Department of Empowerment of Persons with Disabilities (Divyangjan)
Ministry of Social Justice & Empowerment

कौशल शलगुणव त्ताप्रगतिति

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

RE IMAGINE FUTURE

IT - ITeS SSC
NASSCOM

SCPwD
Skill Council for Persons with Disability

Participant Handbook

Sector

IT-ITeS

Sub - Sector

Business Process Management

Occupation

Customer Relationship Management

Reference ID: **SSC/Q2213, Version 3.0**

SCPwD Reference ID: **PWD/SSC/Q2213, Version 3.0**

NSQF Level 3

Domestic Biometric Data Operator

(Divyangjan)
for Locomotor Disability

Scan this QR Code to access eBook

Published by

IT – ITeS Sector Skill Council NASSCOM
Sector Skill Council Contact Details:
Address: Plot No. – 7, 8, 9 & 10 Sector – 126, Noida, Uttar Pradesh – 201303
New Delhi – 110049
Website: www.sscnasscom.com
Phone: 0120 4990111 – 0120 4990172

First Edition, August, 2022

IT – ITeS Sector Skill Council NASSCOM
Sector Skill Council Contact Details:
Address: Plot No. – 7, 8, 9 & 10 Sector – 126, Noida, Uttar Pradesh – 201303
New Delhi – 110049
Website: www.sscnasscom.com
Phone: 0120 4990111 – 0120 4990172
This book is sponsored by IT – ITeS Sector Skill Council NASSCOM

Note: SCPwD
SCPwD has borrowed the qualification of Biometric Data Entry Operator from IT-Ites which is approved by NCVET in the 22nd meeting of NSQC on 25th August 2022 (Link of MOM https://ncvet.gov.in/sites/default/files/MoM%2022nd%20NSQC%20held%20on%2025%20August%202022.pdf And uploaded on NQR WWW.nqr.gov.in The book caters to the job role aligned to the following disabilities as per the NQR codes mentioned below.
For LD- 2022/PWD/SCPWD/06391

> Skilling is building a better India. If we have to move India towards development then Skill Development should be our mission.

Shri Narendra Modi
Prime Minister of India


स्वावलम्बन
Swavlamban
Department of Empowerment of Persons with Disabilities (Divyangjan)
Ministry of Social Justice & Empowerment
IT - ITeS SSC
NASSCOM
SCPwD
दिव्यांग व्यक्तियों के लिए कौशल परिषद्
Skill Council for Persons with Disability
NCVET
कौशल शलगुणव त्तात्प्रगतिति
N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape
Certificate
COMPLIANCE TO
QUALIFICATION PACK – NATIONAL OCCUPATIONAL STANDARDS
is hereby issued by the
Skill Council for Persons with Disability
for
SKILLING CONTENT: PARTICIPANT HANDBOOK
Complying to National Occupational Standards of
Job Role/ Qualification Pack: Domestic Biometric Data Operator(Divyangjan), QP No PWD/SSC/Q2213, NSQF Level 3
Date of Issuance: January 27th, 2022
Valid up to*: January 27th, 2025
*Valid up to the next review date of the Qualification Pack or the 'Valid up to' date mentioned above (whichever is earlier)
Authorised Signatory
(Skill Council for Persons with Disability)

Acknowledgments

This participant's handbook meant for Domestic Biometric Data Entry Operators is a sincere attempt to ensure the availability of all the relevant information to the existing and prospective job holders in this job role. We have compiled the content with inputs from the relevant Subject Matter Experts (SMEs) and industry members to ensure it is the latest and authentic. We express our sincere gratitude to all the SMEs and industry members who have made invaluable contributions to the completion of this participant's handbook. We would also like to thank all the experts and organizations who have helped us by reviewing the content and providing their feedback to improve its quality.

This handbook will help deliver skill-based training in the field of Domestic Biometric Data Entry. We hope that it will benefit all the stakeholders, such as participants, trainers, and evaluators. We have made all efforts to ensure the publication meets the current quality standards for the successful delivery of QP/NOS-based training programs. We welcome and appreciate any suggestions for future improvements to this handbook.

About this book

This participant handbook has been designed to serve as a guide for participants who aim to obtain the required knowledge and skills to undertake various activities in the role of a Domestic Biometric Data Entry Operator. Its content has been aligned with the latest Qualification Pack (QP) prepared for the job role. With a qualified trainer's guidance, the participants will be equipped with the following for working efficiently in the job role:

- Knowledge and Understanding: The relevant operational knowledge and understanding to perform the required tasks.
- Performance Criteria: The essential skills through hands-on training to perform the required operations to the applicable quality standards.
- Professional Skills: The Ability to make appropriate operational decisions about the field of work.

The handbook details the relevant activities to be carried out by a Domestic Biometric Data Entry Operator. After studying this handbook, job holders will be adequately skilled in carrying out their duties according to the applicable quality standards. The handbook is aligned with the following National Occupational Standards (NOS) detailed in the latest and approved version of Domestic Biometric Data Entry Operator QP:

- SSC/N3023 - Undertake Bio-Metric data entry and processing
- DGT/VSQ/ N0102 - Practice Employability Skills

The handbook has been divided into an appropriate number of units and sub-units based on the content of the relevant QP. We hope it will facilitate easy and structured learning for the participants, allowing them to obtain enhanced knowledge and skills.

Symbols Used


Key Learning Outcomes


Exercise


Notes


Unit Objectives


Activitiy

Table of Contents

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

1. Introduction

Unit 1.1 - IT-ITeS/BPM Industry – An Introduction

Unit 1.2 - Introduction to Biometric

Unit 1.3 - Career Progression of a Biometric Data Entry Operator

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Explain the relevance of the IT-ITeS sector.
2. Identify the biometric data entry procedures, tools, and techniques.
3. Define Biometric
4. State evolution of biometric
5. Explain the need for biometric
6. Identify the role and importance of the biometric data operator in supporting business operations.

UNIT 1.1: IT-ITeS/BPM Industry – An Introduction

Unit Objectives

By the end of this unit, participants will be able to:

1. Explain the relevance of the IT-ITeS sector.
2. Conduct internet browsing to collate information and articles regarding the IT- ITeS/BPM industry.
3. Determine the various sub-sectors of the IT-BPM industry where Biometric information is required.

1.1.1 India's IT-ITeS/BPM Industry

- Information Technology (IT), Information Technology Enabled Services (ITes)/ Business Process Management (BPM) are vital to the Indian economy.
- The IT and BPM market accounts for 9.3% of India's GDP and 56% of the global outsourcing market.
- India's IT and business services market is projected to reach US$ 19.93 billion by 2025.
- According to an estimate, IT spending in India is forecasted to increase to US$ 101.8 billion in 2022 from US$ 81.89 billion in 2021.
- India's IT & BPM industry is well-diversified across verticals, such as Banking, Financial Services, and Insurance (BFSI) sector, telecom and retail.
- In FY21, India ranked third worldwide with 608,000 cloud experts across all verticals, including technology.
- The computer software and hardware sector in India attracted cumulative foreign direct investment (FDI) inflows worth US$ 81.31 billion between April 2000 and December 2021.
- IT companies are one of the top employers in the country's organized sector.

Source: www.ibef.org/industry/information-technology-india

Sector Composition

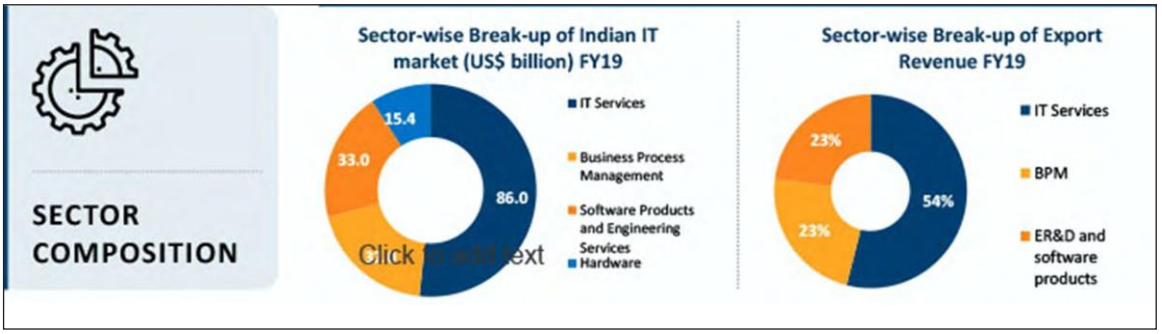

Fig. 1.1.1 Sector Composition of the Indian IT Market

Source: www.ibef.org/industry/information-technology-india/infographi

It has been noticed that the IT Services and ITeS-BPO industries have impacted the Indian economy's growth. The Indian IT/ITeS industry has become one of the country's greatest success stories, putting it on the worldwide map as a leader in Information Technology (IT) and Business Process Outsourcing (BPO). In every way, the Indian information technology (IT) and information technology-enabled services (ITeS) industries are intertwined. The industry has not only improved India's global image. However, it has also fueled economic progress and contributed significantly to social transformation. With its low cost, large resource pool, and competence, India has the opportunity to tap into a booming market.

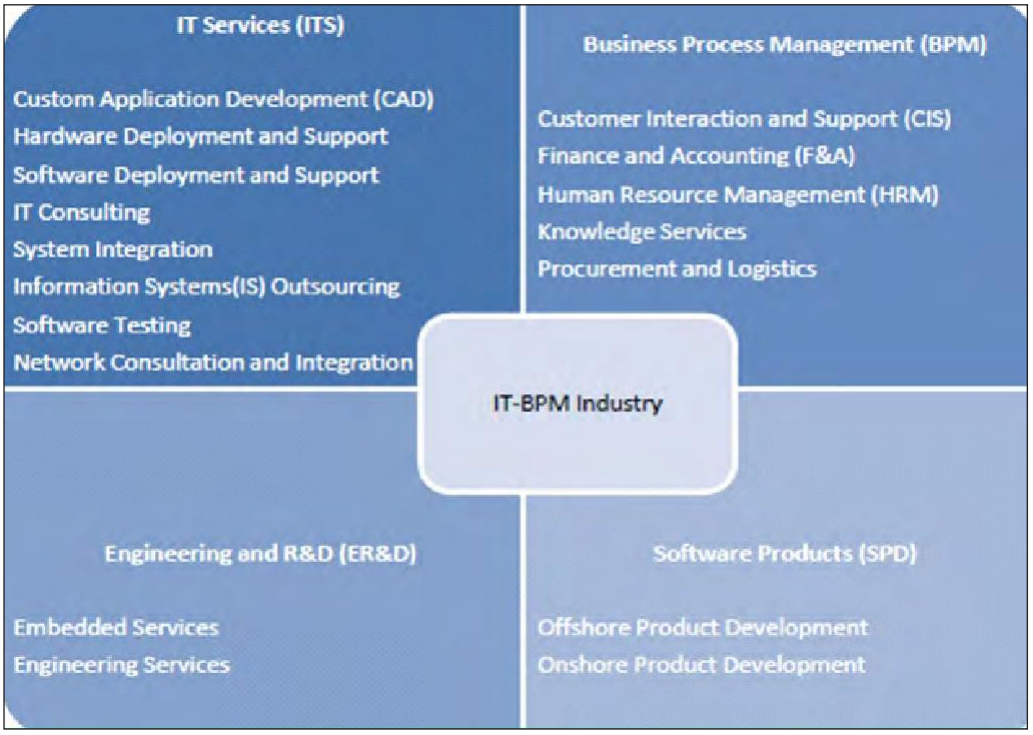

Fig. 1.1.2 Structure of the IT-BPM Industry

1.1.2 Search on the Internet About IT-ITeS/BPM Industry

1. Android/Tablet

- On the Android phone or tablet, open the Chrome app Chrome.
- In the address bar, type IT-ITeS/BPM industry and search.
- Tap the result, Go, or Continue Continue.

Tip: As one types, one may get suggestions based on the web and app activity. Users can delete individual suggestions from the search history or hide sections of suggestions based on the activity when they appear.

2. Computer

- On the computer, open Chrome application.
- In the address bar, enter **IT-ITeS/BPM** industry search.
- Select a result or press Enter.

Tip: As one types, one may get suggestions based on the web and app activity. Users can delete individual suggestions from the search history or hide sections of suggestions based on the activity when they appear.

Notes

UNIT 1.2: Introduction to Biometric

Unit Objectives

By the end of this unit, participants will be able to:

1. Define Biometric.
2. State evolution of biometric.
3. Explain the need for biometric.
4. Categorize the key emerging trends in the biometric data entry domain.

1.2.1 Biometric

Biometrics is a technique for identifying, analyzing and measuring a person's physical and behavioural traits.

Each human being is distinct in terms of features that distinguish him or her from others. Physical traits such as fingerprint, iris colour, hair colour, hand geometry, and behavioural characteristics such as tone and accent of speech, signature, or the way a person types on a computer keyboard make a person stand separate from the rest.

The biometric systems then use this uniqueness of a person to:

- Determine a person's identity and verify it.
- Authenticate a person to grant proper system operating rights.
- Ensure that the system is not subjected to unethical treatment.

Fig. 1.1.2 Structure of the IT-BPM Industry

1.2.2 Evolution of Biometric

The concept of biometrics has been around for a few years now. In the 14th century, China used fingerprints to distinguish merchants and their offspring from the rest of the population. Today, fingerprinting is still utilized.

- An Anthropologist named Alphonse Bertillon created the Bertillionage method of obtaining body measurements to identify people in the 19th century. He noticed that while certain physical characteristics of the human body fluctuate, such as hair length, weight etc., others, such as finger length, stay constant. However, this approach swiftly fell out of favour when it was discovered that people with identical physical dimensions might be mistaken for one another. Following that, Scotland Yard's Richard Edward Henry devised a fingerprinting procedure.
- Dr. Carleton Simon and Dr. Isadore Goldstein developed the notion of retinal identification in 1935. EyeDentify Inc. began doing research and development in 1976. In 1981, the first commercial retina scanning system became available.
- John Daugman of Cambridge University created iris recognition in 1993.
- In Kosovo, the Biometrics Automated Toolset (BAT) was launched in 2001, providing a reliable way of identification.

Biometrics has evolved into its field of study with accurate methods for creating human identities.

1.2.3 Need for Biometrics

With the increased usage of information technology in fields such as finance, research, and medicine, there is a significant need to safeguard systems and data against illegal access.

Biometrics is a technique for authenticating and authorizing a person's identity. Although these phrases are frequently used together, they have separate meanings.

Authentication (Identification)

This procedure aims to answer the questions "Are you the same person you claim to be?" and "Do I recognize you?" This is a one-to-many comparison of a person's biometrics against the whole database.

Verification

Verification is a one-to-one matching procedure in which the candidate's live sample is matched to a previously stored template in the database. The verification is successful if both match with more than 70% acceptable similarity.

Authorization

It is the process of granting access credentials to verified or authorized users. It seeks to answer the question, "Are you qualified to have particular access permissions to this resource?"

ID cards, passwords, Personal Identification Numbers (PINs), and other traditional techniques of information system security were employed. However, they are accompanied by the following drawbacks:

They all refer to identifying a code linked with a person rather than the person who created it.

- They are easily forgotten, misplaced, or stolen.
- They can be readily circumvented or hacked.
- They are not exact.

In such instances, the system's security is jeopardized. When systems require a high level of dependable security, biometrics can assist by tying the identity to the individual.

1.2.4 Emerging Trends in Biometeric

In various phases of development, new trends in biometrics employ a variety of psychological and behavioural characteristics. Each performance is influenced by its surroundings and method of usage.

The new trends includes:

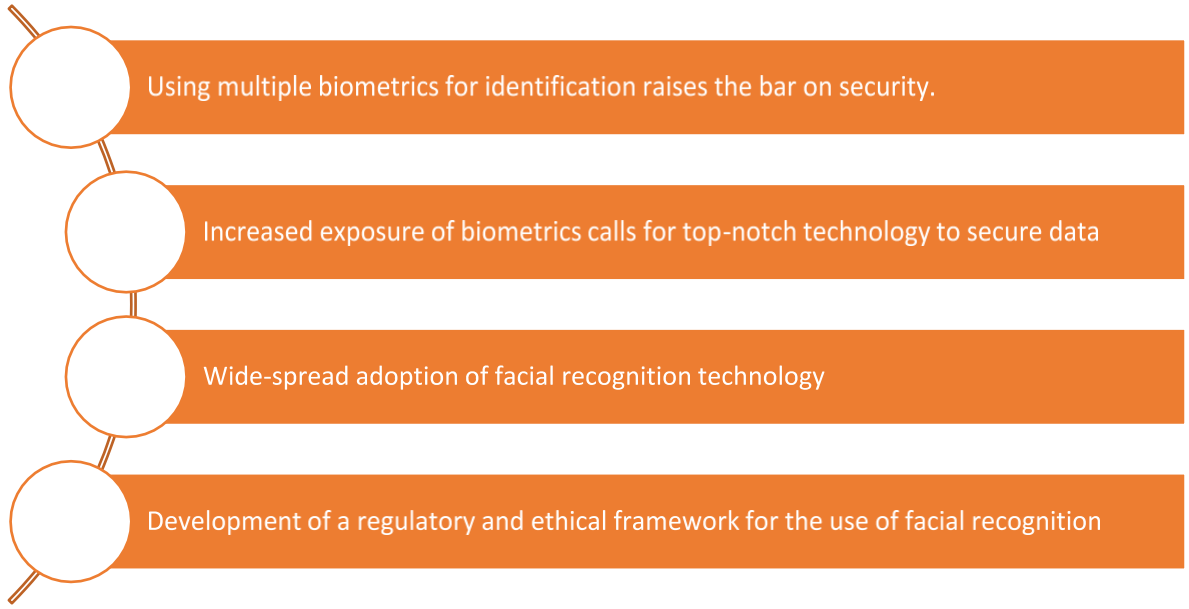

Fig.1.2.2 Emerging Trends in Biometeric

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=Q2ZnqjqQ-Dw

Introduction to Biometric

UNIT 1.3: Career progression of a Biometric Data Entry Operator

Unit Objectives

By the end of this unit, participants will be able to:

1. Identify the career path for a biometric data entry operator.

1.3.1 Biometric Data Operator

The Biometric Operator is in charge of obtaining accurate data that will be utilized for identity validation and authentication. All businesses that employ biometric technology for their services rely on their customers' data being recorded accurately in the end. An erroneously collected piece of data might have a cascading effect on customer contact and the security of transactions that rely on verified identities.

As a result, it is the Operator's responsibility to perform his duties with the utmost care. An organization that hires a biometric operator must guarantee that the operator receives proper training on a regular basis in all of his functional and management domains. This training will be a long-term commitment on the part of the organization in order to make the final system more stable and reliable.

A Domestic Biometric Data Operator in the IT-ITeS Industry is also known as Biometric Technician and Biometric Coordinator.

1.3.2 Career Map for a Domestic Biometric Data Entry Operator

As a Domestic Biometric Data Operator gains knowledge and experience, the individual may progress into different job roles. Please refer to the career map given below to learn about the career progression opportunities available to a Domestic Data Entry Operator:

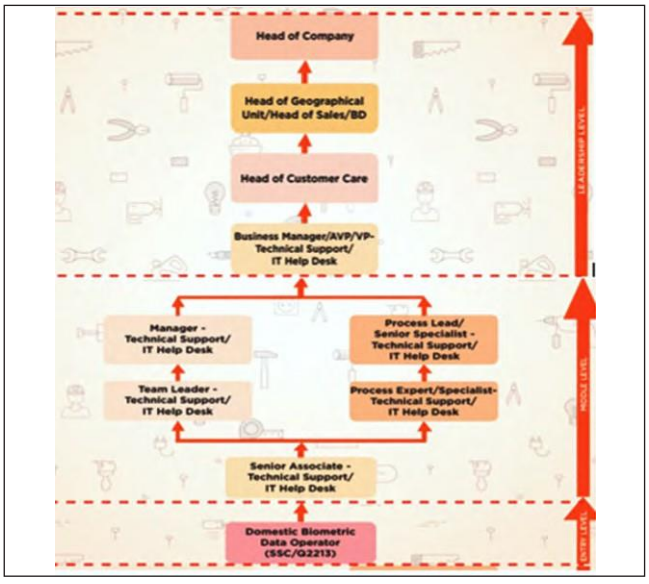

Fig 1.3.1 Career Map of Domestic Biometric Data Operator

Exercise

1. Identify the two sectors of the Indian IT market.
2. State 5 roles and responsibilities of a Domestic Biometric Data Operator.
3. Fill in the Blanks

   Biometrics, Biometric Operator, Authorization, Verification

   a. _____is the process of granting access credentials to verified or authorized users.

   b. _____is a technique for identifying, analyzing and measuring a person's physical and behavioural traits.

   c. The_____is in charge of obtaining accurate data that will be utilized for identity validation and authentication.

   d. _____is a one-to-one matching procedure in which the candidate's live sample is matched to a previously stored template in the database.

Notes

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

2. Undertake Biometric Data Entry and Processing

Unit 2.1 - Biometric Data Entry

SSC/N3023

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Identify the biometric data entry procedures, tools, and techniques.
2. Identify the role and importance of the biometric data operator in supporting business operations.
3. Design plans to collate specific information/data from customer/ client to be entered.
4. Perform a service request, basis standard policies to be adhered to.
5. Examine the specific differences between standard data entry and biometric entries.

UNIT 2.1: Biometric Data Entry

Unit Objectives

By the end of this unit, participants will be able to:

1. Identify the biometric data entry procedures, tools, and techniques.
2. Identify the role and importance of the biometric data operator in supporting business operations.
3. Design plans to collate specific information/data from customer/ client to be entered.
4. Perform a service request, basis standard policies to be adhered to.
5. Examine the specific differences between standard data entry and biometric entries.

2.1.1 Biometric Data

Biometric data is information on a biological organism or group of organisms used in the biometric analysis, the study of biological systems or organisms. Although the term "biometric data" can also apply to information used to research biological processes, it is most frequently used to describe information used to identify particular biological species, mostly people.

2.1.2 Biometric Data Entry Procedure

The process of biometric data entry involves data entry is the process of transcribing information into an electronic medium such as a computer or other electronic device. It can either be performed through fingerprint scanner, digital camera, etc.

2.1.3 Biometric Systems or Tools

A biometric system is a piece of technology that takes an individual's physiological, behavioural, or both attributes as input, analyses them, and determines whether or not they are a legitimate or malicious user.

The Biometric system has two parts:

1. Biometric Devices that capture the biometric details such as fingerprints, facial recognition and iris patterns. These are:
    - Digital Camera which captures facial patterns
    - Fingerprint Scanner which captures fingerprints
    - Iris Capturing Device which captures iris patterns
2. Non Biometric Device that are used to process the data like - enter, read, store, print, scan and photocopying such as a computer, printer, a photocopying machine etc. This is explained in a later session.

Selecting a Biometric System

Few features that are needed to make a biometric system usable

1. The system must be based upon a distinct trait like fingerprints. This has been used in law enforcement for decades. However, new technologies such as face or iris recognition are being commonly used now. Newer technologies keep evolving and could be even more accurate but may need more research to establish their credentials.
2. The system must be 'user-friendly'. Capturing the biometric data should be a quick and easy process. Like a picture being taken by a camera or just speaking into a microphone, or touching your finger to a fingerprint scanner.
3. When looking at costs, not just the initial cost of sensor and software should be looked at but also cost of service support, system management and operator needs to be considered.

2.1.4 Basic Components of a Biometric System

A biometric system may be separated into four essential components:

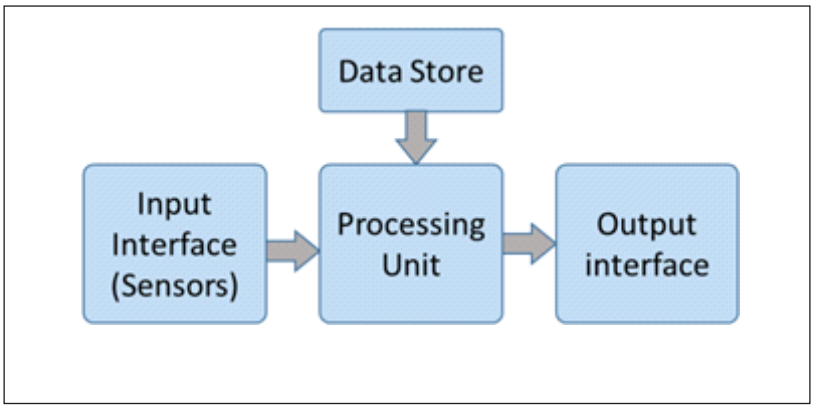

Fig. 2.1.1 Components of a Biometric System

Input Interface (Sensors)

It is a biometrics system's sensing component that turns human biological data into digital form.

For example,

- In the case of the face, handprint, or iris/retinal recognition systems, a Charge Coupled Device (CCD) or a Metal Oxide Semiconductor (CMOS) imager is used.
- In the case of fingerprint systems, an optical sensor.
- In the case of speech recognition systems, a microphone is required.

Processing Unit

A microprocessor, Digital Signal Processor (DSP), computer processes the data gathered by the sensors as part of the processing component.

The processing of the biometric sample involves:

- Enhancement of sample image
- Normalization of sample image
- Extraction of feature
- A comparison between the biometric sample and each sample that has been saved in the database.

Database Store

The enrolled sample is saved in the database and is recalled upon authentication to perform a match. Any memory, such as Random Access Memory (RAM), flash EPROM, or a data server, can be used for identification. In addition, a detachable storage device, such as a contact or contactless smart card, is utilized for verification.

Output Interface

The biometric system's decision to provide access to the user is communicated through the output interface. It is a basic serial communication protocol like RS232 or a higher-bandwidth standard like USB. TCP/IP protocol, Bluetooth, Radio Frequency Identification (RFID), or one of the several cellular protocols are all possibilities.

2.1.5 Types of Data in a Biometric System

The types of data in a biometric systems are:

- **Face recognition:** It is a technique for identifying someone's face. By comparing and analyzing facial contours, one can determine the distinct patterns of a person's face. It is used in security and law enforcement, as well as to verify identification and unlock devices like cellphones and computers. It is used in security and law enforcement, as well as to verify identification and unlock devices like cellphones and computers.
- **Iris Recognition:** The iris, the coloured portion of the eye surrounding the pupil, is used to identify a person's distinct features. It is widely used in security applications, but it is rarely employed in consumer products.
- **Fingerprint scanner:** On a finger, it captures the distinctive pattern of ridges and valleys. This technique is used as a password to unlock a screen on many smartphones and Pcs.
- **Voice recognition:** The distinctive sound waves in the voice when talking to a gadget is measured. The banks use voice as recognition for authenticating their identity.

- **Hand geometry:** The length, thickness, breadth, and surface area of a person's hand are measured and recorded. These gadgets were introduced in the 1980s and primarily were utilized for security purposes.
- **Behaviour characteristics:** Analyzes the interactions with a digital system. How one walks, how they use a mouse, and other movements may all be used to determine who they are and how comfortable they are with the information they are entering.

2.1.6 Biometric Technology

Biometrics technology uses automated systems to recognize a person based on behavioural and biological (anatomical and physiological) characteristics. Traditional data capturing mechanisms used for identification of individuals are filled with errors and data duplications. To remove these deficiencies, biometric technology uses an individual's identity to the his or her unique biometric identity. Biometric data represents a biometric characteristic such as image data, behavioural data or sensor data. This data is captured using camera, scanners and sensors and then stored using specific devices and appropriate individual documents are generated.

Reasons why Biometrics is Gaining Importance

Increasing the biometric technology is finding its way to become the basis for building extremely secure identification and personal verification solutions. Biometrics technology is implemented because of the following :

- **Uniqueness of individuals:** Generally every individual as unique characteristics. This uniqueness is the basis of identification.
- **Permanency:** The individual's unique characteristics remain unchanged with time.
- **Performance:** The technology should deliver same and accurate results in different environments.
- **Circumvention:** Is it not easy to deceive the technology.

More and more, using biometric technology for personal authentication is ever more convenient, quick and easy and comparatively more accurate than current methods like using passwords or pins, as biometric uses personal identifiers to conduct a transaction.

The digital environment now is fast paced and people have to remember number of passwords and PINs for email accounts, computer logins, ATMs, phones, secure sites etc. Biometrics can free people from this hassle. A password or pin can be forgotten or misused by someone else. However, biometric technology is convenient as there is nothing to carry or remember. The technology can provide for positive, trustworthy and low cost method of authentication for various applications. It can easily build an audit trail and is fast gaining wide social acceptance.

Real World Applications of Biometrics

Authentication applications that use biometric technology can include:

- Workstation, computer network, and domain access
- Entity authentication, single sign-on, application logon
- Data protection
- Remote access to resources
- Confidential Financial Transaction security
- Web security.
- Entry devices for offices, buildings
- Law enforcement
- Personal data privacy
- In India, biometrics has found its application in many of the governments initiatives UIDAI (Aadhar)
- NPR (National Population Register)
- E-Passport
- PDS (Public Distribution System)
- RSBY (Rashtriya Swasthya Bima Yojna)
- Transport department for issuing or renewing Driving License, etc.

As biometric technologies mature, evolve, become more commercially acceptable and find increasing usage, users will find it easier to deal with multiple levels or instances of authentication. This is a positive and strong indication of the future for biometric activities. The growth of a digital economy is dependent on how much trust we have in the electronic transactions. Whether used independently or in collaboration with other technologies like smart cards, encryption keys and digital signatures, biometrics will soon become part of every activity in the economy and our personal daily lives.

2.1.7 Importance of a Biometeric Data Entry Operators

With modern businesses generating an enormous amount of data, it is important for them to collect, organize and analyze data to gain insights into their operations, financial health, and what their customers/clients need or prefer. Data insights also help businesses make decisions regarding expansion or streamlining operations.

It is also essential to recognize and authenticate the data of the customer, for which biometric data of a customer or client is required.

A Biometric Data Operator records and secures the various individual's data. Every organization has a vast amount of data accessible to the authorized person, which is identified through their biometrics.

The entry and exit of employees in the organization are registered through biometrics.

A biometric data operator is required in corporate organizations, banking institutes, educational institutes, government offices, etc.

Roles and Responsibilities

In the process of managing identities, the biometric operator is essential. The right data must be recorded in order to validate and authenticate identification, and that is their ultimate duty.

How does this affect businesses? All businesses that offer services utilising biometric technology ultimately rely on accurate client data collection. Inaccurate data collection might have a cascading effect on customer contact and the security of transactions that rely on verified identities.

Duties of a Biometric Data Operator

A Biometric data entry operator is responsible for:

- Gather demographic and biometric data, such as contact information and personal information (such as Facial image, IRIS, and Fingerprint details)
- Deal with any exception situations when capturing data (i.e., missing of eyes, fingers etc.)
- Provide acknowledgement slips to enrollees.
- Obtain consent letters.
- Correct any recorded data as needed. For future use, including checking the status and avoiding acquiring the Biometric Identity Number, this slip will be necessary.
- If necessary, load data from pre-enrolling residents onto laptops at enrolment stations.
- In the event that it is necessary, assists the enrollee in filling out the "Know Your Resident/Enrollee" form.
- If the enrollee is blind or unable to read, read the words on the screen throughout the data validation process.
- Export of data to a memory stick and hand over to his supervisor
- Setting up the enrollment station
- Installing and configuring the Biometric Data Capturing Software Client
- Registering laptops, Enrolment Agency Operators, and Supervisors with the necessary Centralized Authority
- Troubleshooting
- In the case of a government-driven enrollment, such as Aadhar, verify the Enrollee's identification by requesting his or her Aadhar and fingerprints for confirmation, in the case of residents who lack formal identification documents.
- In the case of a government-driven enrollment, such as Aadhar, verify the Enrollee's identification by requesting his or her Aadhar and fingerprints for confirmation, in the case of residents who lack formal identification documents.

Understand limits of your job role

The Operator should work in the defined area as established by organisation and his Supervisor. It's important that he understand the deliverables very clearly and not deviate from this. A predefined work outcome is the single most important priority for the Operator – to capture high quality biometric data. The second most important area is processes that facilitate the capture of data.

The Operator should keep track of both these areas and keep in mind all activities in the centre that can impact his work outcome. The Operator should also ascertain proactively on a day to day basis if any additional responsibilities like answering phone calls, performing any admin duties, need to be undertaken. These would be specific responsibilities that could be time bound.

Keep Updated with Latest Practices

Keep up to date with changes, procedures and practices in your role & expertise The Operator, as a matter of routine, should keep up to date with the organisations' policies and procedures with reference to their role and expertise.

He or she should regularly attend all the training programs that they needs to go through mandatorily as part of his duties. They should also undertake training programs that will help them in their function role.

Few areas where they can take training

- Computer Management
- Understanding Biometric devices
- Learning about customer service
- Do personality development courses
- Undertake grooming classes

2.1.8 Biometric Data Collection

A 10-digit fingerprint scan and a face picture captured with a digital camera and scanner will be used to gather biometric data in a rapid, covert, and non-intrusive manner.

The steps to collect biometric data are:

- Step1: Preliminary Verification
- Step 2: Establishing if the applicant must submit biometric data
- Step 3: Examining the applicant's capacity to submit a photo and fingerprints
- Step 4: How to decide whether or not collecting is possible
- Step 5: A registration meeting
- Step 6: Recording observations and notes from the registration session.

Enrolment Procedures

The following is a standard enrolment procedure followed by a Biometric Operator working in an Aadhar environment. This would be the guideline for biometric data capture in any environment.

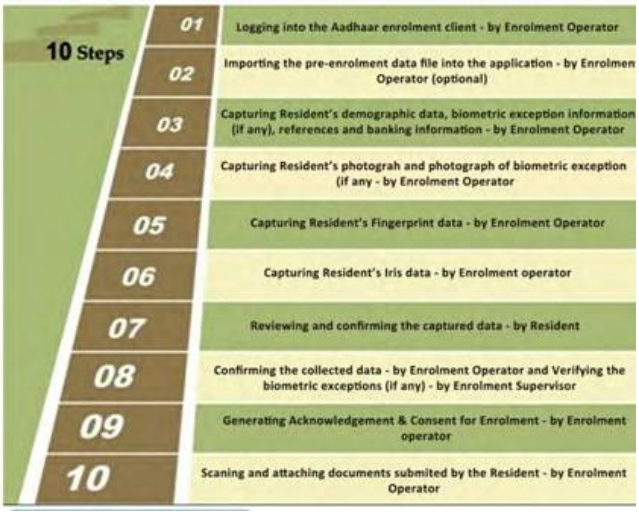

Fig. 2.1.1 Standard Enrolment Procedures Before Enrolment

- Operator must first get on-boarded or enrolled by providing his/her own biometrics in the Enrolment Client or Aadhar client software. An Operator is properly on-boarded when his biometric details verification is successfully completed and stored in local database at the enrolment station.
- The Operator must ensure to login with his own Operator ID in enrolment client, for undertaking enrolments, and log off the application when going away from the seat so that no one else can use your login window for enrolments.
- Operator must make sure that the date and time setting on the computer is current, every time he or she logs into the machine.
- After login, he should check the footer area i.e. left hand bottom corner icons to ensure proper connections of Biometric devices, printers etc.
- Check the pop up message that appears every time the logs in intimating last Sync and
- time left for export. Inform Supervisor accordingly
- He should capture center's GPS coordinates at least once in 24 Hours.
- The enrolment work station should be convenient to the Operator as well as the Enrollee.

2.1.9 Effective Customer Management

An Operator has to handle many types of people in his routine work day. Supervisors, enrolees, technical staff, admin staff, will make multiple demands on his time. He should be able to manage all of them with professional courtesy.

Few principles of customer management that an Operator can deploy in his daily routine are:

- Look for continuous improvement in the work process so that all stakeholder's needs are met.
- When handling customers focus not just on domain knowledge but interpersonal skills as well.
- Ensure that current process and systems are properly mapped so that one can deliver on customer requirement with speed and quality.
- Actively seek customer feedback so one can improve their service delivery.
- Deal with customer queries and problems with current mix of empathy, apology and resolution.
- Ensure that one focus on the real problem and solve it instead of merely the symptoms.
- Focus on prevention of the problem rather than fixing the problem. In the event of the problem being repetitive, pre-empt the problem by fixing it before hand.
- Involve the supervisor and team in articulating a customer management strategy.
- Share the customer management experience with team on a regular basis, take feedback and incorporate into their process.

2.1.10 Service Request Management

A service request is described as a request made by a user or the user's authorised representative to begin a service activity that has been agreed to as a regular component of service delivery. Requests for services are not utilised in reaction to service failures or degradations (which are handled as incidents).

By addressing all pre-defined, user-initiated service requests in an efficient and approachable way, the service request management method supports the agreed-upon quality of a service. In order to operate as efficiently as possible, tracking and automation technologies are used to operationalize well-designed processes and procedures for service request management. Service request management should adhere to the following rules for best results:

- To the maximum extent practicable, service requests and their fulfilment should be standardised and automated.
- To simplify fulfilment, policies should specify which service requests will need little or even no extra approvals.
- Users' expectations should be clearly defined in terms of delivery timeframes and pricing, based on what the business can really provide.
- To increase fulfilment times and make use of automation, opportunities for improvement should be found and put into practise.

Standard modifications shall be taken into account when fulfilling service requests that call for changes to services or their constituent parts. Service requests may typically be formalised, with a clear, standard method for initiation, approval, fulfilment, and administration since they are pre-defined and pre-agreed upon as a routine element of service delivery.

Whatever the request's complexity, the actions to fulfil it should be well-known and supported by evidence. This enables the service provider to set up completion dates and inform users clearly of the request's progress. This is because customer happiness and value perception are greatly influenced by the direct user interface.

Fig. 2.1.2 Service Request Management Activities

There will be a variety of service request fulfilment processes, but if just a few workflow models are found, efficiency and maintainability will be enhanced. Existing workflow models should be used wherever possible when new service requests must be added to the service catalogue. Some service requests can be entirely fulfilled by automation from submission to closure, in keeping with the ITIL philosophy of optimise and automate, enabling a full self-service experience. This offers the service provider enormous benefit in terms of efficiency and effectiveness, as well as a positive client experience.

Contribution of Service Request Management to the Service Value Chain

All service value chain activities—all save the plan activity—involve service request management, as indicated below:

Engage	Regular communication is part of service request management, and it's used to gather user-specific requirements, define expectations, and offer progress updates.
Design and Transition	Service requests can be used to request and provide standard service modifications.
Obtain/Build	Purchase of previously authorised service components could be necessary to fulfil service requests.
Deliver and Support	The main goal of this value chain activity is to ensure users remain productive, and it occasionally significantly rely on fulfilling their requests.
Improve	The route for user suggestions for improvement, praise, and complaints can be provided through service request management. By giving information on trends, quality, and customer feedback about the fulfilment of requests, it also aids in improvement.

Table 2.1.1 Service Request Management Contribution

2.1.11 Difference between Standard Data Entry and Biometric Data Entry

The act of entering data into an electronic format, such as a computer or other electronic device, is known as data entry. It can be carried out either manually or automatically by a device or computer. The majority of data entry activities take a lot of time, yet for most businesses, data entry is a fundamental, essential duty.

Whereas, Biometrics is the measuring of a person's biological characteristics for the purpose of identifying them when it comes to computers and security. A biometric identification, for instance, is when a user logs in to a computer or a facility using their voice or fingerprint. This kind of system is considerably harder to spoof than a password since it is specific to the user. The face, hand, iris, and retina of a person are additional typical biometrics scanning techniques.

Therefore, Standard data entry can be of product, accounting, insurance claim, etc. and biometric data entry relates to human personal characteristics like eyes, fingerprints, etc.

Exercise

1. Explain two types of data in a biometric system.
2. What are the basic components of a biometric systems.
3. State the steps for collecting biometric data.
4. Fill in the blanks

   Biometric Data, Biometrics Technology, Service Request

   a. A_____is described as a request made by a user or the user's authorised representative to begin a service activity that has been agreed to as a regular component of service delivery.

   b. _____uses automated systems to recognize a person based on behavioural and biological (anatomical and physiological) characteristics.

   c. _____is information on a biological organism or group of organisms used in the biometric analysis, the study of biological systems or organisms.

Notes

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

3. Software Requirement for Biometric Operations

Unit 3.1 - Biometric Data Entry Software

SSC/N3023

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Inspect the data being entered from multiple sources to check authenticity and remove errors.
2. Identify the software requirements to collate data from a biometric perspectiv

UNIT 3.1: Biometric Data Entry Software

Unit Objectives

By the end of this unit, participants will be able to:

1. Classify different software needed for report writing including MS office suite or open office.
2. Distinguish between various types of data formats using database management software.
3. Verify data from multiple sources before entry.
4. Analyse the transcribed data with the source document for any corrections required like missing values, incorrect data types, etc.
5. Use identification and access control in biometrics for capturing end user information.

3.1.1 Report Writing

A report is a concise document written for a specific purpose and audience. It usually records and analyses a situation/problem, often recommending future action. A report should be factual, precise and well-structured. It should present facts impartially.

The specific format and information in a report may vary between organizations and departments. To ensure consistency in report writing, one should determine if there are any specific structure or report writing guidelines at the organization level and follow them.

A report's goal is to provide the reader with an organised path through the material so they may quickly and easily locate what they're looking for.

For this reason, reports usually have numbered sections and sub-sections accompanied by a clear and full contents page listing each heading. Page numbering is also essential.

Reports may include any or all of the items listed below:

- A description of a situation or sequence of events
- Interpretations of the significance of the referred situation or events, either an individual's analysis or an analysis informed by the views of others, should have an accurate reference when citing other parties
- An assessment of the data or study findings
- An assessment of the data or study findings;
- Relevant recommendations concerning a course of action
- Conclusions

Some of these elements may not be there in all reports.

3.1.2 Report Writing Software

For writing reports, the word processor is a widely used program. Word processors, such as Microsoft (MS) Word, come with several features. A word processor can be used for various purposes, such as preparing reports, invoices, letters, contracts, resumes, etc. For the ease of making documents, most word processors come with loaded templates that users can utilize to prepare documents quickly in a presentable format. For example – one can use a variety of templates available in the program to prepare a resume quickly.

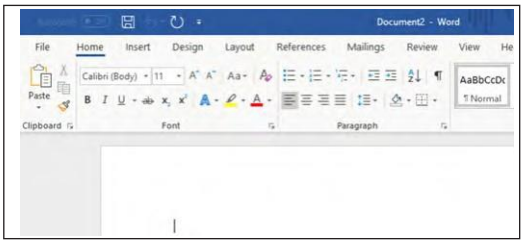

Fig. 2.1.1 MS Word

Following are some of the features available in word processors, making them useful for writing reports:

- One can change the font style, size and colour.
- It is easy to change the line spacing and alignment of text and images.
- One can even organize text in numbers and bullet points for easy reading.
- One can insert tables, charts, graphs, images, shapes, header, footer, etc. These make the report presentable and much easy to go through as compared to a plain text file.
- There are a number of templates or designs that one choose from to create a document. An appropriate template or design helps enhance the appearance of a document.
- One can change the page layout, including orientation, margins, indentation, columns, spacing, etc.
- While writing lengthy documents, such as a white paper, one may need to insert a table of contents, caption, bibliography, citations, footnotes, etc. One can find these features in most work processors.
- Once a document is prepared, it is critical to review it for accuracy. With the review feature available in a word processor, one can.
    - Conduct spelling and grammar checks using a specific language version, e.g. English India or English US
    - Use the thesaurus to substitute words
    - Check the word count
    - Insert comments, etc.

Apart from MS Word, one can prepare reports using PowerPoint also. However, PowerPoint presentations are suitable for preparing brief reports that highlight the key points.

For greater effectiveness, organizations may use both a word processor and PowerPoint, allowing the target audience to go through the summary in PowerPoint and read the details in MS Word.

Apart from Microsoft, one can use the Google software programs and similar other programs from other service providers that offer similar features; however, with some variations usually.

3.1.3 Database Management System

Databases are now used by businesses to store transactional data. Simply described, a database is a collection of structured data that has been kept on a certain computer system or server. Programmers and industry professionals have lauded the DMBS over the years for its well defined procedure for avoiding data redundancy and effectively storing data.

A Database Management System (DBMS) handles data creation and management. It also allows users to access and update data at any time. However, a corporation should select a database management software according to its unique requirements.

Using a DBMS, a company can update, create, define, and send queries to an administrative database instantly.

This can be transformative for companies that want to capitalize on various data formats and retrieval methods. With an attractive visual representation, a DBMS is ideal for small and large companies to manage precious data.

Types of Database Management Software

These can be broadly classified into four types. The most popular types of database management systems with examples include:

1. **Hierarchical**

   A hierarchical Data management solution stores data in a parent-children relationship node, each representing a particular entity. This type of database management software allows one-to-one and one-to-many relationships, i.e., a parent node can have one or multiple child nodes, whereas the children node can only have one parent node.

2. **Network**

   A network DBMS is a model that supports many-to-many relationships, which helps store real-life relationships between entities. It is an extension of the hierarchical data management soluution that allows modelers to design a more flexible model. In this type of DBMS model, the child nodes are represented by arrows.

3. **Relational**

   A relational DBMS is a model where relationships are based on the entities' data. Compared to hierarchical and network models, it offers greater flexibility and allows for more simplified relationships between entities, making it a popular choice among data modelers. Data stored in fixed structures can be organized efficiently using SQL.

4. **Object-Oriented**

   An Object-Oriented DBMS — as the name suggests — is based on object-oriented programming (OOP). It's a data management solution type where entities are represented in objects and stored in memory.

   It provides a unified programming environment and is compatible with various programming languages, including Java, C++, .Net, and Visual Basic, to name a few.

DBMS in Biometric devices

A Database Management Systems can be used to Archive, Store, Retrieve, Edit and Manage the biometric data. Relational Database Management System (RDBMs) is the best approach for storing and securing biometric data in biometric devices.

Here are some Relational Database Management Systems (RDBMs) that can be used for storing the Biometric Data which will guarantee security, reliability and ease of Biometric Data storage and retrieval. They are;

1. Maria DB
2. MSSQL
3. MySQL
4. Oracle
5. PostgreSQL

3.1.4 Data Verification

The dependability of the data is increased by verifying or confirming the accuracy of the replies provided using the Data Entry window, such as filling paper surveys. To make sure the original operator did not make any mistakes, data can be double-entered to be validated. Though it might be a time-consuming procedure, this is a very effective approach to ensure that data is almost error-free.

Typically, a second person inputs some or all of the data submitted by the first person to double-check it. As operators frequently make the same mistakes, it is not advised for users to double-check their own information.

Any discrepancies between the first and second times of data entering are found during the verification phase. Data entering is interrupted and both sets of data are presented if any discrepancies are found, enabling the verifier to enter the right value again.

Before the verification process can begin, the criteria must be defined.

One of the Key Result Areas for an Operator is how much time it takes to enrol a Enrolee/ Enrolee. The Operator needs to balance speed of entering data with the quality of information that is fed into the system. At no instance can speed be more important than quality.

However, the Operator can do few things that can reduce the processing time for each individual. For example, Operators can enter demographic details of Enrolees during off hours. They usually capture the demographic details when the biometric devices are connected to the enrolment station. This reduces the life of the biometric devices. A domino impact of entering data in off hours is that it speeds up enrolment process, reduces device waiting time and also reduces the waiting time for Enrolees, thus impacting crowd management.

Another approach is to ask the Supervisor to load up pre-enrolled data on his or her laptop/ desktop. Pre enrolment data helps in reducing the cycle time for enrolment at centre significantly.

Compare and Correct Data

Track processing time for each individual One of the Key Result Areas for an Operator is how much time it takes to enrol a Enrolee/ Enrolee. The Operator needs to balance speed of entering data with the quality of information that is fed into the system. At no instance can speed be more important than quality. However, the Operator can do few things that can reduce the processing time for each individual. For example, Operators can enter demographic details of Enrolees during off hours. They usually capture the demographic details when the biometric devices are connected to the enrolment station. This reduces the life of the biometric devices. A domino impact of entering data in off hours is that it speeds up enrolment process, reduces device waiting time and also reduces the waiting time for Enrolees, thus impacting crowd management. Another approach is to ask the Supervisor to load up pre-enrolled data on his or her laptop/ desktop. Pre enrolment data helps in reducing the cycle time for enrolment at centre significantly. Comparison of transcribed data, as displayed on a visual screen, with the source document and corrects any errors Operator Reviews Data with the Enrolee After capturing all mandatory/required data (i.e., all the colours next to the screen-names are green), the Operator should ask the Enrolee to observe and verify the recorded data and confirm that all details that have been captured are correct. There should be a monitor facing the Enrolee and displaying the Review screen with Enrolee's data. The Operator must read out the text on the screen to confirm that the data is correct.

1. **The Operator must reconfirm the following fields :**
   - Spellings of the Enrolee's Name
   - Correct Gender
   - Correct Age/Date of Birth
   - Address – Pin Code; Building; Village/ Town /City; District; State
   - Relationship Details – Parent/Spouse/Guardian ; Relative Name
   - Accuracy and Clarity of Photograph of the Enrolee
2. In case of any errors, Operator must correct recorded data and review again with the Enrolee. If no corrections are required, resident will approve the data. Correction Process in Enrolee's Data For correction in any of the data of a Enrolee, the Operator must use Correction menu on software client. In case of Aadhar the Enrolee data can be corrected within 96 hours of the Enrolee's enrolment and in the presence of the Enrolee.
   - All corrections in a Enrolees data are restricted to only one time.
   - The following requests for changes are included in the scope of the Correction Process:
   - All demographic fields i.e., Name, Address, Gender, Date of Birth / Age .
   - Information sharing consent.
   - Relationship to Enrolees.

- Mobile
- Email Address
- NPR Receipt Number
- Relationship Details
- Introducer Name
- If originally the resident was enrolled as a child below 5 years of age it is invalid to correct the resident age to above 5 years because for above 5 we require biometric data as well which would not have been captured during enrolment.
- The previous Enrolment ID of the resident needs to be entered for correction of resident's old data. Check resident's acknowledgement letter for taking Enrolment number, date and time of enrolment for correction.
- PoI, PoI A and Parent/Guardian's acknowledgement letter will also be required at the time of correction process depending on the type of correction.
- A change in Name would require either a verified Enrolment Form and PoI document or an Introducer's Name and UID. A change in Address would require either a verified Enrolment Form and PoA document or an Introducer's Name and UID. A change in verified DoB would require a verified Enrolment Form and DoB certificate. If the correction is in data for a child below 5 years of age, then parent details of relationship type, relative name and EID/UID of parent/guardian is also mandatory.
- Only the fields that need a correction are entered in the Correction menu of the software. Fields that are good in original enrolment are not to be retyped during Correction.
- The resident's photo is also captured during correction process.
- The correction in data will be reviewed with the resident and any one of the biometrics of the resident (provided in drop down menu on client) will also be taken to confirm that the resident is OK with corrections.
- In case the resident is child below 5 years, the biometric of the parent/guardian whose details are entered in the relationship fields, will be taken. The Operator will sign off the enrolment and Supervisor, Introducer sign off will be required in biometric exceptions and Introducer based verification respectively.
- An acknowledgement and consent of correction will be printed at the end of correction process along with the Enrolee's photo. The acknowledgement of correction will be signed by Operator and handed over to Enrolee. The consent will be signed by the Enrolee and filed by the Operator along with the other documents of the Enrolee.

3.1.5 Analysis of Data

Operator Reviews Data with the Enrolee

After capturing all mandatory/required data (i.e., all the colours next to the screen-names are green), the Operator should ask the Enrolee to observe and verify the recorded data and confirm that all details that have been captured are correct.

There should be a monitor facing the Enrolee and displaying the Review screen with Enrolee's data. The Operator must read out the text on the screen to confirm that the data is correct.

1. **The Operator must reconfirm the following fields :**
    - Spellings of the Enrolee's Name
    - Correct Gender
    - Correct Age/Date of Birth
    - Address – Pin Code; Building; Village/ Town /City; District; State
    - Relationship Details – Parent/Spouse/Guardian ; Relative Name
    - Accuracy and Clarity of Photograph of the Enrolee
2. In case of any errors, Operator must correct recorded data and review again with the Enrolee. If no corrections required, resident will approve the data.

Correction Process in Enrolee's Data

For correction in any of the data of a Enrolee, the Operator must use Correction menu on software client. In case of Aadhar the Enrolee data can be corrected within 96 hours of the Enrolee's enrolment and in the presence of the Enrolee.

- All corrections in a Enrolees data are restricted to only one time.
- The following requests for changes are included in the scope of the Correction Process:
- All demographic fields i.e., Name, Address, Gender, Date of Birth / Age
- Information sharing consent
- Relationship to Enrolee
- Mobile ▪ Email Address ▪ NPR Receipt Number ▪ Relationship Details ▪ Introducer Name
- If originally the resident was enrolled as a child below 5 years of age it is invalid to correct the resident age to above 5 years because for above 5 we require biometric data as well which would not have been captured during enrolment.
- To update the resident's old data, the resident's previous enrollment ID must be entered. Verify the resident's acknowledgement letter to make sure the enrollment information, including the enrollment date and time, is correct.

- PoI, PoI A and Parent/Guardian's acknowledgement letter will also be required at the time of correction process depending on the type of correction.
- A change in Name would require either a verified Enrolment Form and PoI document or an Introducer's Name and UID. A change in Address would require either a verified Enrolment Form and PoA document or an Introducer's Name and UID. A verified Enrolment Form and DoB certificate are required for any changes to a validated DoB. If the data has to be corrected for a kid under the age of five, parent details, including relationship type, relative name, and EID/UID of the parent or guardian, are also required.
- Only the fields that need a correction are entered in the Correction menu of the software. Fields that are good in original enrolment are not to be retyped during Correction.
- The resident's photo is also captured during correction process. • The resident will be consulted on the data adjustments, and any of the resident's biometrics (given via a drop-down choice on the client) will also be captured to confirm that the resident is okay with the corrections.
- If the resident is a kid under the age of 5, the parent or guardian whose information is submitted in the relationship areas will have their biometric taken. The enrollment will require the operator's approval, and for introducer-based verification and biometric exceptions, the supervisor's approval will be necessary.
- At the conclusion of the correction procedure, the photo of the enrollee and an acceptance and consent of rectification will be produced. Operator will sign the acknowledgement of rectification before giving it to the enrollee. The enrollee will sign the consent and the operator will submit it alongside the enrollee's other paperwork.

3.1.6 Biometric Access Control

- Access control stops unauthorised individuals from entering your property. Since biometric access control has gained popularity in recent years, many of our prospects and clients have enquired about it. "How does biometric access control operate and what is it?" they have questioned.
- A contemporary security technique that can offer a number of advantages in a variety of businesses is biometric access control.
- Biometrics is the technological examination of biological data. This information frequently pertains to certain physical characteristics that a person may possess. Therefore, biometric access control is the process of granting or denying admission to a facility or a specific section of a building using this biological data.
- What biological information and physical characteristics are we referring to? Biometric access control frequently considers characteristics that are particular to each person. This incorporates voice, facial recognition, retinal scans, and/or fingerprints.

Working of Biometric Access Control:

- Specific biological data, such as fingerprints, are analysed via biometric access control.
- There is a creation of a database comprising all the biological information from those with access.
- When individuals utilise the access control system, they are scanned.
- If their biological information is known, they are given access.
- They are not permitted access if there is no match for their biological information.

Exercise

1. Explain briefly what report writing is.
2. Explain types of data management softwares.
3. What is biometric access control?

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=WdftZZ4G0Vg

Biometric Data Entry Software

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

4. Biometric Data Entry Process

Unit 4.1 - Biometric Data Entry Process

SSC/N3023

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Design suitable plan of action to capture various details like facial expression, iris, fingerprints, electronic signatures, and press print of individuals.
2. Evaluate helpdesk feedback system and its importance with appropriate SLA.
3. Collate valid demographic data of individuals including proof of address, identity proof, etc. for database maintenance.
4. Observe the use of facial expression, iris of individuals and their fingerprint for biometric entry.
5. Perform biometric processing to include prints, electronic photographs, electronic signatures, and press print.
6. Undertake the process of scanning documents and transcription of data into system.
7. Maintain proper security, storage and back up of data files.

UNIT 4.1: Biometric Data Entry Process

Unit Objectives

By the end of this unit, participants will be able to:

1. Discuss the adequacy of existing helpdesk feedback systems.
2. Discuss methods of the data entry process.
3. Collate valid demographic data of individuals including proof of address, identity proof, etc. for database maintenance.
4. Observe the use of facial expression, iris of individuals and their fingerprint for biometric entry.
5. Perform biometric processing to include prints, electronic photographs, electronic signatures, and press print.
6. Undertake the process of scanning documents and transcription of data into system.
7. Maintain proper security, storage and back up of data files.

4.1.1 Helpdesk Feedback System

A helpdesk, also known as a service desk, is a single point of contact for a company's internal and external inquiries, offering consolidated information and support management services. Through the use of a ticket management system and a helpdesk software solution, businesses can easily automate the process of resolving client complaints, which speeds up the process significantly.

The helpdesk systems on the market may be categorised in a variety of ways. For instance, based on their deployment, the size of the company, and the role of customer service. The deployment, company size of the target customers, and source code accessibility are now the main criteria used to categorise different types of helpdesk software.

Importance of Helpdesk Feedback System

Customer Satisfaction

Customers want their query to resolve quickly and with minimal effort. Delight your customers by ensuring First contact resolution (FCR). Keep the customers informed by sending out timely updates about the status of their complaint. Moreover, make it easier for the customers to reach out for support via the channel of their preference. A helpdesk ticketing system creates a ticket for every customer interaction irrespective of the platform through which it originates.

Agent Productivity

Automating the repetitive task to help the agents to do more complex yet fulfilling work. Using the knowledge base, the agents can access a repository of information to help them solve the customer complaints effectively. Also, having a unified interface will enable the support executives to get a 360-degree view of the customer. Thus, enabling them to serve the customers better.

Business Operations

Streamline the operation to meet the SLAs and prioritize certain actions when required. Empowering the supervisor with intuitive graphs and data points to effectively monitor the functioning of the contact center. The supervisor gets to have a bird's eye view of the operations and based on that data, can make informed decisions.

Helpdesk Key Performance Indicators

The help desk KPIs are the most significant quantifiable outcome that shows whether your help desk support activities are successful or unsuccessful. Without them, it is impossible to know for sure what is effective. Additionally, choosing the appropriate help desk KPIs enables the help desk support team to concentrate just on what's most crucial.

There are a number of helpful measures that may be used to evaluate help desk effectiveness, but the top five KPIs are listed below.

1. **Contacts Received:** Knowing the amount of incoming inquiries is crucial since the goal of a help desk support team is to address issues and offer customer care. Using this information, one may manage workforce numbers and get a sense of the team's overall workload. Along with channels, contact tracking should be divided into significant time periods, such as per hour, per week, or per season (phone, chat, email, social media). One can predict the ebbs and flows of incoming requests by using data to identify patterns.
2. **Reaction and Wait Times:** For both service provider and the customers, time is money. Everyone can relate to how annoying it may be to be on the receiving end of a phone call or online chat and wonder whether anything is getting done. Wait time is the "down" time while the agent is processing the request, whereas response time is the amount of time between the first request and the first interaction. The clients will become more dissatisfied the longer these durations are.
3. **Rate of Resolution:** How quickly does the help desk support staff respond to inquiries? Are they resolved after the initial touch, or do they hang around for an arbitrary period of time? In a study by Harvard Business Review, lowering consumer effort was shown to be the most important component in building customer loyalty. A high first contact resolution (FCR) rate significantly increases customer satisfaction.
4. **Cost Per Ticket:** Companies must use their resources as efficiently as possible in the highly competitive climate of today, and help desk support is no exception. By dividing service desk operational costs by the total number of tickets processed in a particular time period, one may calculate the cost per ticket. Spending less money or handling more tickets are the two methods to increase cost per ticket. Both can, of course, help in improve their statistic, but overextending the staff could cost one dearly. As the organization assess the cost per ticket measure of the help desk, it's critical to keep in mind the initial objective, which was to assist the company.
5. **Customer Satisfaction:** The major goal of a help desk support team is to keep customers happy, hence this is the most important KPI. Customer surveys are the most direct method of measurement, although all other KPIs have an influence on this objective. For an accurate picture, make sure to compute the proportion of returned surveys to the total number of surveys issued.

4.1.2 Data Entry Process

The process of entering values into computer software in a systematic way is known as data entry. It can be manual or automated, i.e. handled by a person or a machine. Data entry by an operator is known as manual data entry; if done by a machine, it is known as automated electronic data entry. The process of data entry:

- **Data capturing and entering -** This type of data entry operation focuses on collecting data from different sources – offline or online. The employer often provides this information.
- **Data cleansing -** Data cleansing is a type of operation during which information is filtered to remove duplicates or inaccurate data. This type of data entry operation makes sure that information stored in the database is not only up-to-date but free of errors.
- **Data processing -** Data processing's main focus is not only to store and filter information but to edit information in a way that fulfils its particular purpose. In this way, data processing is also helpful in analyzing information stored so that it can be used later. Some notable tasks of data processing include accounting and photo editing.
- **Data classification -** For the organization of information, data classification is required. This operation is about categorizing data under their appropriate attributes—hence 'classification'. Organizing business cards, for example, is part of this data entry operation type.
- **Data conversion -** Data conversion is about converting one format to another. This means, for instance, changing a word file into PDF format. Typing on a word file coming from a handwritten document is also another illustration of how data conversion operation works.
- **FormaEng and editing operations -** Data formatting operations use the operator's English grammar skills in order to correct grammatical errors and spelling mistakes in the database. This also means this type of operation combines the knowledge in English with that of software such as MS Word in order to correctly format the data to the needs of a company.

4.1.3 Capturing Demographic Data

Guidelines for Demographic Data Capture

- Enter the demographic details of the Enrolee from the verified enrolment form.
- Enter all the data in the Aadhar software as provided in enrolment form. Even the nonmandatory fields like mobile number and email ID are important. If necessary, such as in the event of returned mail, UIDAI may contact the Enrolee using these data. Therefore, if the enrollee has supplied this information, do not leave these fields blank. Similar consents for banking and information sharing should be properly filled out in the software client in accordance with the enrollment form.
- If utilising pre-enrolment data, the operator will use the pre-enrolment ID to get the enrollee's demographic information. Verify the information obtained using the pre-enrolment ID against the information on the enrollment form to ensure that it belongs to the enrollee. Don't only verify the name; rapidly double-check the gender, age, and other pertinent information as well.

- Verify and update the pre-enrolment information in accordance with the information on the validated enrollment form. There can be transliteration, spelling, and data completeness issues with pre-enrollment information that need to be fixed.
- When gathering demographic information, pay close attention to data aesthetics. When entering data, be careful not to use extra spaces, punctuation, or capital or tiny characters.
- Leave those non-mandatory fields blank where no data is provided by Enrolee. Do not enter N/A, NA etc. in fields where Enrolee has not provided any data.
- Filling Father / Mother / Husband / Wife / Guardian field is not mandatory for Enrolees above the age of 5 years in case the adult is not in a position or does not want to disclose. Then select checkbox "Not Given" in "Relationship to Enrolee".
- In case of children below the age of 5 years one of the parents' or guardian's name shall be recorded and UID or Enrolment ID (either of the two numbers) shall be recorded. This is mandatory.
- It is not compulsory for only father's name to be recorded against the 'parent's name.' Mother's name can alone be recorded for the 'parent's guardian's' name if so desired by the parent.
- Enrolment of the parent is mandatory prior to the child. If the child's father /mother / guardian has not enrolled or does not possess UID at the time of enrolment, the enrolment of that child cannot be done.
- For Head of Family (HoF) based verification Name, EID/UID of HoF and Relationship Details of the family member to HoF are mandatory details to be entered.
- Once Demographic Data is entered, Operator will capture the Biometric data of the Enrolee.
- Collect and enter valid demographic data of individuals including proof of address, identity proof, etc As mentioned previously, capture all demographic data including proof of identity, proof of address, proof of relationship, proof of birth etc from verified enrolment forms only. If data is pulled from an enrolment id, ensure that the data belongs to the enrolee by reconfirming with the enrolee
- Good conflict resolution skills can help one contribute to creating a collaborative and positive work environment. With the ability to resolve conflicts, one can earn the trust and respect of co-workers.

4.1.4 Hardware Devices

The hardware tools used to enrol residents fall into one of two categories:

1. Biometric Devices
2. Non-Biometric Devices

The hardware tools used to enrol residents fall into one of two categories:

1. Fingerprint Scanner
2. Iris Capturing Device
3. Digital Camera

The data is entered, read, stored, printed, scanned, and copied using non-biometric devices. To address power-related issues, tools like electric generators and UPSs are employed. These tools are listed below.

1. Computer
2. Printer
3. Storage Devices (CD/DVD /Portable hard disk/Pen Drive)
4. GPS Dongle
5. Scanner
6. Photocopier
7. UPS
8. Universal Serial Bus (USB) Hub
9. Electrical Generator

4.1.5 Fingerprint Scanner

A Fingerprint Scanner is a digital fingerprint capturing device which scans and captures fingerprints with ease. Using a scanner is a low-cost and an effective method. Fingerprint Scanner is connected to the computer through the USB port. The fingerprint is scanned and images captured through a transparent flat glass plate. This plate is called the Platen, on which the Enrollee places his or her fingers are placed. The operator guide the user to keep the fingers in proper place. The image so created by the scan is stored in the computer. With the Slap Fingerprint Scanner, all four fingers of the hand are photographed simultaneously. Then, both thumbs' fingerprints are simultaneously taken.

Non-biometric devices are used to enter, read, save, print, scan, and copy the data. Tools like electric generators and UPSs are used to handle power-related difficulties. Here is a list of these instruments.

Fig. 4.1.1 Figerprint Scanner

Through a computerised fingerprint capture device, often known as a fingerprint scanner, fingerprints may be quickly scanned. The fingers are put on a transparent glass plate known as the Platen, which is used to scan the fingerprints. The computer stores the produced image.

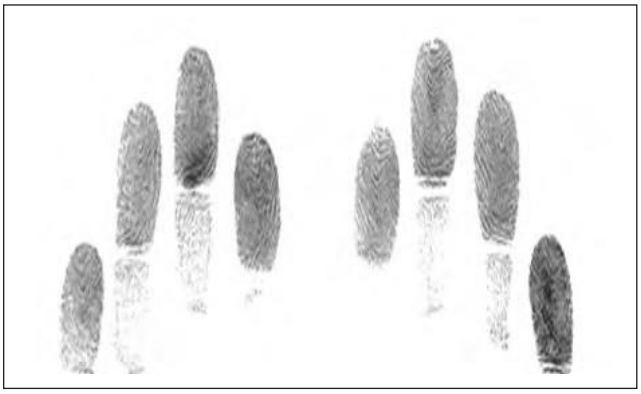

Fig. 4.1.2 Figerprint Sample

The following steps are followed generally how to capture the fingerprint image:

1. Left Hand Fingerprint
2. Right Hand Fingerprint
3. Two Thumb Prints
4. Auto capture
5. Visual Checking

Method of capturing 10-prints on live scan sensor and inkpads

All 10 fingers on both hands must have their fingerprints recorded while taking the fingerprint image. The left hand's four fingers, followed by the right hand's two thumbs, and then the left hand's four fingers again must be used to capture the fingerprints. The actions listed below should be taken by the Operator in order to get the enrollee's fingerprint image.

1. **Capture fingerprint of the left hand:** First, capture the fingerprints of the four fingers of the left hand except the thumb simultaneously.

Fig. 4.1.3 Capturing Fingerprints of the Left Hand

The Enrolee should place the four fingers of the left hand on the platen and apply a little pressure with the right hand so that the fingers have a good contact with the glass surface.

2. **Capture fingerprint of the right hand:** First, capture the fingerprints of the four fingers of the right hand except the thumb simultaneously

Fig. 4.1.4 Capturing Fingerprints of the Right Hand

The Enrolee should place the four fingers of the right hand on the platen and apply a little pressure with the left hand so that the fingers have a good contact with the glass surface.

3. **Capture the two thumb prints:** Thumbprints of both the hands are scanned and captured simultaneously.

   The Enrolee places both thumbs on the platen. Capturing the two thumd prints and applies a little pressure so that the thumbs have good contact with the surface. In case the Enrolee finds putting pressure difficult, the Operator should ask the Enrolee to stand and press the thumbs or take the Enrolees permission and put the pressure on his thumbs.

Fig. 4.1.5 Capturing Fingerprints of Both Thumbs

4. When scanning the fingers and thumbs, the Enrolee must use the maximum area on the glass to get an accurate scan image of the fingerprint. Also the entire finger should be pressed against the glass and not just his fingertips. When taking the thumb prints, ensure that the thumbs are at a one inch distance from each other.
5. The Operator need not use any mouse or press any button to scan the fingerprint. The fingerprint scanner automatically captures the fingerprint when the fingers are placed on the platen. If the fingerprint image is successfully captured, the scanner indicates the successful grab of the image, and the scanner software captures the fingerprints. Each finger will be given a successful signal by the scanner before the programme is able to record the fingerprint picture. When the force capture tab in the enrolling programme is activated, the Operator must manually capture the fingerprint if it is not done automatically by pressing the Force Capture button.
6. In the application programme, the Operator should lastly visually examine the fingerprint photos for quality and common issues. He or she should repeat the preceding methods if there are any issues.

4.1.6 Digital Camera

Digital facial photographs are taken with a digital camera. Through a USB (Universal Serial Bus) connector on a laptop or desktop computer, it is linked to the device. The mounting base and auto-focus lens make up the digital camera. Images are shown as soon as they are captured.

Fig. 4.1.6 Digital Camera

The following are the steps for collecting face biometric data:

- **Verifying the Enrollee's Position:** The resident should be facing the camera directly when the photo is taken. It is not permissible to tilt or rotate the head.
- **Camera Adjustment:** It is suggested that the Operator adjust the camera rather than moving the enrollee to get the proper angle and posture.
- **Verifying the Expression of the Enrollee:** The Operator must make sure the enrollee is using a neutral expression. The resident's lips should be shut and both eyes must be open during the capture. The enrollee, for instance, shouldn't smile when being photographed.

- **Examining the shadow/reflection:** There should be enough light to capture the face accurately. The Operator must make sure the enrollee's face is not cast in shadow and that there is no reflection in his or her eyes. To prevent shadows behind the eyes, a second light source should be put in front of the enrollee.
- **Examining the visibility of the pupil and iris through eyeglasses:** If the enrollee is wearing eyeglasses, they must be worn for the photo to be taken. However, the Operator must make sure that the iris and pupil are both easily visible.
- **Manually taking the photo:** To take the face picture, the operator must press a button on the Aadhaar Enrolment Client application programme. In the case of a photograph, there is no automatic capture process.

4.1.7 Iris Capturing Device

Similar to taking a standard photo, the process for getting an image of the iris also uses infrared light, which is almost imperceptible to human eyes. The iris capture tool takes a picture of the iris and creates a file that may be saved in a computer.

Most people agree that the iris is the biometric that is the most precise. Additionally, there are two different biometric feature sets due to the fact that the iris patterns of each eye are unrelated.

A biometric device is the iris-capturing gadget. There are two different types of iris capture devices.

1. **Single Iris Capturing Device:** Single Iris Capturing Device can capture any one eye at a time.

Fig. 4.1.7 Single Iris Capturing Device

2. Double Iris Capturing Device: Double Iris Capturing Device can capture both the eyes at a time.

Fig. 4.1.8 Double Iris Capturing Device

Steps to Capture Image of Iris

Follow these steps to capture an iris biometric using an iris capturing device:

- **Examining the enrollee's eyes:** If the iris image cannot be taken because one or both eyes are missing, there is a bandage covering one or both eyes, or there is another sickness or deformity, this information must be entered into the Aadhaar Enrolment Client application software.
- **Verifying the enrollee's posture:** Have the enrollee take a fixed seat position. The position should resemble that of shooting a portrait shot.
- **Aiming the Iris Capturing Device:** Direct the device's aim onto the enrollee's eye. Holding the gadget steadily is necessary. If the resident is needed to hold the device, the enrollment operator may assist the enrollee in maintaining a solid grip on the device.
- **Examining the lighting in the space:** The iris capture procedure is sensitive to the level of illumination in the space. Ensure that the enrollee's eyes are not immediately exposed to artificial or direct light. The light source being utilised to take facial images should be turned off when capturing irises.
- **Checking the image quality:** The programme may assess the iris image's quality after it has been captured. To give the Operator feedback while the image is being captured, a preliminary image quality evaluation would be performed. If the iris image that was obtained is of low quality, the device notifies the Operator. Try again to obtain a high-quality photograph of the iris if the first attempt produced a subpar image.

4.1.8 Electronic Signature

An electronic signature is any type of online or computerized signing in which the signer acknowledges the terms of the signed document, such as an email message, a contract clause acceptance button, or a word processing document. It's a broad notion that refers to the legal concept of electronically signing documents.

The electronic signature does not require that the signature or the signatory's acceptance be linked to a person's identification. Furthermore, it is formed only under the authority of the signatory, with no influence over the device, certificate, or system.

When a signer electronically signs a document, the signature is created using the signer's private key, which is always securely kept by the signer. The mathematical algorithm acts like a cipher, creating data matching the signed document, called a hash, and encrypting that data.

Fig. 4.1.9 Digital Signature Device

4.1.9 Scanner

A device that captures images from photographs, posters, magazine pages, and similar sources, etc is known as Scanner. The captured image can be displayed and edited. Scanners can be used to scan black-and white and color documents.

Types of Scanner

- Drum Scanner
- Flatbed Scanner
- Film Scanner
- Hand Scanner
- Document Scanner

Fig. 4.1.10 Scanner

4.1.10 Photocopier

A photocopier or a Xerox machine makes copies of documents and other visual images quickly and cheaply.

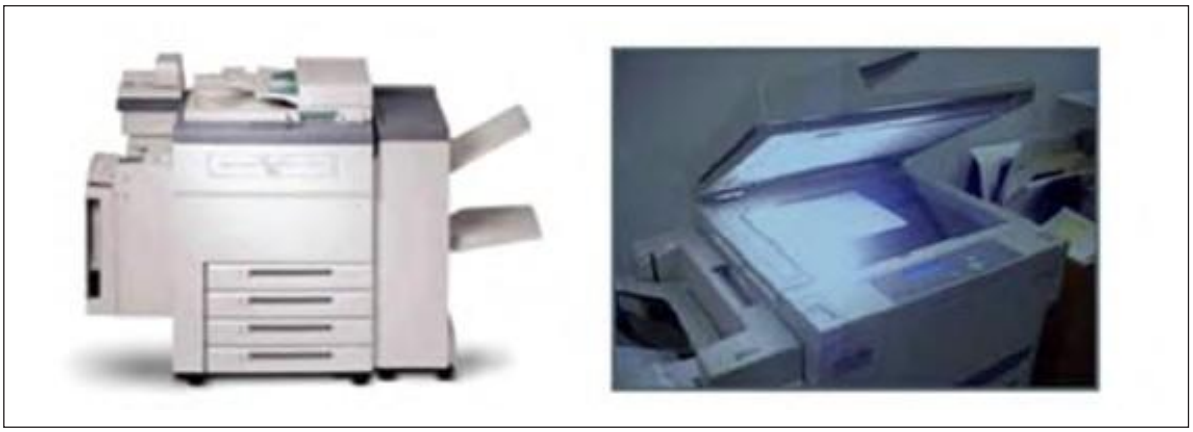

Fig. 4.1.11 Photocopier

4.1.11 Guidelines for Data Security and Backup

Security

All copies of your data, including your working data set, backup copies, and archived copies, need to be taken into account in terms of security.

- Network security
  - Avoid posting private information online.
  - Store private information on a computer not linked to the internet
- Physical Security
  - Only allow authorized personnel to solve computer issues
  - Only allow authorized personnel to solve computer issues
- Computer Systems & Files
  - Update your virus protection.
  - If you must transfer secret material through email or FTP, encrypt it beforehand.
  - On computers and data, use secure passwords.

Storage & Backup

The maintenance of backup copies of your data is among the most crucial data management jobs. Data loss due to hard disc failure or unintentional deletion is a serious possibility.

- Remember to use the Backup 3-2-1 Rule
  - Make 3 copies of your data—2 copies are insufficient!
  - Two distinct formats, such as an internal hard drive with a backup cassette or a DVD (short-term) plus a flash drive
  - 2 physical backups and 1 cloud backup are kept off-site.
- Backup options
  - Departmental or institution server
  - Tape backups
  - University archives
  - Cloud storage
  - External hard drives
  - Discipline-specific repositories
  - Hard drives - personal or work computer

4.1.12 Security of Biometric Storage System

On-device storage

Biometric templates are often stored on local devices, as with most fingerprint readers on mobile devices. This type of biometric storage is exceptionally secure because it does not store sensitive data on servers with large databases. As a result, only the device can be hacked, which, in the rare case that it is successful, will cause damage at a microscopic scale. If locally-stored biometric data does get hacked, the device's internal storage should be deleted (remotely if need be) as soon as possible.

Database server

At times, local device storage is not feasible. For example, large corporations who use biometric authentication to grant special user access and permissions might prefer biometric database storage instead of local device access only. This allows companies to grant user-specific access in multiple locations and tracks behaviour to help suspicious flag activity. Examples of suspicious activity might include users who access secured areas at odd hours of the day or those who interact with the information in unexpected patterns.

Biometric database servers are more cost-effective than other storage options but have a higher security risk. Because servers house multiple templates (often thousands or even hundreds of thousands), their susceptibility to hackers is also high. Should information be compromised, many people and their irreplaceable biometric information will be at risk for malicious behaviour. Though encryption significantly improves biometric security, determining who has access to the encrypted data (and how they use it) is the real crux of the issue.

Portable token

Biometrics stored on portable tokens — security cards or USB drives, for example — work in the same way that on-device biometric storage does. Biometric information is stored on a single device, and that device must be presented during authentication for verification purposes. Biometric tokens tend to be a bit more costly to implement than the alternative because they require both the token and a separate biometric scanner, though the added step also adds another line of security to the mix.

Distributed data storage

Another method of double-backed biometric template storage is called distributed data storage. This method stores biometrics on a local device and a server, both of which must be accessed concurrently for authentication. Because of the split nature of this biometric storage method, hacking biometrics that utilizes distributed data storage is nearly impossible to hack and, therefore, highly secure.

Biometrics and blockchain data storage

For optimum security, personally identifiable information (like biometric templates) should be encrypted and stored off the blockchain instead of in off-chain storage systems. Encrypted biometric templates can further be protected by splitting the information into "shares" and storing each individual "share" in separate locations. For example, part or "share" of a person's biometric template can be stored on the individual's mobile device and the other on a server or blockchain.

Biometric data can also be stored via blockchain though not without special consideration. Specifically, biometric data itself is not blockchain compatible (one does not want the entire scope of the internet to access their biometric profile, after all), but encrypted, segregated bits of biometric data certainly are.

A blockchain is a form of decentralized data storage. The concept of blockchain comes from the notion that publically stored blockchain data cannot be manipulated without altering other data sets along the "chain". For example, if the same data set is accessible throughout the entire digital sphere, alterations to the data should be easily traceable. This makes it extremely difficult for hackers to succeed in an attack, thus increasing data security through a decentralized approach.

Tokenized biometric data

Biometric data security is at the forefront of biometrics discussions and concerns. Yes, individuals must be careful with whom they share their biometric data, but the real burden falls on biometrics companies entrusted with such valuable information. Before any company or organization acquires user biometric information, their biometric software should be tested for accuracy and security.

Many biometrics companies opt for tokenized biometric data rather than encrypted to remedy this concern. Unlike encryption, which uses a unique mathematical formula to alter data in a standardized manner, tokenized biometric data use "tokens" or randomized alphanumeric characters to hold the place of sensitive data. Because they are entirely random, tokens cannot be decrypted. Instead, the token is either encrypted or destroyed after a single-use.

There are many ways biometric data is stored, but one thing remains constant: they rely on encryption to protect user data. However, anything encrypted can be decrypted or returned to its original form. Furthermore, by its design, encrypted data can be reversed using the same algorithm used to alter it in the first place. In other words, no matter how advanced the mathematical formula is, encrypted data is only as secure as those with access to it.

Exercise

1. Explain the steps to capture finger data.
2. What is an electronic signature?
3. What is an Iris Capturing Device?
4. Fill in the Blanks:

   Electronic Signature, Photocopie, Fingerprint Scanner, Data Entry

   a. The process of entering values into computer software in a systematic way is known as _____.

   b. A_____makes copies of documents and other visual images quickly and cheaply.

   c. A_____is a digital fingerprint capturing device which scans and captures fingerprints with ease.

   d. An_____is any type of online or computerized signing in which the signer acknowledges the terms of the signed document, such as an email message, a contract clause acceptance button, or a word processing document.

Notes

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

5. Troubleshooting in Biometric Data Entry

Unit 5.1 - Biometric Data Entry Problems and Solutions

SSC/N3023

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Identify typical problems raised by customers.
2. Understand why manual data entry errors happen and learn ways to avoid them.
3. Examine the common errors in data entry including transcription and transposition error.
4. Observe nature of errors like volume spikes, slow turnaround, format issues, etc. and their root causes.
5. Determine principles of biometric system error rates including false accept, false reject, false match, false non match, equal error rate, detection error trade-off curve.
6. Plan an error mitigation program.

UNIT 5.1: Biometric Data Entry Problems and Solutions

Unit Objectives

By the end of this unit, participants will be able to:

1. Identify typical problems raised by customers.
2. Understand why manual data entry errors happen and learn ways to avoid them.
3. Examine the common errors in data entry including transcription and transposition error.
4. Determine principles of biometric system error rates including false accept, false reject, false match, false non match, equal error rate, detection error trade-off curve.
5. Plan an error mitigation program.

5.1.1 Process of Biometric

Consumer electronics, point-of-sale applications, corporate and public security systems, and biometric authentication are all growing in popularity. However, Biometric verification has been driven by convenience rather than security, as there are no passwords to memorize or security tokens to carry. In addition, some biometric approaches, such as movement patterns, can work without requiring physical touch with the individual being validated.

The following are components of biometric devices:

- A scanning device to record the biometric element being validated;
- Software to transform scanned biometric data into a defined digital format and compare match points of observed and recorded data; and
- A database to securely store biometric data for comparison.

Although biometric data can be stored in a centralized database, current biometric systems frequently rely on capturing biometric data locally and then cryptographically hashing it to allow authentication or identification without direct access to the biometric data.

5.1.2 Common Biometric Data Entry Errors

Biometric technology and systems are becoming increasingly popular in the public and private sectors. Biometric technology (such as facial recognition, voice recognition, fingerprint scanning, and iris scanning) is becoming increasingly affordable, sophisticated, and accurate. As a result, they are becoming increasingly ingrained in people's everyday lives and dealings with the government.

Biometric systems are improving in effectiveness as technology progresses, but they are not a perfect form of authentication or identification. The following are some of the drawbacks of biometric systems.

Inability to Enrol

This error occurs when a template for biometric data cannot be correctly constructed. There are a various potential causes for this, including low-quality reference data (for example, due to sensors or bad ambient circumstances – such as lighting – at the time of registration) or a person's physical or medical condition preventing them from participating in the system. Ensuring reasonable enrollment rates is critical to a biometric verification or authentication system's performance.

Cultural or religious reasons, technological challenges and physical or medical ailments may restrict a group's or individual's capacity to participate in or enrol in a biometric system.

False acceptance and rejection rates

There are two types of faults that biometric systems can make. When the system mistakenly matches an input to a non-matching template, it is called a "false positive," whereas when the system fails to identify a match between an input and a matching template, it is called a "false negative."

Such mistakes in a biometric system might happen for a variety of reasons. For example, individuals with comparable biometric traits (for example, identical twins may be difficult to differentiate based on face biometrics) may have similar biometric characteristics, or user engagement with a sensor may vary between the enrollment and recognition stages (for example, a person may pose differently). In addition, other variables, such as ageing, injuries, or medical problems, might cause changes in a person's biometric characteristics between the time of enrolment and the time of enrollment.

A probabilistic computation is used to match a person with a template stored in a biometric system. The ethnic or age features of the sample data used when the system was trained, as well as the lighting or posture of the subject at the moment of registration or subsequent identification, can all impact the margins of error. Therefore, work to limit the number of false positives and false negatives is a crucial aspect of any biometric system implementation.

Spoofing

Biometric identification has certain advantages for identity management, but it is not a foolproof solution to fraud or identity theft. Biometrics, like other security systems, has flaws and may be hacked. For example, fake artefacts (such as a replica of a biometric trait) can be manufactured and utilized to deceive a biometric sensor. Spoofing is a frequent term for this because it poses a threat to the security of biometric systems. Because computer vision differs from human eyesight, several spoofing techniques may initially seem counterintuitive.

Many biometric systems, such as liveness detection, have mechanisms to try to prevent the potential of spoofing. For example, the technique of liveness detection is used to assess whether the source of a biometric sample is a living person.

Compromised biometrics

Biometric features, unlike passwords or ID tokens, cannot be renewed or revoked, which is another disadvantage of biometric systems. If a person's fingerprint or other physiological biometric is compromised, changing that trait can be exceedingly difficult, if not impossible. This might be an issue if one wants to use that biometric feature for future authentication.

5.1.3 Manual Data Entry Errors

The manual data entries are caused due to the errors in their calibration. The manual data entry falls victim to human error. That could be a spelling, grammar or punctuation mistake, either through a rushed typo or just incorrect usage.

Then there are the occasions when people enter data incorrectly. A erroneous number, data unintentionally placed into the incorrect spreadsheet field, or an incorrect email entered into a CRM record are just a few examples. If not caught right away, the employee finds it frustrating to have to go back and amend the incorrect entry. The records are messed up, but more significantly, if the problem is not fixed, it may result in embarrassing errors.

5.1.4 Biometric Data Breaching

Biometric data breaches are especially problematic because of the sensitive nature of the information. Unlike a username or password, Biometric data is unique to the individual and cannot be changed. Biometric data-based log-ins are becoming more popular. Due to the centralizing nature of this method, consumers may become more exposed to identity theft and data breaches in the long run. While it is suggested that one use passwords for different accounts, this is not possible with biometrics because their biometric data cannot be changed.

The preferred approach for defending individuals and organisations from hackers is gradually evolving to include biometric authentication. Unfortunately, hackers utilise this data to steal identities and perpetrate fraud. As a result, face recognition, iris scanning, and fingerprint scanners are increasingly widely used. Although there are many advantages to this technology in the fight against cybercrime, there are also some hazards. In order to safeguard themselves and their digital data, people and organisations need to be aware of two major issues:

- Individuals should be alert that fingerprint or facial recognition can be 'hacked' by cybercriminals attempting to steal or forge biometric data.
- Organizations that store patient medical histories, blood samples, or DNA profiles, such as hospitals, must consider the security ramifications of a data breach and their possible liability.

5.1.5 Regulation of Biometric Data in India

At the moment, biometric data must be held, used, or handled in accordance with the same laws that must be abided by when managing sensitive personal data or information. However, because it may be accessed and processed through a computer resource and is considered personal data, biometric data is controlled by the IT Act.

Personal information is defined under the Privacy Rules as "information about a natural person that may be used to identify that person, alone or in combination with other accessible information" (Personal Data). Furthermore, for an individual, "sensitive personal data or information" is a type of Personal Data relating to the person's sensitive details that require a higher level of confidentiality, such as a password, some financial information relating to a bank account or cards, or biometric information, among other things (Sensitive Data). Privacy laws generally require more excellent protection and stricter standards when processing, dealing with or handling any data or information classed as Sensitive Data. As biometric data is classified as Sensitive Data, the same safeguards that apply to Sensitive Data must be applied to biometric data. It establishes, among other things, data collecting, retention, disclosure, and transfer standards.

Furthermore, an entity that handles biometric data must follow and implement "appropriate security policies and procedures, the failure of which results in unlawful loss or gain to the entity or any individual, in which case the business is obliged to pay damages to the person affected." The IT Act is an exception to India's general rule for damages, stating that if the wrongful gain is established, the violator entity must compensate the data subject without the data subject has to prove that he or she suffered a wrongful loss as a result of the entity's failure to implement reasonable security practises and procedures in handling biometric data.

5.1.6 Biometric System Error Rates

Technology advancements and the increased need for better levels of security have combined to rekindle interest in biometrics as a method of physical access control. This unique study was written by Bill Spence of IR Security & Safety's Recognition Systems section. This first in a series of reports offers an executive briefing on practical biometrics concerns and the necessity of comprehending mistake rates.

Once the decision is made to embrace biometrics, the first consideration should be, "Is this technology suitable for me?" The next stage is determining which biometrics technology is best for the particular application after being familiar with it and successfully justifying it. Several technologies are incredibly well-suited and well-tested for access control applications. Others are yet primarily untested.

There are several useful and tested techniques, from the hand and finger to the iris, for most access control applications currently in use. For example, comparing systems based on mistake rates is one method.

There are mainly two types of mistakes that biometric devices can make: the false accept, where the device mistakenly admits an unauthorised individual, and the false reject, where the device mistakenly rejects an authorised person.

- **False Rejection Rate:** The risk that a biometric security system may mistakenly deny an authorised user's access attempt is measured by the false rejection rate. The ratio of false rejections to identification attempts, or FRR, is often used to describe a system.

- **False Acceptance Rate:** The average number of false acceptances inside a biometric security system is measured using the false acceptance ratio (FAR), a unit of measurement. By calculating the rate at which unauthorised or illegal users are confirmed on a certain system, it gauges and assesses the effectiveness and accuracy of a biometric system.
- **False Match Rate:** The false match rate (FMR) measures how frequently a biometric procedure misidentifies two different persons' biometric signals as originating from the same person.
- **False Non-Match Rate:** The rate at which a biometric matcher incorrectly classifies two captures from the same subject as being from separate individuals is known as the false non-match rate (FNMR). It may be compared to a normal classification algorithm's false reject rate (FRR).
- **Equal Error Rate:** EER stands for equal error rate. The threshold parameters for a biometric security system's false acceptance rate and false rejection rate are established using the equal error rate (EER) technique.
- **Detection Trade-off Curve:** The false rejection rate vs. false acceptance rate of binary classification systems is plotted graphically in a detection error tradeoff (DET) graph.

5.1.7 Mitigation Plan

Mitigation is the process of taking steps to lessen the effects of an unfavourable occurrence or danger that is produced by nature, technology, or people. While crucial components of the overall emergency management cycle, mitigation and a mitigation strategy are mandated by many new standards and recommendations. The dangers must be located before a mitigation strategy can be created. A sound foundation for mitigation planning will be established by looking at historical records and occurrences, conducting hazard identification inspections, and analysing processes in addition to being aware of potential risks, outcomes, and delivery methods. Systems are kept in a ready state and cost-effective plans are devised and submitted to management for financing and approval.

The actions performed in advance to better position the organisation to react to and carry out its operations in the event of a catastrophic occurrence are known as preparation. Examples of preparedness activities include training, communications systems, resource procurement and administration, and drills and exercises. These initiatives ought to incorporate the staff members' homes and families in addition to the company as a whole.

Exercise

1. Explain the process of biometrics.
2. State errors of Biometric Data Entry.
3. Name the Biometric System Error Rates.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=j7vkRbm1SiI

Biometric Data Entry Problems and Solutions

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

6. Assisting Data Entry Process

Unit 6.1 - Customer Data Management

Unit 6.2 - Network Administration

Unit 6.3 - Data Backup

SSC/N3023

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Plan methods to collate the right information from the customer to enable the data entry process
2. Summarize the importance of documenting, classifying, and prioritizing service requests and crowd management.
3. Manage PC configuration, networking, network admin, layers of networking, etc.
4. Explain the OSI model of networking.
5. Undertake various backup activities of data entered.

UNIT 6.1: Customer Data Management

Unit Objectives

By the end of this unit, participants will be able to:

1. Plan methods to collate the right information from the customer to enable the data entry process.
2. Summarize the importance of documenting, classifying, and prioritizing service requests and crowd management.

6.1.1 Customer Data Management (CDM)

CDM is the process of collecting, organising, and analysing customer data. It is an important mechanism to consider while making changes to:

- Rates of customer acquisition, satisfaction, and retention.
- Strategies for customer visibility and communication.
- Enhanced data quality and revenue.

6.1.2 Collection of Customer Data

Every organization needs to collect customer data and create an effective database. It is also necessary to follow the rules and regulations of the customer's country and location while collecting and storing data about the customers.

The following methods can be used to collect compelling data:

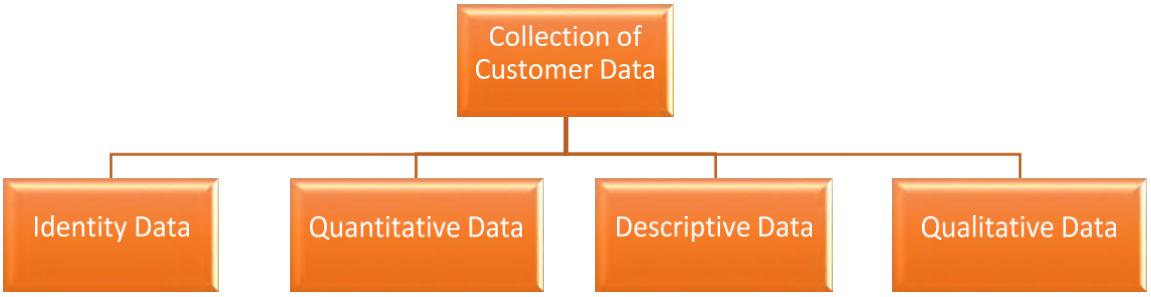

Fig. 6.1.1 Methods for Collecting Customer Data

1. **Identity Data:** Identity data is the collection of information about a particular person. This data can create a relationship and accessible communication with the customer. The collected data includes their name, address, date of birth, region, gender, contact number, social media, banking details, email, etc.

   This type of information can be collected when consumers submit their payment information during the checkout process, sign up for the newsletter, or voluntarily hand it over to obtain a product, service, or reward.

   The following can be used for attaining the data:

   a. Tailored sign-up forms
   b. Discount vouchers for first purchases
   c. Providing pre-order opportunities
   d. Tailored e-Commerce checkout process
   e. Warranty cards
   f. Loyalty/rewards programs

2. **Quantitative Data:** To understand the customer on an individual level, it is necessary to use measurable operational data, or quantitative data, to understand how the consumer interacts with the business.

   Quantitative data is information gathered along the customer journey, including discovery details, channel interactions, and conversion-specific processes that lead to the purchase. Quantitative data examples include:

   a. Online/Offline Transactions: Product Purchased, Time of Purchase, Amount of Purchases, Order/Subscription Value, Order/Renewal Dates, Cart Abandonment, Product Returns, etc.
   b. Customer Service: Complaint Details, Call Center Communication, Customer Query Details, etc.
   c. Inbound/Outbound Communication: Date, Time, etc.
   d. Online Activity: Website Visits, Online Registration, Product Views, etc.
   e. Social Network: Social Handles, Interactions, Interests, Groups, etc.

Channel-specific technologies are available throughout the customer's lifetime and should be adjusted to assess marketing goals and strategy.

To begin gathering quantitative data on customers are:

a. Google Analytics and other web analytics tools
b. Heatmaps based on website cookies and mouse tracking on landing pages.
c. Pixel tracking in emails/newsletters
d. Keeping track of previous purchasing transactions
e. Keeping track of past-customer support communications

3. **Descriptive Data:** A step up from identification data, descriptive data includes additional demographic information that correctly defines the customer. To incorporate optimal timing in the marketing activities, use predictive analysis. Descriptive data examples include:

   - Marital Status, Relationships, Number of Children, and so forth.
   - Property type, car ownership, pet ownership, hobbies, collections, interests, etc.
   - High school, college, further education, and so forth.
   - Job Title, Job Description, Income, Professional Background, and so forth.

   Obtaining high-quality descriptive data is a difficult task that necessitates more creativity. Companies generally use in-depth surveys to collect data, delving into seasonal growth and decrease, purchasing patterns, and the longevity of the customer cycle.

   Here are several approaches for gathering descriptive data:

   a. Questions for an open-ended interview
   b. Comprehensive questionnaires and surveys
   c. Target behaviour observations
   d. Focus group discussions
   e. Forms of advanced leads

4. **Qualitative Data:** The qualitative data describe the reasoning behind the choices customers make. Questions will often begin with the words "How, Why, and How," such as "how ideas and attitudes are formed.

   - **AEtudinal:** Perceived value, rating, feedback, the likelihood of repurchase, and so on.
   - **Motivational:** Purchase Reason, Customer Needs, etc.
   - Likes/Dislikes, Preferences, and soon.

   The following methods can be used to collect qualitative data:

   a. Industry-related websites rating
   b. Social media monitoring tools for customer engagement
   c. Customized newsletter sign-up procedure
   d. Making use of a favourite, save, or rating system
   e. Questions about deep listening and feedback form

6.1.3 Service Request

The tool for tracking initial service contacts is a service request record. In order to resolve a service request, necessary information must be obtained from the person making the request, and then it must be decided whether any additional action is required. One can generate an issue, problem, or work order right from the service request if addressing it necessitates doing so. Additionally, the service request and existing records can be connected.

To record a service requirement, one can create a service request record.

Priortizing Service Request

The service requests can be documented and classified on a priority basis:

- **Low Priority:** Visitors who are not active consumers often make low priority requests. Inquiries such as general product enquiries, sponsorship requests, and so on may fall into this category. They do not necessitate a prompt reaction.
- **Medium Priority:** Medium priority requests include product use and troubleshooting inquiries that do not interfere with the customer's ability to utilise the product; also, they may be casual users or have subscribed to the free version of the product. While they may not necessitate an instant reaction, they should be addressed soon.
- **High Priority:** Customers with high priority requests are those whose product usage is being hampered or impeded by the issue at hand. These queries require a prompt response.
- **First Priority:** Customers who are unable to use the product due to an issue make the highest priority requests. They demand quick attention and should be immediate at the front of the line.

6.1.4 Crowd Management

Crowd management is the planned, organised, and supported guidance provided to the orderly progression of events when huge crowds of people congregate.

Measures can be made to control or restrict the behaviour of crowds of people as part of crowd management. We refer to this as crowd control. The goal of your actions is to ensure public safety.

More than simply events require the use of crowd control. It is also employed in many contexts, such as shopping mall security and safety at plazas and airports.

Crowd management is a technique used to keep a huge crowd under control in an efficient and trouble-free way.

Crowd control techniques include:

- A moderate flow of people keeps things from being too crowded.
- Establishing a controlled public traffic flow.
- Reducing hazards through reducing the frequency of first aid cases, incident reports, and violent crimes.

The following elements have a direct impact on controlling and directing crowd management:

- Pedestrian and automobile traffic flow.
- Barriers, barricades, turnstiles, and signs for crowd control.
- Regulations are communicated, security services, guides and stewards are provided, and rules are planned and adjusted.
- Disaster and emergency plans (and required reserves).
- Communicating with the public and with management.
- Minimising wait times and the sense of being lost (searching).
- Big data-based ambiance makers, colour, lighting, and music forecasts.
- Food service, restrooms, cloakrooms, and car parking shelter from the elements.

Notes

UNIT 6.2: Network Administration

Unit Objectives

By the end of this unit, participants will be able to:

1. Manage PC configuration, networking, network admin, layers of networking, etc.
2. Explain the OSI model of networking.

6.2.1 Network Administration

Network administration entails a variety of operational duties that aid in the smooth and effective running of a network. Except for the smallest networks, maintaining network operations would be impossible without network administration.

The following are the most important network management tasks:

- Network design, implementation, and assessment
- Regular backups are conducted and managed.
- Network diagrams, network cabling manuals, and other technical documentation are created.
- Access to network resources requires proper authentication.
- Assistance with troubleshooting is available.
- Network security administration, including intrusion detection.

6.2.2 Components of Network Administration

There are three main components:

1. **Network Monitoring**

   Network monitoring is required to keep track of unusual traffic patterns, network infrastructure health, and network-connected devices. It aids in the early detection of aberrant behaviour, network difficulties, or excessive bandwidth usage, as well as the prevention and remediation of network quality and security concerns.

2. **Network Management**

   Network management includes network planning, installation, and configuration, among other administrative tasks. It entails:

   - Replanning the network in response to changing organisational needs.
   - Putting the network in place for optimal efficiency.
   - Setting different networking and security protocols, installing security updates, and upgrading networking infrastructure firmware, such as routers, hubs, switches, and firewalls.
   - Examining the network for flaws.
   - Assessing quality and capacity in order to expand or reduce network capacity and control resource waste.

3. **Network Security**

   Network security employs various techniques to ensure a network is secure. To prevent or identify unwanted behaviour in the network, it employs a variety of techniques, including firewalls, intrusion detection and prevention systems, and anti-malware software.

6.2.3 Open Systems Interconnection (OSI) Model

Open Systems Interconnection Model (OSI Model) is a conceptual framework for describing the operations of a networking system. The OSI model describes computer functions into a common set of rules and standards in order to facilitate interoperability across various devices and applications. The OSI reference model divides computer system communications into seven abstraction layers: physical, data link, network, transport, session, presentation, and application.

6.2.4 Functional Layers of OSI Model

The seven abstraction layers are:

1. **Physical Layer:** Open Systems Interconnection Model's lowest level is concerned with electrically or optically passing raw unstructured data bits over the network from the physical layer of the sending device to the physical layer of the receiving device. It may include parameters like voltages, pin layout, cabling, and radio frequencies. One may encounter "physical" resources such as network hubs, cabling, repeaters, network adapters, or modems at the physical layer.
2. **Data Link Layer:** At the data connection layer, directly linked nodes carry out node-to-node data transfer, where data is packaged into frames. The data connection layer corrects any errors that may have occurred at the physical layer.

There are two sub-layers in the data connection layer. The first is media access control (MAC), which rules and multiplexes device communications over a network. The second, logical link control (LLC), controls traffic and errors on the physical media and defines line protocols.

3. **Network Layer:** The network layer is in charge of accepting frames from the data link layer and routing them to their respective destinations depending on the addresses contained inside the frame. The network layer locates the destination using logical IP addresses (internet protocol). Routers are an essential component at this tier because they route information across networks.

4. **Transport Layer:** The transport layer is in charge of data packet delivery and error checking. It governs the size, sequencing, and, ultimately, data flow between systems and hosts. TCP, or Transmission Control Protocol, is a well-known transport layer example.

5. **Session Layer:** The session layer manages communications between machines. At layer 5, a session or connection between devices is established, organised, and terminated. Authentication and reconnections are also session layer services.

6. **Presentation Layer:** The presentation layer prepares or transforms data for the application layer based on the syntax or semantics that the application accepts. As a result, it's sometimes called the syntactic layer. The application layer's encryption and decryption can be controlled by this layer.

7. **Application Layer:** The layer interacts directly with the software application at this tier. This layer provides network services to end-user programmes like a web browser or Office 365. The application layer determines communication partners, resource availability, and communication synchronisation.

Notes

UNIT 6.3: Data Backup

Unit Objectives

By the end of this unit, participants will be able to:

1. Undertake various backup activities of data entered.

6.3.1 Data Backup

Data backup is the process of replicating data from one place. It can be required another in the event of a tragedy, accident, or malicious attack. Data is the lifeblood of modern organisations, and losing it may have disastrous effects and cause operations to be disrupted.

6.3.2 Types of Data Backup

There are three kinds of data backup:

1. **Full Backup**

   A full backup is when all files and folders are copied thoroughly. This is the most time-consuming of all backup techniques, and it may strain the network if the backup is performed over it. It is, however, the easiest to recover from because all of the data required are in the same backup set. Regularly scheduled full backups demand the greatest storage of any option.

2. **Incremental Backup**

   Incremental backup is a backup method that supports only the data that has changed since the previous complete backup. The disadvantage is that if an incremental-based data backup copy is utilised for recovery, a complete restoration takes longer.

3. **Differential Backup**

   Differential backups are a compromise between executing complete backups and incremental backups on a regular basis.

   One full backup is required for incremental backups. Only the files that have changed since the previous complete backup are backed up after that. To restore, all that is required is the most recent complete backup set and the most recent differential backup set.

6.2.3 Data Backup Concept

Data backup includes several important concepts:

- **Backup solutions and tools—**while it is feasible to back up data manually, most companies rely on a technological solution to back up their data regularly and consistently.
- **Backup administrator—**every company should appoint someone to be in charge of backups. That individual should verify that backup solutions are properly configured and tested regularly, and that vital data is backed up.
- **Backup scope and schedule—**a company must establish a backup strategy that specifies which files and systems should be backed up and how often data should be backed up.
- **RPO (Recovery Point Objective)—**The amount of data a company is willing to lose in the event of a disaster is decided by backup frequency. The RPO is 24 hours if systems are backed up once a day. The lower the RPO, the more data storage, computing, and network resources are required to accomplish frequent backups.
- **Recovery time objective (RTM)—**The time it takes for an organisation to restore data or systems from backup and resume regular operations is known as the recovery time objective (RTO). Copying data and fixing systems for significant data volumes and/or backups kept off-premises might take time, and robust technological solutions are required to assure a low RTO.

6.3.4 Data Backup Option

The following are the backup options available:

1. **Removable Media:** Backing up files using removable media like CDs, DVDs, newer Blu-Ray discs, or USB flash drives is a straightforward solution. This is feasible for smaller environments, but one needs to back up to many drives for more significant data volumes, complicating recovery. One should also keep backups in a different location, as they may be lost in the event of a disaster. Tape backups are also included in this category.
2. **Redaduncy:** An extra hard drive, or a completely redundant system, can be put up as a duplicate of a sensitive system's campaign at a given point in time. Another email server, for example, serves as a backup to the primary email server. Redundancy is a strong strategy, but it isn't easy to implement. It necessitates regular replication across cloned systems and is only beneficial in the event of a single system failure unless the redundant systems are located at a remote location.
3. **External Hard Drive:** A high-capacity external hard drive may be installed in the network, and archive software can be used to store changes to local files on that hard drive. With archive software, one may recover files from external storage with an RPO of just a few minutes. However, one external drive will no longer be enough when data quantities expand and the RPO skyrocket. Using an external drive means deploying it on the local network, which is dangerous.

4. **Hardware Appliances:** Many suppliers provide entire backup appliances commonly installed in a 19" rack. Backup appliances come with plenty of storage and backup software already installed. Install backup agents on the systems that need to be backed up, set up a backup schedule and policy, and the data will begin to flow to the backup device. Try to isolate the backup device from the local network and, if feasible, at a remote location, as with previous solutions.
5. **Software Appliances:** Software-based backup solutions are more difficult to set up and operate than hardware backup appliances, but they provide more flexibility. They enable users to specify the systems and data they want to back up, assign backups to the storage device of their choosing, and manage the backup process automatically.

Exercise

1. Fill in the Blanks:

   Identity Data, Data Backup, Service Request Management, Open System Interconnection.

   a. _____is the process of replicating data from one place.

   b. _____is the collection of information about a particular person.

   c. _____is a conceptual framework for describing the operations of a networking system.

   d. _____is the procedures and technologies that enable various departments within an organization.

2. Explain a few backup options available.

3. Explain in brief about CDM.

Notes

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

7. Skillsets of Biometric Data Entry Services

Unit 7.1 - Questioning Techniques

Unit 7.2 - Data Entry and Software

Unit 7.3 - Data Extraction

Unit 7.4 - Data Validation and Error Detection

SSC/N3023

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Illustrate proper ways of upskilling the data entry process through the use of advanced software.
2. Demonstrate application of various IT components that assists in the quick data entry process.

UNIT 7.1: Questioning Techniques

Unit Objectives

By the end of this unit, participants will be able to:

1. Identify various questioning techniques for a better understanding of an issue.
2. Create a Frequently Asked Questions - FAQ for customer-facing issues.

7.1.1 Questioning Techniques

Questioning techniques are to know the appropriate questions to ask to gain the information one needs in customer service and distinguish between an adequate and an outstanding customer service experience.

Questioning techniques refer to the many different types of queries we question customers or clients. Using a range of inquiries will help in identifying valuable data.

7.1.2 Types of Questioning Techniques

Asking the appropriate questions can provide the knowledge one requires when one requires it. As a result, it is a vital talent for customer service representatives.

Fortunately, advisers may utilize various questioning approaches to improve this competence. The following is the list:

1. Open and Close Questions

Open questions most often start with what, why and how. They cannot be replied to with a simple yes or no answer. Open questions are utilized to gain a deeper understanding of the consumer and the call's purpose. Customers' feelings, ideas, and views regarding a product or service can be revealed with their cooperation. This data may then be utilized to assist fix and improving the situation.

Open questions are more likely to be used when:

- Assisting the consumer in changing their mindset.
- To learn more about the consumer.
- Listening and caring about what the consumer has to say.

Closed questions begin with where, what, when, or who but can only be replied to with a single word. Both questions have a function and can help get vital information from customers. Closed questions can assist in establishing the fundamentals. It comprises information such as the customer's name, important dates, and other relevant details. Closed questions are also helpful in verifying that a consumer has been comprehended.

2. Funnel Questions

The Funnel Effect is what gives rise to funnel questions. The Funnel Effect comprises three stages, as seen in the figure below:

Fig 7.1.1 Funnel Effect

Step 1: Ask Open Questions: Begin by asking open questions regarding the topic since this will provide all the information required to continue the conversation.

Step 2: Asking Probing Questions: These are the types of questions that will help in exploring further the reasoning and emotions behind the customer's responses to the open questions.

These are some examples of funnel questions to probe for information:

- Could you elaborate on what you mean by...?
- How long have you been dealing with this problem?
- Can you tell me anything about how it looks or sounds?
- When you attempted to..., what happened?
- When this started, what were you doing?

Step 3: Asking Closing Questions: By asking closing questions, one can ensure that the service provider and the customer understand what has been covered in that particular line of questioning.

The term "funnel questions" refers to how to string these questions together.

3. TED Questions

Tell, Explain, Describe. TED questions can help in asking better probing questions in customer service.

Examples of TED Questioning Include:

- Tell me, how did that make you feel?
- Tell me, how did this affect you?
- Explain to me how did this happen?
- Explain to me what difficulties have you faced?
- Describe how that felt
- Describe how that looked
- Describe your ideal resolution

TED questions are great to use when more information is required.

4. Leading Questions

Leading questions, often known as loaded questions, are inquiries that imply a specific answer. Customers are "led" to the answer, hence the term. As a type of persuasion, they are a successful questioning method in customer service and sales.

5. Signposting

Signposting is an excellent customer service practice that helps conversations, including queries, flow more easily. As the names suggest, signposting involves using statements to indicate the coming question. The signposting technique allows customers to prepare and makes calls more organized.

Some examples of signposting statements include:

- "In a minute, I'll ask you for your account number."
- "In a moment, you'll need a pen and paper."
- "In a minute, I'll transfer you to the relevant department."

6. Validating Customers

Validating customers by questioning them can improve customer service and create an atmosphere of attention and caring. Customers may be more willing to give information in this setting.

Examples of customer validation statements could include, "I understand why you feel like that" or "I think that is a great choice". Statements like these can reassure and support customers.

7. **Understanding Customer**

   Different people communicate in different ways. Therefore, customers will respond better to the questioning if communicated with them in the method that suits them best.

   Customers will typically prefer one of two kinds of communication:

   - Push Communication – This is to ask lots of questions of the customer.
   - Pull Communication – This is to share lots of information with the customer.

7.1.2 Frequently Asked Question (FAQ)

The most common question asked by customers has answers on the FAQ page of the website. However, customers frequently ask the same few issues, and responding to all of their concerns via customer service or e-mails can raise costs and reduce productivity.

For running a successful business, the customers should have all the information about the products and services. Therefore, a well-maintained FAQ page is vital for any business as it reduces the need for constant online customer support.

The following steps are used for creating an FAQ page:

1. **Use the service data to identify the standard questions:** It is important to include questions representing current client problems when creating a responsive FAQ page. It may also gather common inquiries from support e-mails and previous customer care call logs.
2. **For each FAQ, provide concise and accurate solutions:** Customers go to FAQ sites to get answers to their questions. A well-written answer to a frequently asked issue may save numerous support tickets, phone calls, and chat answers. In addition, when a company can help clients with their FAQs, it may simply acquire their trust and urge them to place orders immediately.
3. **Over time, update content and add new solutions:** It is essential to keep up with business developments and changes by updating the FAQs regularly. Customers may quickly lose interest in an outdated and incorrect FAQ page, affecting the company's image.
4. **Add a Quick Search box:** The search tool is helpful on a FAQ page. It helps customers find information on a large website easily. As a result, including a search box on the FAQ page speeds up the process of finding relevant information and improves the user experience.
5. **Structure the FAQ section:** There are several options based on the type of queries the company receives over time when creating a FAQ website.

   To assist visitors in finding appropriate answers to their inquiries, categorize the questions into topics or service areas. It can help in eliminating the need to navigate through queries that are not relevant.

   The FAQ page can be structured in the following:

   - **Descriptive subheads:** guide customers to the answers to their inquiries.
   - **Featured questions:** provide customers with quick access to the most frequently asked questions.

6. **Add the FAQ page to the website:** It is beneficial to build the website in such a manner that the FAQ page is noticeable and easy to find. An FAQ page should be integrated into the general design of a website rather than being an afterthought.

7. **Monitor the FAQ page performance:** Regularly monitoring the performance of the FAQ page is a smart technique for a positive client experience. Consider and address the following elements to determine the effectiveness of the page:

   - Is the page adequately addressing customers' needs?
   - Is the page up-to-date & does it reflect the latest changes and updates in the business?
   - Does the page bring new customers to the site?
   - Does the FAQ page direct customers to other sections of the website?
   - Do the customers' responses to the site reflect trust, satisfaction, and engagement?

8. **Include space for live-support options:** While having a FAQ and an up-to-date knowledge base is essential for rapidly answering client questions, using a Live Chat to provide faster replies is even more beneficial. In addition, many clients prefer live chat to e-mail, phone support, and other customer care options because live chat assistance is quick and convenient.

   Customers may interact with the business regarding the answers they need via live chat. Compared to e-mails, live support works significantly better. However, it is not easy to estimate when customers will receive an e-mail reply.

Notes

UNIT 7.2: Data Entry and Software

Unit Objectives

By the end of this unit, participants will be able to:

1. Discuss various work methodologies to expedite data entry.
2. Evaluate the purpose of the software, including Ninox, Piesync, AutoEntry, etc., in the data entry process.

7.2.1 Data Entry

Data entry includes entering and updating data into an electronic service or database. An individual who enters data does so by directly inputting data into a company database with a computer, mouse, keyboard, scanner or other data entry tool.

There are several methods to enhance data entry skills, with the assistance of a computer system or through structured training. The data entry skills can be improved by:

- **Enhancing current typing skills:** Take note of the present body position and typing structure. Double-check the hand posture's accuracy and comfort for maximum accuracy and comfort.
- **Desk space should be comfortable:** Data entry requires long durations of sitting and typing on a computer. A comfy chair with back support and height adjustment capabilities is one of the most effective methods to increase comfort when working at a desk. Place the computer monitors at eye level as well. Fact-checking, data input speed, efficiency, and productivity may all benefit from dual displays.
- **Use the online typing tools:** Several online programmes helps in evaluating the present typing abilities and identifying areas where to improve. Practising with these typing tools may enhance typing speed and efficiency. In addition, consider viewing online videos that demonstrate data input in the basic computer software to improve fundamental computer and software skills.
- **Master data entry shortcuts:** Use shortcuts with specific software products to save time. For example, use the TAB and ENTER keys in spreadsheet software to insert previously typed information. One may find many spreadsheets and keyboard shortcuts online or ask the supervisor for suggestions.
- **Allow time to proofread:** Mistakes can happen in any work done, so it is essential to examine the work before submitting it. If no editor or proofreader is available, it may be beneficial to take a break from a project. Then, when one returns to it, one may proofread it themselves.

7.2.2 Data Entry Software

Data entry software provides the automation and replacement of costly and inefficient paper and manual data input operations with robust programmes that may be utilized on computers, cellphones, and tablets. Data entry software may either create electronic forms to replace paper forms or entirely automate categorization and data extraction from incoming documents, depending on the user's needs.

7.2.3 Importance of Data Entry Software

The following are the advantages of using data entry software:

- **Reduces Errors:** The automated data input system may reduce errors significantly. It has the potential to save the company much money. The data input tool acts as a dependable technique for preventing data entry errors.
- **Saves time:** With the help of data entry software, a company may handle data more effectively and streamline the entire data management process. The data input tools can extract information from any business document in seconds. For example, the data entry system may handle e-mails, PDFs, faxed order forms, hard-copy invoices, and receipts. In addition, the data entry tool takes the data from each document immediately after it arrives, so there are no human delays in the business process.
- **Increases accuracy:** Data entry software validates data before importing it into the main company applications, such as an ERP system (Enterprise resource planning system). The automatic method will ensure that data is free of errors and missing information.
- Saves Money: Money is saved since the data input software streamlines corporate processes. It becomes much easier to save money on regular tasks this way. Organizations are not required to spend money on inefficient operations.
- **Reduces paperwork and expenses:** Maintaining and organizing the enormous amounts of paperwork completed every day costs a lot of money. The company must spend on file cabinets, ink, printers, and staff to put the papers together. In addition, rental offices are responsible for paying for the office space needed to hold all files. With a data entry system, all of these problems can be solved.
- **Enhances clarity and efficiency:** Organizations may decrease workplace clutter by replacing physical papers with digital counterparts, which improves clarity and productivity. All records may be accessed by authorized personnel and any internet-connected device using data input tools. In addition, users can avoid searching for misfiled papers by using data input software.

7.2.4 Some examples of Data Entry Softwares

The following softwares are used in data entry:

- **Auto Entry:** Auto Entry is an automated data entry platform designed to help accountants and bookkeepers with automatically capturing all accounting information. AutoEntry reduces time spent on inputting invoices, receipts, expenses, and statements by automatically extracting data from documents and publishing it to any accounting solution. AutoEntry includes document scanning, item capture, smart analysis and processing, purchase order matching, auto-publishing, document storage, and more. Utilizing item capture, AutoEntry allows accountants to capture item descriptions, unit price, and quantity line by line from any document/receipt. Accountants can scan and upload any document to AutoEntry's system. With seamless integration tools, AutoEntry is able to publish any extracted document data to any accounting solution. AutoEntry will also remember how invoices and receipts are analyzed and processed and offer the same configurations using smart analysis tools.

- **Ninox:** Ninox is a cloud-based data entry solution used by small and midsize organizations. Utilizing tools like drag-and-drop formulae, custom actions, built-in templates, and scripting, the solution aids in creating database applications. Both on-site and cloud storage options are available for the database. Ninox also enables users to design unique forms and fields. Users of the system may make data entry templates for timesheets, project management, property management, accounts management, and customer relationship management. Role-based access control and real-time data synchronisation between devices are other characteristics of the system. Additionally, the system offers automatic data backups.

- **GoCanvas:** Go Canvas is a mobile business management system that runs on the cloud and is appropriate for field service businesses including electrical, HVAC, pest control, and plumbing. The solution may be accessed on a Windows PC via a Windows app and is made to function on any smartphone or tablet. A dispatch calendar is a feature of GoCanvas that enables users to generate and allocate assignments to field workers. Using a drag-and-drop interface, the form builder tool may be used to construct personalised service forms. Users can select one or more apps to best suit their needs by combining contact management, billing, invoicing, work order management, and scheduling as independent alternatives.

- **Fast Field:** Fast Field is a cloud-based data entry solution that helps businesses of all sizes gather data, create forms and collect information via tablets and smartphones. Primary features include question branching, collaboration, version control, text editing, dispatch and form routing, duplicate detection and more. FastField provides white-label solutions to personalize forms with custom logo, color, themes and fonts. The platform includes automation tools, which allows organizations to manage forms dispatch and delivery of data. Additionally, the geotagging module lets users add latitude/longitude coordinates and timestamps to forms and track attributes of data collection. FastField includes built-in dashboard that enables enterprises to view performance metrics and track trends for businesses. Its mobile applications for Android and iOS devices enable organizations to remotely manage business activities. The product is available on a monthly subscription pricing and support is extended via phone, email and documentation.

Notes

UNIT 7.3: Data Extraction

Unit Objectives

By the end of this unit, participants will be able to:

1. Demonstrate effective use of information technology to input/extract data results.

7.3.1 Data Extraction

Data extraction is gathering or obtaining various data types from several sources, many of which are unstructured or poorly organized. Data extraction allows data to be consolidated, processed and refined before being stored in a centralized location and changed. These sites might be on-premises, cloud-based, or a combination of both.

Data extraction is the first step in ETL (extract, transform, load) and ELT (extract, load, transform) processes. ETL/ELT are themselves part of a complete data integration strategy.

The ETL procedure is divided into three steps:

- **Extraction:** Data is extracted from various sources or systems. The extraction process locates and identifies important data before processing or transformation. Many different data types may be integrated and processed for business insight via extraction.
- **Transformation:** The data may now be refined after being adequately extracted. Data is sorted, structured, and sanitized during the transformation stage. Duplicate entries will be eliminated, missing information will be removed or supplemented, and audits will be conducted to provide trustworthy, consistent, and useable data.
- **Loading:** For storage and analysis, the converted, high-quality data is supplied to a single, unified destination location.

7.3.2 Types of Data Extraction

Data extraction is a flexible and powerful procedure that may help businesses collect various business-related data. Identifying the data needed is the first step in putting data extraction to work. The following are examples of data that are frequently extracted:

- Customer data is the type of information that businesses and organizations use to understand their customers and supporters better. Names, phone numbers, e-mail addresses, unique identification numbers, transaction history, social media activity, and online searches, to mention a few, are all examples of personal information.

- Financial data includes sales figures, purchase expenses, operational margins, and even the competitors' pricing. Companies may use this information to track performance, enhance efficiency, and plan strategically.
- Performance Data by Use, Task, or Process: This broad data category contains information about individual tasks or processes. A retailer, for example, would want to know about its shipping operations, while a hospital might want to track post-surgical results or patient comments.

7.3.3 Importance of Data Extraction

The following are some of the advantages of employing a data extraction tool:

- **More Control:** Companies can use data extraction to import data from other sources into their systems. Consequently, businesses can keep their data from being segregated by out-of-date programmes or software licencing. It is their information, and extraction offers the ability to do anything visitors want with it.
- **Increased Speed:** Companies typically work with multiple sorts of data in different systems as they develop. Data extraction helps to integrate multiple data sets by consolidating that information into a unified system.
- **Simplified Sharing:** Data extraction may be a simple approach for companies to give beneficial but restricted data access to external partners that wish to share some but not all of their data. Extraction also makes it possible to exchange standardized and useable data.
- **Precision and accuracy:** The need to enter, amend, and re-enter massive amounts of data takes its toll on data integrity, and manual processes and hand-coding increase the chances of mistakes. Data extraction automates operations to reduce mistakes and save time fixing them.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=JnudxNoP0Ts

Data Extraction

UNIT 7.4: Data Validation and Error Detection

Unit Objectives

By the end of this unit, participants will be able to:

1. Use proper data validation and error detection mechanisms.

7.4.1 Data Validation

Data validation is the process of validating the accuracy and quality of data. It is accomplished by including various checks into a system or report to guarantee that input and stored data are logically consistent. Data is input into automated systems with little or no human intervention. As a result, it is critical to make sure that the data that goes into the system is valid and fulfils the quality requirements that have been set. If the data is incorrectly recorded, it will be of little utility and may result in more serious downstream reporting issues. Even if unstructured data is submitted accurately, cleaning, converting, and storing it will entail expenses.

7.4.2 Types of Data Validation

Data validation can take numerous forms. Before saving data in a database, most data validation methods will execute one or more tests to confirm that the data is accurate. The following are examples of data validation checks:

1. **Verify the data type**

   A data type check verifies that the entered information is the right type. A field, for example, could only take numeric input. If this is the case, the system should reject any data that contains additional characters such as letters or special symbols.

2. **Code Verification**

   A code check verifies that a field is chosen from a legitimate set of options or that it adheres to specific formatting constraints. For example, checking a postal code against a list of valid codes makes it easy to verify if it is legitimate. Other elements, such as country codes and NAICS industry codes, can be treated in the same way.

3. **Range Verification**

   A range check will see if the input data is inside a specific range. Latitude and longitude, for example, are frequently employed in geographic data. The latitude should be between -90 and 90 degrees, and the longitude should be between -180 and 180 degrees any values outside of this range are regarded as invalid.

4. **Format Check**

   Many data types have a predetermined format. Date columns with a set format, such as "YYYY-MM-DD" or "DD-MM-YYYY," are famous use cases. Data validation that ensures dates are formatted correctly helps preserve consistency across data and throughout time.

5. **Consistency Check**

   A consistency check is a logical check that ensures data is entered in a logically consistent manner. For example, checking whether the delivery date for an item is later than the shipping date.

6. **Uniqueness Check**

   Some data like IDs or e-mail addresses are unique by nature. Therefore, these fields in a database should almost certainly contain unique entries. A uniqueness check guarantees that an item is not put into a database numerous times.

7.4.3 Steps for Data Validation

The steps are:

Step 1: Determine Data Sample

Select the data to be sampled. If the amount of data is large, one should usually validate a portion of it rather than the whole data. It is important to select how much data to sample and what kind of error rate is acceptable to ensure the project's success.

Step 2: Validate the Database

Before moving the data, make sure that all necessary information is available in the current database. Compare the source and target data fields to determine the number of records and unique Ids

Step 3: Validate the Data Format

Determine the data's overall health and the changes that will be necessary to bring the source data into compliance with the direct instruction. Then search for incongruent or incomplete counts, duplicate data, incorrect formats, and null field values.

7.4.4 Error Detection

The techniques used to identify noise or other impairments introduced into data as it is being transferred from source to destination are referred to as error detection in networking. Error detection ensures that data transmission over susceptible networks is dependable.

Error detection reduces the chance of sending wrong frames to the destination, referred to as undetected error probability.

The techniques are:

1. Simple Parity Check:

- In even parity, the extra bit is sent in addition to the original bits, and in odd parity, the extra bit is sent in place of the original bit.
- A frame is created by counting the number of 1s in each frame. In even parity, a bit with the value 0 is added if the number of 1s is even. In this way, the number of 1s remains even. A value of 1 is added to an odd number of 1s to make it even.
- The receiver simply counts how many 1s are in the frame. The frame is considered uncorrupted and approved if the number of 1s is even and even parity is used. There will be no damage to the frame if the number of 1s is odd and odd parity is used.
- Counting the number of 1s can identify a single bit flip in transit. In cases where more than one bit is incorrect, it is extremely difficult for the receiver to identify the problem.

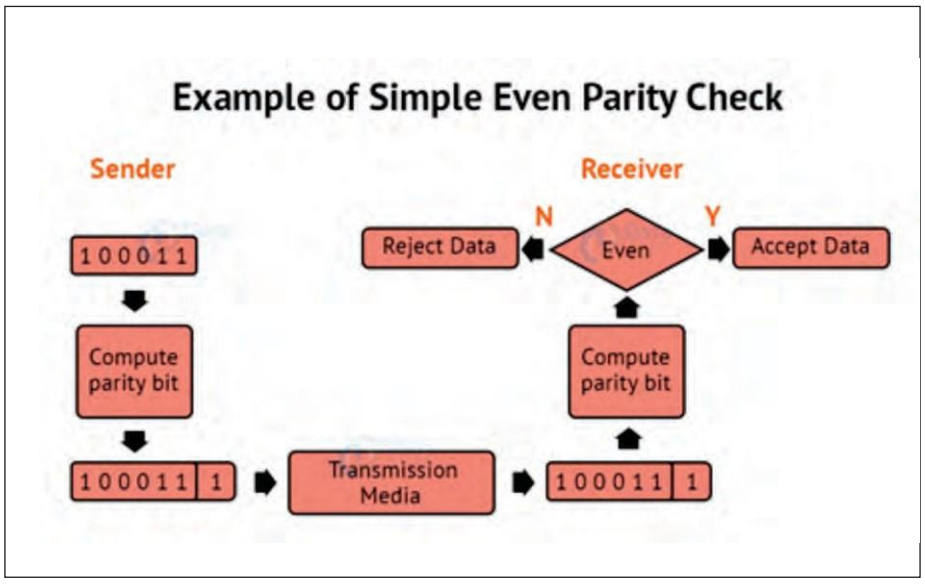

Fig. 7.4.1 Simple Parity Check

2. Two-Dimensional Parity Check:

Parity check bits, which are similar to a basic parity check bit, are computed for each row. Parity check bits are calculated for each column and sent along with the data. At the receiving end, they are compared to the parity bits calculated on the received data.

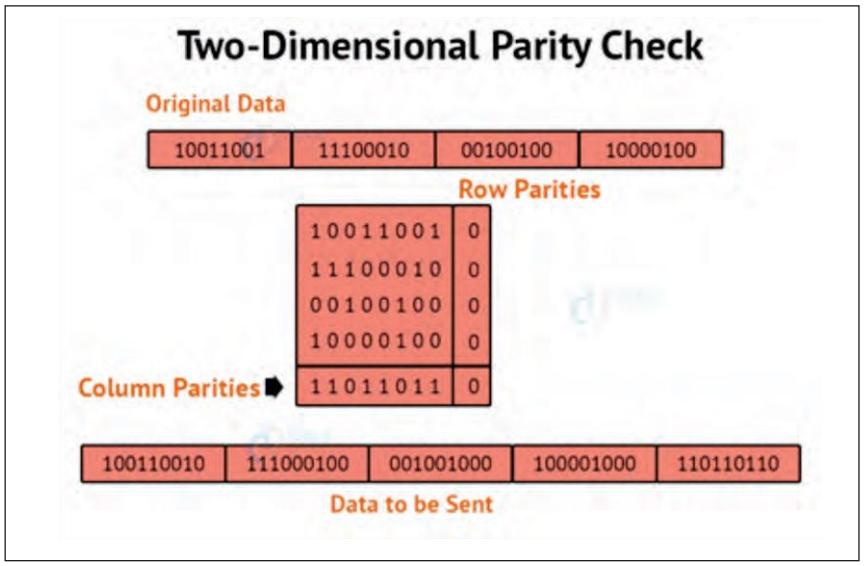

Fig. 7.4.2 Two-Dimensional Parity Check

3. Checksum:

- The data is split into k segments of m bits each in the checksum error detection technique.
- To get the total, the segments are summed at the sender's end using 1's complement arithmetic. To obtain the checksum, a complement of the sum is taken.
- The checksum segment is sent with the data segments.
- To obtain the total, all received segments are summed using 1's complement arithmetic at the receiver's end. The sum is then calculated.
- If the result is 0, the data is accepted; otherwise, it is rejected.

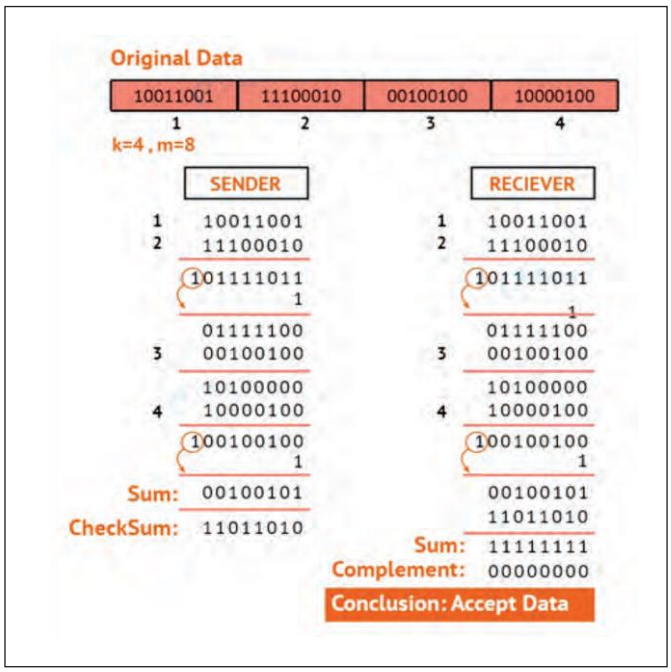

Fig. 7.4.3 Checksum

4. Cyclic Redundancy Check:

CRC is an alternative method for determining whether or not a received frame includes valid data. The binary division of the data bits being delivered is used in this approach. Polynomials are used to generate the divisor.

The sender divides the bits that are being transferred and calculate the remainder. The sender inserts the remainder at the end of the original bits before sending the actual bits. A codeword is made up of the actual data bits plus the remainder. The transmitter sends data bits in the form of codewords.

The receiver, on the other hand, divides the codewords using the same CRC divisor. If the remainder consists entirely of zeros, the data bits are validated; otherwise, it is assumed that some data corruption happened during transmission.

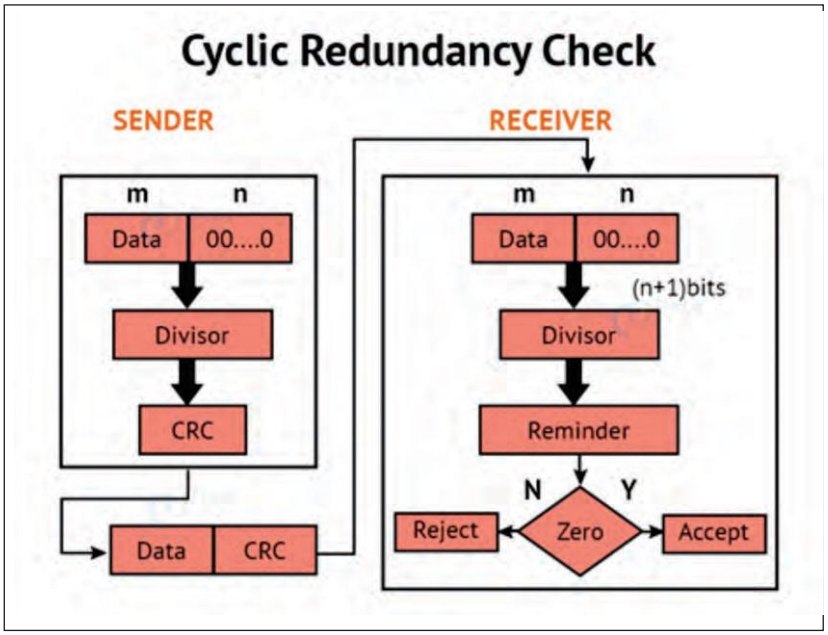

Fig. 7.4.4 Cyclic Redundancy Check

Exercise

1. Write the full form of the following acronyms.

   a. FAQ

   b. ETL

   c. TED

2. Fill in the Blanks

   Error Detection, Data Validation, Data Extraction, Data Entry Software

   a. _____provides the automation and replacement of costly and inefficient paper and manual data input operations with robust programmes that may be utilized on computers, cellphones, and tablets.

   b. _____is gathering or obtaining various data types from several sources, many of which are unstructured or poorly organized.

   c. The techniques used to identify noise or other impairments introduced into data as it is being transferred from source to destination are referred to as_____in networking.

   d. _____is the process of validating the accuracy and quality of data.

3. Explain the steps in the funnel question technique.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=3qKUQweyQ9E

Data Validation and Error Detection

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

8. Incident Management in Biometric Processes

Unit 8.1 - Introduction to Incident Management

Unit 8.2 - Incident Management Tools

SSC/N3023

Key Learning Outcomes

By the end of this module, participants will be able to:

1. Illustrate proper ways of maintaining the confidentiality of storing security and backup files for future use.
2. Demonstrate application of various solutions for different types of incidents/service requests.

UNIT 8.1: Introduction to Incident Management

Unit Objectives

By the end of this unit, participants will be able to:

1. Discuss and identify the various types of incidents during process flow, including storage, applications, and security.
2. Use Error cluster analysis and data event analysis to minimize incidents via analysis of the targeted data.
3. Design frameworks to operate with both internal and external specialists for support to perform correct incident management.
4. Analyse probable solutions for database error management and database access management.

8.1.1 Incident

Any disruption to an organization's operations, whether it impacts a single user or the entire business, is known as an incident. In a nutshell, an incident is anything that disrupts corporate operations.

The situation needs to be handled promptly, or it might turn into an emergency, crisis, or tragedy. An incident can impact corporate operations, services, security, and other critical business processes if it is not managed effectively.

8.1.2 Type of Incidents

Any disruption to an organization's operations, whether it impacts a single user or the entire business, is known as an incident. In a nutshell, an incident is anything that disrupts corporate operations.

The situation needs to be handled promptly, or it might turn into an emergency, crisis, or tragedy. An incident can impact corporate operations, services, security, and other critical business processes if it is not managed effectively.

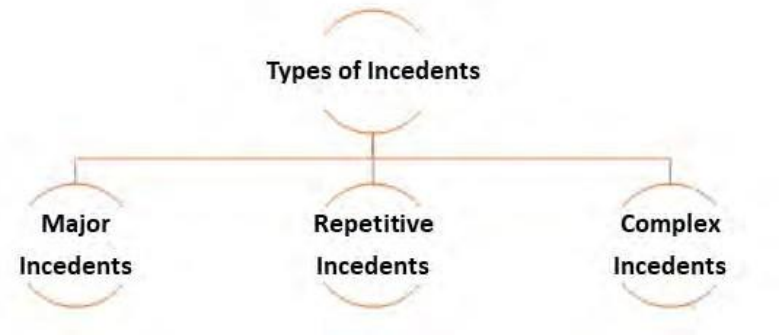

Fig. 8.1.1 Types of Incidents

Mainly there are three types of incidents:

1. **Major Incidents:** These are large-scale incidents that occur suddenly. Every organization need to be prepared to deal with them quickly and efficiently.

   For example, an overnight server restart that causes app login issues for hundreds of users might significantly impact the business. Employees cannot complete their work the next day because they wait for the help desk crew to reset login credentials and distribute updates to users. At the same time, the help desk employees arrive to discover a slew of related support tickets waiting for them, putting them in a position where they must deal with a mountain of paperwork to get started fixing issues.

   In this circumstance, the organization needs an incident management system to handle many support tickets while also recognizing and consolidating similar requests. It can also allow support staff to automatically deliver form messages to end-users and exchange resolutions across the support team to speed up answers. Large-scale difficulties can result in long-term productivity losses; thus, using incident management to deal with these significant issues swiftly and effectively is crucial. It is critical to respond swiftly to these occurrences.

2. **Repetitive Incidents:** Some situations do not go away; no matter what, the organization try to fix them. In many situations, these occurrences indicate underlying issues with the IT setup. If one is not in a position where problem management will help the organization, they have to rely on incident management to resolve these difficulties. Without incident management, the support team would be stuck dealing with these events every time they arise, hoping to remember what they did the last time so they can swiftly resolve the issue.

   A knowledge management system may be integrated with an incident management platform to identify repeated events and provide users with the information they need to address them rapidly. The organization may also write scripts to automatically fix primary, repeatable occurrences, ensuring that the help desk staff is not spending time on frequently occurring issues.

3. **Complex Incidents:** Most events that come into the support desk are pretty straightforward. As a result, the level 1 engineer may enter the ticket, resolve the issue, and tell the user. However, a complicated incident might cause considerable delays in this process. The level 1 technician will open and examine the support case, and if the issue is too complicated, the user will need to escalate the ticket to a level 2 engineer. If using a homegrown system in the organization, these shifts might cause problems to fall between the cracks or take an excessively long time to address.

   A dedicated incident management platform has the feature of workflow optimization, alerting, and incident tracking tools one needs to handle complicated situations without getting into difficulty.

8.1.3 Incident Management

An incident management process is a collection of processes and activities used to respond to and address important occurrences, including identifying and reporting incidents, who is accountable, what tools are utilized, and how the problem is resolved.

Many sectors employ incident management processes, and incidents can range from IT system failure to situations needing the attention of healthcare experts to vital infrastructure maintenance.

It covers every aspect of an incident across its life cycle. It facilitates ticket resolution and makes ticket administration more open. Ticket administration might be complex without incident management. Some of the most common issues that may arise are:

- End users have little visibility into ticket progress or predicted timescales.
- There is no reliable documentation of previous events.
- Unable to document solutions to difficulties that occur frequently.
- Business outages are higher, mainly when large disasters occur.
- Longer resolution times
- Lack of ability to report.
- Customer satisfaction has dropped.

8.1.4 Incident Response Framework

The phrase "incident response" refers to the procedures and policies followed by a company in the event of a cyber-attack or data breach. The purpose of incident response is to lessen the impact of an attack, which means reducing the time, effort, expenses, and reputational harm connected with a cyber assault or data breach. Aside from minimizing the many impacts of a cyber assault, the Incident Response process may assist businesses in preventing future attacks that compromise their information security.

Every organization should have a plan to assist them in recognizing, controlling, and removing cyberattacks. IR strategies define what constitutes an attack and provide organizations with a clear roadmap for what to do in these incidents.

An incident response framework's objective is to assist organizations in developing standardized response strategies. Large businesses with extensive security knowledge and experience are frequently the developers of these frameworks.

The incident management framework is of the following:

Prepare, Respond, Review

Fig. 8.1.2 Incident Management Framework

Prepare (Pre-Incident Paterns)

- Make incidents visible and part of daily work
- Well defined incident roles
- Well defined incident response triggers
- Well defined on-call rotation & schedule
- On-call onboarding and training
- Incident command training & certification
- Well defined communication plan
- Well defined behaviour protocols

Respond (Incident Response Paterns)

- Periodic CAN reporting (Conditions, Actions, Needs)
- Shared incident state document
- Incident call recording
- Incident swarming

Review (Post-Incident Response Paterns)

- Localized incident reviews
- Global incident reviews
- Post review improvement items
- Incident review template
- Incident impact assessment

8.1.5 Incident Management Process

The methods and activities used to respond to and resolve incidents are called incident management processes. Who is accountable for reporting, how incidents are detected and informed to IT teams, and the technologies used are all covered.

When well-designed, incident management methods guarantee that all events are immediately addressed, maintaining a high-quality level. Processes may also aid teams in improving existing operations and avoiding future issues.

Any incident resolution procedure follows a set of five steps. These procedures help teams respond to incidents successfully by ensuring that no component of the issue is neglected.

Fig. 8.1.3 Incident Management Process

1. **Incident Identification, Logging, and Categorization:** User reports, solution analysis, and manual identification are all used to identify incidents. The incident is recorded, and the inquiry and classification process may begin. It is critical to categorize occurrences to determine how they should be handled and prioritize response resources.

2. **Incident Notification and Escalation:** This stage includes event alerting, though the time may vary depending on how incidents are identified or classified. In addition, if the incident is minimal, facts may be recorded or alert conveyed without the need for an official notice. Escalation is determined by the incident's categorization and who is in charge of response processes. Escalation can happen unnoticed if events can be controlled automatically.

3. **Diagnosis and investigation:** Staff can begin examining the kind, cause, and potential remedies for an issue after assigned incident duties. One can select the relevant remedial procedures when an event has been diagnosed. It involves informing affected employees, customers, or authorities about the situation and any anticipated service disruptions.

4. **Resolution and Recovery:** Eliminating threats or fundamental causes of difficulties and returning systems to full functionality is part of resolution and recovery. Additional phases may be necessary depending on the kind and severity of the incident.

For example, when a virus infection occurs, one cannot simply erase the infected files and resume operations. Instead, to prevent the infection from spreading, make a clean duplicate of afflicted systems, isolate the harmful components, and completely replace the systems.

5. **Incident Closure:** Closing incidents usually entails completing paperwork and analyzing the response procedures. This assessment assists teams in identifying areas for improvement and proactive ways to help prevent future accidents.

   Providing a report or retrospective to administrative staff, board members or consumers may also be part of incident closure. This information can help regain any lost trust and openness in business processes.

   The following are some best practices for the incident management process:

   - Detecting issues early—before they have an impact on customers
   - Quickly responding to and resolving incidents Communication, collaboration, and measurement of incident response need central management of event information.
   - Responsibility for incident response and coordination
   - All aspects of incident management are being continually improved.

8.1.6 Cluster Analysis

Cluster analysis is a statistical technique used to classify items into groups according to how similar they are. It can also be referred to as clustering, taxonomy analysis, or segmentation analysis.

The aim of a cluster analysis is to group various objects or data points so that there is a higher degree of association between two items if they belong to the same group and a low degree of correlation if they belong to separate groups.

Because it is frequently utilised when researchers do not have an assumed concept or fact that they are utilising as the foundation of their research, cluster analysis varies from many other statistical techniques.

Since this analytical method doesn't distinguish between dependent and independent variables like factor analysis does, it is often used in the exploratory stage of a study. Instead, cluster analysis is used primarily to identify data structures without offering a justification or meaning.

8.1.7 Data Event Analysis

Data Event Analysis is the evaluation of a business-related event that the company has to be aware of and that needs to be documented in the firm's memory, i.e., the company files. A data event may be created internally or externally, as a consequence of an action being conducted or just as the result of time passing. the occurrence of data events that are somehow documented. The information that must be captured so that the event may be remembered and responded to is determined by data event analysis. It must also establish how the firm learned about the occurrence; in other words, what made them aware of it?

8.1.8 Database Access Control

Database access control, often known as DB access control, is a technique for limiting access to unauthorised individuals and granting access to user groups that are permitted to view important corporate data in order to avoid data breaches in database systems.

Authentication and authorisation are the two key parts of DBMS's Database Access Control.

In order to verify a user's identity when they access your database, authentication is used. It's crucial to bear in mind that user authentication alone cannot safeguard data. An extra layer of security is authorization, which determines if a user's degree of access or data access control is adequate. Data security is ultimately impossible without identification and authorisation.

Notes

UNIT 8.2: Incident Management Tools

Unit Objectives

By the end of this unit, participants will be able to:

1. Examine typical response times and service times for problems through the incident management tool.

8.2.1 Incident Management Tools

IT teams may categorize, organize, and resolve significant incidents that cause downtime or service outages using an incident management tool. When an incident is detected, it remains at the centre of an IT organization's ecosystem, sending real-time warnings to the relevant teams' phones.

8.2.2 Benefits of Incident Management Tools

The benefits of using incident management tools in the workplace are:

- **Increased communication:** Incident management systems like Slack and Zoom allow employees and management to communicate instantly, which would generally take longer or get unorganized if done by email, text, or in-person talks. It can help in reducing the time it takes to respond to employee queries or concerns and make it easier for employees and managers to handle situations.
- **Quicker response time:** Incident management software may significantly minimize time spent recognizing and responding to workplace issues. An employee, for example, may report a technological issue at their workstation in minutes using an incident management application, with management receiving prompt notification of the occurrence and being able to respond just as swiftly.
- **Detailed records:** Incident management software is also helpful for keeping detailed records of the many occurrences that occur in the workplace over time. For example, a virtual service desk solution may keep track of the many events and reports that employees submit, with management and IT having access to that reported history as needed.
- **Reduced workload:** Incident management software can help create a more efficient workplace by minimizing the workload that would otherwise be spent keeping track of various issues. Employees, particularly those in human resources, might profit from the reduced burden by focusing their energies on more vital responsibilities at work.

8.2.3 Criteria for Selecting Incident Management Tools

The following steps would assist in selecting incident management tools that are compatible with the company's practices:

1. **Evaluate the company's needs**

   The first step in determining which incident management tool is best for the company is to assess its objectives and needs. Next, make a report outlining some of the company's most frequent problems, and think about how alternative management tools may help relieve or handle those situations. Next, consider getting input from employees on what they feel are the most prevalent issues in the company and how they presently handle them. It may be accomplished by sending out a survey or questionnaire to employees to learn about the most critical matters in the company.

2. **Evaluate the options**

   The next step is to undertake extensive research to get completely aware of the market's various incident management tools. Then, make a spreadsheet where one may take notes on different tools and categorize them depending on their purpose, features, price, and any other significant criteria that might influence the ultimate pick. It might help limit the selections and focus on products that will impact the company's incident management strategy.

3. **Consider compatible tools**

   After narrowing down the list of viable event management systems, it is required to assess their software compatibility. To further improve the incident management process, several management technologies may collaborate and extract information and resources from one another. Consider comparing the top tools to evaluate their cohesion and determine which is most consistent with the workplace's goal, duties, and occurrences before making a final decision.

8.2.4 Commonly Used Incident Management Tools

The most commonly used incident management tools are:

1. **Resolver**

   Resolver is an incident management tool that investigates security issues that could disrupt an organization's operations. Employees may utilise Resolver to report problems, which management can address in minutes. Resolver simplifies incident management activities like record-keeping while also providing other benefits like effective data quality and the ability to quickly translate languages using artificial intelligence.

2. **Splunk Enterprise**

Splunk Enterprise is a tool that gives extensive data reports to managers and IT professionals so they can make key technical and business choices while dealing with problems. The package includes email and help desk assistance, in-person and live online training, anti-spam and virus protection, archiving, and interoperability with many common software programmes. Splunk, as an incident management tool, may help speed up problem resolution by alerting IT teams to potential issues in real-time.

3. **Fresh service**

Fresh service, as an IT service management system, allows customers to submit tickets via a number of channels, including email, chat, and even its own support site, which serves as a service desk. Fresh service evaluates tickets using intelligence technology and provides related articles to the reporter that may assist them in fixing their reported trouble. This tool is most advantageous to a company's IT department since it allows them to send automatic answers to tickets, which may aid in the incident management process.

4. **Pager Duty**

Pager Duty is a tool that allows businesses to notice problems and respond to them in real-time. It allows customers to report and handle issues, while managers may reply right away with a swipe on their mobile app. Pager Duty also integrates with other incident management applications, such as Slack, and allows management to schedule on-calls from their mobile device, potentially increasing scheduling efficiency.

5. **Manage Engine Service Desk Plus**

Manage Engine Service Desk Plus is an incident management tool that works in a service desk structure, allowing employees to create tickets, make purchases, manage contracts, and track assets. Manage Engine provides an Integrated Package that combines the software with additional management solutions to improve productivity and optimise the issue management process. In comparison to other prominent incident management products on the market, this management tool has a comparatively modest pricing point.

6. **Ops Genie**

Ops Genie is an incident management tool which provides a fresh approach to dealing with unexpected technical and operational issues at work. When an employee reports an event or another concern emerges, the programme focuses on giving workers immediate notifications and alerts. It's connected with more than 200 IT service management solutions, allowing customers to make use of the most valuable resources available across several programmes to handle their specific corporate issues.

7. JIRA Service Management

JIRA Service Management is among the most widely used incident management tools, providing staff with a variety of choices for reporting, monitoring, and responding to unexpected events. It employs a collaborative platform to expedite incident management procedures, such as its self-service site, where employees may discover answers to problems without the intervention of management or supervisors. In addition, the JIRA application focuses on improving communication across many departments within a company, such as IT, development, and business operations.

8. iAuditor

iAuditor software is a common incident management tool that inspects and monitors numerous systems for possible dangers to a company's security, quality control, and general business operations. The programme provides users with in-person and online training, as well as extra educational tools such as webinars and videos. It also employs collaboration technologies to make it easier for staff to work together on audits, financial report investigations, and other safety and quality assurance inspections.

9. xMaters

As an incident management tool, xMatters provides businesses with a simplified platform for preventing, monitoring, and resolving technical catastrophes like software problems or internet outages. The xMatters program's major purpose is to prevent and resolve technical issues before they disrupt company operations. Therefore it takes a proactive approach to incident management. Furthermore, the application links its own systems with standard management tools like JIRA, Splunk, and Slack, making it a viable alternative for managers looking for solutions that are compatible with other incident management programmes.

10. Slack

Slack is a collaborative work hub that allows employees to connect in real-time across several channels. Users can contribute images and documents, share links, and vote in surveys to assist management in making organisational choices. Slack simplifies employee communication by allowing managers to build channels for individual departments, projects, and subjects. Employees may also promptly report issues on Slack and share them with colleagues who can take fast action.

Exercise

1. Fill in the Blanks

   Complex, Incident Management Process, Respond

   a. An_____is a collection of processes and activities used to respond to and address important occurrences, including identifying and reporting incidents, who is accountable, what tools are utilized, and how the problem is resolved.

   b. The incident management framework consists of Prepare,_____, and Review.

   c. The three major incidents are: Major, Repetitive, and_____.

2. Name any three commonly used incident management tools.

3. Explain the incident management process.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=9ZQ-H_aGlmo

Incident Management Tools

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

9. Employability Skills

DGT/VSQ/N0102

Employability skills can be defined as those soft skills which employers look for in a potential employee. These skills equip the employees to carry out their role to the best of their ability and client satisfaction. For example, the ability to explain what you mean in a clear and concise way through written and spoken means, helps to build a better relationship with the client or the customer. Similarly, handling stress that comes with deadlines for finishing work and ensuring that you meet the deadlines can be done through effective self-management training. It can also be done by working well with other people from different disciplines, backgrounds, and expertise to accomplish a task or goal. In today's digital age, employers expect that the employees should be able to make use of elementary functions of information and communication technology to retrieve, access, store, produce, present and exchange information in collaborative networks via the Internet. Students need to develop entrepreneurial skills, so that they can develop necessary knowledge and skills to start their own business, thus becoming job creators rather than job seekers. Potential employees need to develop green skills, which are the technical skills, knowledge, values and attitudes needed in the workforce to develop and support sustainable social, economic and environmental outcomes in business, industry and the community. Thus, students are expected to acquire a range of skills so that you can meet the skill demands of the organisation that you would work for or to set up and run your own business.

This chapter is about employability skills, Constitutional values, becoming a professional in the 21st Century, digital, financial, and legal literacy, diversity and Inclusion, English and communication skills, customer service, entrepreneurship, and apprenticeship, getting ready for jobs and career development.

The scope covers the following :

- Introduction to Employability Skills
- Constitutional values – Citizenship
- Becoming a Professional in the 21st Century
- Basic English Skills
- Career Development & Goal Setting
- Communication Skills
- Diversity & Inclusion
- Financial and Legal Literacy
- Essential Digital Skills
- Entrepreneurship
- Customer Service
- Getting ready for Apprenticeship & Jobs

The details of Employability module is available on eskill India. Please find below the link.

https://eskillindia.org/NewEmployability

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=PI8U2W2pnHQ

Work ethics to Follow

https://www.youtube.com/watch?v=fWLZj4ufMRE

Work Effectively with Colleagues

https://www.youtube.com/watch?v=1Rfrgd-eyhU

Evacuation Procedures

https://www.youtube.com/watch?v=N4kgu1qi9_A

Health Safety and Accident Reporting

https://www.youtube.com/watch?v=Vk5vbZXT-U4

Workplace Data Management

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

IT - ITeS SSC
NASSCOM

10. Annexure

Chapter No.	Unit No.	Topic	Page No.	QR Code Links	QR Code (s)	Video Duration
Chapter 1: Introduction	Unit 1.2 - Introduction to Biometric	1.2.1 Biometric 1.2.2 Evolution of Biometric 1.2.3 Need for Biometrics 1.2.4 Emerging Trends in Biometeric	10	https://www.youtube.com/watch?v=Q2ZnqjqQ-Dw	Introduction to Biometric	00:02:09
Chapter 3: Software Requirement for Biometric Operations	Unit 3.1 - Biometric Data Entry Software	3.1.1 Report Writing 3.1.2 Report Writing Software 3.1.3 Database Management System 3.1.4 Data Verification 3.1.5 Analysis of Data 3.1.6 Biomatric Access Control	43	https://www.youtube.com/watch?v=WdftZZ4G0Vg	Biometric Data Entry Software	00:02:18
Chapter 5: Troubleshooting in Biometric Data Entry	Unit 5.1 - Biometric Data Entry Problems and Solutions	5.1.1 Process of Biometric 5.1.2 Common Biometric Data Entry Errors 5.1.3 Manual Data Entry Errors 5.1.4 Biometric Data Breaching 5.1.5 Regulation of Biomatric Data in India 5.1.6 Biometric System Error Rates 5.1.7 Mitigation Plan	73	https://www.youtube.com/watch?v=j7vkRbm1SiI	Biometric Data Entry Problems and Solutions	00:02:01

Chapter No.	Unit No.	Topic	Page No.	QR Code Links	QR Code (s)	Video Duration
Chapter 7: Skillsets of Biometric Data Entry Services	Unit 7.3 - Data Extraction	7.3.1 Data Extraction	107	https://www.youtube.com/watch?v=JnudxNoP0Ts	Data Extraction	00:02:20
		7.3.2 Types of Data Extraction				
		7.3.3 Importance of Data Extraction				
	Unit 7.4 - Data Validation and Error Detection	7.4.1 Data Validation	114	https://www.youtube.com/watch?v=3qKUQweyQ9E	Data Validation and Error Detection	00:02:21
		7.4.2 Types of Data Validation				
		7.4.3 Steps for Data Validation				
		7.4.4 Error Detection				
Chapter 8: Incident Management in Biometric Processes	Unit 8.2 - Incident Management Tools	8.2.1 Incident Management Tools	131	https://www.youtube.com/watch?v=9ZQ-H_aGlmo	Incident Management Tools	00:02:39
		8.2.2 Benefits of Incident Management Tools				
		8.2.3 Criteria for Selecting Incident Management Tools				
		8.2.4 Commonly Used Incident Management Tools				
Chapter 9: Practice Employability Skills	Employability Skills	Work ethics to Follow	135	https://www.youtube.com/watch?v=PI8U2W2pnHQ	Work ethics to Follow	00:01:50
		Work Effectively with Colleagues		https://www.youtube.com/watch?v=fWLZj4ufMRE	Work Effectively with Colleagues	00:02:36

Chapter No.	Unit No.	Topic	Page No.	QR Code Links	QR Code (s)	Video Duration
	Employability Skills	Evacuation Procedures	135	https://www.youtube.com/watch?v=1Rfrgd-eyhU	Evacuation Procedures	00:02:03
		Health Safety and Accident Reporting		https://www.youtube.com/watch?v=N4kgu1qi9_A	Health Safety and Accident Reporting	00:02:03
		Workplace Data Management		https://www.youtube.com/watch?v=Vk5vbZXT-U4	Workplace Data Management	00:02:15

Scan this QR Code to access eBook

https://eskillindia.org/Home/handbook/1387

Skill Council for Persons with Disability

Sector Skill Council Contact Details:

Address: 501, City Centre, Plot No. 5 Sector 12 Dwarka New Delhi - 110075

Website: www.scpwd.in

Phone: 01120892791

Price: ₹