BLOCK 2
DATA HANDLING

BLOCK 2 DATA HANDLING

This is the second block of the course "Computer Applications in Business". This block focuses on the usability of computers for handling available data that is of great use for the organizations. This block will familiarize the learners with various data handing techniques, services and security measures and their applications in business. It also focuses on the applicability of Internet in business to facilitate the organizations in conducting their business smoothly comprise of four units, the detail of which is mentioned below:

Unit-5: The very first unit of this block introduce the readers with the concepts of data and information and highlights the need and implication of Business Information System (BIS), Data Base Management System (DBMS), Enterprise Resource Planning (ERP), Decision Support System (DSS), Management Information System (MIS), General Data Protection Regulation (GDPR) etc. for the effective decision making in organizations.

Unit-6: This unit makes the learners aware with the cyber security and its various principles for business. It further discusses the steps which need to be taken for securing the assets of business organizations with briefs on advanced security measures in a form of code such as One Time Password (OTP), Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

Unit-7: This particular unit familiarizes the learners with the concept of internet, its benefits, functions and various services such as Email, SMTP, IMAP, POP, Web browsers etc. It also discusses various applications offered to and convenience to end users. The unit also describes the significance of domain names and URLs.

Unit-8: This unit discusses how plastic money came into existence and its usage in Present times. It further, also identifies various models of digital payments used in commercial activities, their development, significance and usage in present time. The units also briefs on the impacts of demonetization policies on digital payment system in India.

UNIT 5 BUSINESS INFORMATION SYSTEM

Structure

5.0 OBJECTIVES

After studying this unit, you will be able to:

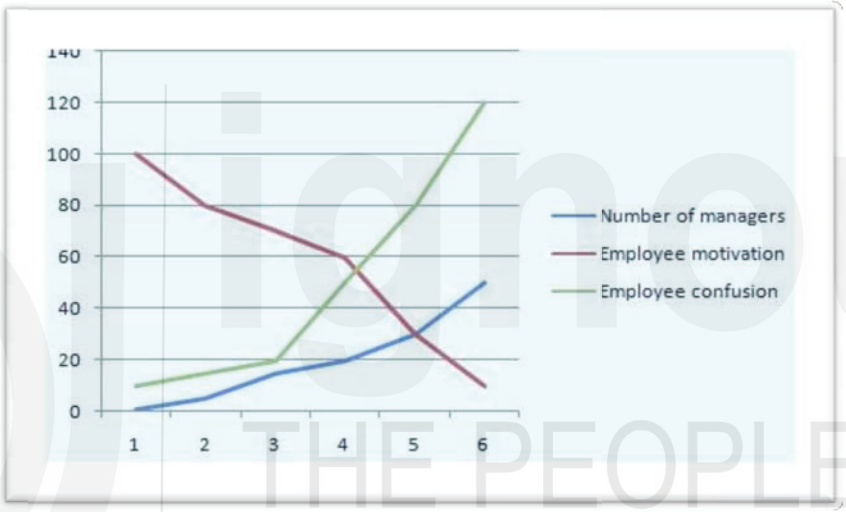
- introduce the readers with the concept of data and information;
- highlight the organization of the available information in the effective decision making; and
- highlight the need and implication of business information system.

5.1 INTRODUCTION

Business is very essential for the working of the economy of a country. It is the driving force behind the economy. The absence of business infrastructure in a country leads to an economy which is primitive or ineffective in the overall growth of the country. The stronger the business foundations in a country, the stronger are the economy. In order to understand the relationship between economy and business, let us consider an example; suppose someone starts a company, then for its proper working, he would hire people for fulfilling various purposes like working staff, account staff, lower-level staff, cleaning staff, and administrative staff. This will in turn give job opportunities to many people for their sustenance. Stable sustenance of a

country is very essential for its growth. This growth at a very fundamental level is related to the understanding of business basics which eventually leads to formation of data and information required to be analysed. As once a business starts running, it generates data. This data can be transformed into information, knowledge and wisdom. This is all required for effective decision making in an organization. It also helps in understanding the potential risks involved in running a particular organization/institution. There are few considerations before setting up a business which will subsequently affect the economy. These considerations are:

- How the trends of the business behave?
- What is the connection to the economy?
- What are the specific segments of the business?



***Source:** Officevibe

Fig. 5.1: Sample Growth Chart for a Business

The business not always has a smooth running curve. The growth of a business is not uniform always, it may rise and then a fall or may be a flat like a plateau and then again a rise and so on (Figure 5.1) based on increase in the number of managers or employee motivation. So why is this so? It is because of normal economic fluctuation like staffing needs, inventory, physical (machinery) maintenance, and resource levels.

In today's time, modern organizations are like open system. There is an information exchange between these open systems to adapt to the changes which are continuously imposed by the changing technology and market dynamics. The need of the hour is to have the right information at the right time. In order to achieve this, information needs to be gathered, organized, processed and evaluated in the form which is effective for decision making. The information system has given rise to various other branches of information processing where there is increased need of data processing, effective decision making in complex situations and a phenomenal rise of knowledge workers. Any basic information system comprises of computer

hardware and software, pre-defined procedures, analytical models, planning and control of various decision making situations.

The rise of information system largely is due to the change in business environment which has effectively led to globalization. The global market place involves proper management and control of the world markets, work groups, and delivery systems. It is due to this changing environment that the global economies have transformed their structure to knowledge and information based vision. This structure consists of generation of new products and services, productivity, time-based competitions, shorter product life, building leadership and a hasty turbulent environment. In view of changing environment there is transformation of the enterprise also which has numerous characteristics like – decentralization, location independence, flexibility, low transaction and co-ordination cost, empowerment and collaborative teamwork. There are numerous factors that lead to the design of a business information system. These are:

- Organization's environment
- Organization's structure
- Organization's functionalities
- Policies of the organization
- Effective management of the decision making capabilities
- Role of management

It is also important to understand that once the design of the information system is conceived, there are operating elements which should be considered. These are transaction processing, maintaining of master files, process inquiries, reports, and interactive support. The users are benefitted by the design and operational structure of the information system by having documents of the transaction, advance reports, ad-hoc inquiries, user machine dialogue and proper inquiry responses. In view to understand this information system and its related concepts, this chapter provides a comprehensive view to all the important dimensions of any business information system.

5.2 DATA AND INFORMATION

The origin of the word '*Data'* dates back to 1640's, where it was first used as an English word. The meaning of this word is transmissible computer information and was used in 1946. The origin and usage of the word data processing was first done in 1954. Now-a-days, it has a more abstract usage in day to day life where it encompasses the observations and facts as *data.* It is sometimes believed that data and information mean the same and are interchangeable. However, *Latin* word data *(plural of datum)* and information carry different perspective. A data, in literal sense, would mean any character, word, number. If this data is not put in relevant context, it means nothing or little to us. On the other hand, information is known to be processed data which can be utilized for effective decision making.

Jaspreet, 7464566835, Mandawali, New Delhi

Fig. 5.2: Representation of Data

Jaspreet
7464566835
Mandawali
New Delhi

Fig. 5.3: Representation of Information

Figure 5.2, represents the form of data in terms of random characters, numbers which do not make much sense. Figure 5.3, represents the processed data, i.e., the information which is organized and formatted. Once it is processed, it is easier to understand that this is the address of *Jaspreet*.

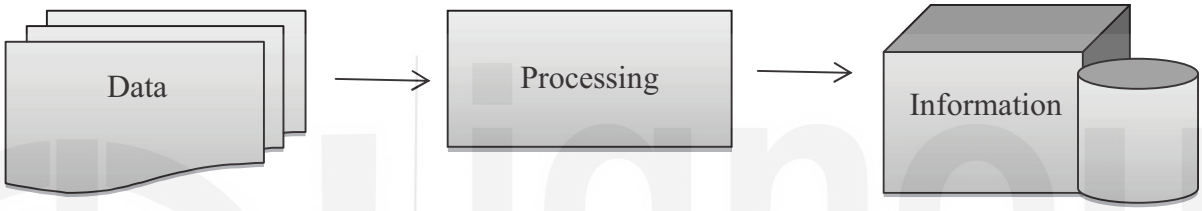


Fig. 5.4: Transformation of Data to Information

When the data is transformed through processing, it is termed as Information. Figure 5.4, shows this transformation from data to information. This information once processed gives knowledge and wisdom which can be used for effective decision making. This transformation of data to information is not the only brick stone required for decision making. In further steps, this information is utilized to form knowledge and wisdom. Figure 5.5, depicts the level wise transformation of data to wisdom.

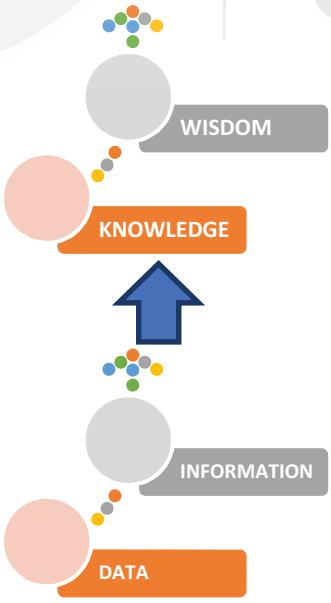


Fig. 5.5: Transformation of Data to Wisdom

Data is very crucial for any information system. This data is the running force behind many business information systems. The understanding of the type, context, concept, and semantics of the data/information is necessary for effective wisdom. In the subsequent sections, the need of business information system, database management system, decision support system is discussed which will further elevate the need of data analysis.

5.3 INTRODUCTION TO BUSINESS INFORMATION SYSTEM

Formally, a business is a commercial activity of a person who has a regular occupation, trade or any line of work. The economy is essentially dependent on the businesses running in various spheres. It is also defined by the exchange of goods or services or one another for money. The pricing of a good, change in the demand, consumer tastes/preferences, effect of change of costing are some of the ideas that relate business with economics. Business is important for the efficient running of an economy. It is an imperative factor in the economic system. In India also, for the effective growth of the economic system, various loans and schemes are provided. In order to ease the process of credit availability India partnered with different financial bodies for small scale businesses/young /woman/SC/ST entrepreneurs. Some of the popular loan schemes are The Credit Guarantee Fund Scheme (CGS), MUDRA loan scheme and Stand Up India Scheme. The Confederation of Indian Industry (CII) and Federation of Indian Chambers of Commerce and Industry (FICCI) are two major industry chambers which are designed to bridge the gap between government and the industry. They supervise the regulations, policies and organization of the industry.

A business can be categorised in different classes. These classes define the operations, protocols, investment options, legal implications, economic dependencies and independencies. The ownership of a business defines its class.

They are as follows:

- Privately owned
- Not for profit
- State owned

As stated earlier, these classes have different operational scenarios. The other classification of business is as follows:

- Partnership
- Limited Partnership
- Limited Liability Company (LLC)
- Cooperative (Co-op)

Out of these classes, Sole Proprietorship is one of the oldest schemes prevalent in the world. In this a sole person is responsible for the management and controlling of the activities, whereas, in Partnership, two or more individual agrees to share their profit and loss (under some predefined protocols) in a business. Some basic differences in sole proprietorship and partnership are enlisted in Table 5.1.

Table 5.1: Difference between Sole Proprietorship and Partnership

S.No	Sole Proprietorship	Partnership
1.	It is simple to establish.	It requires agreement between two or more partners.
2.	It is controlled and managed by sole person.	It is managed and controlled by two or more partners.
3.	Decision making is quick as it involves no partners	Decision making requires mutual consent of all the partners.
4.	The liabilities/profit/loss is all borne by the proprietor.	The liabilities/profit/loss is shared by the partners.
5.	Finances can only be raised up to a limit.	Scope of raising finances is high.

How can we relate Business to information system?

The various facets of business within information system shows the amalgamation of many terms related to business operations. Now we need to understand the relation between a business and an information system. Now a day people talk about data analytics& statistics. These terms are nothing without appropriate data. This data is generated by the business organizations which can be further used for knowledge discovery and other potential applications. The generated data is to be analysed for effective decision making. This is done with the help of specialized software called as Information System.

The dependency of business intelligence with decision making cannot be accomplished without these information systems. These are sophisticated software which manage, maintain and store the powerful information in the most elegant way. Figure 5.6, illustrates this dependency which relates all the major components of Business intelligence.

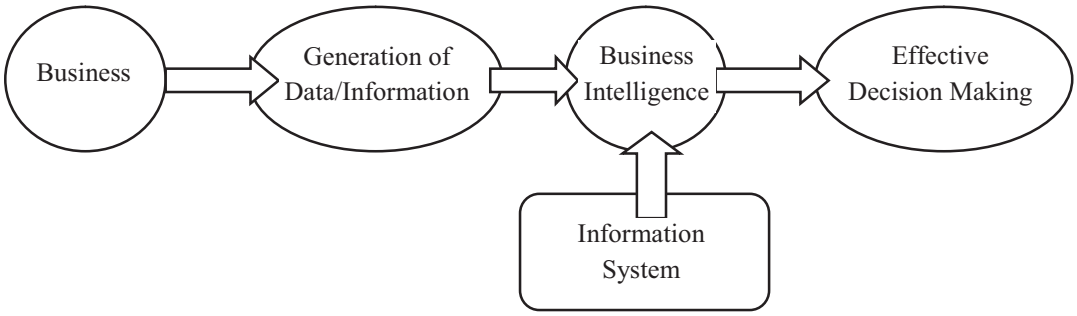


Fig. 5.6: Relationship of Business with Information System

Now since, we have formalised the information system, there is a need to understand the architecture of a Business Information System which contains other important components for efficient working of an organization. Figure 5.7, explains the architectural components of a Business Information System.

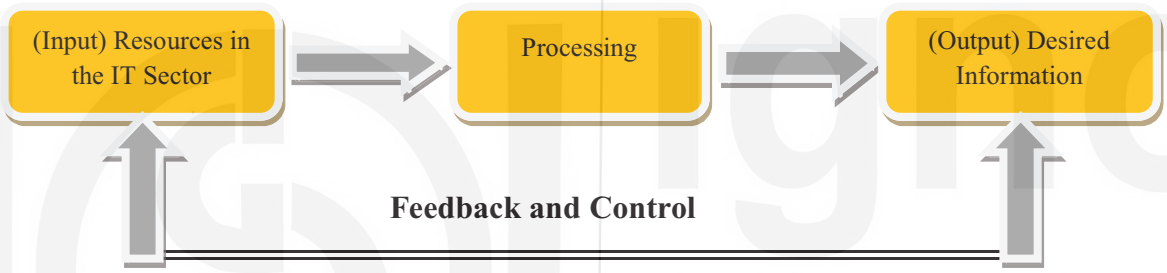


Fig. 5.7: Business Information System Architecture

In the broadest perspective a Business Information System can serve four basic functional systems – Sales & Marketing; Manufacturing & Production; Finance & Accounting and Human Resources. All these functional systems vary in their protocols, usage, maintenance and support. The only common goal of the functional system share is with effective overall business development. Apart from these systems, a Business Information System can further be categorised from a constituency perspective. These systems are as follows:

- Transaction Processing System (TPS)
- Management Information System (MIS)
- Decision Support System (DSS)
- Executive Support System (EIS)

Out of these basic systems, the MIS provides support to DSS. Subsequently, MIS and DSS provide support to EIS and TPS provides support to MIS and DSS. The functionalities of these systems are explained in next sections.

Check Your Progress A

1) How a DBMS differs from a File Processing Systems?

……

……

……

……

……

2) Discuss the difference between Schema and Instance.

……

……

……

……

3) What do you understand by Information Processing?

……

……

……

……

4) What is Sole-Proprietorship? What are its advantages over Partnership?

……

……

……

5.4 DATABASE MANAGEMENT SYSTEM (DBMS)

A Data Base Management System (popularly known as DBMS) consists of a collection of logically related data and a set of operations which are required to access this data. A Database system eventually consists of:

- Data Base
- Data Base Management System

The information/data gathered from various operational units running in a business are stored in a repository. This repository is called as a *Data Base*. Once the data is collected, now the need is to analyse the data effectively. To effectively analyse it one needs to store it properly so that the data is secure, consistent and maintains its integrity. It is also important to manage this data efficiently. This efficient management of data is done via *Data Base Management System (DBMS).*

There are implicit properties of a DBMS. These are given as follows:

- Some predefined aspect should be identified, for example, a company, institute, college etc.
- It must have logically coherent data.
- The semantics of the data must be understood well in advance.
- It should be designed and implemented for a specific purpose with identified source of information, related events and intended users.

The major functions of DBMS are to define the database structure, data type definition, perform, update, delete, and read operations on stored information, preserve consistency, prevent unauthorized access, and facilitate database recovery (Figure 5.8).

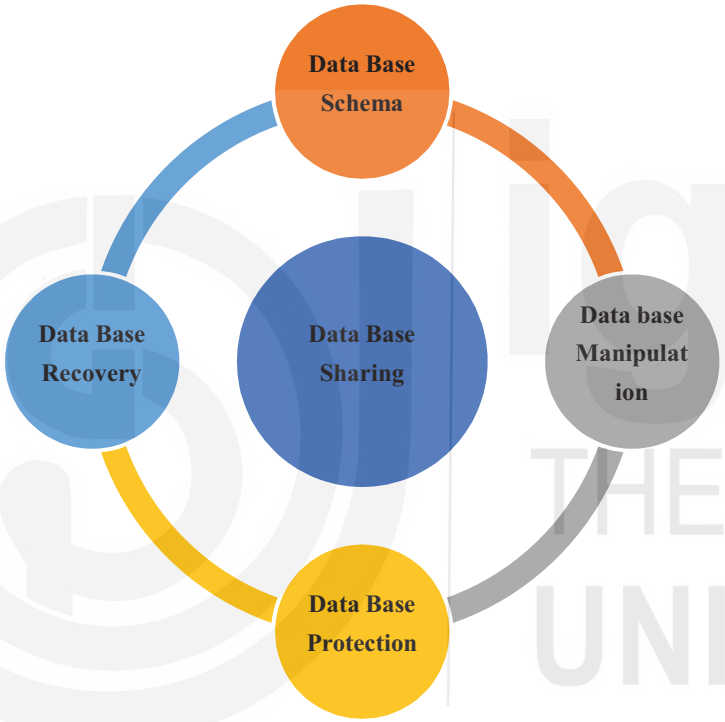


Fig. 5.8: Major Functionalities of a Data Base Management System.

Traditionally, File Processing Systems (FPS) was used to handle the repositories of institutions/organizations. In FPS, the structure of the files which were used had to be hard-coded in the application. Although the handling with FPS was easy, it lacked in many major applications. With the advent of DBMS, the limitations of FPS can be easily understood. Figure 5.9 shows the various areas where FPS lacks.

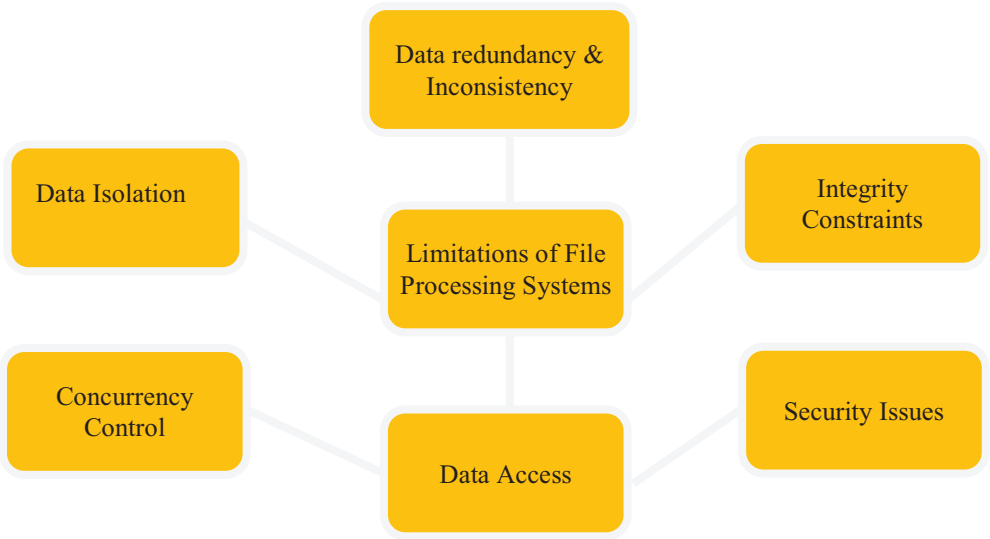


Fig. 5.9: Limitations of File Processing Systems over Data Base Management Systems

- A database system has many features that overcome the limitations of an FPS. It encompasses a data dictionary, has a storage management, transaction management, concurrency control, database recovery and language interfaces. In order to implement these features a data model is used to describe the data, handle data relationships, data semantics, and data integrity constraints. There are two kinds of data models such as Record based model and Object based model which is explained in Figure 5.10 as follows:

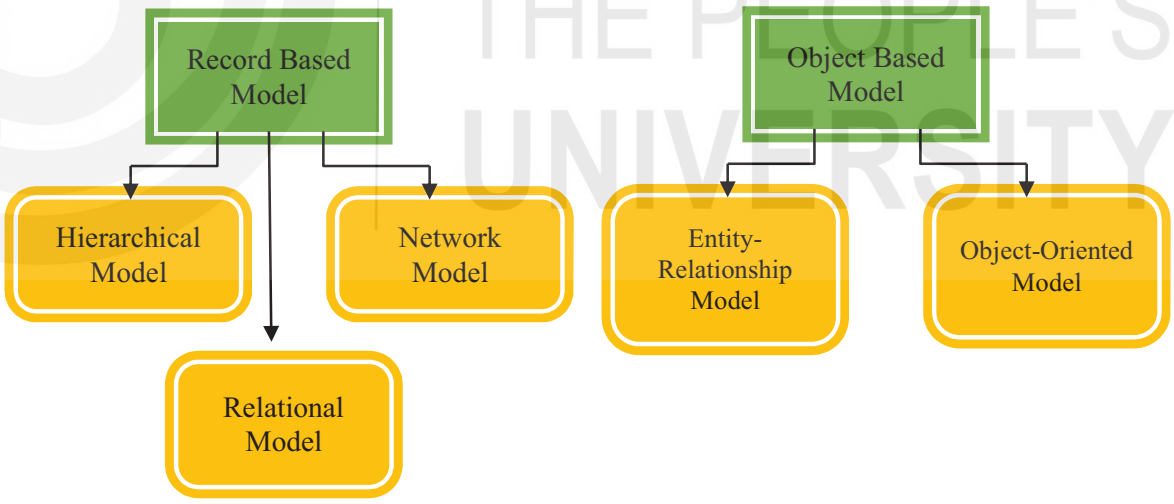


Fig. 5.10: Types of Data Models

Object based models are further classified as Entity Relationship (E-R) model and object oriented model whereas the record based models are generally classified as hierarchical, network and relational model (Figure 5.10). Out of these classes of various types, ***relational model*** is the most common and widely used model. It is because the relational model is simple to understand, easy to implement, has a strong mathematical foundation and strong standard

for maintaining data. The relational DBMS is further explained in the next subsection.

5.4.1 Relational Data Base Management System (RDBMS)

Relational Data Base Management System (RDBMS) is based on relational model. This is the most commonly used record based model. In this, tables are used to store the data, which are also called as relations. The relationship between data and tables are also represented in the table itself. Table 5.2, describes the widely used terminology of RDBMS.

Table 5.2: Terminology of RDBMS

S. No	Terminology	Description
1.	Relation	Table (with a unique name) is called as Relation
2.	Tuple	Each row of the table is called as a Tuple
3.	Attributes	Each column of the table is an attribute of the Relation
4.	Schema	The overall structure (Blueprint) of the database
5.	Instance	Actual collection of data (snapshot of data)
6.	DBA	Database Administrator is responsible for overall control of the database

5.4.2 Data Abstraction

Data abstraction is a very integral part of RDBMS. It helps in easy visualization and implementation of the database schema without causing much change to the dependent features. Figure 5.11, refers to this data abstraction in an architectural way. It consists of three major levels: physical level, logical level and external level.

At the lowest level is the schema/database which is connected to the physical view of the model. The logical level consists of all the conceptual intricacies and dependencies required by external view. The uppermost layer is the external view level which is connected to the user application.

In order to support the dependencies of these levels, two data independence mechanisms are defined:

- Physical Data Independence
- Logical Data Independence

In physical data independence, the changes at the physical level do not affect the functioning and working of the logical level. Whereas, in logical data independence, if there is any change at the logical level, then it will not

reflect itself at the external level. Thus, with these mechanisms the data independence is restored in data abstraction.

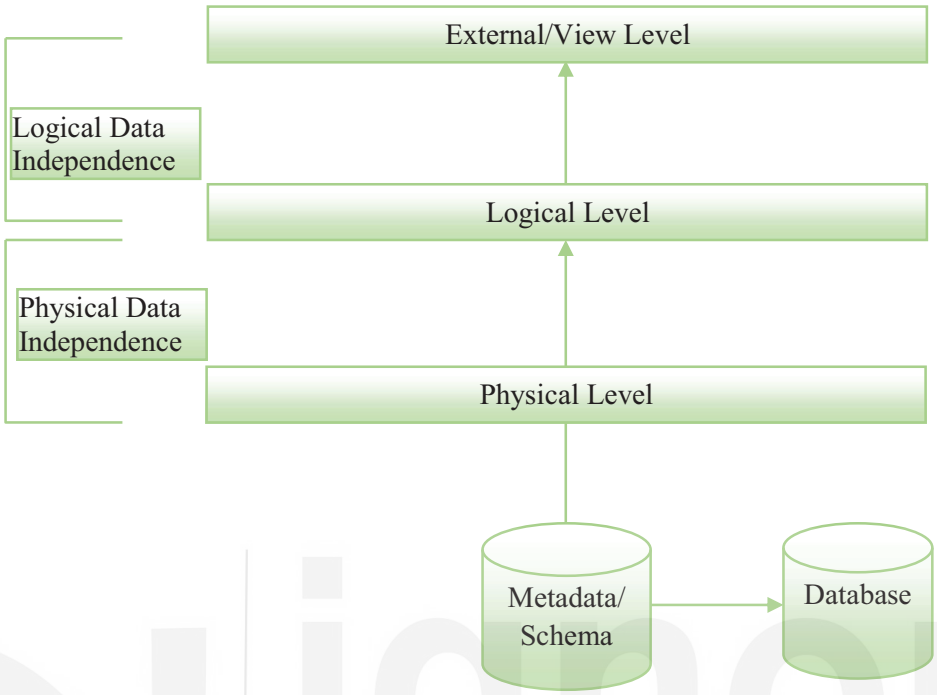


Fig. 5.11: Data Abstraction

5.4.3 Data Base Administrator

A Data Base Administrator (DBA) acts as a supreme controller of the database responsibilities. The tasks which a DBA has under his control are as follows:

- The designing of conceptual schema and update it under any changed requirements
- The efficient working of the storage structure and its methods of access
- Ensuring that the users get the desired information
- Ensure system security, as each user has a role and his rights has to be managed
- Ensuring the database against any malicious activity/attack
- Ensuring periodic backups and proper archival of data
- Executing recovery procedures in case of sudden disruptions/failures
- Ensuring proper functioning of system performance, procedures, and requirements
- To provide technical support for necessary tools and software up-gradations

A DBMS is a self-describing system which handles data abstraction, multiple view support, multi-user support, concurrency control, efficient recovery, effective access rights, restricting unauthorized access, controlling redundancy. It is also important to ensure the data integrity constraints,

concurrent access support, regular backup and recovery mechanism, easy adaptability, and ensure successful standards of maintenance.

So far, the readers are familiar with the concepts of a DBMS, RDBMS and roles and responsibilities of a DBA. In order, to view, manage and maintain a RDBMS, a Structured Query Language (SQL) is used. SQL is used to manage interactions with RDBMS. It is a non-procedural language, which is used to efficiently update, insert and delete the data from the database. It has 'English-like' syntax and is flexible. A query can be written in many different ways without affecting the output.

Table 5.3 and 5.4 illustrates the different types of SQL commands and SQL operators used to form a SQL Query.

Table 5.3: SQL Commands and their description

S. No	SQL Command	SQL Command Description
1	Data Definition Language (DDL)	CREATE, ALTER, DROP
2	Data Manipulation Language (DML)	INSERT, UPDATE, DELETE
3	Data Query Language (DQL)	SELECT <list of attributes> FROM <List of tables> WHERE <attributes of tables> GROUP BY <list of attributes> HAVING <predicate having aggregate values> ORDER BY ACS/DESC
4	Data Control Language (DCL)	GRANT, REVOKE
5	Transaction Control Statements (TCS)	SET TRANSACTION, SAVEPOINT, COMMIT, ROLLBACK

Table 5.4: SQL Operators

S. No	SQL Operators	Description
1	Arithmetic Operators	Addition (+), Subtraction(-), Multiplication (*), Division (/)
2	Logical Operators	AND, OR, NOT
3	Set Operators	UNION, INTERSECT,MINUS
4	Comparison Operators	=, >,<,>=,<=,!=,<>,

5.4.4 Data Retrieval

SELECT statement is used to extract information from the table. The query formation can be understood with the following example: *List Student names along with the names of their respective department heads.*

⇨ SELECT S.ENAME AS STU_NAME, H.E_NAME AS HEAD_NAME

FROM STUDENT S, DEPT D, HEAD H

WHERE S.DNO= D.DEPT_NO AND D.DEPT_HEAD=H.EID

INSERT, UPDATE AND DELETE OPERATIONS

Insert information of a new student with SID: '754874857', NAME: 'Ram Kumar'; DNO: 5, in the student table.

➔ INSERT INTO STUDENT VALUES ('754874857', 'Ram Kumar', 5)

Update the DNO of student with SID '857575858' to 6.

➔ UPDATE STUDENT

SET DNO=6

WHERE SID='857575858'

Delete Student with SID '89852579' from STUDENT Table.

➔ DELETE FROM STUDENT

WHERE SID='89852579'

Create Tables on the following Schema: Student (StuID#, S_Name, S_class)

➔ CREATE TABLE STUDENT (StuID# INT(5) PRIMARY KEY,

S_Name Varchar (30) NOT NULL,

S_class Varchar (30) NOT NULL);

SQL is not just a query language but it efficiently manages and updates the database in a simple and flexible manner. It has powerful features which makes it a robust language to implement complex queries.

5.5 DECISION SUPPORT SYSTEM (DSS)

A Decision Support System (DSS) is a computer application which analyses data (organizational/institutional) and presents it in such a way so that users can make business decisions effectively. It works on the principal of,

"Decide → Act → Review"

The decision support system works on training input (rudimentary parameters) and then outputs the target like decisions, reports. There are different types of DSS: Communication-Driven, Data Driven, Document Driven, Knowledge Driven and Model Driven. The basic working of a DSS constitutes of creating information and models, then elaborating the situation under observation with examples, processing the knowledge for domain intelligence which is finally required for data analysis (Figure 5.13).

Fig. 5.12: Overall Functionalities of a Decision Support System

Today taking decisions in complex environment is difficult as there is information overload and distortion in data. So, the decision makers emphasize on the approach of "*factual learning and decision making*".

Source: Health Catalyst

Fig. 5.13: Managerial Decision Making with Multiple Options is Difficult

This approach is not only simple to understand but improves the quality of decision making. Thus, the process of decision making is more efficient as

opposed to traditional approach. It is also important to understand that the amount of data to be analysed is increasing at a very fast pace. According to a recent article in Forbes by Bernard Marr, in May 2018, it is stated that 2.5 quintillion bytes of data is created everyday over internet. With this mind-boggling data figure, it is imperative to note that there is a need to have automated tools which can analyse this huge data effectively. In business scenario, managers are required to make decisions in complex environment and they have to understand the benefits and risks involved with a decision. In such cases, managers can make informed decisions and can support effective design & implementation of their choices.

Properly designed DSS is computer based software which helps the decision maker to compile useful information from raw data, documents or personal knowledge in order to solve complex problems. The structure of a DSS primarily comprises of:

- Managers & Staff Specialists
- Staff Assistants
- Expert Tool User
- Business Analyst
- DSS Facilitator

The major functionalities of a DSS can be summarized as follows:

- Provide support to mangers, individuals or groups
- Controlling and managing the decision making process
- Support to individual, group or interdependent decisions
- Adaptive and user friendly interfaces
- Support of decision making in structured or semi structured situations

The traditional ways of analysing data for a decision making process has certain drawbacks. Some of these include – less efficiency, scope of manual error, personal bias and testing overhead. To overcome these limitations, various DSS Support Tools are available. These tools help in easy management and visualization of the various important aspects of a decision making process. One of the popular tools is *'DSS Generator'*. A DSS Generator is a specialised package of hardware and software that has functionalities to quickly and easily build the modalities of a DSS. The Generator is flexible and adaptive and permits easy development of a wide spectrum of specific DSS. Due to its additional compatibility with today's complex environment, it has ousted *Excel and Expert Choice.*

The techniques and technical advancements in large databases, software engineering, optimization, artificial intelligence and human computer interaction will continue to enhance the functionalities of a DSS.

5.6 ENTERPRISE RESOURCE PLANNING (ERP)

Enterprise Resource Planning (ERP) is a planning system which evolved from Material Resource Planning II (MRP II) which aims at providing integration of information between customer, vendor and manufacturer using networks such as LAN, WAN, Internet etc. MRP II have again evolved from MRP systems which is a technique that explores the end product demands obtained from Master Production Schedule (MPS) for a given product structure. This product structure is taken from Bill of Material (BOM) into a schedule of planned orders considering inventory in hand.

Despite various advantages, MRP II has certain drawbacks:

- Ineffective integration of multiple functional areas to share resources
- In application, each transaction is treated separately
- No generic functionality is provided; specific functions cater to specific applications.

For the overall growth of the business environment the demands of the industry need to be understood. These demands could be the cost control initiative, cost analysis (product based or customer based), changing business requirement, effective decision making and many more. To handle such demands many applications or planning systems are available. Some of them are:

- Management Information System (MIS)
- Integrated Information System (IIS)
- Executive Information System (EIS)
- Corporate Information System (CIS)
- Enterprise Wide Systems (EWS)
- Material Resource Planning (MRP)
- Manufacturing Resource Planning (MRP II)
- Money Resource Planning (MRP III)

In comparison to MRP II, ERP is more effective in predicting and balancing Demand & Supply. In the next section, an introduction to Management Information System (MIS) is provided to gain a better understanding of the working of a management system.

Now by this time, the readers are familiar with Business Intelligence (BI) and ERP. It is the correct time to introduce two very important concepts: On-Line Analytical Processing (OLAP) and On-Line Transactional Processing (OLTP). Table5.5, generalizes the differences between OLAP and OLTP.

Table 5.5: Difference between OLAP and OLTP

S. No	On-Line Analytical Processing (OLAP)	On-Line Transactional Processing (OLTP)
1.	It has longer transactions (complex SQL Queries)	It has relatively short transactions (simple SQL Queries)
2.	It involves sequential access and updates	It has random updates
3.	The data is modeled using Dimensional modeling	The data is modeled using ER (Entity-Relationship) modeling
4.	Example: Business Intelligence (BI)	Example: Enterprise Resource Planning (ERP)

A BI framework has robust analytical applications, balanced dashboard, and high speed access to reports whereas, ERP being an OLTP records the transactions as and when they occur. The ERP software is designed for handling high speed transactions and minimum disk space utilization. A BI makes organizations agile and has future centric capabilities whereas; ERP delivers efficiencies to an organization. The similarity with both BI and ERP is that they are focused towards business improvement and deliver much significant results.

5.7 MANAGEMENT INFORMATION SYSTEM (MIS)

Information system is broadly divided into two types: Management Support Systems and Operation Support Systems. Management Information System (MIS) is a type of information system which falls under the category of Management Support System. An MIS is different from a DSS. Table 5.6, highlights the major aspects on which both of them differ.

Table 5.6: Major Aspects of Difference between MIS and DSS

S. No.	Aspect	Management Information System (MIS)	Decision Support System (DSS)
1.	Decision Making Level	Primary Level	Highest Level
2.	Operational Mode	Reports and Documentation	Practice choices and their analysis
3.	Objective	Operational Efficiency	Effective Decision making for the company
4.	Input	Large volume of data from various transaction processing units	Low volume of data as the data gets filtered till it reaches the DSS
5.	Output	Summary Reports	Decision Analysis

Examples of MIS are Bank Management System, Railway Management System, and Inventory Management System. Any MIS involves itself in the comprehensive report generation required for effective communication between the corporate employees (mangers). Despite various assets that an MIS provides, it suffers from many limitations also. There are areas where a management system needs to understand the relationship among various dependent and independent factors. These areas are as follows:

- Maintenance
- Cost
- Client Relationship
- Usage of various modules
- Customer Needs
- Ignorant to special needs of the organization

The primary motive of any MIS is to provide information required by managers which will enable them in effective decision making. The managers can use MIS as a tool to identify the problems they might face afterwards. It also helps in building a good solution to the problem. It gives a quick access of information to managers at various levels. It is also to be understood that while designing MIS, the managers should consider the behavioural aspects of the employees.

5.8 GENERAL DATA PROTECTION REGULATION (GDPR)

In today's age of digitization, people have a lot of their personal data online. It is because of this increase in the usage of online applications. That it is necessary to understand the need of data privacy. Companies worldwide are storing and archiving lot of personal data which needs to be regulated so as to protect the personal lives of people from getting affected. As a business gets, it is essential to have an understanding of various data protection laws/regulations. The concept of data privacy spans across the critical personal information, citizen unique identity, health and medical records, financial data, credit/debit card numbers, more basic personal information like residence address, date of birth and so on. All this information falls under *Personally Identifiable Information* (PII) and there is a need to secure PII. In view of this, the European Union in 1995 adopted Data Protection Directive officially known as Directive 95/46/EC. The directive aimed at the protection of processing and movement of individual personal data. Table 5.7, shows the official notification of this directive.

Table 5.7: Official Circular of Directive 95/46/EC

EUR-Lex
Access to European Union law

31995L0046

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Official Journal L 281 , 23/11/1995 P. 0031 - 0050

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

Source: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

This directive apart from many advantages was superseded by GDPR, acronym of General Data Protection Regulation. In December 2015, the European Parliament reached to an agreement for formulating new rules for data protection, "*the EU General Data Protection Regulation*". Figure 5.15, shows the nature of GDPR functionalities.

Source: Endpoint Protector

Fig. 5.14: Pictorial representation of General Data Protection Regulation

The GDPR aims at phasing out DPD at various levels of security like changing requirements for data protection, and widen scope, its enforcement and non-compliance to penalties. The major policy differences between them are tabulated in Table 5.7. Apart from all the extended functionalities, GDPR follows a simple regulatory environment for businesses that handles user's PII.

Table 5.7: Data Protection Directive (DPD) vs. General Data Protection Regulation (GDPR)

S.No	Policy Issue	Data Protection Directive (DPD)	General Data Protection Regulation (GDPR)
1.	Redefining Personal Data	DPD incorporated privacy to data such as names, addresses, email, phone, citizen's unique ID	Apart from data included in DPD , GDPR includes any information related to an individual (biometric, genetic, economic, social identity
2.	Individual Rights	The opt-out consent is not very friendly in DPD	GDPR empowers the people the right to access their data and the right to be forgotten where the user can explicitly opt out for his data display
3.	Data Controllers vs. Data Processors	Only data controllers were responsible for mishandling of data	Data processors and Data controllers are in compliance over monitoring of privacy protection
	Governance & Security	Lack of stiff enforcements	GDPR follows "privacy by design" and encourages organization to assess the automated data processing activities

Check Your Progress B

1) What schemes are available to support and establish small businesses in India?

……

……

……

……

……

……

2) What are the objectives of a Business? Explain with the help of examples.

……

……

……

……

……

3) What are the security issues in Information Technology?

……

……

……

……

……

4) Name the two kinds of Data Models.

……

……

……

……

……

5.9 LET US SUM UP

In order to maintain a good relationship between business and economy, it is always beneficial to know the end-user (of your product). Business information systems are designed to support effective decision making in an enterprise. Management Information System is a computerized database which is designed to handle, manage, and store, financial information of an enterprise and produces reports on a regular basis. Key aspects for any

management system to work efficiently are Business Plan, Market Analysis, Sales and Funding, Organization management and financial projections.

Now a day's people talk about data analytics & statistics. These terms mean nothing without appropriate data. This data is generated by the business organizations which can be further used for knowledge discovery and other potential applications. The generated data is to be analysed for effective decision making. This is done with the help of specialized software called as *Information System.*

A Data Base Management System (popularly known as DBMS) consists of a collection of logically related data and a set of operations which are required to access this data. A Database system eventually consists of Data Base and Data Base Management System. The information/data gathered from various operational units running in a business are stored in a repository. This repository is called as a *Data Base*. Once the data is collected, now the need is to analyse the data effectively.

Relational Data Base Management System (RDBMS) is based on relational model. This is the most commonly used record based model. Data abstraction is a very integral part of RDBMS. It helps in easy visualization and implementation of the database schema without causing much change to the dependent features.

A Decision Support System (DSS) is a computer application which analyses data (organizational/institutional) and presents it in such a way so that users can make business decisions effectively. It works on the principal of *"Decide → Act → Review".* The decision support system works on training input (rudimentary parameters) and then outputs the target like decisions, reports.

Enterprise Resource Planning (ERP) is a planning system which evolved from Material Resource Planning II (MRP II) which aims at providing integration of information between customer, vendor and manufacturer using networks such as LAN, WAN, Internet etc.MRP II have again evolved from MRP systems which is a technique that explores the end product demands obtained from Master Production Schedule (MPS) for a given product structure.

The GDPR aims at phasing out DPD at various levels of security like changing requirements for data protection, the widened scope, its enforcement and non-compliance to penalties. Apart from all the extended functionalities, GDPR follows a simple regulatory environment for businesses that handles user's PII.

5.10 KEY WORDS

Business: Business is a commercial activity of a person who has a regular occupation, trade or any line of work. It is also defined by the exchange of goods or services or one another for money.

Information Technology: IT is the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.

Data Privacy and Protection: Data protection is about securing data against unauthorized access. Data privacy is about authorized access who has it and who defines it. Another way to look at it is this: data protection is essentially a technical issue, whereas data privacy is a legal one.

Business Intelligence: Business intelligence is a set of processes, architectures, and technologies that convert raw data into meaningful information that drives profitable business actions. It is a suite of software and services to transform data into actionable intelligence and knowledge.

Data and Information: A data, in literal sense, would mean any character, word, number. If this data is not put in relevant context, it means nothing or little to us. On the other hand, information is known to be processed data which can be utilized for effective decision making.

Decision Support System: A Decision Support System (DSS) is a computer application which analyses data and presents it in such a way so that users can make business decisions effectively.

Data Abstraction: Data abstraction is a very integral part of RDBMS. It helps in easy visualization and implementation of the database schema without causing much change to the dependent features.

5.11 TERMINAL QUESTIONS

1) Explain three levels of data abstraction. Distinguish between physical and logical data independence.
2) Explain the role of Data Dictionary in DBMS.
3) Discuss the characteristics of information in strategic decision making.
4) Explain the importance of data models in business intelligence.
5) What is the role of information strategy document?
6) Discuss the benefits and limitations of centralized and decentralized information in business organizations.

Note: These questions are helpful to understand this unit. Do efforts for writing the answer of these questions but do not send your answer to university. It is only for yours practice.

UNIT 6 IT SECURITY MEASURES IN BUSINESS

Structure

6.0 OBJECTIVES

After studying this unit you should be able to:

- understand the meaning and importance of Cyber Security;
- understand the difference between Identification, Authentication and Authorization;
- understand what is Digital Signature and Digitization; and
- understand what is CAPTCHA Code and OTP.

6.1 INTRODUCTION

In the previous unit we have learned about securing business organizations from unauthorized users such as hackers. In this unit we will discuss the steps which are taken for securing the assets of business organizations. For small business organization checking the cyber-security may not be the top priority, because of its dimensions, but this aspect is important for their growth & survival. In the present scenario of digital era, organizations are migrating to online platforms to serve their customers better and their availability is enhanced by using internet. Because of migrating online the business organizations are vulnerable to a wide array of cyber attacks & threats. The organizations are being targeted constantly as well as security breaches are happening, but they hide it for the sake of their business.

Hackers are constantly looking to hack businesses organizations and many times they succeed in their efforts. The good cyber security system can protect the business organizations and hence, from the threats of these hackers. Cyber-security is the most important aspect of security for any organizations and hence should be taken seriously. Not only organizations are secure by adopting cyber security measures but their employees are also safe. All business organizations want to secure their assets and hence the role of cyber-security becomes extremely important. If a business organization has an effective security plan in place before any attack happens then only it can protect its assets from the hackers.

6.2 WHY SYSTEMS ARE NOT SECURE?

System security can be classified in two categories. First one is the physical machine security which is used to prevent theft of computer hardware. It is much more important now days to prevent theft or damage to the information system available in business data. Further, in today's corporate world, data is money and value is greater than the value of hardware in terms of cost. We can access the data of any business organization just by using remote access technology and networking devices, and thus physical security has no sense & meaning in today's digital world. We can only secure physical components of computer system by physical security. To secure the systems we have to define the policy on every system that what actions can be performed on a particular system and at what time. Thus we have to define the user category and the rights normal users and administrators well in advance. It may not be secure for beyond the specific policy and for advances in technology over the passage of time.

Although significant advances have been made in the state of the art of computer security in recent years, the information in computers is much more

vulnerable than ever because of online frauds. Every major technological advance in computing systems brings new security threats. The technology grows at a much faster rate than the rate at which solutions to curb the treats arising thereof can be developed. Further there is a need to cautiously deal with hackers, given their ability to acquire latest expertise in this regard. Therefore, we would be fighting a lost battle if the systems of a business organization are compromised. The system security is team work and it can't be achieved in isolation. By following logical piece of well-defined security architecture in the business organization we can protect our system from external threats & hackers.

We don't have any control on the way the world works and it is beyond our imagination and scope also, but just by understanding why it works &the way it functions, we can us avoid the typical pitfalls and choose acceptable security for any organization. This unit contains some basic and fundamental reasons why the implementation of computer security is not an easy task for any business organization.

6.3 CYBER SECURITY

In present scenario, cybercrime is not only problem of a country but it's a global problem. The boundaries of cybercrime are invisible & are spread world-wide. The cyber crime news is becoming headlines in recent times. Cyber crime is a threat to individual security and an even bigger threat to large international companies, banks, government organization and business organizations. The cyber crime is a type of organized crime and is committed by large organized & skilled cyber criminals online. The cyber criminals often employ highly-trained developers and these developers keep on updating their online attacks constantly. The cyber security has become essential now days for all the business organizations because no business organization wants can afford online attacks in present digital world. We can define cyber security in following words:

Cyber security is a pre-defined set of techniques used to protect the integrity of computer networks, programs, and data of business organizations from attack, damage or unauthorized access. The term security of business data has two important components, and these are namely cyber security and physical security. The enterprises have to protect their confidential data against unauthorized access from physical security as well as cyber threat. The term Information security, is designed to maintain the confidentiality, integrity, and availability of data, all the time and by all means. The use of cyber security can help prevent cyber attacks, data breaches, identity theft and can aid in risk management.

Cyber security involves protecting the system from un-authorized access, un-authorized deletion & un-authorized modification from the hackers. Cyber security provides a protocol that protects against all cyber attacks and makes sure that business data is secure from the hackers.

Fig. 6.1: Cyber security threats posed by hackers

The present generation uses smart phones and is connected with the internet all the time, and has no idea, how information reaches securely to their computers from unsecured media. This provides golden opportunity to hackers to hack data of these youth. There are so many access points, public IP's and constant traffic and tons of data to exploit by hackers. Furthermore, cyber attacks are evolving by the day. The hackers are becoming smarter and more creative now days with the state of art of training they receive from their trainers. It is a very tough task for the security administrator of big companies to outsmart the hackers and to protect their data from malwares & viruses which are tools used by hackers to bypass the firewalls of any organization.

6.3.1 Principles of Cyber Security

In implementing cyber security, there are two specific goals to be attained: first, confidential information must be kept out of reach of potential cyber attackers and other unauthorized individuals. Second, cyber security measures must not hinder authorized users' access to the information. Three main principles of cyber security are follows:

1) **Confidentiality:** Cyber security should ensure that the information to be secured is only accessible to authorized users and prevents the disclosure of information to unauthorized parties. For example, to implement confidentiality of company information on a cloud-based Customer Relationship Management (CRM) system, access can be restricted to users with the right username-password combination. Most systems also

implement confidentiality through data encryption, which is an additional layer of security. Decryption of the data requires an individual or system to attempt access using the requisite key.

2) **Integrity:** Cyber security efforts should ensure information remains accurate, consistent and not subject to unauthorized modification. For example, from the CRM example provided, integrity is achieved when measures are put in place to ensure that email communication between a sales representative and a customer is not intercepted and modified by an intruder when it is still in transit.

3) **Availability:** Efforts to secure information in cyberspace should not hinder its access by an authorized party. Additionally, cyber security implementation has to provide for redundancy access in case of any outage. For example, the company using cloud-based CRM system can implement proxy servers and firewalls as a security measure against Denial of Service (DOS) attacks, which would create system unavailability if successful.

6.4 IDENTITY THEFT

The term identity theft means cyber criminals illegally acquire credentials of innocent users and use these credentials to do online cyber crime by hiding their actual identity and using the identity of other innocent users. It is the criminal act of illegally and deceptively assuming the identity of another individual without their expressed consent with the intent of committing a crime; it also includes fraudulent and illicit attainment of personal information through the usage of unsecured websites. Through the use of stolen documentation attained upon illicit means of electronic acquisition - individuals can fraudulently assume the identity of others in order to engage in fraudulent purchases and illicit economic gain by using internet. In other words, identity theft is also called as identity fraud and is the act of a person obtaining information illegally about someone else without consent. The Hackers try to find out information about users such as full name, maiden name, and address, date of birth, UID, passwords, phone number, e-mail, and credit card numbers & CVV No. etc. to harm the users.

Fig. 6.2: Protecting the User Credential from Hackers

The hackers then use this information to gain access to other details of users such as his bank accounts, e-mail, cell phones, etc. Doing such acts, of acquiring information about others illegally is a crime under IT Act 2008 and may attract strict punishment by the judiciary under IT Act and such persons can be send to imprison for entire life if found guilty.

Methods to prevent identity theft:

i) At the time of entering any personal information on the Internet, please make sure that connection is encrypted.

ii) Avoid storing credit card or personal information on any website if you do online shopping over the Internet.

iii) Do have an active and up-to-date spy ware protection software & antivirus software.

iv) Make yourself aware about fake e-mails and phishing e-mails that claim to be a company

v) Never use unknown & unsecured systems & smart phones.

vi) Always have strong password & keep answer of secret question unguessable.

Check Your Progress A

Part A: Multiple Choice Questions

1) What is need of a Proxy Server?
   a) It is used to create a stronger connection with the target.
   b) It is used to create a ghost server on the network.
   c) It is used to obtain a remote access connection.
   d) It is used to hide malicious activity on the network.

2) In securing the environment against an attack which of the following is not needed?
   a) Education level of the attacker
   b) Configuration of system
   c) Architecture of network
   d) Companies business strategy
   e) Employees level of access to website

3) Which technology is used to hide information inside a picture?
   a) The Root kits
   b) The Bitmapping
   c) The Steganography
   d) The Image processing

4) Why Denial of Service attack is used?
   a) To exploit a weakness in the TCP/IP stack

b) For executing Trojan on a system

c) Just to overload a particular system so that it is no longer operational

d) Shutting down the service by turning them off

Part B: Short Answer Type Questions

1) What do you mean by Cyber Security?

……

……

……

……

……

2) Explain the reasons why systems are not secure.

……

……

……

……

……

3) What is do you mean by Identity Theft? Explain with example.

……

……

……

……

……

6.5 KEY SECURITY PRINCIPLES

IT security has to respect three contradictory requests; protection of confidentiality, integrity and availability of information. The key IT security principles are identification, authentication and authorization. Defining the security policies and designing the security elements lead to a safe and secure environment for information systems as a main support for open and dynamic business systems. User identification is a procedure during which a potential user identifies him to the information system when logging in. Generally, it is a process during which one entity introduces itself and identifies to another entity.

Authentication is the authenticity check procedure, i.e. it checks the user's identity, by comparing the data received from the entity with those stored in the base. It should be mentioned that the entity integrity is not necessary. For example, when logging on ISP it is possible to connect more people from the

same telephone line and the same computer, under the same user name and password.

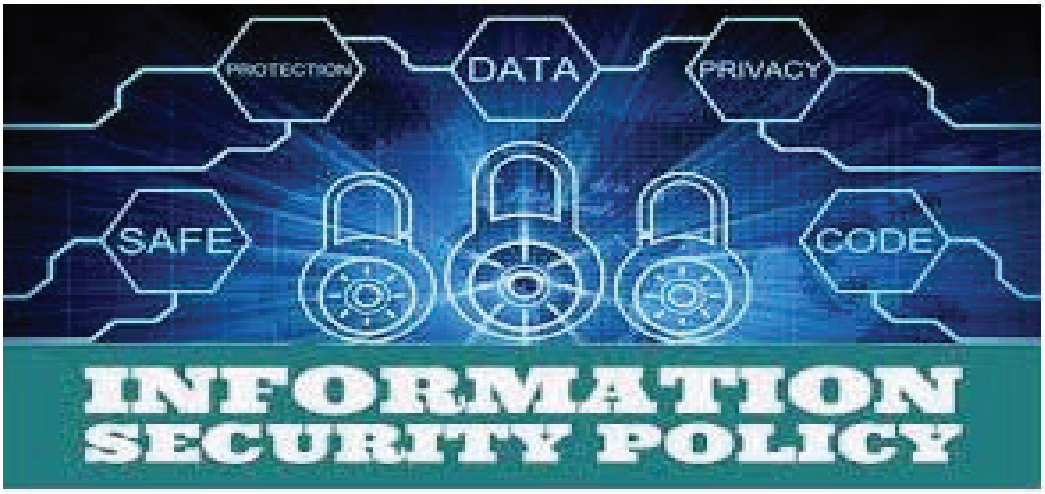


Fig. 6.3: Displaying the Steps of Information Security Policy

Authorization is the procedure of a system user access rights definition and most often it is a part of authentication. We will discuss details of these three principles of IT security in this section.

6.5.1 Identification

The term Identification in computer science is used to define and manage the roles and access privileges of individual users on the network. It also deals with the circumstances in which users are granted (or denied) those privileges. The user may be either customers or employee of the company. Identification is used to give the digital identity per individual, &once that digital identity has been established, it must be updated, maintained, and monitored throughout each user's "access lifecycle".

In other words: identification in computer science is an organizational process for identifying, authenticating & authorizing users to get access to applications, systems or networks by associating each user unique rights and restrictions with established identities. The identities are also referred as software processes that need access to organizational systems. Identification is used to uniquely identify user of a system as well as application that is running in the system.

In most information systems a username and a password are used as for checking the identity of a valid user. Anyone who enters the correct username and password is a valid user for information system. Therefore, to protect the system we should always keep secret the user name and password; otherwise the information stored in the system will not be secure. As long as the combination of username and password is secret the information stored in the database is secure.

6.5.2 Authentication

Authentication is the process to check the credentials of users before they are given access to use the resources of the system. It is the ability to prove that a user or application is genuine & on this basis it can use the resources of the organization or network. Authentication Identification is done on the basis of the identity of the user. Authorization process involves by giving username, a process ID, a smart card, or anything else that can uniquely identify that object at the time of authentication. If a user wants to access the information system which is available on a server then it must show its identity. In authentication, the user has to prove its identity to the server or client before it is allowed to use resources.

When a user provides appropriate credentials to prove its identity then only it is allowed to use the resources and this process is known as authorization. For example, when a user enters the correct username & right password then it proves that the user is the lawful owner of the username. In short, the authentication gives proof of a claimed identity& is allowed to access the resources. Server uses authentication process to know exactly who is accessing their information or site. Authentication is used by a client to establish connection with the server. There are several definitions of authentication; some of them are given below:

i) Server identifies a user by its username & password. Other ways to authenticate in a system are through cards, retina scans, voice recognition, and fingerprints.

ii) The third trusted party such as VeriSign is used to check the validity of each user certificate before it could be allowed by user to login.

iii) In bank websites username, password & CAPTCHA is used for authentication purpose.

iv) Authentication only identifies and verifies who the person or system is.

v) In bank ATM's password or PIN is used for authentication purpose.

vi) Smart cards and biometric credentials are used by employees to prove their identity. In the organization.

6.5.3 Authorization

The name authorization is methodology adopted by software companies to allow lawful users to system resources including files, services, computer programs, data and application programs. It is the process to grant or deny access to a network resource based on the user's identity. The authorization can also be defined in following words:

i) It is a process by which a server determines if the client has permission to use a resource which is available on the network.

ii) Authorization is followed by authentication by the server & it determines who the client is & what he is requesting for over the network.

iii) There are several types of authorizations and requirements for each of them may vary;

iv) There is no authorization required in some cases and in other authorization is required.

Some web security systems are based on a two-step authorization process, in which first step is authentication process, and the second stage is authorization process. The present operating systems work on effectively designed authorization processes to facilitate application deployment and management of resources. The main factors on which the modern operating systems work are: number of users and their credentials to login the system. The moment a user is identified and authenticated, it can be granted authorization based on its profile.

In other words, if all the users logs on by using same account, then they will be allowed to access the resources. In such situations it is very difficult to differentiate between the users of the system. Further, if users have been authenticated by different user accounts, they can be granted access to different resources based on their identity & profile.

Check Your Progress B

Part A: Multiple Choice Questions

1) Aim of Authentication is to:
   a) Restrict what operations/data the user can access
   b) Determine if the user is an attacker
   c) Flag the user if he/she misbehaves
   d) Determine who the user is
   e) None of the above

2) Cyber Attack is:
   a) DOS Attack
   b) Phishing attach
   c) Sending malware
   d) All the above

3) Authentication method is:
   a) Secret question
   b) Biometric
   c) Password
   d) SMS code
   e) All of the above

4) In role-based access control, each user is assigned one or more roles, and the roles determine which parts of the system the user is allowed to access.

   a) True

   b) False

Part B: Short Answer Type Questions

1) What are the key security principles of IT security for business organization? Explain with example.

   ……

   ……

   ……

   ……

   ……

2) Explain the need for user identification in online banking system.

   ……

   ……

   ……

   ……

   ……

3) What do you mean Authentication? Explain with example.

   ……

   ……

   ……

   ……

   ……

4) What is the difference between Authentication and Authorization? Explain with example.

   ……

   ……

   ……

   ……

   ……

6.6 SIX ESSENTIAL SECURITY ACTIONS

All the business organisations have to protect their IT security from unauthorized users and need to take steps to protect them from illegal users. The number of cyber attacks is increasing day by day and are affecting

businesses of all sizes. In such situations, it is necessary for every company to be aware of the dangers posed by cyber criminals and be ready to safeguards their data from such criminals and having in place proper security mechanisms. There are several approaches for securing the systems in the market and installation cost and time of use is also involved in their selection.

But which is the best security tool can be used in an organization depends upon various parameters. If the parameters of a security tool are best fit for any organization then it has to be purchased and installed. Further, the heads of organizations and heads of Security Company can discuss and negotiate to finalize the software which is best for any company. We have to also keep in mind that the software which is most advanced and which provides long-term protection can be given priority over the short protection time.

Almost all small businesses organizations use web-based technology tools to carry out transaction. For example, conducting long-distance conferences, giving advertisement, marketing products, doing research, identifying new markets, and communicating with customers and suppliers, have become integral part to the smooth functioning of small businesses organizations.

Fig. 6.4: Scurrying the Hardware from theft in Business Organization

We can install cameras to protect systems from physical theft now days. The advancement of technological aids and state-of-art security cameras, have made physical theft negligible. But protection from virtual world in current digital era is not easy and it needs technical skill set to protect data from outside world. The modern organisations are connected worldwide by internet and latest networking devices, which a boon and makes communication easy, but at the same time vulnerable to online theft. Along with several benefits of internet, there are many risks involved in digital era and is only growing every day. The small businesses organizations have many loopholes due to that they are prone to cyber-attackers. To protect the organization from cyber attacks following six measures are necessary to be adopted by them.

1) **Firewall:** Firewall is a type of virtual protection wall which helps to protect network traffic inbound and outbound to any organization. It stops unauthorized hackers from attacking the network by blocking them from the systems of organizations. Firewalls are programmed in such a way that they restrict the network from sending out proprietary data and confidential emails. The present era hackers have become more sophisticated with the state of art hacking technologies due to this reason firewall have become obsolete to stop them from the network of organizations.

   The firewalls are the most core of security tool of any organization, and will continue to remains for times to come. The firewalls are useful for the security of business organizations, but they have limitations too. The trained & skilled hackers have learned how to create data and programs that trick firewalls into believing that they are trusted one. This makes them to go through the firewall without facing any difficulty. Despite above limitations, firewalls are still very effective in detecting the unauthorized and less sophisticated malicious attacks on the data of business organizations.

2) **Antivirus Software:** The Antivirus program is used to remove the virus from system and network of business organizations. It is basic software and should be the part of any cyber security system. In addition to this use of anti-malware software is also essential now days. The antivirus works as the final frontier in securing and defending unwanted attacks from intruding the network of business organizations. The antivirus works by detecting and removing virus and malware, adware and spyware from the network. It also scans & filter out potentially harmful downloads and emails of systems of all the organizations. Install antivirus and anti-spyware software - any computer or network used by an organization should be secured with a good firewall that takes Wi-Fi into consideration. The latest versions of anti-spyware and antivirus software should be installed. Vendors provide security patches and updates for software, so be sure to update to the latest version regularly. Configure all software to install updates automatically.

3) **Use Complex Passwords:** The user-id and password is essential to access the resources of business organization over the network. We should always have strong password and keep it confidential from the hackers. The passwords should be changed periodically. Strong password is difficult for users to crack it and thus makes the data secure. We should confidential and complex answers to secret questions, so as to make it difficult for hackers to crack it. We should have strong password on social media sites so that our data on these sites is safe and its security is not compromised. We should use space before or after passwords to

throw the hacker off from the hacking the system. Keeping space makes password difficult to guess by unknown persons. If some has access to your password but is unaware that password has space then he or she can't access to your data. We should also use combination of upper and lower characters and special characters to make it complex for users to guess or crack. A combination of alphanumeric characters and symbols could also be used to make the password strong.

4) **Regular Backup:** The process of saving data regularly and taking backup saves organizations from the risks of data loss. In case of data loss backup is very useful and could be used to restore the data in business organisation. With advancements in hacking technology no network is safe & perfect now days. In present time data hacking and money hacking from banks become headlines in newspapers in which hackers try to bypass the bank network security and steal money illegally. In case of hardware failure backup data is very important to run the business smooth and business interest can be safeguards with regular backup.

   To reduce the risk, regular back of data is very much essential. We should set automatic backup option on in the servers of modern business organization. If the backup is regularly taken then it provides piece of mind to the management and helps to protect the interest of the business in the market. We should have multiple physical copies of our important documents in present digital age so that we can get back it in case of loss of data from physical or software failures, and in case of our systems are compromised by the hackers.

5) **Penetration Testing and Limit Access to Critical Data:** Testing is used to test the software with the objective of finding faults in it. There are several types of testing in software engineering and penetration testing is one of them. The penetration testing is used to test the security of business organizations by calling security professionals to test the network security of business data. The security professionals; use the same technique which the hackers use to find the potential weakness and vulnerability in the security systems. We should follow the advice of security professionals and add more security tools as per the suggestions to further enhance the security of servers.

   Penetration testing is one method to secure and enhance the security of data in business organizations. In addition to this we should have restriction on the access of critical business data from its employees. The critical data should be accessed by authorized users only and by means of authentication and authorization. Unauthorized and outsiders should not be allowed to access the critical data and should use mechanism to do

the needful this regard. We should keep the number of people with access to critical data to a minimum such as the company's CEO, CIO, and a handful of trusted staff only and should have a clear plan that mentions which individual has access to which sensitive information for increased accountability.

6) **Employee Training:** All the employees of business organizations handling critical data must be trained before they are given responsibility to secure the data. There are several types of attacks and phishing is one of them. To protect the business organizations from phishing attacks the employees must be trained how to handle keep secure data from such attacks.

   If the employee is trained enough for phishing attacks then only he can protect the critical data from loss. The phishing attack is making similar websites like original one and targeting customers and stealing their user id and password illegally. Once user's credentials are collected over phishing websites and then this credential could be used later on to withdraw money and the original users illegally. Thus training of employee's makes organization secure from online attacks and thus the data is made secure from unauthorized access.

   The employee who is handling the security tools must be trained to handle it properly before they are given responsibility to secure the organization. The first step in securing the organization from online threats is to recognize threat. Second step is to track the threat. The third step is to find the tools and antivirus to resolve the threat. The employees or the users who are accessing the network must be trained about the risk and precautions to which they have applied in case of cyber attack in business organization so that the risk is minimized. Further, in case of online usage, usage policy, usage rights, and usage profiles must be monitored to know the behaviour of employees and safeguard the business data from illegal access.

6.7 APPLYING PRINCIPLES TO INFORMATION SECURITY POLICY

The information security for all the organizations must be framed keeping in mind the level of its security required as per the suggestions and recommendations of cyber security experts. Important information security practices should be enforced and must not be overlooked by the security team at any cost. As we know that prevention is better than cure and if we have all the security measures in place then we can save the business data from wrong hands. The businesses must adhere to strict policies for information security inside their organizations.

It has been observed that preventive steps are only taken after the cyber attacks happen inside the business data. We should not wait for attacks to happen but take steps to secure the data from the very fist day of organization commencing its business. There are several steps to protect business data of any business organization. In addition to cyber attacks there are self propagating malwares which are risks for business organizations. All business organization wants their online presence to boost their business due to this reason their security becomes prime factor and utmost important for the management.

In view of above, business needs to look into tightening their security policies before it is too late for them to act. In this section we shall mention some steps which must be adopted to secure the business data in current digital age. These are:

Fig. 6.5: Applying IT Security Policy in Business

1) **Access control policy:** The term access control management plays very important role in securing the critical data from outsiders. Every business organization should implement access control policies strictly to protect it data. The social websites now days have become threat for the business organizations. These websites and Internet itself poses a lot of hidden threat for the data and we should deal these threats effectively by applying access control policy.

   The better password management techniques also helps to reduce the online risks involve in present digital era. The system admin should monitor the online threats regularly and advise all the users of business organization to adhere the security policy used in the organization. The system admin should advise all the users to change their passwords periodically and frequently to safeguard their system from hackers. Only authorized users should be allowed to use the resources of the system and unauthorized users must be stopped to access the system.

2) **Two-factor authentication policy:** The one time password technique is also known as two factor authentication policy and can be implemented to mitigate the illegal use of accounts. In this mechanism one time

password is send to the registered mobile number of the user. The user is then asked to enter the onetime password received through SMS. If user enters right one time password then his authentication is authorized and he is allowed to use the resources online.

The one time password technique has some limitations also and is not the best technique for two factor authentication policy. The alternate email authentication process is another method for double authentication of the users in the business organizations. We should use any of the double authentication policy to make secure the critical data of business organization.

3) **Encrypt your interactions:** The term encryption means hiding the plain text data and converting it to some code which is difficult for outsider to crack. To protect confidential data from outsiders it is encrypted before it is send from source computer to destination computer by using insecure network. Once the encrypted data reaches to the destination computer it is once again converted to actual form by using decryption techniques.

   This way of sending encrypted data over insecure network is known as encryption and decryption. The term encryption is used to convert plain text into coded form, and decryption is used to convert coded form into plain text at destination server. By using encryption and decryption techniques we can protect the critical business data from the hands of hackers.

4) **Safeguard your keys:** It is very much important to keep the login credentials secret to protect the data from unwanted hands, and access to the keys gives access to the information. Further, in case of physical lockers one should always have second set of keys which can be used in case first set is lost or stolen. Furthermore in case of loss of keys the second set of keys must be used to open the locker and may be at later time can be changed to avoid data or information loss from the business organization. Thus by safeguarding the keys we can stop business organizations data and information from unauthorized users and hackers.

5) **Backup your information:** One has to always make them sure about the backup and make it safe and protected. The term backup means making copies of business data and storing it at safe place at regular period to avoid loss of data in case of hardware failure or software failure. Business data &information should be accessible and must be encrypted and stored in a secure place. Sometimes business contracts have confidential information clause(s), which should not be disclosed to any organization which can misuse that information for its advantage. Such confidential data should always be maintained confidential and should not be disclosed to competing organization.

The business organizations do sign memorandum of understanding (MOU) for various types' partnership and exchange of goods from each other for the purpose of running their business in the market. Such MOU's should always be kept confidential and should not be disclosed any third party which has potential to misuse the data and information of MOU's between two business organizations. In case of any misuse of private and confidential data and information of a business organization by other competeting organization can be challenged in court of law and quantum of punishment and penalty is given by the courts for compensation the loss of any business organization.

The breach of confidentiality may occur without signing MOU agreement between cooperating organizations also. In India, employees of a business organization are required to keep confidential any secret information disclosed to them by the other party during their service time. Further, if employee does breaches of confidentiality then it may be challenged in the courts to get justice. The courts may hear the argument of both the parties and give justice to decide the case as per the proceedings and evidence produced in the court. The following types of questions may be asked by the court during hearing:

i) Information about confidentiality of facts

ii) Is discloser has any link in circumstances of case

iii) Is the party who received the information had misused it or not

Further, this is to be mentioned that although the law implies a duty of confidentiality – its scope, nature, and obligations are indeterminate and subject to judicial determination. The Frequency of leakage of confidential data and its nature should be dealt with utmost confidentially during the arguments in the courts. Some examples of such cases is given below to understand the confidentiality of data and information

i) Stealing of (laptop, computer, paper, MOU's etc. – physical security)

ii) Improper disposal of confidential information

iii) Unauthorized access type and its nature (access controls, authentication, lack of understanding of confidentiality agreements, negligence, etc.)

iv) Quantum of Loss of confidential data (negligence, etc.)

v) Hacking incident logs etc. (most often Internet security)

vi) The way of leakage of confidential data is measured by cyber security experts.

6.8 SECURITY SELF-ASSESSMENT

The ever-changing IT environment within organizations has evolving technology platforms, adoption of new devices, subscriptions and solutions. It is for this reason that enterprises must continually keep up with the reality of everyday routines that ultimately drive business (or slow it down). Practices that may have been efficient a year ago can rapidly diminish and become limiting today. Routine security risk assessments can help organizations stay proactive. With the right cloud tools and controls, enterprises can quickly adapt to the present changes.

It's important to ensure that physical devices are secured well in the business organization from physical theft. The cameras must be installed at strategic locations to deter & prevent physical theft in the business organization. The attackers try to gain the access of servers of business organizations through internet-enabled devices and un-patched exploits. The physical networking devices such as wireless printers, Wi-Fi routers, Hubs, UTP cables and moveable devices may be exploited by the hackers to get access of entire network of business organization. There are different levels of risk assessment and cyber security experts may be used by business organizations to check for loopholes in the security of computer network and suggest the measures to resolve it. The security analysis of business organization can be done by expert network administrator of business organization also. The cyber security companies specialized in vulnerability and risk assessment testing for clients may be roped in to suggest the means and ways to secure the network. The services of cyber security experts have some cost involved, and this cost may not be feasible for small business organizations.

The employees of business organization should do risk assessment and must make it a routine process, irrespective of size and scale of businesses industry. The security breaches may happen to any business organization, especially small businesses, either because hackers believe that they are easy target while trying to breach a larger company by chance. The self-assessment and monitoring should be made a compulsory and continuous process for securing the business assets. Further, a comprehensive security risk assessment should be conducted at least once or twice in a year, which has been suggested by Information Systems Audit and Control Association.

The self assessment method is very effective in finding vulnerabilities in any business organization. It is the responsibility of IT staff to present self assessment plan to management and implement it in association with management to find the vulnerability in the network. The creator of a network understands the network structure well and his services may be utilized for assessing the vulnerability in the network. Since he is the network creator he would be able to assess the security issues, more quickly than

others. To protect the business we should secure the network first and do the needful assessment periodically.

Further, if online transaction is accepted by any business organization then it is much essential to call the cyber security experts for assessing the vulnerability in the network and to fix the vulnerability by initiating steps to secure the network as per the suggestions received by the cyber security experts. If any business organization has not done security assessment then it is prone to cyber theft and it must take steps for security assessment as soon as possible. In today's digital world cyber-attacks on businesses organizations are increasing everyday and it is a reality. In past year several cyber attacks were reported by print and electronic media such as phishing scams, ransom etc. In future several cyber attacks shall be carried out by cyber attackers to steal the data and information of business organization. It is the duty of all the internet governing agencies of the world to sit together to plan the strategy to check the cyber attacks and frame the policies to punish the hackers worldwide to protest the interest of business community world wide to secure business organizations.

Basic Steps of Risk Assessment

The basic steps of security assessment could be as follows:

1) **Identify:** Characterize the system (process, function, or application)
2) **Protect:** Identify Threats
3) **Detect:** Determine inherent risk & impact
4) **Respond:** Analyse the control environment
5) **Recover:** restoration of systems and improvements

Empowering Users: In most cases, the biggest threat to an organization is the people who work there. Employees within an organization are the main threat to cyber security. Those without knowledge have the most opportunity to expose your data, second to vendors with access to your systems. Recognizing phishing mail and proper management of user access and authentication, to recognizing phishing emails, users can make or break your security. Keeping employees educated is the key to preventing attacks and responding to them accurately.

Creating a Risk Assessment: In today's digital world, 85% of business assets are in digital format. Therefore, it is critical that organizations take precautions before it's too late. Risk assessments of any business organization should be assessed by cyber experts including application program, functional part, or the processes followed in by that organization. First of all we have to understand the size, scope and complexity of the business organization to go for security assessment. Once it is estimated then the time, cost, and manpower needed for security assessment should also be

estimated. In risk estimation process we have to identify internal and external systems of business organization which critical for running the organization. In this process we have to take the backup of sensitive business data including operations, process, legal MOU's, credit card information and many more, before we start security assessment.

Risk assessment can be done on the basis criticality and sensitivity of information. The assessment results gives us idea how to secure the business data, how much time is needed and what methodology to be followed and how much man power is required to secure the data in given time period. All these help us to recognize the missing piece of business data.

In recent years several automated tools and application have been developed by software developers for assessing the network security of nay business organization. Some of the tools are open source and you can directly download them from internet. Some tools are paid and you can download them just by paying nominal charges online and can use them to secure your business organization. The Microsoft windows- 0 is equipped with security assessment tool and same can be used to protect the data of business organization.

Check Your Progress C

Part A: Multiple Choice Questions

1) The Network Layer Firewall works as per the following
   a) The Frame filter
   b) The Packet filter
   c) Both Frame as well as Packet filter
   d) None of the mentioned
2) What is Firewall
   a) A hardware
   b) A software
   c) A hardware as well as software
   d) Neither hardware nor software
3) The full form of DPI is
   a) Dots processing Inch
   b) Dots per Inch
   c) Diagram per Inch
   d) Diagram processing Inch

Part B: Short Answer Type Questions

1) Explain six security essentials for action with example.

……

……

……

……

……

2) Explain principles of IT security with example.

……

……

……

……

……

3) What do you mean Security Self-Assessment? How it is implemented?

……

……

……

……

……

4) What do you mean by Empowering Users? Explain with example.

……

……

……

……

……

6.9 DIGITIZATION

The term digitization is used to convert paper based data and information into electronic way of saving, so that it can be retrieved, processed and updated by using computer system. The integration of digital technologies into computer readable format is known as digitization. The everyday routine things can be digitized by using electronic devices such as computer system and mobile phones. The digitization is a process of converting information into a digital format. In digital format, information and data is organized & stored on storage devices such as hard-disk, into discrete units of data, which could be separately recognized & addressed. In digitization data is stored in computer

hard disk in the form of binary number, which can be processed by using computer systems.

The text, audio, images and video data can be digitized by using scanners, cameras and apps. The scanners are used to scan the images and save them in the form of jpg or bitmap images which can be stored in the computer memory for future use. An Optical Character Recognition (OCR) technology is used to analyse and identify the digits and data written on bank cheques and to convert each character into an ASCII code.

The audio and video digitization is used to convert analog-to-digital & vice versa by using computer system. In this process analog signals are converted into digital signals and their quality is enhanced by using the tools and apps, without compromising the actual basic content of picture data. In this process analog signal strength is also enhanced and its resolution can be enhanced by using computer software. Thus the digitization process is very much helpful in storing and keeping the paper format for longer time and for future reference purpose for the knowledge society. For example all the court paper based judgments are now being digitized in India and stored in binary format in computer which can be easily referred in another case by Judge in the courts.

The digitized information makes it easier to preserve, access, and share by using Internet and computer network. For example, an original historical document may only be accessible to people who visit its physical location, but if the document is digitized, it can be made available to the people of entire country and even for whole world. In today's digital world there is a growing trend towards digitization of historically and culturally data in our country.

6.9.1 Impact of Digitization in Business World

Digitization is very vital in business world in the present digital era. It requires constant change and development in the business organization. With the advancement in hardware and software technology, digitization is now very easy task in compared to times decades ago. Digitization has made life simple and with the help of digitization digital data is 24×7 available to intended user with latest state of art internet technologies. In present digital era digitization is rapidly changing the business world and all the business houses must adapt to digitization to survive in the present digital age to reach to their customers.

1) **Artificial Intelligence (AI):** Artificial intelligence is the design and development of artificially intelligent machines which can do the work the way human do AI has already changed the business world to such an extent, that all the business organizations are using AI in their products.

For example AC, Refrigerators and all electronic house hold devices are not IOT based and these can communicate for better utilization and their use can be optimized. AI is now days being used for performing data analysis, creating algorithms, and even improving the communication between the company and clients worldwide including India.

2) **Flexible Work:** Digitization has given choice to IT employees to work from home rather than from office, thus saving in terms of travelling time, cost and office expenses. All the data and information is now days is stored on digital media and can be accessed just by sitting at home. Many IT companies are now offering at home jobs to their employees to decrease company cost and to increase the productivity. The technological progress and digitization in today's digital age has made it possible to adjust work schedule as per our personal needs and lifestyle. Because of flexibility and better productivity more and more IT companies are relying on freelancers and remote workers to work for them by using internet and state of art network technologies.

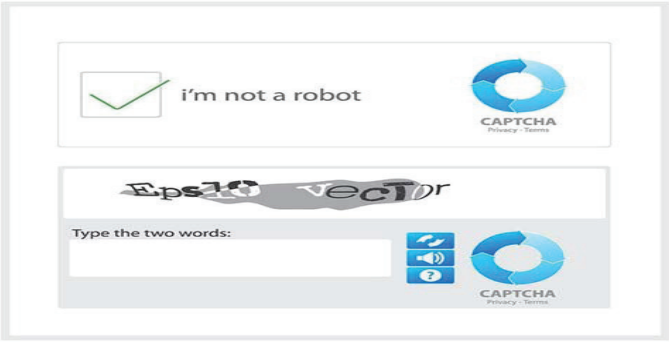
3) **Innovation:** The digitization is now days being used to convert paper data into binary form to be stored in computer systems. These digital contents are now days being used widely for doing research by many research scholars in Universities and Colleges throughout India and rest part of the world. Digitization has made availability of digital data 24×7 for the researchers due to that many researchers are developing new and innovative products in the market. Because of digitization many new, innovative solutions have come into the market and thus are making the life simple of all types of people. The can be applied to almost any aspect of the business world, including traffic management, workforce management, production management and many more. The latest Innovations in technology have generated new ideas in business world to reach to a wider internet savvy customer to sell their product online thus making customers happy, satisfied, and product is available to the customer 24×7 by means of internet and network.

4) **New Business Models:** The digitization in today's digital world has made it possible to create many new business models to deal and offer to customers. We can buy products online instead of physically visiting the shops and incurring travel and time cost. In today's digital age all the information and tools are available online and business organizations can create and propagate their business models to their customers freely and easily. The companies can apply new ideas to reach to the customers to sell and market their products and just making their business flourishing day by day.

5) **Communication:** Business organizations have to communicate with their counter parts and customers in their business process. The Internet and social media such as Facebook, WhatApp, and Instagram has made the communication very simple in today's digital age. Further, communication plays very vital role in life as well as in business. The proper communication makes business thrive and develop and present the right product to the customer. The lack of right information transfer leads to misunderstandings and conflicts. There are many tools, channels and apps via which a business can communicate, both with the employees and with its clients. The Internet has provided various platforms for smooth exchange of information, and even files, documents, data etc between company and its users. In today's digital age one can use, Skype, Slack, Blogs, videos, Facebook and other "tools" to communicate and exchange their thoughts, with their customers and cooperating organizations.

6.10 CAPTCHA CODE

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a method used to protect websites against spam. The goal is to stop interactive websites from being spammed by filtering out automatically generated input. The full form of CAPTCHA is to differentiate between humans and computers. CAPTCHA was invented by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford in the year 2003. As early on as the year 1950, the computer scientist '**Alan Turing'** suggested a method for testing the intellectual capacity of artificial intelligence. According to the computer pioneer, a machine is able to mimic the human mind when it manages to converse with people in a chat without then realizing it is a computer. To stop spam IT companies use CAPTCHA codes to differentiate between users and computers as users. The CAPTCHA is used in the login process by secure websites. The CAPTCHA letters are a way to check if the person registering in website is a real live human being or a computer program attempting to spam the into the website.



Source: CAPTCHA

Fig. 6.6: System generated CAPTCHA Code

The use of CAPTCHA makes website secures from the hackers but at the same time it irritates the genuine users. By using CAPTCHA we can be secure from getting spam emails from unauthorized users, thus it makes website secure and safe for the users.

6.10.1 Purpose of CAPTCHA

CAPTCHA are usually used when web applications require user input. Imagine you are running an online store and want to give your customers the opportunity to write product reviews in a comments section. In this case, you want to ensure that the entries are actually from your customers or at least from human site visitors.

You can reduce the risk of this happening **by** protecting online forms with a **CAPTCHA**, by making users verify that they are human before they can submit their comment. CAPTCHA are now found in almost all sectors where human users need to be distinguished from bots. For example, this includes registration forms for e-mail services, newsletters, communities and social networks, as well as online surveys or web services, such as search engine services.

6.10.2 Types of CAPTCHA

CAPTCHA based methods for Human Verification can be roughly divided into text and image-based CAPTCHA, audio CAPTCHA, mathematical CAPTCHA, logic CAPTCHA, and gamification CAPTCHA**.**

1) **Text-based CAPTCHA:** The oldest form of Human Verification is the text-based CAPTCHA. Known words or random combinations of letters and digits are alienated. In order to continue, a user has to decipher the code represented in the CAPTCHA box and enter the solution into the text box. Classic techniques used to create text-based CAPTCHA are Gimpy, ez-Gimpy, Gimpy-r, and Simard's HIP.

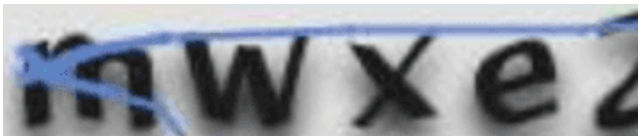


Fig. 6.7: Text based CAPTCHA

Text distortion and background noise should make it difficult for recognition systems to read. Text CAPTCHA only provide reliable protection against spam when the solution can't be cracked by programs with automatic text recognition.

2) **Image-based CAPTCHA:** An alternative to text CAPTCHA is the image-based method. Instead of presenting users with an alienated solution comprising of numerals and letters, image-based CAPTCHA are based on quickly recognizable graphical elements**.** As a rule, several

photos of everyday objects are displayed side by side. The user has to click on the images that are similar to the original image, or to show which ones represent a semantic content. This next example shows a cat as the main image. The user then has to decide which of the other 9 photos depict cats, and then click on them in order to complete the CAPTCHA.

Fig. 6.8: Image based CAPTCHA

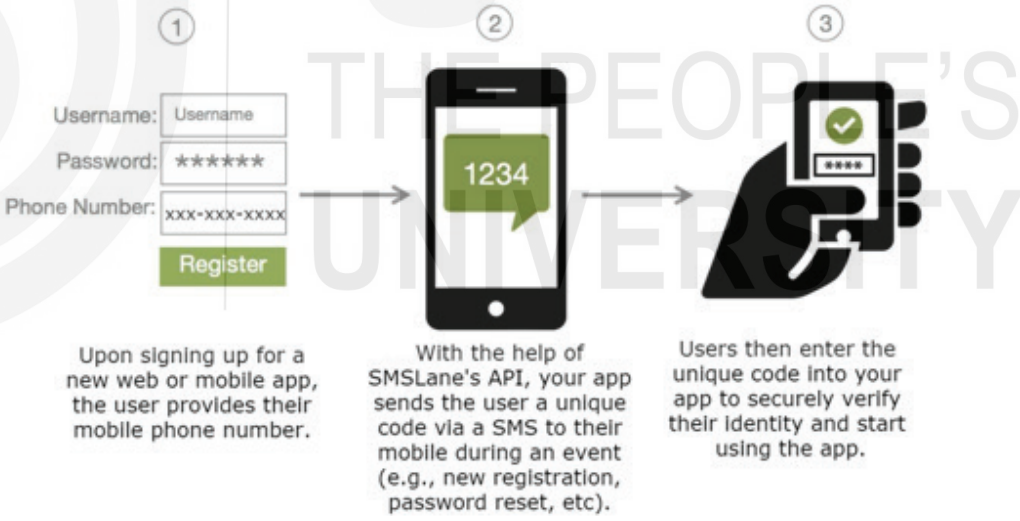
3) **Audio CAPTCHA:** Text and image CAPTCHA can be assigned to the graphical Human Verification process. Whether a human user can easily pass this step depends on how good their ability is to recognize the displayed text or image information. How will a visually impaired person be able to read a CAPTCHA? Website operators should ensure that their selected CAPTCHA method has several solutions to increase their website's usability**.** So that visually impaired people can also successfully solve CAPTCHA codes, text-based or image-based test methods are usually combined with so-called audio CAPTCHA. There's often an extra button that the user can press in order to hear an audio recording, e.g. a short sequence of numbers, which is then entered into the input field.

4) **Mathematical tasks and logic CAPTCHA:** A CAPTCHA alternative, which also takes into account the needs of the visually impaired, relies on mathematical tasks or puzzles to filter out spam bots. A task like the following can be read out with a screen reader, if required, meaning that it can also be used by users with non-visual output devices. To verify themselves as human beings, users have to solve a mathematical problem. These mathematical equations are simple to solve, but the problem is that they aren't much of a hindrance to computers since

computer people are good at dealing with numbers. This type of CAPTCHA is therefore often combined with various kinds of text alienation so that it's impossible for screen readers to make sense of it. For example, calculate 7 x 7 and only enter the first digit of the result in the box. The result would be 49, so the CAPTCHA solution would be 4.

6.11 ONE TIME PASSWORD (OTP)

The full form of OTP is one-time password. It is also known as one-time pin. OTP is a password which can be used only once to login into the computer system and also to make secure online transactions. The OTP is numeric or alphanumeric automatic generated string which is used as one-time password for a single transaction or login session. The OTP is more secure than a static password, and is sent to the registered mobile number of the user. Since OTP is received on registered mobile number of the user due to this reason it has less chances of misuse by cyber hackers. The OTP is an additional authentication process used by website to double authenticate the real user before he is allowed to access the resources of the computer system or any server. OTP security tokens are microprocessor-based smart cards or pocket-size key fobs that produce a numeric or alphanumeric code to authenticate access to the system or transaction.



Source: smslane.com

Fig. 6.9: Two Factor SMS Authentication (2F OTP SMS)

This secret code changes every 30 or 60 seconds, depending on how the token is configured. Mobile device apps, such as Google Authenticator, rely on the token device and PIN to generate the one-time password for two-step verification. OTP security tokens can be implemented using hardware, software or on demand. Unlike traditional passwords that remain static or expire every 30 to 60 days, the one-time password is used for one transaction or login session.

6.11.1 How to Get a One-time Password

When an unauthenticated user attempts to access a system or perform a transaction on a device, an authentication manager on the network server generates a number or shared secret, using one-time password algorithms. The same number and algorithm are used by the security token on the smart card or device to match and validate the one-time password and user. Many companies use Short Message Service (SMS) to provide a temporary pass-code via text for a second authentication factor. The temporary pass code is obtained out of band through cell phone communications after the user enters his username and password on networked information systems and transaction-oriented web applications. For two-factor authentication (2FA), the user enters his user ID, traditional password and temporary pass-code to access the account or system.

6.11.2 How a One-time Password Works

The encryption and decryption techniques of cyber security are used to generate OTP. We use mathematical Hashed Message Authentication Code (HMAC) algorithm of cyber security to generate OTP-based authentication message. This OTP message is then sent to the user's registered mobile number. For security reasons OTP values are valid for few seconds of their generations and users should enter them during that specified time to do login to access the resources of the computer system or server. The one-time password is delivered to a user through several channels, such as SMS-based text message, an email or a dedicated application on the endpoint.

6.11.3 Benefits of a One-time Password

The OTP is used to verify and validate the genuine users to allow them to login secure website by using their credentials as well as securely received OTP text message received on the registered mobile number of the user. It is very useful for IT managers IT administrators of any business organization and secures for the users as well as for customers of the company. The advantage of OTP is that they become invalid in seconds thus it prevents unauthorized attackers from obtaining the secret codes and reuse it hack the business data illegally.

Check Your Progress D

Part A: Multiple Choice Questions

1) What is Cyber Crime?
   a) The virus attack
   b) The worm attack
   c) Hacking the system
   d) All the above

2) Use of internet to harass a person or group of individuals known as:

   a) The cabernet

   b) The cyber policing

   c) The cyber stalking

   d) The cyber space

3) We should follow below steps to stop harassment using internet

   a) By installing Anti-Virus

   b) By taking regular back-up

   c) By not clicking on unknown links

   d) All the above

4) An unsolicited mail sent to a large number of persons without their consent, is known as

   a) The worm

   b) The spam

   c) The trojan

   d) The online marketing

Part B: Short Answer Type Questions

1) Explain the term Digitization.

   ……

   ……

   ……

   ……

   ……

2) What are CAPTCHA's? Explain their use in user authentication.

   ……

   ……

   ……

   ……

   ……

3) Explain the impact of digitization & IT Security in Business organizations.

   ……

   ……

   ……

   ……

   ……

4) What is the full form of OTP? How it is used for online transaction in banking sector?

……

……

……

……

……

6.12 LET US SUM UP

Identification, authentication and authorization are the main prerogatives for the data contents security and for the safe communication among the users of the open distributed systems, as well. These measures are performed on the physical and logical level, and special attention is paid to communication between the Internet and intranet. The implementation itself, without adhering to security principles important for their introduction and use, does not guarantee security – neither of the data contents in database, or the one in communication.

Data contents should be protected by means of cryptographic algorithms, where complexity and speed depend on the required security level. The example of this is an electronic signature, the means of accuracy confirmation and message credibility. Authenticity protocols, even complete authentication systems were generated as the means of cryptographic algorithm implementation, security methods and principles (of data contents) in dynamic and distributed systems, which become very important in the case of electronic financial transactions, i.e. electronic cash payment protocols.

6.13 KEY WORDS

Key: In cryptography, a key is a piece of information that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into cipher text, and vice versa for decryption algorithms.

Private Key: A private key is a tiny bit of code that is paired with a public key to set off algorithms for text encryption and decryption.

Public Key: Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.

Encryption: Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

Decryption: Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or un-encrypting the data using the proper codes or keys.

OTP: OTP is a password which can be used only once to login into the computer system and also to make secure online transactions. It is numeric or alphanumeric automatic generated string.

CAPTCHA: CAPTCHA based methods for Human Verification can be roughly divided into text and image-based CAPTCHA, audio CAPTCHA, mathematical CAPTCHA, logic CAPTCHA, and gamification CAPTCHA.

Authentication: Authentication is the process to check the credentials of users before they are given access to use the resources of the system. It is ability to prove that a user or application is genuine& on this basis it can use the resources of the organization or network.

Authorization: Authorization is methodology adopted by software companies to allow lawful users to system resources including files, services, computer programs, data and application programs. It is the processes to grantor deny access to a network resource based on the user's identity.

6.14 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress A

1) d 2) d 3) c 4) c

Check Your Progress B

1) d 2) d 3) e 4) a

Check Your Progress C

1) b 2) c 3) b

Check Your Progress D

1) d 2) c 3) d 4) b

6.15 TERMINAL QUESTIONS

1) What is phishing?
2) List some security attacks.
3) Which technique is based on Vernam Cipher?
4) Define Cryptanalysis.
5) What is plain text cipher text and coded text? Explain.
6) Explain digital signature.

7) Define integrity & non repudiation.
8) Explain any two classical ciphers.
9) Explain one time password.
10) What are active and passive attacks? Explain with suitable example.
11) What do you mean DES in cryptography?
12) Explain the use Hash function in cryptography.
13) What do you mean by Private and public key?
14) What do you mean by hackers? Also explain ethical hacking.
15) Discuss Digital Signature.

Note: These questions are helpful to understand this unit. Do efforts for writing the answer of these questions but do not send your answer to university. It is only for yours practice.

UNIT 7 INTERNET SERVICES AND E-MAIL CONFIGURATION

Structure

7.0 OBJECTIVES

After studying this unit, you should be able to:

- identify various usages and advantages of Internet;
- explain how Internet functions;
- describe different types of Internet services; and
- describe the significance of domain names and URLs.

7.1 INTRODUCTION

With the developments in the domain of Information Technology, Internet has become a ubiquitous tool for accessing information, providing opportunities which were unheard of, and easing the exchange of information, It provides us with a gateway to access, interact and connect with people and resources. The rise in popularity of Internet can be attributed to the services provided by it which are used for business, interactions, improving the knowledge/skills, banking etc.

E-mails (Electronic mails) are the most popular service provided by the Internet. E-mail is basically electronic message communication between people across globe. Few other popular services include World Wide Web (WWW), Web services, File Transfer Protocol (FTP), Chat Rooms, Video conferencing, News groups, Instant messaging etc. Most of these services are discussed in detail in upcoming sections of unit.

7.2 ABOUT THE INTERNET

As defined by Strauss, El-Ansary, Frost (2003) "The Internet is a whole network that is connected to each other. Some computers in this network store files, such as web pages, which can be accessed by all network computers." While O'Brien (2003) posited "the Internet is a rapidly growing computer network of millions of businesses, education, and government networks that are interconnected by the number of users more than 200 countries."

Based on above definitions the basic concept of Internet is global network of physically connected devices for exchange of information. It can be referred to as 'network of networks' consisting of millions of interconnected devices linked by networking technology. The Internet offers myriads of benefits and opportunities. Some of these are listed as follows:

- **Ease of communication:** with emailing and chatting options available, we can easily connect to other individuals in real time.
- **Available round the clock:** the Internet services are available round the clock.
- **Information source:** Internet has enabled us to access unlimited amount of Internet from anywhere on earth.
- **E-commerce:** Electronic commerce owes its birth to Internet. We can shop online across different websites at just one click. We need not visit the stores to order things.
- **Other services:** Internet has made available, services like online banking, hotel booking ticket booking, job search and counseling services in electronic form conveniently over the Web.

7.2.1 How the Internet Functions

The Internet functions via a packet routing network following the protocols - specifically IP (Internet Protocol) and TCP (Transport Control Protocol). Each of the term has been explained below for clarity:

- **Protocol:** Set of rules in accordance of with computer communicates with each other's is known as protocol.

- **Packet Routing Network:** Fragments of data sent across the Internet is called packets. In case of the packet routing network, the packets are directed the source to the destination computer.
- **Internet Protocol:** Set of rules for specifying how to route information by attaching addresses onto the data sent by it.
- **Transport Control Protocol:** TCP handles the reconstruction of message at destination, re-sending of the information in case any information is missed.

7.3 TYPES OF INTERNET SERVICES

As explained in the previous section Internet is the interconnected global computer network which operates through certain set of rules called protocols. From an end-user perspective it's the services that Internet provides make it popular.

- **E-mail:** E-mail is digital form of message exchange between people. The ability to send the message across globe within seconds has made it the most popular form of message communication and has replaced almost every other physical form of communication such as letters in many spheres of life.
- **World Wide Web:** Most important service of Internet which is essentially for global information sharing. It is combination of all resources- text pages, digital photographs, music files, videos and through communication model enables the exchange of the information over Internet.
- **Web Services:** Web services are the standardized medium for propagation of communication taking place between the client and server applications on the Internet.
- **File Transfer Protocol (FTP):** FTP is used for exchange of files across computers through Internet.
- **Chat Rooms:** They are the mediums which are used for real time conversations between persons in form of text, voice or video.
- **Mailing list:** It is the collection of names or/and addresses for including the people who subscribe to mailing distribution on regular basis.
- **News groups:** It is an Internet-based forum for discussion on various topics by remotely connecting different users across the globe.

Check Your Progress A

1) What is an Internet?

…….

…….

…….

…….

2) List down any four benefits of Internet.

…….

…….

…….

…….

…….

3) Fill in the blanks:

i) ……are the mediums which are used for real time conversations between persons in form of text, voice or video.

ii) A …….. is a network that directs packets from the source to destination computer.

iii) …… is used for exchange of files across computers through Internet.

iv) …….. can be referred to as 'network of networks'.

7.4 ABOUT E-MAIL AND ITS CONFIGURATION

E-mail or electronic mail is one of the most popular services provided by Internet where we can send or receive message from people sitting anywhere in globe in seconds over Internet. The electronic mail was introduced in 1960s. In today's world most of us are using emails to make our lives easier.

The communication in an electronic mail is usually done via three protocols:

- **SMTP:** The SMTP stands for "Simple Mail Transfer Protocol" which is used for sending mails. The message in the mail is sent by a mail client (like Gmail) to a receiver comprising of receiving email server. The sender uses SMTP server for carrying out the process of transmitting an email message.
- **IMAP:** The IMAP stands for "Internet Mail Access Protocol" which deals with managing and retrieving email from receiving servers. These protocols are used only while receiving the email and they cannot be used for sending the email. The emails will be present in the server and not get downloaded to the user's device and they can be edited as if they are on the user's device. The user can also simultaneously connect with the server from multiple devices.
- **POP:** POP stands for "Post Office Protocol" which is also used for incoming emails. The current version is 3 and POP3 is most widely used version. Unlike IMAP it downloads the entire email into the local user device. Once the mail is downloaded on the user system, it would delete the data on the server which is quite helpful in a server with less free

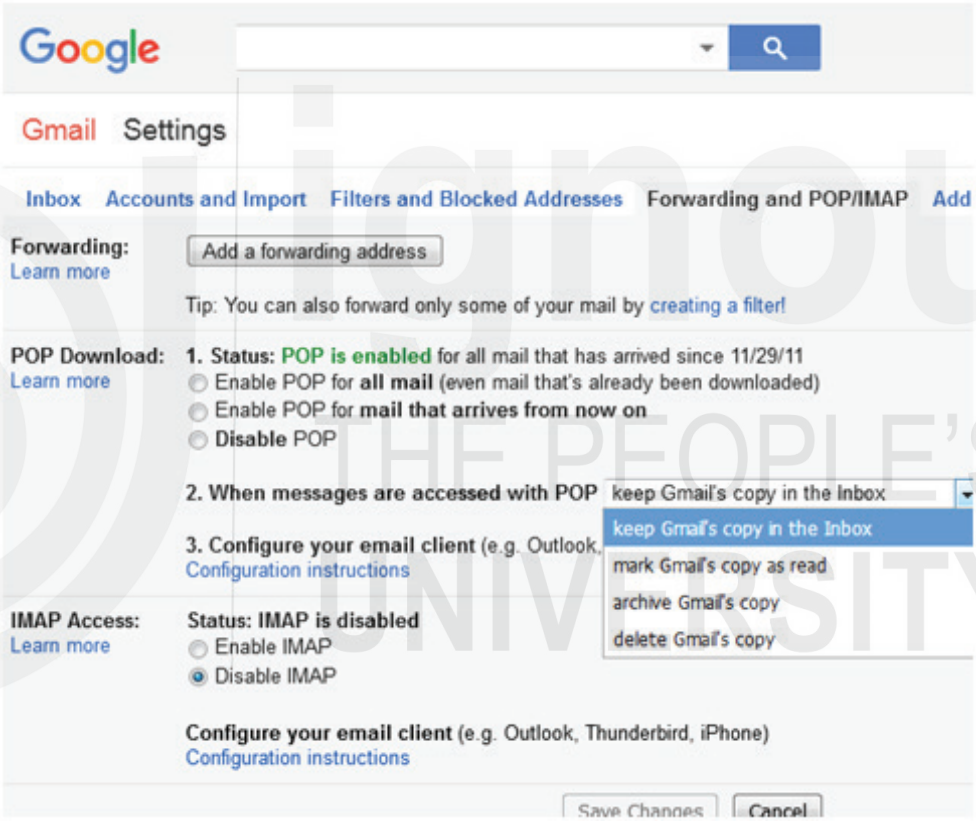
memory. It works like a post office where letters are temporarily stored before being delivered to the end user.

Should you be using IMAP or POP3?

Essentially, it depends on the way we would be accessing our emails. In case of working across multiple devices the recommended method for receiving email would be IMAP or Internet Mail Access Protocol. However, if we have a designated device for email and prefer to have all emails accessible offline, then we can go with POP as suitable option.

Gmail: IMAP and POP3 configuration

As an example we would be showing the IMAP and POP3 settings in Gmail and how they are configured:



Source: Gmail Settings

Fig. 7.1: IMAP and POP3 settings in Gmail

7.5 WEB BROWSERS

Imagine you want to go out for a picnic, how do you get there? We can opt for a car, public bus, metro, rickshaw or any other mode of transportation depending on our choice and convenience. A web browser is a digital mode of transportation which allows us to travel through the Internet and visit our favourite websites. Depending on our taste and convenience, we can go for any web browsers.

Web browsers are the computer software application installed in one's computer, which is used for viewing the web pages on the Internet. There are different web browsers used today.

Source: Interactive Powers' Elaboration

Fig. 7.2: Different Web Browser

Most popular out of them are:

- **Apple Safari:** The Safari is a web browser which has been developed by Apple Inc. It was first released by Apple in 2003.
- **Mozilla Firefox:** The browser was developed by Mozilla released in 2004 and is second most popular browser as of today.
- **Google Chrome:** This web browser was developed by Google in 2008. It is one of the most popular web browsers of world today.
- **Microsoft Edge**: Microsoft's Edge is a new built-in browser that's meant to replace Internet Explorer. Though Edge will still come with Windows, the older browser is being relegated to "legacy compatibility" duties. Microsoft is urging everyone to use Edge for its faster performance and improved features.
- **Opera Browser:** Opera is smaller and faster than most browsers was released first in 1996 by Opera Software ASA.

All of these browsers are free to download. They allow the users to access resources that have been stored on a server through the hyperlinks present in resources. For e.g. if you visit www.ignou.ac.in, then you are actually viewing a file that is displayed through the web browser using Hyper Text Mark-up Language or HTML. Web browser is not only good for viewing web pages, but can be used for downloading and uploading files using FTP.

Check Your Progress B

1) What are the three protocols for communicating via email?

……

……

……

2) What are web browsers?

…….

…….

…….

…….

…….

3) Fill in the blanks:

i) …….. is a web browser developed by Apple Inc.

ii) Web browser is not only good for viewing web pages, but can be used for downloading and uploading files using …….. .

iii) …….. Web browser was developed by Google in 2008.

iv) ……. protocol works like a post office where letters are temporarily stored before being delivered to the end user.

7.6 WORLD WIDE WEB (WWW)

The World Wide Web or WWW is commonly known as web was created by Timothy Berners Lee in 1989 at the European Particle Physics Laboratory in Geneva for allowing researchers to work together at the Laboratory. Eventually in 1996, it became World Wide Web.

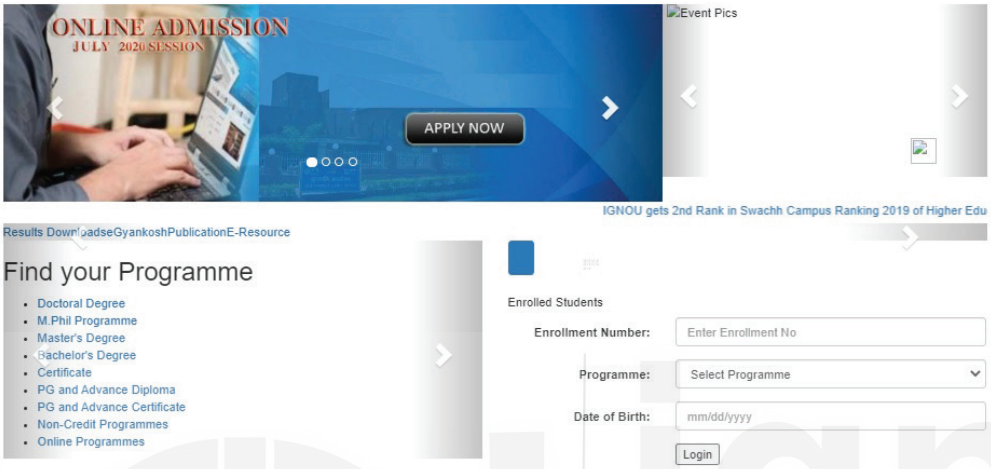
The World Wide Web is simply a mode of information exchange between computers on the Internet. The information is essentially documents and other web resources linked through hypertext and are identified by URL (Uniform Resource Locators); which we would be discussing in upcoming sections. These resources of WWW or web are first transferred via HTTP and then can be accessed by the users through the web browsers which we already discussed above. The web pages are formatted in Hypertext Markup Language (HTML) with embedded hyperlinks containing URLs that help users to navigate to other web resources. The web pages are displayed in the web browsers and may contain references to text, images, video, audio, and software components.

If there are multiple web resources using a common theme or domain name then they are termed as websites which are stored in computers running a program called a web server. It responds to every request which is made by the users over the Internet from web browsers. The contents on these websites can vary depending on the publisher who is responsible for the content. Different websites are targeted for different audiences based on the requirements of users. Today, in the Information age in which we are living, billions of people across the globe use WWW for accessing information

through websites, interacting on Internet making it the central of all its development.

7.7 UNIFORM RESOURCE LOCATOR (URL)

As discussed above the web resources are identified by URL. Technically URL or web address is just an address of a particular resource on the Internet.



Source: www.ignou.ac.in

Fig. 7.3: URL of IGNOU

Now taking our previous example http://www.ignou.ac.in is an URL to access the resources made available to public by IGNOU. An URL has three elements:

- Protocol
- Server name or host name
- Path to directory or file

Let's take our above example with some modification, if you will click on the below given URL http://www.ignou.ac.in/userfiles/ContactUs-2019.pdf, it will take you to the important contact details of IGNOU which would be a PDF file. Let's break the URL to have greater clarity.

http://www.ignou.ac.in/userfiles/ContactUs-2019.pdf

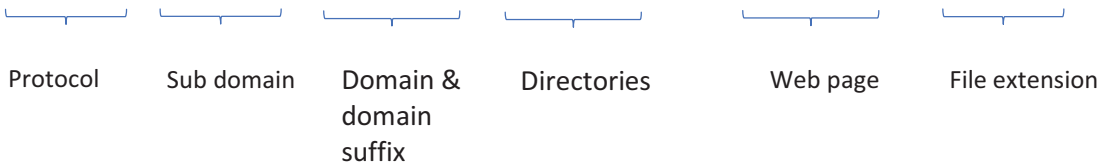


Fig. 7.4: Website Sub-pages

Let's discuss each element one by one.

- http:// or https:// - "Http" stands for Hypertext Transfer Protocol which tells the protocol to be used by browser for accessing the information. If the information transmitted is encrypted and secure, it's called "https", where "S" stands for secure. We need to put the colon (:) and two forward slashes (//) which separate the protocol from remaining of the URL.
- Next, "WWW" stands for World Wide Web which we already discussed in detail in above section. This portion is optional and can be left out. In the above example typing http://ignou.ac.in would still take you to the IGNOU website.
- "Ignou.ac.in" is the domain name of the website. The trailing portion of domain also called as domain suffix. It helps in identifying the type or location of the website. For example, "ac.in" domain is used by educational organization of India,".com" is for commercial, ".org" is for an organization, and ".co.uk" is for the United Kingdom, ".in" is used for Indian website as usual. We will read about domain in detail in the last section.
- "/userfiles" this portion of the above URL are the directories where the webpage is located on the server. The web pages can be two or more directories deep. In our example, it is one deep level.
- "/ContactUs-2019.pdf" Finally this is the actual web page on the given domain we are viewing. The trailing ".pdf" is the file extension which indicates that the web page file is a PDF file. There are many other extensions such as .jpg, .gif, .php, .xml, .html etc.

7.8 DOMAIN NAMES

Domain names are part of URL which helps in identifying the specific web pages. As discussed above in our example "ignou.ac.in" was the domain name. There are essentially two parts of the domain name:

- **Website's name** – In our case IGNOU is the website name. If we are using "facebook.com" then Facebook is the website's name
- **Domain suffix** – The trailing part or extension of the domain is called domain suffix which is kind of identifier for the website we are looking, helps in identifying the type of organization or location of organization. It indicates which TLD (top-level domain) they belong to.

Domain names are used as a shortcut to the server that is hosting the website. In absence of a domain name, we need to enter the full physical address also called IP address for the website, we are visiting. The problem with IP address is that they are difficult to remember. In our example of ignou.ac.in, let's say that it is pointing towards an IP address 192.90.80.70. There would

be similar IP addresses for other websites and as you can see that this can be time-consuming and confusing. So, majority of website owners including *IGNOU* opt to use a service which offers bundles domain names with web hosting packages. Every web server requires a Domain Name System (DNS) server to translate domain names into IP addresses, as Internet is based on IP addresses.

Different types of domains

The most common types of domain is TLD. The top-level domain is at the top level of the Internet's domain name.

- **ccTLD** – Country code Top level domain uses codes for country. The code is two letters based upon the country, such as .uk for United Kingdom, .in for India, .us for United States. They help users to identify the regions in which website is operating.
- **gTLD** - A generic top level domain is the type of domain which are intended for specific use-case and does not rely on any country code. There are more than thousand gTLDs available but the most common include ".com" for commercial business, ".org" for organizations, ".net" for network and ".edu" for educational institutions.

The domain sitting directly below the TLD are second level domains. Indian companies using ".co.in" instead of ".com", Indian academic institutions and universities using ".ac.in", these are perfect examples of second level domains.

Check Your Progress C

1) What are the different parts of URL?

……

……

……

……

2) What is World Wide Web?

……

……

……

……

……

3) Fill in the blanks:

i) The World Wide Web was created by ……... .

ii) Every web server requires …….. server to translate domain names into IP addresses.

iii) If there are multiple web resources using a common theme or domain name then they are termed as …… .

iv) The web resources are identified by …… .

7.9 LET US SUM UP

Internet is global network of physically connected devices for exchange of information. It can be referred to as 'network of networks' consisting of millions of interconnected devices linked by networking technology. Advantages of Internet are ease of communication, e commerce, available round the clock etc.

E-mails (Electronic mails) are the most popular service provided by the Internet. E-mail is basically electronic message communication between people across globe. IMAP used only while receiving the email and they cannot be used for sending the email. The emails will be present in the server and not get downloaded to the user's device and they can be edited as if they are on the user's device. Whereas, Unlike IMAP; POP downloads the entire email into the local user device. Once the mail is downloaded on the user system, it would delete the data on the server which is quite helpful in a server with less free memory.

Web browsers are the computer software application installed in one's computer, which is used for viewing the web pages on the Internet. Some of the popular web browsers are Google chrome, opera mini, apple safari, mozila firefox, etc.

The World Wide Web is simply a mode of information exchange between computers on the Internet. The information is essentially documents and other web resources linked through hypertext and are identified by Uniform Resource Locators (URL). URL or web address is just an address of a particular resource on the Internet. Domain names are part of URL which helps in identifying the specific web pages. Domain names are used as a shortcut to the server that is hosting the website. In absence of a domain name, we need to enter the full physical address also called IP address for the website, we are visiting.

7.10 KEY WORDS

Internet: Internet is global network of physically connected devices for exchange of information. It connects millions of computers together globally,

forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet.

Protocol: A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

E-mail or Electronic mail: It is one of the most popular services provided by Internet where we can send or receive message from people sitting anywhere in globe in seconds over Internet.

Web Browsers: A web browser is a software application for accessing information on the World Wide Web. When a user requests a particular website, the web browser retrieves the necessary content from a web server and then displays the resulting web page on the user's device.

URL or Web Address: A uniform resource locator (URL) is the address of a resource on the Internet. A URL indicates the location of a resource as well as the protocol used to access it. It is an address of a particular resource on the Internet

Domain Name: Domain names are part of URL which helps in identifying the specific web pages. Domain names are used as a shortcut to the server that is hosting the website.

7.11 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress A

i) Chat rooms

ii) Packet routing network

iii) File Transfer Protocol (FTP)

iv) Internet

Check Your Progress B

i) Safari

ii) FTP

iii) Google Chrome

iv) Post Office Protocol

Check Your Progress C

i) Timothy Berners Lee

ii) Domain Name System (DNS)

iii) Websites

iv) URL

7.12 TERMINAL QUESTIONS

1) Write brief notes on following:
   i) World Wide Web
   ii) Domain Name
   iii) URL (Uniform Resource Locator)
   iv) Web Browsers
2) Differentiate between the following:
   i) IMAP and POP3
   ii) ccTLD and gLTD
3) Explain the meaning of different components of URLs.
4) Explain the advantages of using Internet.
5) Should you use IMAP or POP3?

Note: These questions are helpful to understand this unit. Do efforts for writing the answer of these questions but do not send your answer to university. It is only for yours practice.

UNIT 8 PLASTIC MONEY, E-WALLETS AND ONLINE PAY

Structure

8.0 OBJECTIVES

After studying this unit, you should be able to:

- identify various modes of virtual payments used in commercial activities;
- explain how digital payment system has developed over years;
- describe different types of E-payment systems used in commercial transactions; and
- understand how demonetization affected digital payment system in India.

8.1 INTRODUCTION

In the previous unit, we have discussed the concept and application of IT Security measures in Business. These IT security measures have made online transactions far safer and secure than they used to be, thus resulting in improved consumer trust. This has further to increased adoption of digital payment system. This unit will cover the diverse aspects of digital payment systems.

The developments in information technology and emergence of technological innovations have led to evolution of money first from paper money to plastic money. Plastic money includes credit cards, debit cards, ATMs, prepaid cards, etc. and lately to the electronic or digital form. Both forms are essential forms of money which have reduced the risk of handling cash. They are challenging the role of cash in the economy making the transactions easier and cheaper. At the same time, they also influence the money supply of an economy thus raising a number of policy issues for country's central banks.

This unit would help in understanding the origin of plastic money and digital wallet, their usage and role in the economy especially in context of Indian economy. We would also try to understand the role of government on the digitalization of payment, demonetization and effects of demonetization on digital wallets.

8.2 ORIGIN OF PLASTIC MONEY

Plastic money derived its name from "plastic" which is used in the construction of cards, as opposed to paper and metal currency. Plastic cards market in India, comprising of Credit cards, Smart cards, Debit cards, Charge cards, stored value cards, and others have become increasingly popular, only in last decade. Many Indian banks have entered plastic card business during the last few years; including the premier bank namely State Bank of India.

The origin of trade can be dated back to evolution of human society. Trade was done with direct exchange of goods and services popularly known as "barter system". Barter system suffered from several constraints, the most important being the non-availability of desired items with the parties involved. With passage of time, these inconveniences encountered in barter system became grave and unbearable. To search for the solution to barter problem leads to evolution of money. Money is one of the most important and useful creations of mankind which played an instrumental role in development of social economy. It is rightly said that 'Money is what money does' (Walker). Anything that performs the functions of money is money. It plays an important role in the economic system.

It is said that in ancient Mesopotamia, there were secure places for the safekeeping of grain and other commodities in the temples and royal palaces, leading to origin of banking system. As society grew in scale of civilization, with the development of economic systems the development in the banking was also inevitable. As banking system grew, the role of money became more significant with the development of paper money in around 17^{th} century followed by cheque in late 19^{th} century. In the 1920s, in USA "buy now, pay later" was introduced by a shopper's plate. This is identified as first use of magnetic stripes on cards. However, these cards could only be used in the

issuance shops. The beginning of plastic money can be traced back to 1946, when John Biggins, an end user specialist at the Flatbush National Bank of Brooklyn, NY launched "Charge-it" credit plan. The plan featured a form of scrip which was accepted for small purchases by local merchants. After the sale was completed the merchant needed to deposit the scrip in their bank account and the customer was billed by the bank for the total scrip issued. Diners Club in 1951 issued the charge cards to 200 customers which could be used at 27 specified restaurants in New York. This was continued until the standards for the magnetic strip were established in 1970. In 1951, the Franklin National Bank in NY issued the first modern plastic money. This was copied by many banks during 50s and 60s, with American Express launching card in 1958. However, till that point all cardholders could shop only in their geographic area. The merchants only with their bank were able to sign up. This problem was solved by Bank of America, when Bank of America began forming licensing agreement with other banks. Bank Americard was issued which facilitated transactions interchange between the participating banks in 1965, which changed its name to VISA in 1976. In 1966, to compete with the Bank Americard program, four Californian banking institutions formed the "Western States Bankcard Association" and introduced the Master Charge program, which eventually changed to MasterCard in the year 1979. These two international cards are very popular and are accepted and honoured all over the world. In 1989, debit cards were introduced by Visa, where cards were linked to customer's accounts. Today, plastic money transactions are rapidly replacing cash transactions and are widely used across the world.

8.3 USAGE OF PLASTIC MONEY

In the previous section we have discussed how plastic money came into existence. Now we would look deep into its usage. Credit card and Debit card are two most popular form of plastic money used by people worldwide. Few other popular plastic cards are – Store value card, ATM card, Smart card, Pre-paid card, Agricultural card etc. Ease in storage, security with convenience to use it almost everywhere lead to rise in the popularity of plastic money.

There are varieties of places where one can use plastic money.

- For purchasing groceries at grocery stores. No need to carry cash. In India almost everywhere, plastic money is accepted at groceries stores.
- At fuel station, we can use credit or debit card for purchasing fuel for your vehicles.
- For paying at restaurants, hotels.
- We can book bus, train, flight tickets using our debit or credit card.

- For paying our gas, mobile, landline, electricity bills.
- Debit cum ATM card can be used to withdraw money from ATMs.
- With increase in e-commerce websites, we can use credit, debit for our online shopping purchases.
- Smart card a form of plastic money is being used to pay for small purchases like bus fare, metro fare. Most popular example would be Delhi Metro Smart Card.
- Farmers use agricultural card, for example in India kisan credit card, for improving their credit flow under agriculture and allied activities.

We can site hundreds of examples where we use plastic money. Essentially, it has penetrated every sphere of our economy, and to put it simply, all transactions which could have been done by cash can be done using plastic money also.

Check Your Progress A

1) What factors contributed to adoption of plastic money on large scale?

……

……

……

……

……

2) List down any four usage of plastic money.

……

……

……

……

……

3) Fill in the blanks:

i) ……. said, "Money is what money does".

ii) Direct exchange of goods and services takes place in …… system.

iii) The beginning of plastic money can be traced back to the year ……...

iv) The origin of banking system can be traced back to ancient …….

8.4 E-WALLET

In today's world almost, everyone's wallets contain cash, credit and debit cards and more. It is quite cumbersome to keep track of all these items. E-wallet or electronic wallet can help us eliminate the need for several cards by providing all of the benefits of cash and cards without the hassles of physically carrying them around. Additionally, it also offers myriad security features which are not available with regular wallets.

E-wallet or Electronic wallet is a type of electronic card in which one can stock money similar to saving accounts (with no interest being paid on money saved) and which is used for making digital transactions enabled by a computer or a Smartphone. It is a preloaded facility and offers the same functionalities as a credit or debit card. Consumers can buy a range of products from grocery to airline ticket.

E-wallet is especially very convenient for frequent online shoppers; offering a safe, convenient, and easily accessible tool for online shopping. They also store personal and financial information such as card details, passwords, PINs, etc. Similar to physical wallet, E-wallet keeps most important personal information in cards. E-wallets can also save information related to our utility and merchant bills, thus allowing the customers to keep track of various payments to be made. A popular example of an E-wallet in the Indian market is Paytm.

Users have to register for the E-wallet which can be web based or app based. Lately majority of them has moved to the app-based system which first requires installation of the software. Once user has created the E-wallet account, he can transfer the money to wallet using online transfer, or his debit card/credit card. This balance can be used whenever he uses wallet on any of the supported sites. There is almost no chance of decline of payment as it is a prepaid account. The payment details provided by the user which usually includes their name, payment method, debit or credit card details can also be saved for quicker balance transfer next time. This feature is optional and depends on the user if he/she wants to store this information. In the next section we would explore more about the development of the E-wallet system.

8.5 DEVELOPMENT OF E-WALLET SYSTEM

Wallets have been in use since time immemorial. Since then, they have taken several forms but two things remained constant: they are portable and they help us to store items of value. In the early days, they were made of animal skin, which were then replaced with clothes, which were then replaced by modern wallets of diverse shape and sizes from multiple brands. Wallets

enable us to conveniently hold and carry coins, money, cards and other valuables. With the advancement of Information and Communications, Technology helped a lot in transforming our wallets, wherein currency notes were slowly replaced by plastic money. Plastic money was an improvement over traditional money as it greatly reduced the dangers of carrying traditional money around. Nevertheless, this was not the end of all problems, unavailability of ATMs, loss of cards, loss of card quality due to mishandling, long lines at ATMs, are some of the problems plastic money suffers from. Therefore, the next reasonable step was to gain independence from physical presence of plastic money. This led to the evolution of E-wallets. Internet provided a way out of these problems, now money can travel with us to any place on the face of earth without any restrictions of the physical world. The details of these Electronic wallets reside in trusted secure servers and can be accessed from any internet enabled device.

In 1996, Sam Pitroda, the founder of digital wallets said "a digital wallet would consist of a liquid crystal display not much bigger than a regular plastic bank card, which preferably a touch-sensitive screen and simple user interface that lets the user flip through the digital wallet in the same manner he/she flips through a leather wallet". Since then, there has been no looking back for E-wallets. Today, E-wallets are the engines of E-commerce. With widespread internet access, improved band-width and high-performance IT enabled devices, E-wallets are rapidly being adopted and accepted by customers. It can be used for any or all of the following activities:

- Online merchant payments
- Utility payments
- Flight ticket purchases and hotel booking
- Mobile recharges
- Movie ticket booking, etc.

8.6 E-PAYMENT SYSTEM IN COMMERCE

Payment systems are the enablers of trade and commerce. Electronic payment or E-payment system facilitates commercial transactions by enabling the payments for goods and services through electronic medium, without involving the use of cash or checks. With the growth in E-commerce and internet-banking system, E-payment system has grown increasingly over last decade. This growth has further been supported by recent technological advancements, which not only improved the ease of use but also helped in addressing our security concerns.

E-payment system is rapidly replacing the traditional payment system. For example, if we are making cash payment for our purchase; then we will have

to withdraw cash from our account, make payment using this cash, which in turn will be deposited by the shopkeeper in his account at the end of the day. This time-consuming process has been made simple with E-Payment system wherein the amount to be paid can be directly transferred to the shopkeeper's account. The E-payment system involves several different technologies. This section provides an overview of these technologies:

Fig. 8.1: E-payment System

- **Quick Response Code (QR Code)**: A QR Code contains encoded information, which can be decoded by simply scanning the 2 D matrix barcode with any device with code reader/camera. The information leads the individual to the website, app, etc, to which the payment has to be made.
- **Unified Payment Interface (UPI):** UPI enables the creation of a virtual address for money transfer. The user need not disclose the account number for sending or receiving money. All banking applications provide UPI facility to enable real-time money transfer.
- **Digital Wallets:** Digital wallets are virtual wallets that enable the customer to load money digitally. The user can load money into these wallets using their credit/debit cards and this money can then be used for making merchant payments or can be transferred to another individual.

The only constraint in case of digital wallets is that the funds can be transferred to the same wallet only. For example, money can be transferred from one Paytm wallet to another Paytm wallet only.

- **Unstructured Supplementary Service Data (USSD):** USSD code enables the user to make payments even without a smart phone or mobile data facility. Using their basic phones, users can dial *99# (Common across all telecom service providers) using their basic phones and transact using the interactive menu displayed on their mobile screen. It can be used for services like balance enquiry, fund transfer, mini statement, etc.
- **Mobile Money Identifier (MMID):** MMD is a unique seven-digit number provided by the banks to the customers who have registered their mobile number with the bank. Both, user as well as senders needs to have MMID issued by their banks for transaction through MMID. MMID can be used for transfer of amount up to INR 10,000 only.
- **Immediate Payment Service (IMPS):** It is an instant payment inter-bank electronic funds transfer system in India. It offers an inter-bank electronic fund transfer service through mobile phones.
- **Aadhar Enabled Payment System (AEPS):** AEPS is based on the Unique Identification Number (UID) of individuals possessing Aadhar Card. Users can make payment by using their Aadhar number at PoS or micro ATMs. This is an important step towards financial inclusion as it can be used for payments and transactions even in rural areas.
- **Near Field Communication (NFC):** NFC enables devices to communicate without contact. The user can simply wave the Smartphone/tablet near a Point of Sale (PoS) device to enable payment.
- **Banking Cards:** There are multiple variants of banking cards available, viz. debit cards, credit cards, prepaid cards, travel cards, etc. Users can use these cards to make payments online as well as offline. For secure payments, these cards use secure PIN or OTP. Example: RuPay, Visa, etc.
- **Internet Banking:** Internet banking is an electronic payment system which enables users to conduct financial transactions through bank's website. There are several different types of internet banking transactions:

Table 8.1: Difference between E-banking Transactions

S. No.	National Electronic Fund Transfer (NEFT)	Real Time Gross Settlement (RTGS)	Immediate Payment Service (IMPS)
1	It enables one to one transfer fund electronically to individuals/businesses having bank account with any bank.	RTGS is primarily used for large value transactions (min. INR 2 Lakhs) and there is no upper cap on RTGS transactions.	IMPS enables electronic money transactions round the clock. Using IMPS, funds can be transferred instantly to any bank account across the country.
2	Is a nation-wide payment system facilitating one-to-one funds transfer.	The minimum amount to be transferred through RTGS is Rs 2 lakh.	This is an inter-bank electronic fund transfer system that uses mobile phones as a platform for the transfer process.

Check Your Progress B

1) What are the three most important characteristics of E-wallets?

……

……

……

……

……

2) List four E-payment methods.

……

……

……

……

……

3) State whether the following statements are True or False.

i) There are very high chances of payment decline in case of E-wallets.

ii) For NFC usage, it is mandatory that the two devices should be in contact.

iii) USSD can be used even on a basic phone

iv) IMPS enable round the clock money transfers.

v) There is upper cap on RTGS transactions.

8.7 MOBILE WALLETS, PAYMENT & CARD NETWORK

Mobile wallets provide payment services which can be performed through mobile phones, tablets, personal digital assistants, etc. The development and adoption of mobile wallet is the result of massive growth in mobile communications, mobile internet services and wireless network services. Mobile wallets are electronic accounts operating through a mobile device. Mobile wallet architecture has three different components:

- **Payment Component:** for payment authentication and secure transaction
- **User Interface:** for providing convenient access to payment services
- **Umbrella UI Component:** provided by the wallet issuing company, it manages the portfolio of payment services on the mobile devices

Rather than just being a source of revenue for the issuing company, mobile wallets are enablers of commercial activities. Retail financial institutions often compete with each other to gain top space so that their cards are the most used ones for adding money and performing transactions through mobile wallets. Wallet issuing company often earns revenue by charging commission from the financial institutions on the sales made through the wallet. Some of the wallet service providers also charge upfront fee from financial institutions for allowing them to enter the marketplace along with the commission while some make money by allowing advertisements on their platform.

The rapid growth of telecommunication in India has empowered the users and improved the productivity of the economy by drastically reducing the communication costs. With cheap internet connection and improved speed coupled with declining sets, smartphones are becoming the primary devices for shaping the day to day lives of users by influencing how they search for items, and how they purchase and pay for different goods and services.

Mobile wallets have contributed immensely to the field of digital payments by taking the mobile payments right in the hands of end customers. Mobile wallets can be categorized under three heads, depending upon who operates the wallet, the available transaction limit and the overall purpose of the wallet.

Open Wallets: These wallets exist with the support of banking institutions and they allow users to pay for goods and services directly from the wallet. They also allow users to withdraw cash and hence are most flexible. Examples are Google pay by Google, Pocket Wallet by ICICI and PayZapp by HDFC Bank.

Semi-closed Wallets: These wallets can be used for making payments to selected merchants but they do not allow customers to withdraw cash. Few of these wallets also permit their users to transfer the amount directly to another wallet. Examples are Amazon Pay, Paytm, Ola Money.

Closed Wallets: This type of wallets are merchant-specific wallets and they can be used for transactions exclusively at the issuing merchant sites. Examples closed wallets are 'My wallet' issued by Make My Trip, 'Big basket wallet' issued by Big basket.

8.8 CONSUMER ADOPTION IN MOBILE WALLET

Whenever, a new product is launched in the market, the adoption cycle of the product depicts its adoption and acceptance. The ease of use and flexibility offered by mobile wallets has contributed a lot towards their adoption and acceptance. The adoption stages can be explained with the help of "Rogers' diffusion of innovation" process. E. M. Rogers identified five distinct categories of users based on their readiness to adopt an innovative product or service. The same principle is applicable to mobile wallets as well which is rapidly making its place in consumers' day to day lives.

Innovators: They are leaders for change and innovation and are individuals who first conceive the ideas. Younger generation living in metros mainly of age group 18-30 years are innovators in case of mobile wallets. They use mobile wallets for making payments for services like cab, DTH, phone bills, payments to merchants, etc. The companies offering mobile wallet services need to be continuously innovative while giving their offerings so that they can keep this category of users engaged as they tend to constantly look for innovative offerings and they can help in expanding the customer base by encouraging others to adopt the product.

Early Adopters: These are inquisitive individuals who are on constant lookout for latest trends. They belong to similar age groups as innovators and based on the feedback they tend to try new products if they feel that it will make their life easier and will be value for money. They are also familiar with other digital payment modes and mobile banking services. Mostly they belong to metro and Tier 2 cities. They are attracted only if they feel that these mobile wallets are safe for use and will provide them with good return.

Early Majority: They are more practical users who wait till the technology proves itself before they dive in. While adopting new products like mobile wallet, these users search for offers and use them on very selective offerings. Their usage would be much lesser than their regular payment

methods due to their habits. They are often attracted by the introductory promotional offers by mobile wallet companies.

Late Majority: These are individuals who will adopt the technology only when it becomes a norm and cannot be avoided. In case of mobile wallets, these users are in the age bracket of 40–55 years. Most of these users are still not much acquainted with mobile wallets and prefer debit cards or online transfers. Mobile wallet companies will have to work on traditional ways of educating these customers about their offerings and benefits so as to instill confidence in them.

Laggards: They are last to adopt, typically older generation that never purposefully adopts a new technology which comprises of customers who are over 55 years of age and are not very comfortable with smart phones. It is not very likely that they will use mobile wallets as their preferred mode of payment is cash.

Indian consumers no longer just like the idea of mobile wallets but see the real benefits in using it. With market penetration at a strong 39%—Paytm alone has more than 200 million customers and 5 million merchants. Further augmenting their core product offering with value-added services such as utility bill payments, cash back offers, ticket booking etc. help in pushing adoption. Mobile wallets as a product has already established itself and is in "Early Majority" phase. It is easy to see that mobile wallets are now in the "Early Majority" phase. People no longer just "like the idea" of mobile wallets, but see real benefit in using it and are increasingly adopting it. One of the important factors that helped in spreading the mobile wallet adoption is Government policy. One of such policy was demonetization which we would study in next section in details.

8.9 EFFECTS OF DEMONETIZATION ON DIGITAL PAYMENT

Demonetization is the "act of stripping a currency unit of its status as a legal tender". In other words, it is withdrawal of particular form of currency in circulation. Government of India boldly announced the demonetization on 8 November, 2016. The circulation of ₹500 and ₹1000 for any form of liquid transaction was banned from midnight and no more a legal tender from 9th November 2016. The ATM withdrawal limit was set to ₹2500 for that particular period.

The unexpected announcement of demonetization and prolonged cash shortages helped in increasing the digital transactions. Every sphere of economy ranging from a small shop to big malls witnessed a spurt in digital transactions across the country. After demonetization, switching to cashless

payment methods becomes a necessity for both rural and urban populations. Every citizen of the country, be it a farmer, teacher, soldier or even a CEO of a big brand, needs to know about the available methods to make cashless transactions. They become more aware about the existing facilities - how they can perform online transactions such as checking account balance, bill payment, funds transfer, etc. through internet banking. Also, it is available 24x7 for the customer's convenience. Small sellers also flocked to e-wallet methods – Paytm, Mobikwik, etc. to continue doing their business. These all gave a big push to the overall digital transactions across the country.

Also, to help the citizens with short term cash-crunch in the country, the Indian government aggressively promoted digital modes of banking. The transaction charges were waived off on few payments' methods. The total electronic and card payments grew 46% by value and 65% by volume in 2016-17 over the previous fiscal year. Some segments like the Unified Payments Interface (UPI, the government's real-time payments system) and Aadhaar-based payment grew fastest from a very low base. Online banking transactions and debit card payments grew the most. E-wallet companies like Paytm welcomed the decision of demonetization as this gave them an opportunity to increase their customer base. The Paytm wallet went from 125 million wallet customers before demonetization to 185 million in three months and it has continued to grow, with almost 300 million customers bases. In conclusion demonetization gave the digital payment a thrust which led to success of many payment wallet companies along with increase in acceptance of digital mode of payment among the masses.

8.10 SUCCESS STORY OF WALLETS

Earlier digital wallets were seen merely as E-commerce payment tools but post demonetization masses adopted it for day to day transactions of their daily usage. Be it grocery stores, street vendors, tea stalls, petrol pumps and even to pay cabs and auto-rickshaws. The wallets like Paytm, Mobikwik, PhonePay, Google pay rode with the wave of demonetization.

Although, Credit cards and online transfers hold the highest market share in digital payments. The growth story of mobile wallet is significantly attractive especially post demonetization.

Nowadays, mobile wallets have evolved as a mainstream payment mode. Survey conducted by Global Data, stressed upon the fact that the share of Cash on Delivery as preferred mode of payment for e-commerce purchases has declined from 31 % in 2013 to almost half i.e. 16% in the year 2017. Also, the share of payments made through digital wallets during this period increased from mere 7% to 29%. Also, the use of cards for making payments decreased from 38 % to 32% in this period.

To tap this rapidly growing market Google launched its mobile payment service called *'Tez'* in August, 2017. It specifically targeted Indian customers. In fact, within a short span of 37 days, the app was installed on over 8.5 million devices. With an eye on the ever-growing Indian payments market, Google re-launched its payments app, Google Tez as Google Pay in August, 2018 in line with its payment services used globally. This app supports several regional languages spoken in India including Hindi, Telugu, Marathi, etc. The app uses UPI based platform and users can use it for utility and merchant payments as well as for money transfers. As of now, it supports payments on over 2,000 apps and websites. Google claims that over 22 million users are using this app for transactions every month. Tez, which started out as a bank linked payment app is pushing its way into offline retail stores as well with payment facilities available at Big Bazaar, e-zone, etc. Google pay is also planning to enter micro-loan segment, which will enable a user to avoid the trouble of paper works and phone calls, it will be available in their bank account at a click.

Check Your Progress C

1) What are the different components of mobile wallets?

   ……

   ……

   ……

2) What are the three different categories of mobile wallets?

   ……

   ……

   ……

3) Fill in the blanks:

   i) …….wallets exist with the support of banking institutions and they allow users to pay for goods and services directly from the wallet.

   ii) ……..are individuals who will adopt the technology only when it becomes a norm and cannot be avoided.

   iii) According to the process of diffusion of innovation, mobile wallets are now in the **……**phase.

   iv) …….is the "act of stripping a currency unit of its status as a legal tender".

   v) Google re-launched its payments app ……as Google Pay in Aug'18 in line with its payment services used globally.

8.11 LET US SUM UP

World is moving from paper money or cash to the plastic money – credit cards, debit cards. Recently with the telecom revolution, the people got access to smart phone and cheaper internet. This has led to succession of e-wallet or mobile wallet system to the conventional electronic payment system. With push from the government's Digital India program and growing awareness, confidence is being built especially among the rural consumers. Policies that promote electronic payment, rise in smart phone penetration (Mobile phone subscriptions crossed the 1 billion mark in 2016 and an estimated 371 million users are now subscribed to mobile internet), improved telecom and payment infrastructure and promotions by wallet players have helped digital wallet user base expand and maintain a steady foothold.

8.12 KEY WORDS

Plastic Money: Money made out of plastic or polymer predominantly referring to all kinds of cards- credit card, debit card, pre-paid cash card and store card.

E-Wallet: An electronic wallet which is used for making transactions electronically either through a device – smart phone or online service. It needs to be linked to the individual's bank account.

E-Payment System: Electronic payment or E-payment system is an electronic mode of payment which facilitates transactions by enabling the payments for goods and services electronically, without involving the use of cash or checks.

Mobile Wallet: Mobile wallet is a form of electronic wallet which provide payment services performed through devices such as mobile phones, tablets, personal digital assistants etc.

Demonetization: It refers to the "act of stripping a currency unit of its status as a legal tender". In other words, it is withdrawal of particular form of currency in circulation.

8.13 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress A

i) Walker

ii) Barter

iii) 1946

iv) Mesopotamia

Check Your Progress B

i) False

ii) False

iii) True

iv) True

v) False

Check Your Progress C

i) Open wallets

ii) Late Majority

iii) Early Majority

iv) Demonetization

v) Tez

8.14 TERMINAL QUESTIONS

1) Write brief notes on following:
   i) AEPS
   ii) QR Code
   iii) NFC
   iv) MMID
2) Differentiate between the following:
   i) Open and Closed Wallets
   ii) NEFT and RTGS
3) Explain the meaning of E-wallet. Discuss briefly the factors which have contributed towards the adoption of E-wallets in India.
4) Explain the impact of demonetization on E-wallets.
5) How is E-payment system better than traditional payment system?

Note: These questions are helpful to understand this unit. Do efforts for writing the answer of these questions but do not send your answer to university. It is only for yours practice.