner three layers,

all in blue. These standards are of direct relevance to biometric system developers and users. The next layer (gray), deals with the interfaces which link the biometric components to the rest of the application. Then there are the outer two layers (orange) which define how to deal with biometrics in terms of privacy, legal issues and even the language used to describe them. Finally, there are the thin shells that separate and surround each layer. These layers represent the conformance standards, which describe exactly how adherence to each of the other standards can be measured.

Biometric Data Interchange Formats

At the inner core, the biometric data interchange format standards define the basic format of biometric images or templates. The biometric modality such as face, finger, iris, vein, and hand needs at least one of these standards to allow interoperability of data produced by different systems using that modality. In



ISO/IEC JTC 1 SC 37, the data interchange format standards being developed for finger image and for three types of processed biometric samples — finger minutiae, finger pattern spectral and finger pattern skeletal. This reflects the maturity of the fingerprint market with multiple technologies available to process the raw biometric data.

Logical data structure

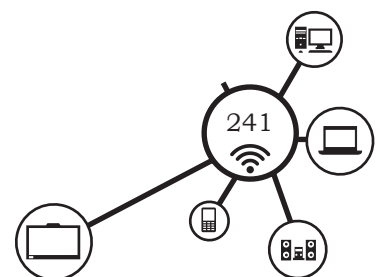
The logical data structure or exchange format framework is used to wrap the biometric data so that systems receiving a file know how to interpret the different data fields that might be associated with the biometric data. These could include demographic information or a digital signature to verify the data packet has not been tampered with. CBEFF (Common Biometric Exchange File Format) is currently the most important standard in this layer.

Data security

It is necessary to protect the standard biometric data. There are numerous encryption schemes that can be used apart from digital signatures and secure transmission protocol HTTPS.

System properties

The next layer involves the properties of the biometric system, such as performance, security and specification. The performance of the biometric system can be judged by the ability to enroll a sufficient percentage of the target population and its ability to correctly match biometric samples. One of the key purposes of biometric standards is to allow interoperability among components and systems involving biometrics. Security is one of the important aspect of any biometric system. It permits methodologies to be developed by which biometric systems can be evaluated so that their security level is well established. The next property of biometric system is the specification required for a particular application domain. There is a need to develop the number of biometric applications as per the growth of



NOTES

biometrics market.

Interfaces

Biometric interfaces is the next layer of the onion (gray). These are interfaces between the core biometric systems, represented by the inner four layers of the onion and the outside world. BioAPI is the foremost among them.

Vocabulary

The final two layers of the onion (orange) represent the outside world. A biometric vocabulary is used to interact in a biometric group to avoid miscommunication. The industry practice has accepted particular usages of certain terms.

Societal and cross-jurisdictional issues

Societal and cross-jurisdictional issues involve the impact of biometrics on privacy, health and safety. It is a challenging task to develop international standards for measuring or managing these issues.

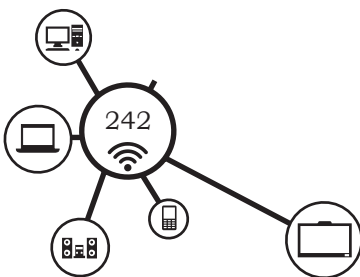
Character Encoding Schemes

Biometric data captured by the biometric devices is processed further for comparison. The data is stored and processed by the computing machine. As we know that the data is stored and processed in computer in machine code consisting of 0s (zeros) and 1s (ones). The computer can express any numerical value as its binary translation, which is a simple mathematical operation.

A set of standards was developed. There are two major translation codes that are used to represent the characters, such as numbers, letters and special characters and symbols like \$, %, and many mathematical characters. These standards are — ASCII and EBCDIC.

ASCII (American Standard Code for Information Interchange)

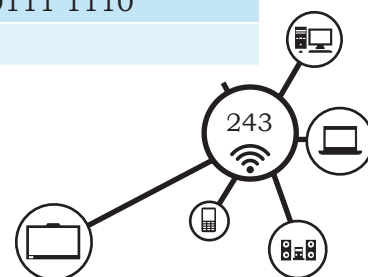
It is the coding system traditionally used with personal computers. ASCII is a 7-digit (7-bit) code, although there are several different 8-bit extended versions of ASCII that contain additional symbols not included in



the 7-bit ASCII code. Table 4.1 shows the ASCII Code.

Table 4.1: ASCII code

Character	Decimal Number	Binary Number	Character	Decimal Number	Binary Number
Blank space	32	0010 0000	^	94	0101 1110
!	33	0010 0001	-	95	0101 1111
'	34	0010 0010	'	96	0110 0000
#	35	0010 0011	a	97	0110 0001
\$	36	0010 0100	b	98	0110 0010
A	65	0100 0001	c	99	0110 0011
B	66	0100 0010	d	100	0110 0100
C	67	0100 0011	e	101	0110 0101
D	68	0100 0100	f	102	0110 0110
E	69	0100 0101	g	103	0110 0111
F	70	0100 0110	h	104	0110 1000
G	71	0100 0111	i	105	0110 1001
H	72	0100 1000	j	106	0110 1010
I	73	0100 1001	k	107	0110 1011
J	74	0100 1010	l	108	0110 1100
K	75	0100 1011	m	109	0110 1101
L	76	0100 1100	n	110	0110 1110
M	77	0100 1101	o	111	0110 1111
N	78	0100 1110	p	112	0111 0000
O	79	0100 1111	q	113	0111 0001
P	80	0101 0000	r	114	0111 0010
Q	81	0101 0001	s	115	0111 0011
R	82	0101 0010	t	116	0111 0100
S	83	0101 0011	u	117	0111 0101
T	84	0101 0100	v	118	0111 0110
U	85	0101 0101	w	119	0111 0111
V	86	0101 0110	x	120	0111 1000
W	87	0101 0111	y	121	0111 1001
X	88	0101 1000	{	122	0111 1010
Y	89	0101 1001		123	0111 1011
Z	90	0101 1010	}	124	0111 1100
[91	0101 1011	~	125	0111 1101
/	92	0101 1100		126	0111 1110
]	93	0101 1101			

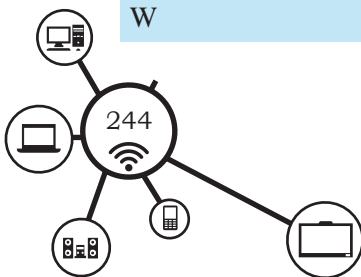


EBCDIC (Extended Binary-Coded Decimal Interchange Code)

EBCDIC was developed by IBM, primarily for use with mainframes. EBCDIC represents each character as a unique combination of 8 bits. One group of 8 bits (1 byte) allows 256 (28) unique combinations. The 8-bit code can represent up to 256 characters. It is enough to include the characters used in English alphabet, some non-English characters, 10 decimal digits, other characters usually found on a keyboard, and many special characters.

Table 4.2: EBCDIC Code

Character	EBCDIC Code	Character	EBCDIC Code
A	1100 0001	a	1000 0001
B	1100 0010	b	1000 0010
C	1100 0011	c	1000 0011
D	1100 0100	d	1000 0100
E	1100 0101	e	1000 0101
F	1100 0110	f	1000 0110
G	1100 0111	g	1000 0111
H	1100 1001	h	1000 1000
I	1100 1010	i	1000 1001
J	1101 0001	j	1001 0001
K	1101 0010	k	1001 0010
L	1101 0011	l	1001 0011
M	1101 0100	m	1001 0100
N	1101 0101	n	1001 0101
O	1101 0110	o	1001 0110
P	1100 0111	p	1001 0111
Q	1100 1000	q	1001 1000
R	1100 1001	r	1001 1001
S	1100 0010	s	1010 0010
T	1100 0011	t	1010 0011
U	1100 0100	u	1010 0100
V	1100 0101	v	1010 0101
W	1100 0110	w	1010 0110



X	1100 0111	x	1010 0111
Y	1100 1000	y	1010 1000
Z	1100 1001	z	1010 1001
0	1111 0000	5	1111 0101
1	1111 0001	6	1111 0110
2	1111 0010	7	1111 0111
3	1111 0011	8	1111 1000
4	1111 0100	9	1111 1001

Unicode

Unlike ASCII and EBCDIC, which are limited to only the Latin alphabet used with the English language, Unicode is a universal international coding standard designed to represent text-based data written in any ancient or modern language. Unicode uniquely identifies each character using 0s and 1s, no matter which language, program, or computer platform is being used. Unicode is quickly replacing ASCII as the primary text-coding system. In fact, Unicode includes the ASCII character set so ASCII data can be converted easily to Unicode when needed. Unicode is used by most web browsers and is widely used for web pages and web applications. Google data, for instance, is stored exclusively in Unicode.

Practical Activity 11

Use ASCII code to write words

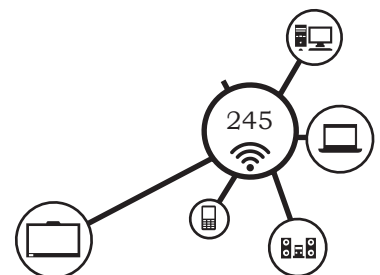
Material required

Pen, paper

Procedure

1. Find the ASCII code for each letter in the word 'Data'.
2. Write the binary code of each letter as shown in the table below.

Letter	Binary representation of the letter							
D	0	1	0	0	0	1	0	0
a	0	1	1	0	0	0	0	1
t	0	1	1	1	0	1	0	0
a	0	1	1	0	0	0	0	1



NOTES

- Use ASCII code to write your first name or nickname in binary numbers beginning with an uppercase letter and continuing with lowercase letters. Put the letters of your name in the first column.
- On a separate sheet of paper, write a short message in ASCII. Exchange messages with a partner and decode each other's message.

Letter	Binary representation of the letter							
D								
i								
p								
a								
k								

- Use the EBCDIC code to write your last name in binary numbers beginning with an uppercase letter and continuing with lowercase letters. Put the letters of your last name in the first column.

National Standards of Biometric Data

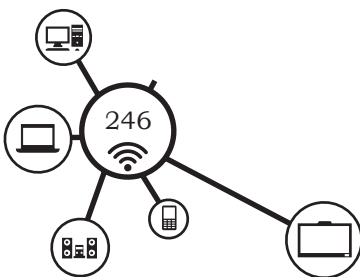
Biometric standards are developed to ensure interoperability of biometric devices and algorithms so as to avoid vendor lock-in and also ensure long-term storage of data with technology independence. The defined biometric standards are applicable to all e-Governance applications in India as per the government's policy on open standards.

Tailoring of fingerprint image standard

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-4 Fingerprint Image Data Standard as Indian Standard and specify certain implementation values (tailoring).

Image acquisition requirements

The duplicate check during the enrolment phase will use 1:N matching. 1:N matching for large gallery size and high enrolment rate will require substantial computing resources. The matching time and matching accuracy is directly related to the quality of the images. Therefore, it is essential that the highest quality of images be consistently captured. It is also required that all 10 fingers are captured whenever physically possible. The



goal during authentication is to achieve fast overall response while permitting a wide variety of capture devices and associated software. It is sufficient to capture only one or two fingers for reliable 1:1 authentication. The image quality needed for authentication is not as stringent as in enrolment.

For enrolment setting level 31 or higher as shown in Table 4.3.

Table 4.3

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
31	197	500	8	200	EFTS/F

For authentication setting level 28 or higher as shown in Table 4.4.

Table 4.4

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
281	118	300	4	12	UID (Unique Identification)
30	197	500	8	80	None

Finger Image Record Format

Enrollment Code 0 and 1 are strongly recommended. For legacy purposes only, lossless compression of code 2, 4 and 5 will be accepted.

Authentication Code 4, compressed — JPEG 2000 is recommended. Code 0, 1, 2 and 5 are also acceptable. Code 3 must not be used. Maximum compression ratio is 15.

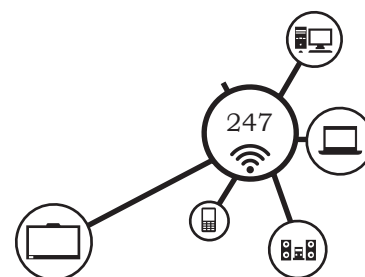
Iris Image Specifications

Iris image type

The interchange format type of the Iris images that is defined in this standard is for rectilinear images only.

If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required.

Cameras that capture images of both eyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.



NOTES

Pre-processing to calculate rotation angle before compression, the Iris image will have to be pre-processed to calculate rotation angle.

Rectilinear Image Rotation Uncertainty

Number of eyes

For Enrollment – Two eyes

- For Verification/Authentication: One/two eyes depending upon the sensitivity of application

Iris diameter

As per ISO 19794-6:2005(E) only medium and higher quality images are acceptable. Hence for this standard, minimum acceptable Iris diameters will be 150 pixels.

Image Margin Segmentation

25% top and bottom of Iris diameter
50% left and right of Iris diameter

Colour and pixel depth

The iris images shall be captured and stored in grayscale with pixel depth 8bits/pixel.

Illumination

The eye should be illuminated using near-infrared light with wavelength between 700 and 900 nanometres (nm) approximately.

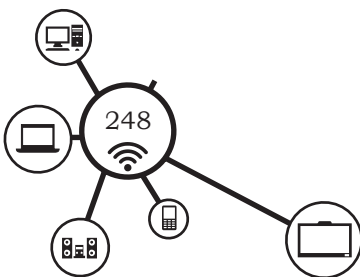
Image acquisition format

Lossless format (Raw/PNG/Lossless JPEG 2000)

Storage specifications

Since there is no standard template available to store extracted Iris image data features, original Iris images would be stored in specified format from which features can be extracted and used for matching.

The data format specifications for storage or archival should adhere to the Policy on Open Standards to ensure interoperability, long-term availability, vendor independence and optimal utilisation of storage space, without affecting the quality of image.



Format for storage or archival

Iris image storage and archival shall be done in PNG format.

Note: One additional value for bytes 22–23 to be used for Image format in Iris Record Header (refer table 2 of ISO/ IEC 19794-6:2005(E)) to incorporate PNG format with respect to this standard, which is as follows:

IMAGE_FORMAT_MONO_PNG=18 (0X0012)

Practical Exercise

List the organisations using biometric data

Material required

Pen, paper

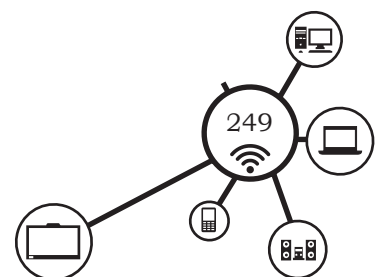
Procedure

1. Visit the organisations, such as Passport office, RTI office, colleges, private and government organisations which are using biometric attendance system for taking attendance of employees.
2. Prepare the list of such organisations.

Check Your Progress

A. Fill in the blanks

1. ASCII stands for American Standard Code for _____.
2. ASCII is a _____ bit code.
3. The extended version of ASCII is _____ bit code.
4. ASCII code is used for binary representation of letters and _____.
5. ASCII code is also called _____ code.
6. The ASCII code for the character A is _____.
7. EBCDIC code means _____.
8. EBCDIC code can represent _____ characters.
9. By using EBCDIC code _____ can be represented in binary form.
10. In ASCII code _____ characters can be represented in binary form.
11. Unicode means _____ code.
12. All characters in Indian languages, such as Hindi, Marathi and Tamil can be represented in binary form by using _____.

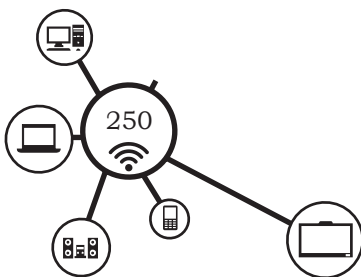


NOTES

13. IEC stands for _____.
14. The industry consortia includes _____ Consortium, _____ Biometric Consortium and _____.

B. Multiple choice questions

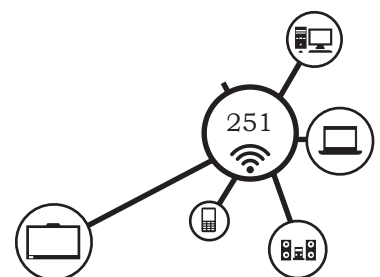
1. The ASCII code for the character D is _____.
- (a) 0100 0100 (b) 0100 0101
(c) 0100 0110 (d) 0100 1100
2. National standards of biometric data are developed as per _____.
- (a) Government policy
(b) Government policy on open standards
(c) private sector policy
(d) standard organisations
3. UIDAI means _____.
- (a) Unique Identification Authority of India
(b) Universal Identification Authority of India
(c) Unique Identification Authority of Internet
(d) Unique Isolated Authority of India
4. The fingerprint image standard adopted in India is _____.
- (a) ISO/IEC (b) ISO/IEC 19794
(c) ISO/IEC 19794-4 (d) None of these
5. In image acquisition the scan resolution standard is _____ dpi.
- (a) 100 (b) 200
(c) 400 (d) 500
6. In image acquisition the number of bits to be used per pixel is _____.
- (a) 2 (b) 4
(c) 8 (d) 16
7. In fingerprint image the format compressed _____ is recommended.
- (a) jpeg 2000 (b) png 2000
(c) xml 2000 (d) wav 2000
8. In iris images, the iris diameter should be _____ pixels.
- (a) 100 (b) 150
(c) 200 (d) 250
9. In iris images, the iris margin segmentation must be _____ % left and right of the iris diameter
- (a) 30% (b) 50%
(c) 60% (d) 80%



10. Iris images shall be captured and stored in grayscale with pixel depth _____ bits per pixel.
 - (a) 2
 - (b) 4
 - (c) 6
 - (d) 8
11. The eye image should be eliminated by using light having a wavelength between _____ and _____ nanometers.
 - (a) 500, 700
 - (b) 700, 900
 - (c) 900, 1100
 - (d) 1100, 1300
12. CBEFF stands for _____.
 - (a) Common Biometric Exchange Formula Framework
 - (b) Common Biometric Electronic Form Format
 - (c) Common Biometric Exchange Format Framework
 - (d) Common Based Electronic Format Framework
13. INCITS stands for _____.
 - (a) International Council for Information Technology Standards
 - (b) International Committee for Information Technology Standards
 - (c) International Committee for Internet Technology Standards
 - (d) International Committee for Information Technology Solutions
14. Which of the following subcommittees focus on the security issues of biometrics?
 - (a) SC 17
 - (b) SC 27
 - (c) SC 37
 - (d) None of these
15. Which of the following is not the organisation to develop biometric standards?
 - (a) ISO
 - (b) ICAO
 - (c) ANSI
 - (d) ISO/IEU

C. State whether the following statements are True or False

1. As per CBEFF, biometric data block is used for rectilinear iris image.
2. ISO 19794-6 do not describe CBEFF.
3. Biometric data standards are used so that the quality of biometric data is maintained.
4. While taking a picture of the eye it should be eliminated with a light having wavelength between 100 to 200 nanometers.
5. The pixel depth used in iris image is 16 bits per pixel.
6. Google data makes use of Unicode.
7. EBCDIC code is a 16-bit code.
8. ASCII code is an 8-bit code.



NOTES

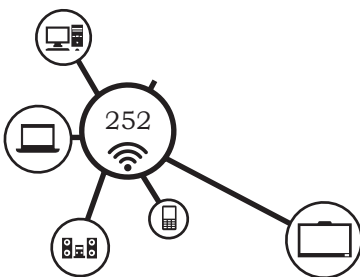
9. In ASCII code control characters cannot be represented in binary form.
10. All letters from A to Z, numbers from 0 to 9 and punctuation symbols can be represented in binary form by using ASCII code.

D. Short answer questions

1. What do you mean by standards of data?
2. State the advantages of using standards of data.
3. What is ASCII code? State its features.
4. What are image acquisition requirements as per the biometric standards?
5. Give the image acquisition formats.
6. Why are biometric standards important?
7. What are the various e-Governance applications in India using Biometrics.
8. How can the accuracy of a biometric system be measured?
9. State colour, pixel depth and elimination requirement in capturing eye image.

SESSION 4: IT PRACTICES

Biometric systems capture and record human biological and behavioural characteristics. Biometric data is the unique way to identify the human, which brings it close to the technology. However, there are serious ethical issues in the use of biometric technology, such as personal privacy, protection and use of personal biometric data. The technology should deal with the ethical and legal aspects of usage and protection of personal biometric data. An important fundamental human right with regards to biometric data usage is the right to protection of personal data with regard to the processing. By considering this, law on information technology has introduced Information Technology Act, 2000. In this session, you will understand the best IT practices to protect the biometric data, concept of data audit, ethics in information technology, addiction to social networks, cyberspace and computers, addiction to online unethical sites, addiction to violent computer games and verbal attacks.



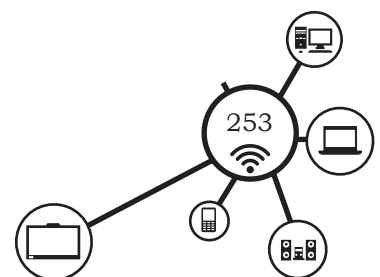
Information Systems Ethics

Ethics is an important concern in information systems. The term 'ethics' is defined as 'a set of moral principles' or 'the principles of conduct governing an individual or a group. Digital technologies have created new categories of ethical dilemmas. Ethics and moral play an important role where any law is not formulated. Moral includes values, such as respect, honesty, fairness accepted by the people on belief. Many organisations set up a code of ethics with some standards and it is expected to follow code of ethics by every member of the organisation. A code of ethics is a document that outlines a set of acceptable behaviours. The document details different actions that are considered appropriate and inappropriate.

Some of the possible considerations of code of ethics for an organisation related to information technology can be:

- Do not use other users computer system, software, or data files without permission.
- Take appropriate approval or permission before using system resources, including communication ports, file space, other system peripherals and computer time.
- Organisations implementing the computer system must consider the personal and professional development, physical safety and human dignity of all workers.
- Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.
- Avoid sending mails from or borrowing other's login ID and password.
- Hosting of personal pages on official compute and providing access for commercial purposes should not be allowed.
- Sending out unsolicited e-mail to a large group of people should be prohibited.
- Honour copyrights, patent and trademark. Violation of copyright, patents, trademark and

NOTES



NOTES

terms of license agreement is prohibited by law. Even the pirated software should not be used. Also give the proper credit to others for intellectual property.

Intellectual Property

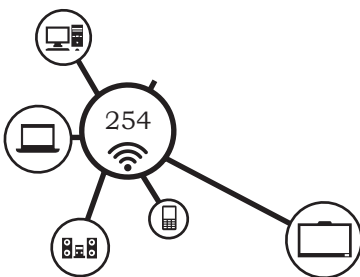
Intellectual property is an idea, invention, or process that derives from the work of the mind or intellect. One must not take credit for other's idea or work. It is difficult to protect an idea. Intellectual property laws are written to protect the tangible results of an idea. Protection of intellectual property is important because it gives people an incentive to be creative. While protecting intellectual property is important because of the incentives it provides, it is also necessary to limit the amount of benefit that can be received and allow the results of ideas to become part of the public domain. Three of the best-known intellectual property protections — copyright, patent and trademark.

Copyright

Copyright is the protection given to the original creation, such as design, computer programs and books. The author or publisher can provide the terms of copyright, such as

- make copies of the work,
- make derivative works from the original work,
- perform the work publicly,
- display the work publicly and
- distribute the work,

The publisher holds the copyright with the original author with some agreement. In return the publisher will market and distribute the work and then pay the royalty to the original author. In the case of a copyrighted work owned by a publisher or another third party, the protection lasts for 95 years from the original creation date. Fair use is a limitation on copyright law that allows for the use of protected works without prior authorisation in specific cases.



Fair use is a well-known and respected concept and will only be challenged when copyright holders feel that the integrity or market value of their work is being threatened.

Freeware, Shareware and Public Domain Software

In software development community the free and open-source software (FOSS) has few or no copyright restrictions. The software developers publish their code and make their software available for others to use and distribute for free. People can use, copy and modify the freeware in the manner they want. But still its copyright is held by the developer. Linux operating systems come under this category.

Shareware is the software that can be shared with other users with owner's permission, provided it should not be copied. Normally these types of software are made available with the magazines.

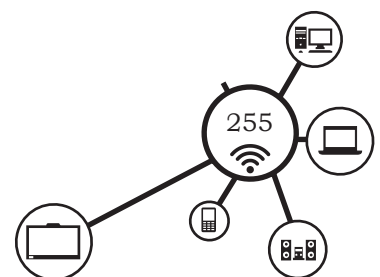
The public domain software are waived copyright. Anybody can use them, copy or modify it in any manner they want without taking the permission. But due to this they are not trustworthy. There are various software available on Internet under public domain.

For other materials, such as text, figures or any artistic work 'creative commons' is the solution to this problem.

Creative commons

It is a nonprofit organisation that provides legal tools for artists and authors. Creative Commons licenses are indicated with the symbol (cc). Creative Commons and public domain are not the same. The matter in the public domain has absolutely no restrictions on its use or distribution. Creative Commons license is used by authors to control the use of their work. There are various licenses under creative commons.

- **CC BY:** is the least restrictive license. It allows others to distribute and modify the work, even commercially, provided credit should be given to the author for original work.



NOTES

- **CC BY-SA:** allows others to freely distribute and modify the work while giving credit to the original author and share the modified work by using the same Creative Commons license.
- **CC BY-NC:** is same as CC-BY, however, here NC refers to 'non-commercial' and adds the restriction that no one can make money with this work.
- **CC BY-NC-ND:** is the same as CC-BY-NC, however, here ND is the restriction to CC-BY-NC, which means that no derivative works may be made from the original.

Patent

It is another important form of intellectual property protection. A patent creates protection for someone who invents a new product or process. The definition of invention is quite broad and covers many different fields. A patent holder has the right to exclude others from making, using, offering the product for sale. Patent protection is valid for a limited period of 20 years before the invention or process enters the public domain. A patent will only be granted if the invention or process being submitted is original, non-obvious and useful.

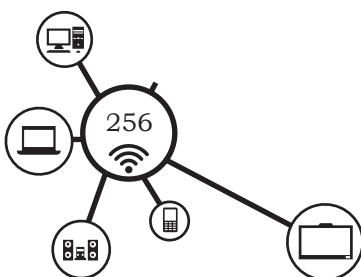
Trademark

It is a word, phrase, logo, shape or sound that identifies a source of goods or services. For example, 'f' is the trademark of Facebook. The concept behind trademarks is to protect the consumer. There are two types of trademarks that exist — a common-law trademark and a registered trademark. A common-law trademark is designated by placing 'TM' next to the trademark. A registered trademark is one that has been examined, approved and registered with the trademark office. A registered trademark has the circle-R (®) placed next to the trademark.

Protection of Intellectual Property in Biometric Systems

In biometric systems, it is important to protect the intellectual property. Privacy is the ability to control

DOMESTIC BIOMETRIC DATA OPERATOR – CLASS XI



information about oneself. In the digital age of information technology everybody is scared to maintain the privacy of their data. During the biometric enrollment process the information about a person that can be used to uniquely establish that person's identity is called personally identifiable information (PII) and is collected by the organisation. The organisations that collect PII are responsible to protect it. The PII may consist of the following information of the employee:

- name
- date of birth
- father's name
- biometric records (fingerprint, face, etc.)
- medical records
- educational records
- financial information
- employment information

Protecting Information of Log Files

A centralised web server holds the biometric data of the users. Web servers are neurotic. They keep the record of each activity in a text file called log file. For example, every image download, error, page load gets stored in the log file. A log file is a file that records either events occurring in an operating system or application software running on that system, or messages between different users of communication software. Logging is the act of keeping a log written to a single log file as shown in Fig. 4.37.

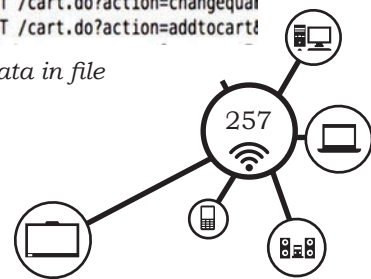
Biometric terminal consists of three main components — a low-cost computer, a commodity fingerprint reader, Iris reader, and a low-end mobile phone connected via USB. Messages sent from the terminal are received by an SMS server and made available over the Internet to administrative users, who can download the messages from any location and automatically

```

209.160.24.63 -- [03/Mar/2016:18:22:16] "GET /product.screen?productId=W
209.160.24.63 -- [03/Mar/2016:18:22:16] "GET /oldlink?itemId=EST-6&JSESS:
209.160.24.63 -- [03/Mar/2016:18:22:17] "GET /product.screen?productId=B
209.160.24.63 -- [03/Mar/2016:18:22:19] "POST /category.screen?categoryId
209.160.24.63 -- [03/Mar/2016:18:22:20] "GET /product.screen?productId=F
209.160.24.63 -- [03/Mar/2016:18:22:20] "POST /cart.do?action=addtocart&
209.160.24.63 -- [03/Mar/2016:18:22:21] "POST /cart.do?action=purchase&i
209.160.24.63 -- [03/Mar/2016:18:22:22] "POST /cart/success.do?JSESSIONID
209.160.24.63 -- [03/Mar/2016:18:22:21] "GET /cart.do?action=remove&item
209.160.24.63 -- [03/Mar/2016:18:22:22] "GET /oldlink?itemId=EST-14&JSESS:
112.111.162.4 -- [03/Mar/2016:18:26:36] "GET /product.screen?productId=W
112.111.162.4 -- [03/Mar/2016:18:26:37] "POST /cart.do?action=addtocart&
112.111.162.4 -- [03/Mar/2016:18:26:38] "POST /cart.do?action=purchase&i
112.111.162.4 -- [03/Mar/2016:18:26:38] "POST /cart/error.do?msg=CreditD
112.111.162.4 -- [03/Mar/2016:18:26:37] "GET /category.screen?categoryId
112.111.162.4 -- [03/Mar/2016:18:26:38] "GET /oldlink?itemId=EST-7&JSESS:
74.125.19.106 -- [03/Mar/2016:18:32:15] "GET /cart.do?action=addtocart&i
74.125.19.106 -- [03/Mar/2016:18:32:15] "GET /category.screen?categoryId
117.21.246.164 -- [03/Mar/2016:18:36:02] "POST /cart.do?action=changequa
117.21.246.164 -- [03/Mar/2016:18:36:03] "POST /cart.do?action=addtocart!

```

Fig. 4.37: sample of log data in file



import them into a database for further analysis and visualisation.

Practical Activity 13

Record useful information from log file

Material required

Writing material

Procedure

1. Find useful information regarding data access from the sample log shown in Fig. 4.37 and record the information as shown in the following table.

IP Address	Date	Time	Method
209.160.24.63	03 March 2016	18:22:16	GET
209.160.24.63	03 March 2016	18:22:16	GET
209.160.24.63	03 March 2016	18:22:17	GET
209.160.24.63	03 March 2016	18:22:19	POST
209.160.24.63	03 March 2016	18:22:20	GET
209.160.24.63	03 March 2016	18:22:20	POST

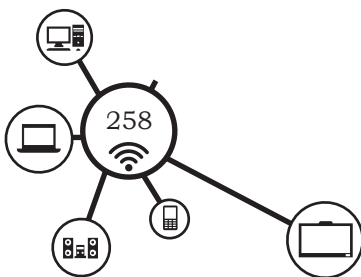
2. Continue to find other useful information regarding data access from the sample log file data and record it as shown in the table above.

Information Technology Act of India (IT Act 2000)

Rapid development in Information Technology and increased use of Internet in every walk of life has resulted in sharing of personal information and making it available on a single click. The data is vulnerable to cyber-crime. Therefore, with the need to provide the legal framework, Parliament of India, passed the Information Technology Act in 2000. This first cyber law addressed various issues to discourage the misuse of digital medium and punishment for various offenses prescribed.

IT Act, 2000 focusses on three main highlights:

1. Providing legal recognition to the transactions which are carried out through electronic means or use of Internet.
2. Allow the government departments to accept filing, creating and retention of official documents in the digital format.



3. To amend outdated laws and provide ways to deal with cyber crimes.

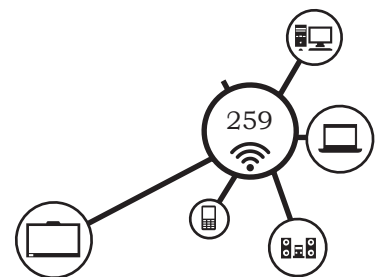
Objectives of IT Act 2000

The following are the objectives of IT Act 2000:

- (a) To give legal recognition to electronic transaction done by electronic way or use of internet.
- (b) To give legal recognition to digital signature for accepting any agreement.
- (c) To provide facility of online filling documents relating to school admission or registration in employment exchange.
- (d) According to IT Act 2000, any company can store their data in electronic storage.
- (e) To stop cyber crime and protect privacy of Internet users.
- (f) To give more power to IPO, RBI and Indian Evidence act for restricting electronic crime.
- (g) To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.

The IT act gives the legal recognition to electronic record and digital signature. The encrypted record will be considered as secure electronic record. The act allows punishment for computer related crimes. The punishment can be fine or fine with imprisonment. For example, the penalty for tampering source code is an imprisonment for three/two years and/or fine upto ₹ 2,00,000. On second count it gets doubled. To enforce the punishments, the government will appoint an Adjudicating officer having the powers of Civil Court. The Act constitutes the Cyber Regulation Appellate Tribunal with Presiding Officer. Tribunal will hear appeals from orders passed by the Adjudicating Officer. The various terms used in the IT Act are given below.

- **Data** means the facts and figures collected to process by the computer system. It may be in the form of print or non-print, handwritten or digitised, stored on the paper or secondary storage devices or stored internally in the computer memory.



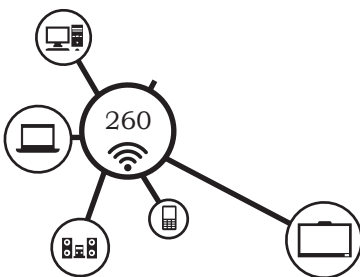
NOTES

- **Digital signature:** is the authentication on of any electronic record by electronic method in accordance with provisions of section 3.
- **Electronic form:** is any information generated, sent, received or stored in digital storage devices.
- **Electronic Gazette:** is the official Gazette published in electronic form.
- **Electronic Record:** is the digital data, such as text, image, sound, video stored in digital storage devices.
- **Information:** is the processed data, which may include text, image, sound, voice, codes, programs and software.
- **Private key:** is the key to create digital signature.
- **Public key:** is the key used to verify digital signature and listed in digital signature certificate.

Importance of the IT Act 2000

In the perspective of e-commerce in India, the IT Act 2000 is an important milestone in the following aspects.

- The e-mail is now a valid and legal form of communication in our country that can be duly produced and approved in the court of law.
- Digital signatures have been given legal validity and sanction in the Act.
- Companies are now able to carry out electronic commerce using the legal infrastructure provided by the Act.
- The Act allows Government to issue notification on the web under e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to be passed



through a system of a security procedure, as stipulated by the Government at a later date.

- Under the IT Act, 2000, it is possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 5 crore.

Amendments to Information Technology Act

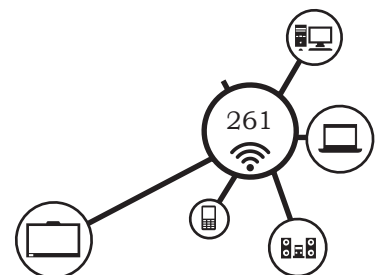
With the exponential growth of technology give rise to cybercrimes. To counter this growing cyber threats IT Act was amended in 2008. This amendment came into force on October 29, 2009. IT Act Amendment 2008 has broadly covered the following aspects.

- Liability of Body Corporate towards sensitive personal data
- Identity Theft
- Spamming and Phishing
- Introduction of virus, manipulating accounts, denial of services, etc., made punishable
- Cheating and stealing of computer resource or communication device
- Cyber Terrorism
- Child pornography
- Intermediary's liability
- Surveillance, interception and monitoring
- Cognizance of cases and investigation of offenses
- Security procedures and practices

Check Your Progress

A. Fill in the blanks

1. A simple text file that records every activity, such as downloads, page loading and errors is called _____ file.
2. A log file records _____ that occur in an operating system.
3. Violation of copyright, patents, trademark and terms of license agreement is prohibited under _____.

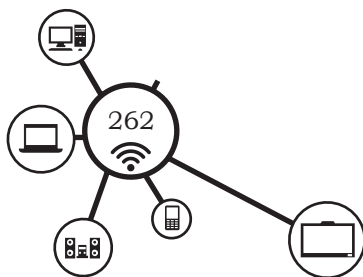


NOTES

- The information to uniquely establish a person's identify is called _____.
- In creative common license CC BY-NC-ND, the ND stands for _____.
- In creative common license CC BY-NC, the NC stands for _____.
- The Information Technology services in India are regulated by using _____.
- The _____ is the key to create digital signature and _____ is the key to verify digital signature.
- IT Act 2009 gives legal recognition to _____ transaction and _____ signature.
- If a person intentionally destroys the computer source code then it is treated as _____ under IT Act.

B. Multiple choice questions

- When did IT Act 2000 come into effect?
(a) October 17, 2000 (b) November 11, 2000
(c) October 17, 2001 (d) November 11, 2001
- What are the components of IT Act 2000?
(a) Legal recognition to digital signature
(b) Regulation of certification authorities
(c) Digital Certificates
(d) All of the above
- Computer crime includes _____.
(a) creating viruses
(b) stealing a credit card number
(c) unauthorised use of a mainframe computer
(d) All of the above
- A suite of guiding beliefs, standards, or ideals that pervades an individual, group, or community of people is _____.
(a) ethics (b) morals
(c) integrity (d) laws
- What are computer ethics?
(a) Honest, moral code that should be followed when on the computer
(b) A computer program about honesty
(c) A computer that fits on or under a desk
(d) A list of commandments in the Bible
- Creative commons licenses are indicated with the symbol _____.
(a) ® (b) T
(c) © (d) cc



7. Which of the following creative commons licences is used for non-commercial distribution?

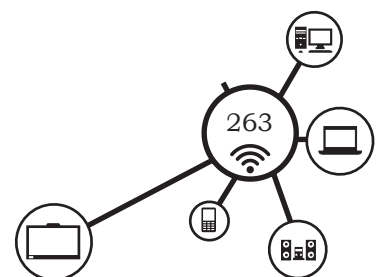
(a) CC-BY	(b) CC BY-SA
(c) CC BY-NC	(d) CC BY-NC-ND
8. Which of the following is not allowed as per IT Act 2000?
 - (a) Electronic transaction
 - (b) Storing official documents in the digital format
 - (c) Do the cybercrimes
 - (d) Punishment for computer related crimes

C. State whether the following statements are True or False

1. As per code of ethics, you can use any computer system, software, or data files without the permission of owner is comes under the code of ethics.
2. As per code of ethics, always send emails from your own e-mail ID.
3. As per code of ethics, it is allowed to send unsolicited e-mail to a large group of people.
4. Proper credit should be given to others for intellectual property.
5. Anybody can use copy or modify the public domain software.
6. The e-mail is not a valid and legal form of communication.
7. According to IT Act, electronic transactions are legal.
8. A log file records the events that occur in operating system or application software.

D. Short answer questions

1. What is log data file?
2. Why was IT Act 2000 introduced?
3. Which is the act that provides legal framework for e-Governance in India?
4. What are the salient features of the IT Act?
5. What are the basic ethics in information technology?
6. What is code of ethics? What is one advantage and one disadvantage of a code of ethics?
7. What does the term intellectual property mean? Give an example.
8. What are the advantages of using Creative Commons License?
9. What are freeware, shareware and public domain software? Give examples.
10. What is fair use?
11. What protections are provided by a patent?
12. What does a trademark protect?



Domestic Biometric Data Operator-Class 11- Unit 4 Session 1

A. Fill in the blanks

1. Collection of computers and other hardware components interconnected by communication channel is called _____.
2. Computer network allows sharing of _____ and _____.
3. Computers can be connected through _____ or _____.
4. Resources in computer network include devices, such as _____.
5. Printer sharing is possible through _____.
6. There are _____ types of computer networks.
7. LAN stands for _____.
8. Computers networked within a limit of geographical area are called _____.
9. WAN means _____.
10. LANs at different locations, when connected together are called _____.
11. MAN stands for _____.
12. LANs beyond the boundaries of a city, when connected together are called _____.
13. P2P networking model stands for _____ model.
14. When each computer can act both as a server and client, then that networking model is called _____ model.
15. HTTP stands for _____.
16. IP address means _____ address.
17. When there is one server and many clients, then such networking model is called _____ model.
18. In Aadhaar card biometric data the _____ networking model is used.
19. Internal network of an organisation is called _____.
20. The network that is not accessible to the public is known _____.
21. The network that is accessible to the public is known _____.

B. Multiple choice questions

1. The computer network that is used outside the Intranet is known as _____.
(a) Internet (b) Extranet
(c) Cable (d) Router
2. The global system of interconnected networks that use TCP/IP protocol is known as _____.
(a) Internet (b) WAN
(c) Intranet (d) LAN

3. The largest network of the computers in the world is _____.
- (a) Internet (b) Extranet
(c) MAN (d) LAN
4. Which of the following are network devices?
- (a) Repeater (b) Modem
(c) Router (d) All of these
5. _____ is used to regenerate the signal when it becomes weak.
- (a) Network hub (b) Network switch
(c) Repeater (d) Router
6. To join the two physical segments of the same network _____ is used.
- (a) Network bridge (b) Network switch
(c) Repeater (d) Router
7. Multiple nodes in the network are connected by using the _____.
- (a) Network hub (b) Wi-Fi
(c) LAN (d) router
8. The combination of network hub and network bridge can be performed by using _____.
- (a) Bluetooth (b) network switch
(c) gateway (d) modem
9. The device that routes the data packets based on their IP addresses is _____.
- (a) UTP cable (b) telephone
(c) repeater (d) router
10. Two networks working on different networking models can be connected together by using a _____.
- (a) network gateways (b) desktop
(c) Internet (d) Wi-Fi

11. Modem means _____.
- (a) modulator demodulator (b) modulator
(c) de-modulator (d) router
12. The cheapest way to send and receive the data through the telephone lines can be performed by using a _____.
- (a) modulator demodulator (b) modulator
(c) de-modulator (d) modem
13. Wireless access point is also known as _____.
- (a) spot (b) soft spot
(c) hot spot (d) Wi-Fi spot
14. The device that is a combination of router and an access point is _____.
- (a) modem (b) hot spot
(c) Wi-Fi router (d) repeater
15. The set of standards that allow network devices to communicate an exchange information is called _____.
- (a) Wi-Fi router (b) protocol
(c) repeater (d) modem

C. State whether the following statements are True or False

1. Protocols are the set of rules for communication.
2. In a computer network, all computers need not use the same protocol for communication.
3. Protocols may include signaling, authentication, error detection and correction.
4. TCP/IP stands for Transmission Control Protocol/Internet Protocol.
5. TCP/IP is not a core protocol of Internet.
6. IP is the primary protocol used for relaying data across the network boundaries.
7. Ipv4 uses 64 bit addressing scheme.
8. Ipv4 provides 232 possible addresses.
9. IANA means Internet Assigned Numbers Authority.
10. Ipv6 uses 64 bit address.
11. Ipv6 address consists of 8 groups of four hexadecimal digits.
12. Most of the operating systems support Ipv4 and Ipv6.

D. Short answer questions

1. What is a computer network?
 2. List the advantages of a computer network.
 3. What are the different types of computer networks?
 4. Write the features of LAN.
-
5. Write the features of WAN.
 6. State the networking models used in computer networks.
 7. Give the diagrams of networking models.
 8. What is Intranet?
 9. What is Internet?
 10. Explain the function of the following network devices—
 - (a) repeaters
 - (b) router
 - (c) modem
 11. What is network protocol? Explain TCP/IP network protocol.

Domestic Biometric Data Operator-Class 11- Unit 4 Session 2

A. Fill in the blanks

1. The _____ is the largest network in the world.
2. Internet is run by a non-profitable organisation called _____.
3. Every website address starts with _____.
4. WWW stands for _____.
5. URL means _____.
6. The domain name .gov indicates that it is a _____ website.
7. Every computer connected to the Internet is identified by its _____ address.
8. IP address contains _____ numbers.
9. ISP stands for _____.
10. IP addresses are stored in _____.
11. Testing of the network can be performed by using _____ command.
12. Domain name gives _____ to all the websites on the Internet.
13. Commercial websites are indicated by _____ in the domain name.

B. Multiple choice questions

1. Normally all Indian websites are indicated by _____ in the domain name.
(a) .au (b) .us
(c) .in (d) .uk
2. Which of these is a protocol used in the Internet?
(a) TCP/IP (b) HTTP
(c) FTP (d) All of these
3. FTP stands for _____.
(a) File transfer protocol (b) File transfer practice
(c) File to punch (d) Former transfer protocol
4. The main usage of FTP protocol is _____.
(a) electronic mail exchange
(b) file exchange
(c) informing and controlling messages
(d) HTML document exchange
5. The main usage of HTTP protocol is _____.
(a) controlling IP addresses
(b) file exchange
(c) electronic mail exchange
(d) HTML document exchange
6. The main usage of TCP/IP protocol is _____.
(a) controlling the exchange of IP addresses
(b) file exchange
(c) electronic mail exchange
(d) HTML document exchange

7. Electronic mail exchange can be achieved by using _____ protocol.
- (a) FTP (b) SMTP
(c) HTTP (d) TCP/IP
8. SMTP stands for _____.
- (a) Simple mail transfer protocol
(b) Simple mail transfer process
(c) Super mail transfer protocol
(d) Super mail to process
9. Error messages are informed and controlled by using _____ protocol.
- (a) FTP (b) SMTP
(c) ICMP (d) TCP/IP
10. The computer that distributes the resources is called _____.
- (a) Client (b) Server
(c) Down-loader (d) Up-loader
11. The process of retrieving information from the server computer to the client computer is _____.
- (a) uploading (b) downloading
(c) managing (d) printing
12. The process of providing information from the client computer to the server computer is _____.
- (a) uploading (b) downloading
(c) managing (d) printing
13. DNS server is used _____.
- (a) to manage printing services
(b) to manage electronic mails
(c) for storing of webpages
(d) for translating URL to IP addresses

C. State whether the following statements are True or False

1. Web server is used for storing of web pages and providing these to the client computers.
2. DNS server is used to manage electronic mails.
3. FTP means file transfer practice.
4. Mozilla Firefox is a web browser.
5. Sir Tim Berners Lee is considered as the father of world wide web.
6. Safari is a text editing software.
7. Computers connected to the Internet cannot be controlled remotely.
8. Using remote access functionality, sometimes hackers can steal important data without the owner's knowledge.
9. Checking of examination result online is an example of file sharing.
10. Any information on the Internet cannot be found using search engine.
11. Google is an example of search engine.
12. Unique identity of a website cannot be reflected by its domain name.

13. By using electronic mail we can exchange our messages or files to two or more people.
14. Cost of the use of Internet is very high.
15. E-mail can be sent from one country to any other country in the world.

D. Short answer questions

1. What is electronic mail? State its advantages.
2. Give the steps for sending and receiving e-mail.
3. What do you mean by search engine? Give the steps for obtaining useful information using search engine.
4. Explain the role of DNS server.
5. What is FTP? How is FTP used for sharing of files?
6. Illustrate the concept of remote access in Internet.
7. What is a web browser? State any four commonly used web browsers.
8. What is a website? Give examples.
9. Explain the role of the following servers—
(i) web server (ii) mail server (iii) print server (iv) DNS server
10. What do you mean by uploading and downloading on Internet?
11. Explain how Internet works.
12. What is domain name? Explain the different domain name extensions and their meaning.
13. Give the steps for connecting biometric attendance system to the Internet.
14. Give the steps to check your computer's IP address.

Domestic Biometric Data Operator-Class 11- Unit 4 Session 3

A. Fill in the blanks

1. ASCII stands for American Standard Code for _____.
2. ASCII is a _____ bit code.
3. The extended version of ASCII is _____ bit code.
4. ASCII code is used for binary representation of letters and _____.
5. ASCII code is also called _____ code.
6. The ASCII code for the character A is _____.
7. EBCDIC code means _____.
8. EBCDIC code can represent _____ characters.
9. By using EBCDIC code _____ can be represented in binary form.
10. In ASCII code _____ characters can be represented in binary form.
11. Unicode means _____ code.
12. All characters in Indian languages, such as Hindi, Marathi and Tamil can be represented in binary form by using

13. IEC stands for _____.
14. The industry consortia includes _____ Consortium, _____ Biometric Consortium and _____.

B. Multiple choice questions

1. The ASCII code for the character D is _____.
(a) 0100 0100 (b) 0100 0101
(c) 0100 0110 (d) 0100 1100
2. National standards of biometric data are developed as per _____.
(a) Government policy
(b) Government policy on open standards
(c) private sector policy
(d) standard organisations
3. UIDAI means _____.
(a) Unique Identification Authority of India
(b) Universal Identification Authority of India
(c) Unique Identification Authority of Internet
(d) Unique Isolated Authority of India
4. The fingerprint image standard adopted in India is _____.
(a) ISO/IEC (b) ISO/IEC 19794
(c) ISO/IEC 19794-4 (d) None of these
5. In image acquisition the scan resolution standard is _____ dpi.
(a) 100 (b) 200
(c) 400 (d) 500

6. In image acquisition the number of bits to be used per pixel is _____.
- (a) 2 (b) 4
(c) 8 (d) 16
7. In fingerprint image the format compressed _____ is recommended.
- (a) jpeg 2000 (b) png 2000
(c) xml 2000 (d) wav 2000
8. In iris images, the iris diameter should be _____ pixels.
- (a) 100 (b) 150
(c) 200 (d) 250
9. In iris images, the iris margin segmentation must be _____% left and right of the iris diameter
- (a) 30% (b) 50%
(c) 60% (d) 80%
10. Iris images shall be captured and stored in grayscale with pixel depth _____ bits per pixel.
- (a) 2 (b) 4
(c) 6 (d) 8
11. The eye image should be eliminated by using light having a wavelength between _____ and _____ nanometers.
- (a) 500, 700 (b) 700, 900
(c) 900, 1100 (d) 1100, 1300
12. CBEFF stands for _____.
- (a) Common Biometric Exchange Formula Framework
(b) Common Biometric Electronic Form Format
(c) Common Biometric Exchange Format Framework
(d) Common Based Electronic Format Framework
13. INCITS stands for _____.
- (a) International Council for Information Technology Standards
(b) International Committee for Information Technology Standards
(c) International Committee for Internet Technology Standards
(d) International Committee for Information Technology Solutions
14. Which of the following subcommittees focus on the security issues of biometrics?
- (a) SC 17 (b) SC 27
(c) SC 37 (d) None of these
15. Which of the following is not the organisation to develop biometric standards?
- (a) ISO (b) ICAO
(c) ANSI (d) ISO/IEU

C. State whether the following statements are True or False

1. As per CBEFF, biometric data block is used for rectilinear iris image.

2. ISO 19794-6 do not describe CBEFF.
3. Biometric data standards are used so that the quality of biometric data is maintained.
4. While taking a picture of the eye it should be eliminated with a light having wavelength between 100 to 200 nanometers.
5. The pixel depth used in iris image is 16 bits per pixel.
6. Google data makes use of Unicode.
7. EBCDIC code is a 16-bit code.
8. ASCII code is an 8-bit code.

9. In ASCII code control characters cannot be represented in binary form.
10. All letters from A to Z, numbers from 0 to 9 and punctuation symbols can be represented in binary form by using ASCII code.

D. Short answer questions

1. What do you mean by standards of data?
2. State the advantages of using standards of data.
3. What is ASCII code? State its features.
4. What are image acquisition requirements as per the biometric standards?
5. Give the image acquisition formats.
6. Why are biometric standards important?
7. What are the various e-Governance applications in India using Biometrics.
8. How can the accuracy of a biometric system be measured?
9. State colour, pixel depth and elimination requirement in capturing eye image.

Domestic Biometric Data Operator-Class 11- Unit 4 Session 4

A. Fill in the blanks

1. A simple text file that records every activity, such as downloads, page loading and errors is called _____ file.
2. A log file records _____ that occur in an operating system.
3. Violation of copyright, patents, trademark and terms of license agreement is prohibited under _____.

7. Which of the following creative commons licences is used for non-commercial distribution?
(a) CC-BY (b) CC BY-SA
(c) CC BY-NC (d) CC BY-NC-ND
8. Which of the following is not allowed as per IT Act 2000?
(a) Electronic transaction
(b) Storing official documents in the digital format
(c) Do the cybercrimes
(d) Punishment for computer related crimes

C. State whether the following statements are True or False

1. As per code of ethics, you can use any computer system, software, or data files without the permission of owner is comes under the code of ethics.
2. As per code of ethics, always send emails from your own e-mail ID.
3. As per code of ethics, it is allowed to send unsolicited e-mail to a large group of people.
4. Proper credit should be given to others for intellectual property.
5. Anybody can use copy or modify the public domain software.
6. The e-mail is not a valid and legal form of communication.
7. According to IT Act, electronic transactions are legal.
8. A log file records the events that occur in operating system or application software.

D. Short answer questions

1. What is log data file?
2. Why was IT Act 2000 introduced?
3. Which is the act that provides legal framework for e-Governance in India?
4. What are the salient features of the IT Act?
5. What are the basic ethics in information technology?
6. What is code of ethics? What is one advantage and one disadvantage of a code of ethics?
7. What does the term intellectual property mean? Give an example.
8. What are the advantages of using Creative Commons License?
9. What are freeware, shareware and public domain software? Give examples.
10. What is fair use?
11. What protections are provided by a patent?
12. What does a trademark protect?

Answer Key

Unit 1: Fundamentals of Data and Computing

Session 1: Power of Computing

A. Fill in the blanks

- | | |
|----------------------------------|------------------------------|
| 1. digital | 2. <i>computare</i> |
| 3. logical | 4. program |
| 5. Central Processing Unit | 6. arithmetic and logic unit |
| 7. arithmetic and logic unit | 8. Input |
| 9. output | 10. Universal Serial Bus |
| 11. Uninterruptable power supply | 12. CPU registers |
| 13. cache | 14. Random Access Memory |
| 15. Read Only Memory | 16. boot strap |
| 17. motherboard | 18. impact, non impact |

B. Multiple choice questions

- 1.(d), 2.(b), 3.(c), 4.(d), 5.(c), 6.(b), 7.(d), 8.(c), 9.(a), 10.(d), 11.(b), 12.(a), 13.(a), 14.(a), 15.(c), 16.(c), 17.(c), 18.(c), 19.(c), 20.(b)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(T), 4.(T), 5.(F), 6.(F), 7.(F), 8.(T), 9.(T), 10.(F), 11.(F), 12.(T)

Session 2: Data Types and Formats

A. Fill in the blanks

- | | |
|------------------------|--------------------------------|
| 1. <i>datum</i> | 2. facts |
| 3. letters and numbers | 4. demographic |
| 5. personal | 6. demographic |
| 7. demographic | 8. digital/electronic |
| 9. one time password | 10. Bharat Interface for Money |
| 11. qualitative | 12. qualitative |
| 13. quantitative | |

B. Multiple choice questions

- 1.(d), 2.(a), 3.(a), 4.(c), 5.(b), 6.(c), 7.(a), 8.(b), 9.(a), 10.(a), 11.(b), 12.(c), 13.(d), 14.(b), 15.(b)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(F), 4.(T), 5.(T), 6.(T), 7.(F), 8.(T), 9.(T), 10.(F), 11.(F), 12.(T), 13.(T), 14.(F), 15.(T), 16.(F)

Session 3: Biometric Data

A. Fill in the blanks

- | | |
|--------------------------|----------------------------------|
| 1. bio, metric | 2. life, standard of measurement |
| 3. physical, behavioural | 4. biometric, |
| 5. eye | 6. shape and writing |
| 7. authentication | 8. error |
| 9. age | 10. unique |
| 11. behavioural | 12. physiological |
| 13. fingerprint | 14. unique |
| 15. fingerprint | 16. ridges |

B. Multiple choice questions

- 1.(a), 2.(b), 3.(a), 4.(c), 5.(b), 6.(c), 7.(d), 8.(a), 9.(b), 10.(b), 11.(a), 12.(d), 13.(c), 14.(a)

C. State whether the following statements are True or False

- 1.(F), 2.(F), 3.(F), 4.(F), 5.(T), 6.(F), 7.(T), 8.(F), 9.(F), 10.(T)

Session 4: Collect and Digitise Data

A. Fill in the blanks

- | | |
|-------------------------|----------------------------------|
| 1. gathering, measuring | 2. public |
| 3. government | 4. acquisition |
| 5. misread | 6. solutions |
| 7. survey | 8. data collection |
| 9. handwritten | 10. entering correct information |
| 11. digital | 12. binary or machine |
| 13. digital | |

B. Multiple choice questions

- 1.(d), 2.(d), 3.(b), 4.(b), 5.(a), 6.(d), 7.(c), 8.(d), 9.(b), 10.(c), 11.(d), 12.(d), 13.(b), 14.(d)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(T), 4.(T), 5.(F), 6.(T), 7.(T), 8.(T), 9.(F), 10.(F), 11.(T), 12.(F), 13.(T)

Session 5: Store and Handle Data Securely

A. Fill in the blanks

- | | |
|-------------------------|-----------------|
| 1. storing | 2. retrieving |
| 3. safe and secure | 4. harm |
| 5. randomly | 6. sequentially |
| 7. randomly | 8. hard disk |
| 9. handwritten/analogue | 10. removable |
| 11. close | |

B. Multiple choice questions

- 1.(a), 2.(c), 3.(a), 4.(d), 5.(b), 6.(a), 7.(c), 8.(c), 9.(d)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(F), 4.(F), 5.(F), 6.(T), 7.(F), 8.(T), 9.(T)

Unit 2: Procedure and Tools for Biometric Data

Session 1: Biometric System and Devices

A. Fill in the blanks

- | | |
|---|--------------------------------|
| 1. authentication | 2. fingerprint scanner |
| 3. iris scanner | 4. Biometric Automated Toolset |
| 5. finger print sensor | 7. light emitting diode (LED) |
| 6. optical | |
| 8. charged couple devices (CCD), complementary metal oxide semiconductor (CMOS) | |
| 9. scanner | 10. hand-held scanner |
| 11. photographic films | 12. iris |
| 13. Pixel | 14. number of pixels |
| 15. resolution | 16. 3648, 2752 |
| 17. ISO | |

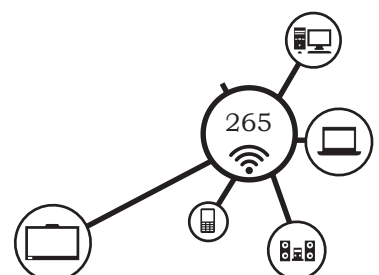
B. Multiple choice questions

- 1.(c), 2.(c), 3.(d), 4.(a), 5.(a), 6.(b), 7.(d), 8.(c), 9.(b), 10.(a)

C. State whether the following statements are True or False

- 1.(T), 2.(T), 3.(F), 4.(T), 5.(F), 6.(F), 7.(F), 8.(T), 9.(T), 10.(T)

ANSWER KEY



Session 2: Setting up Biometric Devices

A. Fill in the blanks

1. setup / install
2. authentication USB
3. device driver
4. face
5. plug and play
6. installed
7. USB
8. eye
9. fingerprint
10. operating system
11. device driver
12. height of the device
13. 5 volt AC
14. battery backup
15. four
16. four
17. open
18. Wi-Fi

B. Multiple choice questions

- 1.(a), 2.(b), 3.(a), 4.(c), 5.(b), 6.(b), 7.(a), 8.(b), 9.(b), 10.(c)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(T), 4.(T), 5.(F), 6.(T), 7.(T), 8.(F), 9.(T), 10.(F), 11.(F)

Session 3: Biometric Data Entry

A. Fill in the blanks

1. biometric data entry
2. master data
3. ID number
4. religion
5. joining date
6. administrator
7. enrolment
8. employee registration
9. fingerprint
10. Aadhaar enrolment client
11. Aadhaar enrolment
12. data validation
13. error
14. 50%
15. low

B. Multiple choice questions

- 1.(c), 2.(d), 3.(b), 4.(a), 5.(b), 6.(b), 7.(a), 8.(a), 9.(a), 10.(b), 11.(d), 12.(c)

C. State whether the following statements are True or False

- 1.(F), 2.(T), 3.(F), 4.(T), 5.(T), 6.(T), 7.(F), 8.(T), 9.(F), 10.(T)

Session 4: Interfacing of Biometric Devices

A. Fill in the blanks

1. biometric interface
2. hardware, software
3. biometric data
4. interoperability
5. intra-system
6. Biometric human-machine interface
7. end users
8. punch cards

B. Multiple choice questions

- 1.(b), 2.(c), 3.(a), 4.(c), 5.(a), 6.(d)

C. State whether the following statements are True or False

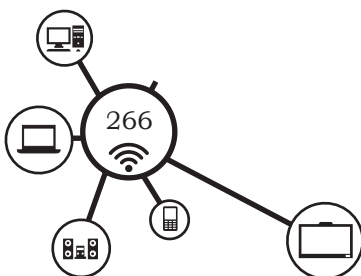
- 1.(T), 2.(F), 3.(F), 4.(T), 5.(T), 6.(T)

Unit 3: Operating System and System Maintenance

Session 1: Operating System

A. Fill in the blanks

1. operating system
2. interface
3. operating system
4. embedded
5. embedded
6. operating system
7. data management
8. memory management
9. process management
10. file management



- 11. time sharing
- 12. access
- 13. security
- 14. deadlock

B. Multiple choice questions

- 1.(a), 2.(a), 3.(a), 4.(b), 5.(a), 6.(b), 7.(c), 8.(c), 9.(b), 10.(d), 11.(a), 12.(b)

C. State whether the following statements are True or False

- 1.(F), 2.(T), 3.(F), 4.(T), 5.(F), 6.(T), 7.(F), 8.(T), 9.(T), 10.(F), 11.(T), 12.(F) 13.(T)

Session 2: Maintenance of Biometric System

A. Fill in the blanks

- 1. system maintenance
- 2. hardware, software
- 3. malware
- 4. computer virus
- 5. computer worm
- 6. Trojan horse
- 7. Trojan horse
- 8. adware
- 9. bots
- 10. bots

B. Multiple choice questions

- 1.(c), 2.(b), 3.(a), 4.(d), 5.(a), 6.(c), 7.(b), 8.(d), 9.(b)

C. State whether the following statements are True or False

- 1.(F), 2.(T), 3.(F), 4.(T), 5.(F), 6.(T), 7.(F), 8.(F), 9.(T), 10.(T)

Session 3: Updating of Biometric System

A. Fill in the blanks

- 1. updating
- 2. limited lifespan
- 3. 20 to 30%
- 4. wear and tear
- 5. android
- 6. unlimited

B. Multiple Choice Questions

- 1.(a), 2.(a), 3.(c), 4.(a), 5.(a), 6.(c), 7.(d), 8.(a)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(F), 4.(F), 5.(T), 6.(T), 7.(F), 8.(F), 9.(T)

Unit 4: Computer Networks, Internet and Standard of Biometric Data

Session 1: Computer Networks

A. Fill in the blanks

- 1. computer network
- 2. resources, information
- 3. wire, without wire
- 4. printer
- 5. computer network
- 6. three
- 7. Local Area Network
- 8. LAN
- 9. Wide Area Network
- 10. Metropolitan Area Network
- 11. Metropolitan Area Network
- 12. MAN
- 13. peer to peer
- 14. peer to peer
- 15. Hyper Text Transfer Protocol
- 16. Internet Protocol
- 17. client server
- 18. client server Intranet
- 19. Internet

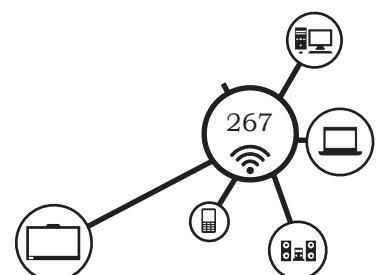
B. Multiple choice questions

- 1.(b), 2.(a), 3.(a), 4.(d), 5.(c), 6.(a), 7.(a), 8.(b), 9.(d), 10.(a) 11.(a) 12.(d) 13.(c) 14. (c) 15.(b)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(T), 4.(T), 5.(F), 6.(T), 7.(F), 8.(T), 9.(T) 10.(T), 11.(F), 12.(T)

ANSWER KEY



Session 2: Internet and its Applications

1. Internet
2. Internet society
3. http
4. World Wide Web
5. Uniform Resource Locator
6. government
7. IP
8. four
9. Internet Service Provider
10. text files
11. ping
12. identity
13. .com

B. Multiple choice questions

- 1.(c), 2.(d), 3.(a), 4.(b), 5.(d), 6.(a), 7.(b), 8.(a), 9.(c) 10.(b), 11.(b), 12.(a), 13.(d)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(F), 4.(T), 5.(T), 6.(F), 7.(F), 8.(T), 9.(T) 10.(F) 11.(T), 12.(F), 13.(T) 14.(F)

Session 3: Standards of Biometric Data

1. Information Interchange
2. 7
3. 8
4. numbers
5. alphanumeric locator
6. 0100 0001
7. Extended Binary Coded Decimal Interchange Code
8. 256
9. 8
10. universal
11. Unicode
12. International Electro technical Commission
13. BioAPI, Biometric, OASIS

B. Multiple choice questions

- 1.(a), 2. (b), 3.(a), 4.(c), 5.(d), 6.(c), 7.(a), 8.(b), 9.(b) 10.(d), 11. (b), 12.(c), 13.(b), 14.(b), 15.(c)

C. State whether the following statements are True or False

- 1.(T), 2.(F), 3.(T), 4.(F), 5.(F), 6.(T), 7.(F), 8.(F), 9.(F) 10.(T)

Session 4: IT Practices

A. Fill in the blanks

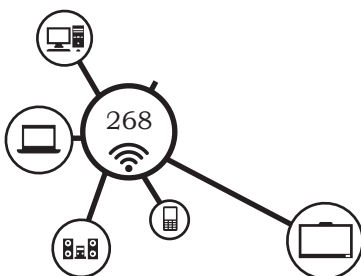
1. log
2. events
3. law
4. personally identifiable information (PII)
5. no drives
6. non-commercial
7. IT Act 2000
8. private key, public key
9. electronic, digital
10. crime

B. Multiple choice questions

- 1.(c), 2.(d), 3.(d), 4.(a), 5.(a), 6.(d), 7.(c), 8.(c)

C. State whether the following statements are True or False

- 1.(F), 2.(T), 3.(F), 4.(T), 5.(T), 6.(F), 7.(T), 8.(T)



Glossary

Accuracy: *the actual statistic for performance will vary by task (verification, open-set identification (watch list), and closed-set identification).*

Algorithm: *a limited sequence of instructions or steps that tell a computer system how to solve a particular problem.*

American National Standards Institute (ANSI): *a private, non-profit organisation that administers and coordinates the US voluntary standardisation and conformity assessment system.*

American Standard Code for Information Interchange (ASCII): *the character set used in the Disk Operating System (DOS) of the original IBM Personal Computer (IBM/PC) line.*

Android: *it is a linux based operating system designed Primarily for touchscreen mobile devices, such as smartphones and tablets.*

Application Program Interface(API): *a set of services or instructions used to standardise an application. An API is computer code used by an application developer. Any biometric system that is compatible with the API can be added or interchanged by the application developer. APIs are often described by the degree to which they are high level or low level. High level means that the interface is close to the application and low level means that the interface is close to the device.*

Arch: *a fingerprint pattern in which the friction ridges enter from one side, make a rise in the center, and exit on the opposite side. The pattern will contain no true delta point.*

Attempt: *the submission of a single set of biometric sample to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual.*

Authentication: *the process of establishing confidence in the truth of some claim. The claim could be any declarative statement in biometrics, 'authentication' is sometimes used as a generic synonym for verification.*

Automated Fingerprint Identification System (AFIS): *a highly specialised biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications.*

Behavioural Biometric Characteristic: *is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioural and biological characteristic. Examples of biometric modalities for which behavioural characteristics may dominate include signature recognition and keystroke dynamics.*

Benchmarking: *the process of comparing measured performance against a standard, openly available, reference.*

Biological Biometric Characteristic: *a biometric characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry.*

Biometric Data: *the information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).*

Biometric Sample: information or computer data obtained from a biometric sensor device, for example, images of a face or fingerprint.

Biometric System: multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system.

Biometrics: a measurable biological (anatomical and physiological) and behavioural characteristic that can be used for automated recognition.

Capture: is the process of collecting a biometric sample from an individual via a sensor.

Comparison: is the process of comparing a biometric reference with a previously stored reference or references in order to make an identification or verification decision.

Computer Network: is a system or communication among two or more computers. The computer networks can be broadly classified as 'Homogenous' and 'Heterogeneous'.

Data: the word data has been derived from latin word datum (means facts). It is a collection of facts and figures which are not in directly usable form.

Database: is a collection of data files integrated and organised into a single comprehensive file system. It is arranged to minimise duplication of data and to provide convenient access to information within that system, to satisfy a wide variety of user needs.

E-mail: electronic mail, abbreviated e-mail is a method of composing, sending, storing and receiving messages over electronic communication systems.

EBCDIC (Extended Binary Coded Decimal Interchange Code): an 8-bit character encoding used on IBM mainframe operating systems.

End User: is the individual who interacts with the system to enroll, to verify, or to identify.

Enrollment: the process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

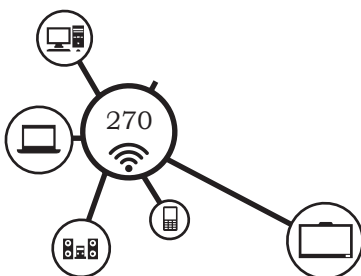
Extraction: the process of converting a captured biometric sample into biometric data so that it can be compared to a reference.

Face Recognition: a biometric modality that uses an image of the visible physical structure of an individual's face for recognition purposes.

Feature(s): distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference.

Fingerprint Recognition: a biometric modality that uses the physical structure of an individual's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems are minutiae points that include bifurcations and ridge endings.

Hard drive: also known as a hard disk drive (HDD); the standard form of permanent magnetic storage for a computer system. HDDs are durable metal boxes containing one or more discs with a magnetic coating and connected by one of a few standard interfaces to the computer's input/output (I/O) bus.



Hardware: includes the case and chassis, the circuit boards, the storage devices, and the peripheral components, such as the monitor, printer, keyboard, and mouse.

Host: a networked device with an IP address; a mainframe computer system; the operating system on which a hypervisor runs. IP hosts are named after the mainframes of legacy and modern centralised networking environments.

Hub: a Layer-1 ethernet device with multiple network interfaces; in general, the central concentrating device in a star-wired hub-and-spoke topology. The Ethernet hub is essentially a multiport repeater dealing only with regenerating inbound signals before sending them out all ports simultaneously. As the generic center of a star-wired topology, the hub device can be a hub, switch, concentrator, router, or a multifunction device offering a combination of such functions.

Identification: a task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is 'closed-set' if the person is known to exist in the database. In 'open-set' identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity.

Indifferent User: an individual who knows their biometric sample is being collected and does not attempt to help or hinder the collection of the sample. For example, an individual, aware that a camera is being used for face recognition, looks in the general direction of the sensor, neither avoiding nor directly looking at it.

Interface: a physical port used for connectivity to a network or peripheral device; a point of interconnection between two cables, two components, two protocols, two software processes, or two networks. Cabling interfaces are often interchangeably referred to as ports. Interfaces between software or protocol objects can also be referred to as ports in a logical sense. The term socket is also used in some cases with the same meaning.

International Organisation for Standardisation (ISO): a non-governmental network of the national standards institutes. The ISO acts as a bridging organisation in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users.

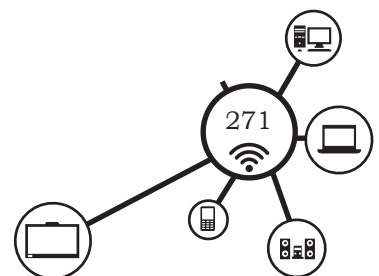
Iris Recognition: a biometric modality that uses an image of the physical structure of an individual's iris for recognition purposes. The iris muscle is the colored portion of the eye surrounding the pupil.

LINUX: is an open source operating system, meaning that the source code of the operating system is freely available to the public.

Live Capture: typically refers to a fingerprint capture device that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface).

Match: a decision that a biometric sample and a stored template comes from the same human source, based on their high level of similarity (difference or hamming distance).

GLOSSARY



Matching: the process of comparing a biometric sample against a previously stored template and scoring the level of similarity (difference or hamming distance). Systems then make decisions based on this score and its relationship (above or below) a predetermined threshold.

Memory: temporary storage for information, including applications and documents. Computer memory is measured in terms of the amount of information it can store, commonly in megabytes or gigabytes.

Minutia(e) Point: friction ridge characteristics that are used to individualise a fingerprint image. Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae (as opposed to the images) are compared for recognition purposes.

Modality: a type or class of biometric system. For example, face recognition, fingerprint recognition, iris recognition.

Model: a representation used to characterise an individual. Behavioural-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates.

Multitasking: simultaneously working with several programs or interrelated tasks that share memories, codes, buffers and files.

Multiuser: the term describing the capability of a computer system to be operated at more than one terminal at the same.

Node: any active device anywhere in a network. Node is a generic term that comes in handy whenever the speaker or writer needs a term that does not commit to a function. On occasion, 'node' is used in place of the term host as an adjective to mean 'related to one of the devices on an IP network,' as in 'node ID' in place of 'host ID.'

Noise: unwanted components in a signal that degrade the quality of data or interfere with the desired signals processed by a system.

One-to-many: a phrase used in the biometrics community to describe a system that compares one reference to many enrolled references to make a decision. The phrase typically refers to the identification or watch list tasks.

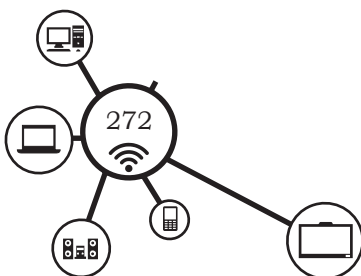
One-to-one: a phrase used in the biometrics community to describe a system that compares one reference to one enrolled reference to make a decision. The phrase typically refers to the verification task (though not all verification tasks are truly one-to-one) and the identification task can be accomplished by a series of one-to-one comparisons.

Open Source Software: software that makes the underlying source code available to all users at no charge. Linux is the example of open source software.

Operating System (OS): the primary systems software on a computer system or other intelligent electronic device. Applications software is written to run on a particular family of OS. Each OS is responsible for certain core functions.

Palm Print Recognition: a biometric modality that uses the physical structure of an individual's palm print for recognition purposes.

Performance: a catch-all phrase for describing a measurement of the characteristics, such as accuracy or speed, of a biometric algorithm or system.



Peripheral: a term designating the various kinds of machines and devices that work in conjunction with a computer but are not necessarily part of the computer structure. Typically, peripherals refer to the hardware devices external to a computer.

Pixel: a picture element. This is the smallest element of a display that can be assigned a colour value.

Population: the set of potential end users for an application.

RAM (Random Access Memory): a type of memory characterised by allowing the access of any addressable location in any order; the main system memory of a computer. Most forms of memory are technically RAM, including magnetic and solid-state drives, flash memory, optical drives, and even read-only memory (ROM) chips.

Recognition: a generic term used in the description of biometric systems (for example, Face recognition or iris recognition) relating to their fundamental function. The term 'recognition' does not inherently imply the verification, closed-set identification or open-set identification (watch list).

Record: the template and other information about the end user (for example, Name, access permissions).

Resolution: the number of pixels per unit distance in the image. Describes the sharpness and clarity of an image.

Server: a device that shares a resource with a client. In the client or server architecture, servers are often specialised devices with specialised operating systems installed. However, a server is any device in any architecture that shares a resource at any time.

User-Friendly Program: a software program that has been designed to easily direct the user through the operation or application of a program. A menu-driven program is considered to be 'user-friendly'.

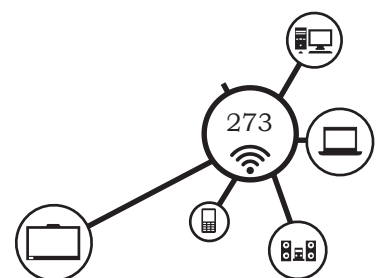
Webcam: a video camera/computer setup that takes live images and sends them to a Web browser.

Wi-Fi: the term used by the Wi-Fi Alliance to refer to the technology that the IEEE calls 802.11. There are five protocols in the Wi-Fi family that have enjoyed a respectable amount of support: 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac.

Window: a portion of a computer display used in a graphical interface that enables users to select commands by pointing to illustrations or symbols with a 'Windows' is also the name Microsoft adopted for its popular operating system.

Wireless security: a group of protocols that are used for authentication and to secure wireless lans (wlans) to varying levels. Security for wlans also includes not broadcasting the SSID, or name of the network, and keeping a list of MAC addresses to filter based on allowed or denied wireless supplicants.

Wireless: a form of node connectivity that replaces cables with radio waves or invisible wavelengths of light.



Notes

© NCERT
not to be republished