LECTURE NOTES

ON

E-COMMERCE

(For 6th semester IT)

Prepared By :

Mrs Swetalina Das

Lecturer (Computer Application)

INTRODUCTION TO E-COMMERCE

E-Business (E-Business), or Electronic Business, is the administration of conducting business through the Internet. This would include the buying and selling of goods and services, along with providing technical or customer support through the Internet. e-business is a term often used in conjunction with e-commerce, but includes services in addition to the sale of goods.

Online shopping is getting popular, just because of its simplicity and convenience. This is possible only because of two electronic networks, namely, as e-commerce and e-business.

e-commerce is concerned with the firm's dealings with its customers, clients or suppliers. Conversely, e-business refers to undertaking industry, trade, and commerce, with the help of information technology and communication.

e-commerce is nothing but buying and selling of goods around the web. On the contrary, **e-business** is a little different as it is not limited to, commercial transactions, but it also provides other services. These are the two emerging modes of doing business, which are gaining importance with the passage of time.

DEFINITION OF E-COMMERCE

e-commerce is an abbreviation used for electronic commerce. **It is the process through which the buying, selling, dealing, ordering and paying for the goods and services are done over the internet is known as e-commerce.** In this type of online commercial transaction, the seller can communicate with the buyer without having a face to face interaction.

Some examples of real world application of e-commerce are online banking, online shopping, online ticket booking, social networking, etc.

The basic requirement of e-commerce is a website. The marketing, advertising, selling and conducting transaction are done with the help of internet. Any monetary transaction, which is done with the help of electronic media is e-commerce. The following are the types of e-commerce:

- **B2B** – The process where buying and selling of goods and services between businesses is known as Business to Business. **Example**: Oracle, Alibaba, Qualcomm, etc.
- **B2C** – The process whereby the goods are sold by the business to customer. **Example**: Intel, Dell etc.
- **C2C** – The commercial transaction between customer to customer. **Example**: OLX, Quickr etc.
- **C2B** – The commercial transaction between customer to the business.

E-BUSINESS

Electronic Business, shortly known as **e-business, is the online presence of business. It can also be defined as the business which is done with the help of internet or electronic data interchange i.e. is known as E-business.** E-commerce is one of the important components of e-business, but it is not an essential part.

e-business is not confined to buying and selling of goods only, but it includes other activities that also form part of business like providing services to the customers, communicating with employees, client or business partners can contact the company in case if they want to have a word with the company, or they have any issue regarding the services, etc. All the basic business operations are done using electronic media. There are two types of e-business, which are:

- **Pure-Play**: The business which is having an electronic existence only. **Example**: Hotels.com
- **Brick and Click**: The business model, in which the business exists both in online i.e. electronic and offline i.e. physical mode.

KEY DIFFERENCES BETWEEN E-COMMERCE AND E-BUSINESS

The points presented below are substantial so far as the difference between e-commerce and e-business is concerned:

1. Buying and Selling of goods and services through the internet is known as e-commerce. Unlike e-business, which is an electronic presence of business, by which all the business activities are conducted through the internet.
2. e-commerce is a major component of e-business.
3. e-commerce includes transactions which are related to money, but e-business includes monetary as well as allied activities.
4. e-commerce has an extroverted approach that covers customers, suppliers, distributors, etc. On the other hand, e-business has an ambivert approach that covers internal as well as external processes.
5. e-commerce requires a website that can represent the business. Conversely, e-business requires a website, Customer Relationship Management and Enterprise Resource Planning for running the business over the internet.
6. e-commerce uses the internet to connect with the rest of the world. In contrast to e-business, the internet, intranet and extranet are used for connecting with the parties.

FEATURES

E-Commerce provides the following features −

- **Non-Cash Payment** − E-Commerce enables the use of credit cards, debit cards, smart cards, electronic fund transfer via bank's website, and other modes of electronics payment.
- **24x7 Service availability** − E-commerce automates the business of enterprises and the way they provide services to their customers. It is available anytime, anywhere.
- **Advertising / Marketing** − E-commerce increases the reach of advertising of products and services of businesses. It helps in better marketing management of products/services.
- **Improved Sales** − Using e-commerce, orders for the products can be generated anytime, anywhere without any human intervention. It gives a big boost to existing sales volumes.
- **Support** − E-commerce provides various ways to provide pre-sales and post-sales assistance to provide better services to customers.
- **Inventory Management** − E-commerce automates inventory management. Reports get generated instantly when required. Product inventory management becomes very efficient and easy to maintain.
- **Communication improvement** − E-commerce provides ways for faster, efficient, reliable communication with customers and partners.

TRADITIONAL COMMERCE V/S E-COMMERCE

BASIS FOR COMPARISON	TRADITIONAL COMMERCE	E-COMMERCE
Meaning	Traditional commerce is a branch of business which focuses on the exchange of products and services, and includes all those activities which encourages exchange, in some way or the other.	e-Commerce means carryng out commercial transactions or exchange of information, electronically on the internet.
Processing of Transactions	Manual	Automatic
Accessibility	Limited Time	24×7×365

BASIS FOR COMPARISON	TRADITIONAL COMMERCE	E-COMMERCE
Physical inspection	Goods can be inspected physically before purchase.	Goods cannot be inspected physically before purchase.
Customer interaction	Face-to-face	Screen-to-face
Scope of business	Limited to particular area.	Worldwide reach
Information exchange	No uniform platform for exchange of information.	Provides a uniform platform for information exchange.
Resource focus	Supply side	Demand side
Marketing	One way marketing	One-to-one marketing
Payment	Cash, cheque, credit card, etc.	Credit card, fund transfer etc.
Delivery of goods	Instantly	Takes time

ADVANTAGES OF E-COMMERCE

E-Commerce advantages can be broadly classified in three major categories −

- Advantages to Organizations
- Advantages to Consumers
- Advantages to Society

ADVANTAGES TO ORGANIZATIONS

- Using e-commerce, organizations can expand their market to national and international markets with minimum capital investment. An organization can easily locate more customers, best suppliers, and suitable business partners across the globe.

- E-commerce helps organizations to reduce the cost to create process, distribute, retrieve and manage the paper-based information by digitizing the information.
- E-commerce improves the brand image of the company.
- E-commerce helps organization to provide better customer services.
- E-commerce helps to simplify the business processes and makes them faster and efficient.
- E-commerce reduces the paper work.
- E-commerce increases the productivity of organizations. It supports "pull" type supply management. In "pull" type supply management, a business process starts when a request comes from a customer and it uses just-in-time manufacturing way.

ADVANTAGES TO CUSTOMERS

- It provides 24x7 support. Customers can enquire about a product or service and place orders anytime, anywhere from any location.
- E-commerce application provides users with more options and quicker delivery of products.
- E-commerce application provides users with more options to compare and select the cheaper and better options.
- A customer can put review comments about a product and can see what others are buying, or see the review comments of other customers before making a final purchase.
- E-commerce provides options of virtual auctions.
- It provides readily available information. A customer can see the relevant detailed information within seconds, rather than waiting for days or weeks.
- E-Commerce increases the competition among organizations and as a result, organizations provide substantial discounts to customers.

ADVANTAGES TO SOCIETY

- Customers need not travel to shop a product, thus less traffic on road and low air pollution.
- E-commerce helps in reducing the cost of products, so less affluent people can also afford the products.
- E-commerce has enabled rural areas to access services and products, which are otherwise not available to them.
- E-commerce helps the government to deliver public services such as healthcare, education, social services at a reduced cost and in an improved manner.

DISADVANTAGES OF E-COMMERCE

The disadvantages of e-commerce can be broadly classified into two major categories −

- Technical disadvantages
- Non-Technical disadvantages

TECHNICAL DISADVANTAGES

- There can be lack of system security, reliability or standards owing to poor implementation of e-commerce.
- The software development industry is still evolving and keeps changing rapidly.
- In many countries, network bandwidth might cause an issue.
- Special types of web servers or other software might be required by the vendor, setting the e-commerce environment apart from network servers.
- Sometimes, it becomes difficult to integrate an e-commerce software or website with existing applications or databases.
- There could be software/hardware compatibility issues, as some e-commerce software may be incompatible with some operating system or any other component.

NON-TECHNICAL DISADVANTAGES

- **Initial cost** − The cost of creating/building an e-commerce application in-house may be very high. There could be delays in launching an e-Commerce application due to mistakes, and lack of experience.
- **User resistance** − Users may not trust the site being an unknown faceless seller. Such mistrust makes it difficult to convince traditional users to switch from physical stores to online/virtual stores.
- **Security/ Privacy** − It is difficult to ensure the security or privacy on online transactions.
- Lack of touch or feel of products during online shopping is a drawback.
- E-commerce applications are still evolving and changing rapidly.
- Internet access is still not cheaper and is inconvenient to use for many potential customers, for example, those living in remote villages.

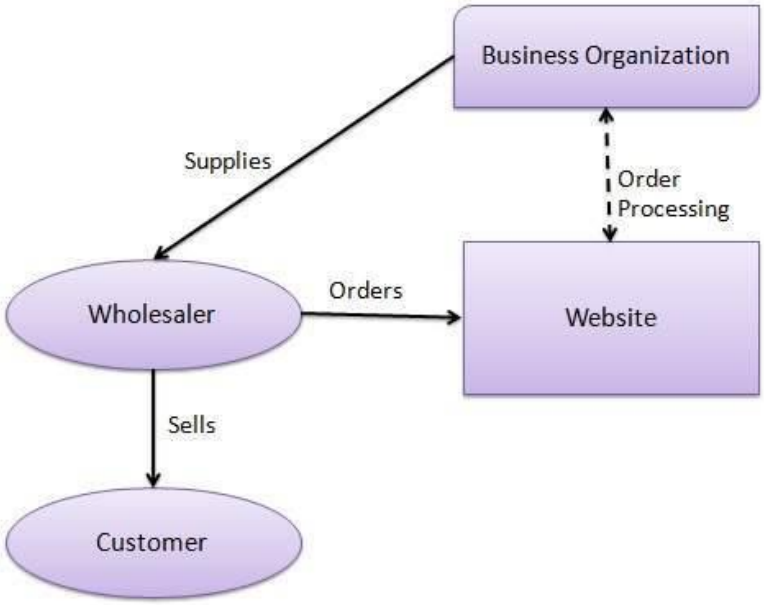
E-COMMERCE BUSINESS MODELS

E-commerce business models can generally be categorized into the following categories.

- Business - to - Business (B2B)
- Business - to - Consumer (B2C)
- Consumer - to - Consumer (C2C)
- Consumer - to - Business (C2B)
- Business - to - Government (B2G)
- Government - to - Business (G2B)
- Government - to - Citizen (G2C)

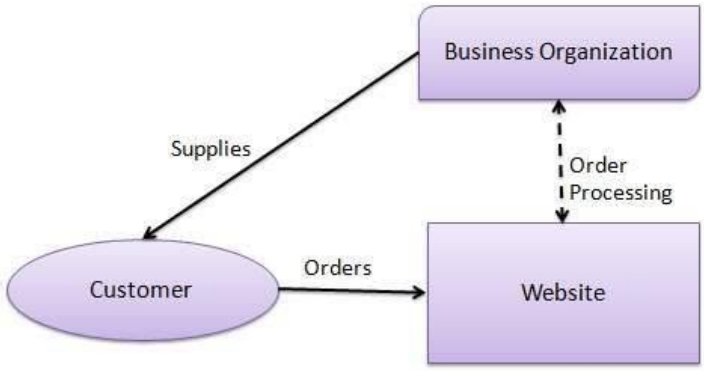
Business - to - Business

A website following the B2B business model sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the end product to the final customer who comes to buy the product at one of its retail outlets.



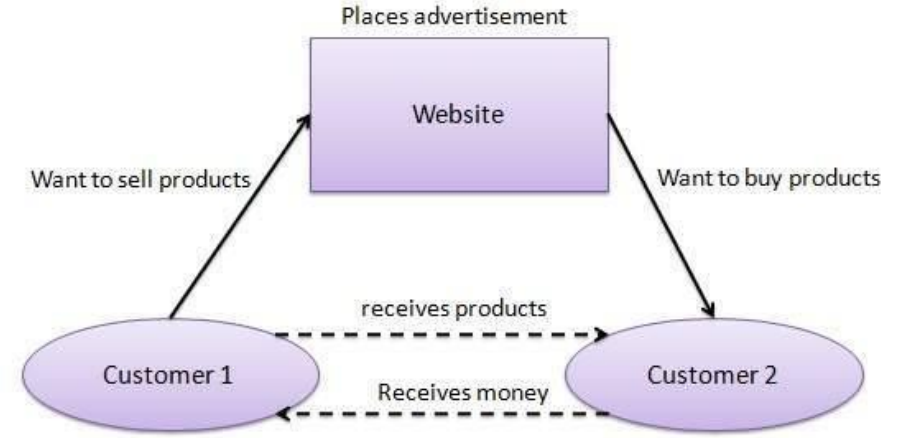
Business - to - Consumer

A website following the B2C business model sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same. The website will then send a notification to the business organization via email and the organization will dispatch the product/goods to the customer.



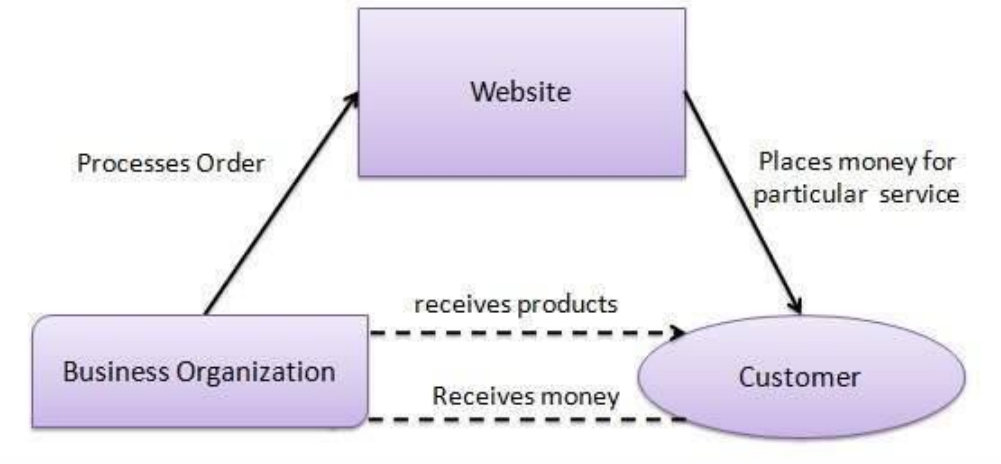
Consumer - to - Consumer

A website following the C2C business model helps consumers to sell their assets like residential property, cars, motorcycles, etc., or rent a room by publishing their information on the website. Website may or may not charge the consumer for its services. Another consumer may opt to buy the product of the first customer by viewing the post/advertisement on the website.



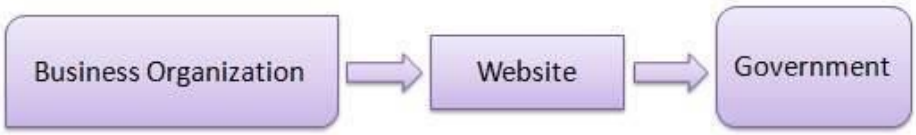
Consumer - to - Business

In this model, a consumer approaches a website showing multiple business organizations for a particular service. The consumer places an estimate of amount he/she wants to spend for a particular service. For example, the comparison of interest rates of personal loan/car loan provided by various banks via websites. A business organization who fulfills the consumer's requirement within the specified budget, approaches the customer and provides its services.



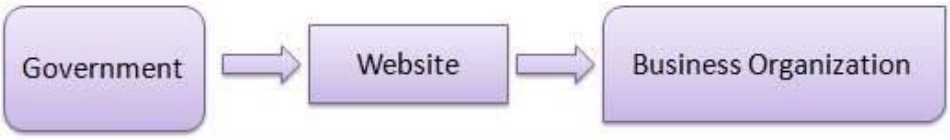
Business - to - Government

B2G model is a variant of B2B model. Such websites are used by governments to trade and exchange information with various business organizations. Such websites are accredited by the government and provide a medium to businesses to submit application forms to the government.



Government - to - Business

Governments use B2G model websites to approach business organizations. Such websites support auctions, tenders, and application submission functionalities.

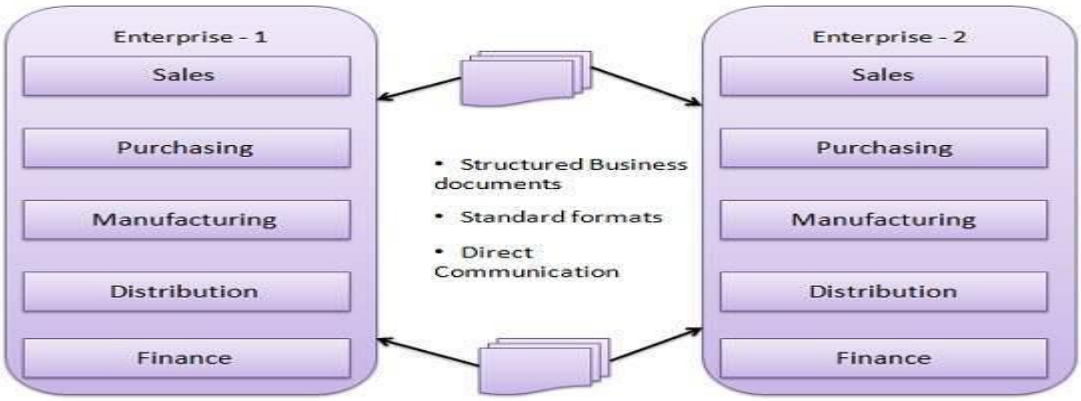


Government - to - Citizen

Governments use G2C model websites to approach citizen in general. Such websites support auctions of vehicles, machinery, or any other material. Such website also provides services like registration for birth, marriage or death certificates. The main objective of G2C websites is to reduce the average time for fulfilling citizen's requests for various government services.

ELECTRONIC DATA INTERCHANGE (EDI)

EDI stands for Electronic Data Interchange. EDI is an electronic way of transferring business documents in an organization internally, between its various departments or externally with suppliers, customers, or any subsidiaries. In EDI, paper documents are replaced with electronic documents such as word documents, spreadsheets, etc.



EDI DOCUMENTS

Following are the few important documents used in EDI −

- Invoices
- Purchase orders
- Shipping Requests
- Acknowledgement
- Business Correspondence letters
- Financial information letters

STEPS IN AN EDI SYSTEM

Following are the steps in an EDI System.

- A program generates a file that contains the processed document.
- The document is converted into an agreed standard format.
- The file containing the document is sent electronically on the network.
- The trading partner receives the file.
- An acknowledgement document is generated and sent to the originating organization.

ADVANTAGES OF AN EDI SYSTEM

Following are the advantages of having an EDI system.

- **Reduction in data entry errors.** − Chances of errors are much less while using a computer for data entry.
- **Shorter processing life cycle** − Orders can be processed as soon as they are entered into the system. It reduces the processing time of the transfer documents.

- **Electronic form of data** − It is quite easy to transfer or share the data, as it is present in electronic format.
- **Reduction in paperwork** − As a lot of paper documents are replaced with electronic documents, there is a huge reduction in paperwork.
- **Cost Effective** − As time is saved and orders are processed very effectively, EDI proves to be highly cost effective.
- **Standard Means of communication** − EDI enforces standards on the content of data and its format which leads to clearer communication.

ELECTRONIC FUND TRANSFER

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in the same bank or different banks. Fund transfer can be done using ATM (Automated Teller Machine) or using a computer.

Nowadays, internet-based EFT is getting popular. In this case, a customer uses the website provided by the bank, logs in to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers the amount to other account if it is in the same bank, otherwise the transfer request is forwarded to an ACH (Automated Clearing House) to transfer the amount to other account and the amount is deducted from the customer's account. Once the amount is transferred to other account, the customer is notified of the fund transfer by the bank.

COMPARISON OF HTML AND XML

HTML	XML
HTML is an abbreviation for HyperText Markup Language.	XML stands for eXtensible Markup Language.
HTML was designed to display data with focus on how data looks.	XML was designed to be a software and hardware independent tool used to transport and store data, with focus on what data is.
HTML is a markup language itself.	XML provides a framework for defining markup languages.
HTML is a presentation language.	XML is neither a programming language nor a presentation language.
HTML is case insensitive.	XML is case sensitive.

HTML is used for designing a web-page to be rendered on the client side.	XML is used basically to transport data between the application and the database.
HTML has it own predefined tags.	While what makes XML flexible is that custom tags can be defined and the tags are invented by the author of the XML document.
HTML is not strict if the user does not use the closing tags.	XML makes it mandatory for the user the close each tag that has been used.
HTML does not preserve white space.	XML preserves white space.
HTML is about displaying data,hence static.	XML is about carrying information,hence dynamic.

EDI WITH ITS TRADE CYCLE

Electronic Data Interchange (EDI)

- EDI provides a standardised system for coding trade transactions so that they can be communicated directly from one computer system to another.
- EDI removes the need for printed orders and invoices and avoids the delays and errors implicit in paper handling.
- EDI is used by organisations that make a large number of regular transactions. Examples are the large supermarket chains and the vehicle assemblers which use EDI for transactions with their suppliers.

The trade cycle

- Conducting a commercial transaction involves the following steps:
  - Pre-Sale:
    - Search - finding a supplier
    - Negotiate – agreeing the terms of trade
  - Execution:
    - Order
    - Delivery
  - Settlement:
    - Invoice
    - Payment
  - After-sales, e.g. warrantee and service

ELECTRONIC DATA INTERCHANGE

Commercial transactions that are repeated on a regular basis, such as supermarkets replenishing their shelves, is one category of trade cycle. EDI is the e-Commerce technology appropriate to these exchanges, see Figure 1.

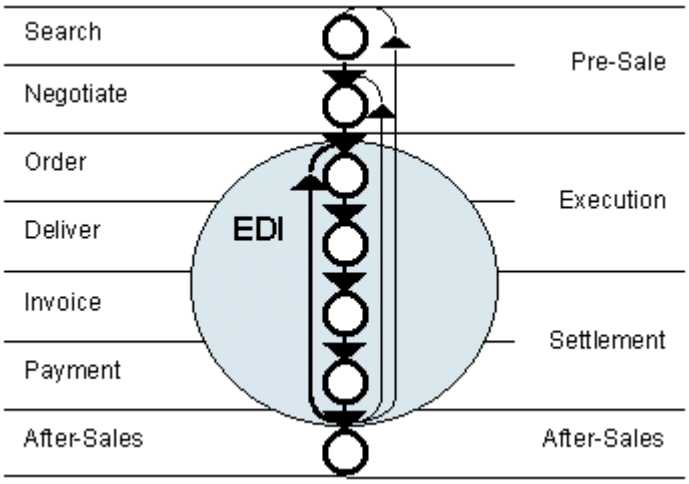


Figure 1: EDI Trade Cycle.

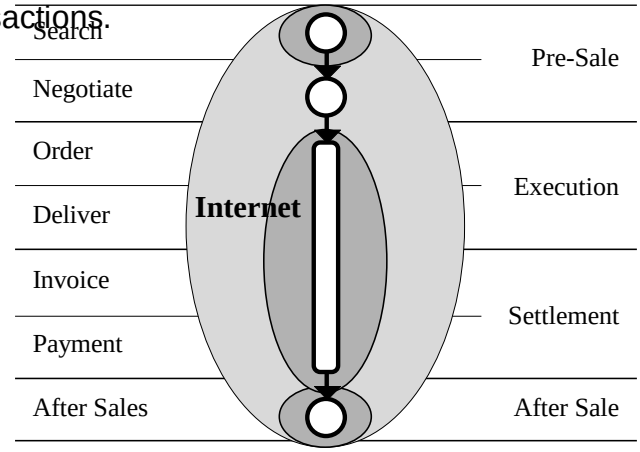
INTERNET COMMERCE WITH ITS TRADE CYCLE.

INTERNET COMMERCE

- Information and communications technologies can also be used to advertise and make once-off sales of a wide range of goods and services.
- This type of e-Commerce is typified by the commercial use of the Internet. The Internet can, for example, be used for the purchase of books that are then delivered by post or the booking of tickets that can be picked up by the clients when they arrive at the event.
- It is to be noted that the Internet is not the only technology used for this type of service and this is not the only use of the Internet in e-Commerce.

THE TRADE CYCLE

- Used for once-off transactions – consumer or inter-organisational transactions.



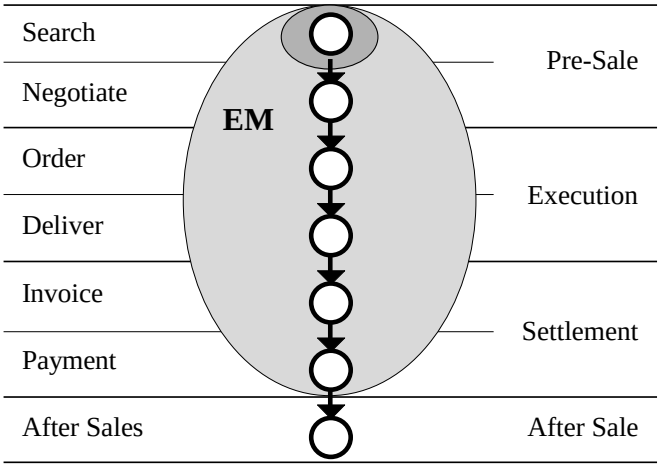
- Can apply to Search, Execution / Settlement and / or After Sales.

- Consumers pay at time of ordering – businesses may have credit arrangements with the suppliers.

ELECTRONIC MARKET WITH ITS TRADE CYCLE.
ELECTRONIC MARKETS

- The use of information and communications technology to present a range of offerings available in a market segment and hence enable:
  - the purchaser to compare the prices (and other attributes);
  - make a purchase decision.
  - The usual example of an electronic market is an airline booking system.
- There is the potential for new electronic markets to be created using Internet technologies.

THE TRADE CYCLE



- Emphasis on the search phase of the trade cycle
- Typically an inter-organisational credit trade cycle
- Limited applications – airline seat bookings and financial sector – the operation of the electronic market is not necessarily in the vendor's interests.

SUPPLY CHAIN

A supply chain involves a series of steps involved to get a product or service to the customer. The steps include moving and transforming raw materials into finished products, transporting those products, and distributing them to the end-user. The entities involved in the supply chain include producers, vendors, warehouses, transportation companies, distribution centers, and retailers.

The elements of a supply chain include all the functions that start with receiving an order to meeting the customer's request. These functions include product development, marketing, operations, distribution networks, finance, and customer service.

Supply chain management is a very important part of the business process. There are many different links in this chain that require skill and expertise. When supply chain management is effective, it can lower a company's overall costs and

boost profitability. If one link breaks down, it can affect the rest of the chain and can be costly.

WHAT IS EPROCUREMENT?

EProcurement, also known as electronic procurement or supplier exchange, is the purchase and sale of supplies, equipment, works and services through a web interface or other networked system.

The technology is designed to centralise and automate interactions between an organisation, customers, and other value chain partners to improve speed and efficiency of procurement practices.

It boasts a suite of innovative features – all designed to bolster the efficiency, effectiveness and total cost of procurement.

e-Procurement consists of Indent Management, RFX creation, e-Tendering, e-Auctioning, Vendor Management and Contract Management among other processes.

BENEFITS OF EPROCUREMENT

EProcurement offers significant benefits for your organisation and the most common are listed below:

- Automates laborious tasks – tasks such as auctioning orders and document management for purchase orders, evaluating and selecting suppliers, price negotiations, agree and storing supplier contracts and more can all be automated between an organisation and its suppliers to increase the speed you do business, freeing up staff for other tasks
- Improved workflows for procurement – this enables end-user self-service and decentralisation with control through company-approved catalogues, and more frictionless processing of employee requisitions (the ordering of goods and services) and supplier payments
- Visibility of your purchasing behaviours – eProcurement will give your organisation visibility into what it spends. This data is invaluable and will help you control things such as non-compliant (or maverick) spend , identify areas for consolidation of suppliers, or to leverage buying power to negotiate cost savings
- Connecting to external supply chains and ERP – Realtime information can be shared between ERP or finance systems and supply chains for better overall visibility of supplier information and supplier transactions.

WHAT ARE THE MAIN FUNCTIONS OF EPROCUREMENT?

The primary functions of eProcurement are far-reaching, offering a range of benefits for a company’s day-to-day operation and supply chain activities. Below, we list the main functions of eProcurement for business:

- Automates processes to free up resource and reduce errors.
- Improves communication between stakeholders and partners to streamline the procurement cycle.
- Provides a single platform for all procurement activity, giving stakeholders and managers a centralised platform for managing and auditing.
- Offers real-time updates for vendors, management, stakeholders and partners, as well as the chance to curate and store procurement data.
- Allows for streamlined negotiation between multiple partners and stakeholders.

WHAT ARE THE MAJOR EPROCUREMENT TOOLS?

There are several tools and processes used in the field of eProcurement, including:

- **Electronic data interchange system**

  An electronic data interchange (EDI) is used to exchange data and information between electronic devices. Messages and information from partner companies are transmitted and stored via EDI, streamlining invoicing and order logistics.

- **Internet applications and platforms**

  Businesses implement a variety of eProcurement tools and web platforms to facilitate day-to-day working, including eSourcing, eTendering, eAuctioning and eOrdering tools. Email is also used predominantly, as well as XML-based data transfer.

- **E-ordering and purchasing tools**

  Major tools relating to product purchasing include a web-based ERP and digital mechanisms for eAuctions.

- **Web3**

  web3 is used as part of a Purchase to Pay solution, providing procurement personnel with greater insights into buying patterns across a variety of devices, whilst also allowing for substantial savings across the supply chain.

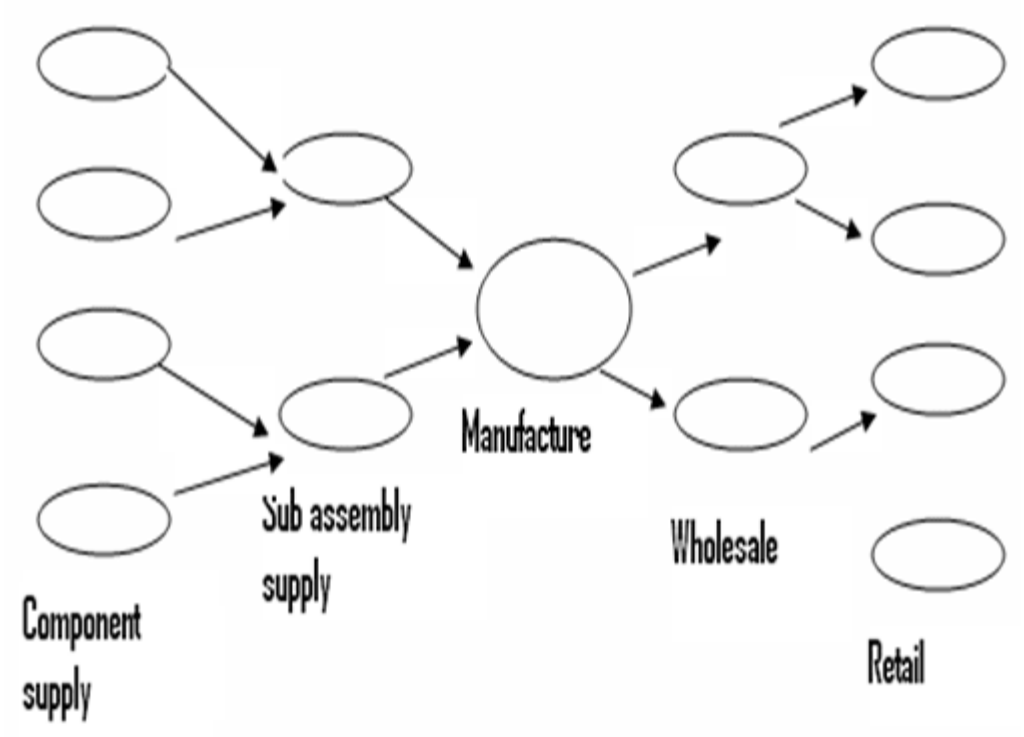
ECOMMERCE APPLICATIONS IN DIFFERENT SECTORS

e-commerce or Electronic Commerce, that is business done online or electronically with the use of Internet or any other computer networking system is applied into the four main section of business given below:

- e-Commerce applications in the Manufacturing Sector
- e-Commerce applications in the Wholesale Sector
- e-Commerce applications in the Retail Sector

- e-Commerce applications in the Service Sector

MANUFACTURING



E-COMMERCE APPLICATIONS IN MANUFACTURING:

Manufacturing can be defined as the process of collecting and then converting raw materials into finished, qualitative goods or products for the consumers.
Manufacturing requires a web of various components, contracts personnel etc working intricately together and in synch in order to produce goods or services.
Manufacturing requires components, assemblies, transportation, storages, paper works, etc.

e-commerce applied to the supply chain management process helps in reducing the overall costs drastically and improves quality and efficiency by automating most of the supply chain.

ECOMMERCE APPLICATION IN WHOLESALE:

Selling goods or products in large quantities to anyone other than the consumers, take for example the retailers, industrial/ commercial or other business users or even distributors are known as wholesalers.

Physical assembling, sorting & grading goods in large lots, breaking bulk, repacking & redistributing in smaller lots is all a part wholesale.

PROBLEMS FACED BY THE TRADITIONAL SYSTEM OF WHOLESALE:

The local wholesalers could not compete with the foreign wholesale enterprises who had acquired highly advanced management and operational skills over due time.

The wholesale sector was characterized for its high input and low output.

Wholesale operating costs which included staffing, setting up and acquiring land for local warehouses, establishing distribution centers etc were extremely high.

ROLE OF ECOMMERCE IN WHOLESALE:

- Reduced operating costs, access to accurate and correct information on time & quick responses helps in qualitative and efficient decision making.
- Ability of doing global marketing in less time and cheaper
- Gaining and catching up to the competitive edge held by foreign wholesalers such as MNC's
- Offers a wide and extensive range of information, intermediary and business services.

ECOMMERCE APPLICATION IN RETAIL:

Selling of goods and services to the consumers for their personal consumption and use is known as **retailing.**

For example Ebay.com, departmental stores, then services like dentists, doctors, hotels, etc.

Retailers provide a link between the consumers and the manufacturers and add value to the product and service by making their sales easier.

Retailers answer any queries that we may have, they display and demonstrate products to the consumers before selling it to them. This makes the services by retailers less risky and more fun to buy products.

They even provide extra services from personal shopping to gift wrapping and home delivery.

ROLE OF ECOMMERCE IN RETAILING:

The Internet has made retailing an exciting and challenging field in recent days with various companies hosting their stores online via the internet.

People can now sit at their computers, open the website they desire to do so and browse the catalogues put up by the company (retailer), choose their product and either pay for it online itself or on delivery. We don't need to step out our room to make a purchase nowadays.

Having our store online helps drastically in cost cutting as companies don't need to purchase stores, they can cut down on staff, provide services to a much wider audience etc

ECOMMERCE APPLICATION IN THE SERVICE SECTOR

One of the three main industrial categories of a developed economy is the service sector.

It involves basically the provision of all services such as distribution and sales of goods to other businesses and consumers such as pest control, entertainment and even services such as transportation.

It also includes the public utilities and the soft parts of the economy such as insurance, banking, education, insurance, etc.

The service sector focuses mainly on people-to-people services.

ISSUES FACED BY THE SERVICE SECTOR:

Since services are intangible, it's extremely difficult to make customer understand and aware about their benefits.

Quality of services depends solely on the quality of the individual providing the services.

There's no special technology or anything like in manufacturing to attract people.

ROLE OF ECOMMERCE IN THE SERVICE SECTOR:

e-commerce helps in improving and increasing the speed of transactions, reduces management expenditure, increases efficiency and increases competitiveness.

Helps the insurance, banking and mainly all the financial sectors, real estate, telecommunications, tourism, logistics, and postal services.

e-commerce also helps services gain a competitive advantage by providing strategies for differentiation, cost leadership and customer satisfaction.

E-COMMERCE TECHNOLOGY

IT INFRASTRUCTURE

IT infrastructure refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment.

IT infrastructure allows an organization to deliver IT solutions and services to its employees, partners and/or customers and is usually internal to an organization and deployed within owned facilities.

IT infrastructure consists of all components that somehow play a role in overall IT and IT-enabled operations. It can be used for internal business operations or developing customer IT or business solutions.

The IT infrastructure consists of all elements that support the management and usability of data and information. These include the physical hardware and facilities (including data centers), data storage and retrieval, network systems, legacy interfaces, and software to support the business goals of an enterprise. The structure also includes hiring, training, policy, testing, process, upgrades, and repairs.

COMPONENTS OF IT INFRASTRUCTURE

Typically, a standard IT infrastructure consists of the following components:

Hardware

This is the “physical” part of an IT infrastructure, and comprises all the elements necessary to support the basic functioning of the machines and devices constituting the infrastructure itself.

Servers, computers, storage and data centers, switches, hubs and routers, as well as all other equipment such as the power, cooling, cabling and dedicated rooms.

Software

It refers to all the applications used by the enterprise both for internal purposes and to provide its services to customers.

Software includes web servers, Enterprise resource planning (ERP), customer relationship management (CRM), productivity applications and the operating system (OS).

The OS is the most important software component and is responsible for managing the hardware itself and connect the physical resources to the network infrastructure.

Facilities

Facilities or physical plants provide space for networking hardware, servers and data centers. It also includes the network cabling in office buildings to connect components of an IT infrastructure together.

Network

Although is not strictly necessary for an IT infrastructure to function, the network is essential to establish internal and external communication of all elements and devices.

The network part includes all the hardware and software elements necessary to ensure network enablement, internet connectivity, firewall and security. It ensures that personnel get access to stored and transferred data only from strictly controlled access points to reduce the risk of data theft or damage.

Meatware

Since they contribute to constituting the enterprise environment and guarantee its functions, associated personnel and processes such as ITOps or DevOps are also part of an IT infrastructure.

Human users, such as network administrators (NA), developers, designers and end users with access to any IT appliance or service are also part of an IT infrastructure, specifically with the advent of user-centric IT service development.

Server

A core hardware component needed for an enterprise IT infrastructure is a server. **Servers** are essentially computers that allow multiple users to access and share resources.

Server room/data center

Organizations house multiple servers in rooms called server rooms or data centers. Data centers are the core of most networks.

INTERNET

The Internet is a global network of computing systems which are connected to each other and help in providing information to everyone who has access. When a web address is entered, the internet makes use of internet protocol address which tells the exact location of the computer, where it is present. From there it gets the information from sets of devices known as the web server which can have a domain name and an address which is then displayed with the help of a browser. It has a basic level of security and does not have firewalls to protect it. There is no requirement of the password to use it and people anywhere, who have the availability of a computer can get all the information which they require.

Uses of the Internet

Some of the important usages of the internet are:

1. **Online Businesses (E-commerce):** Online shopping websites have made our life easier, e-commerce sites like Amazon, Flipkart, Myntra are providing very spectacular services with just one click and this is a great use of the Internet.
2. **Cashless transactions:** All the merchandising companies are offering services to their customers to pay the bills of the products online via various digital payment apps like Paytm, Google pay, etc. UPI payment gateway is also increasing day by day. Digital payment industries are growing at a rate of 50% every year too because of the INTERNET.
3. **Education:** It is the internet facility that provides a whole bunch of educational material to everyone through any server across the web. Those who are unable to attend physical classes can choose any course from the internet and can have the point-to-point knowledge of it just by sitting at home. High-class faculties are teaching online on digital platforms and providing quality education to students with the help of the Internet.
4. **Social Networking:** The purpose of social networking sites and apps is to connect people all over the world. With the help of social networking sites, we can talk, share videos, images with our loved ones when they are far away from us. Also, we can create groups for discussion or for meetings.
5. **Entertainment:** The Internet is also used for entertainment. There are numerous entertainment options available on the internet like watching movies, playing games, listening to music, etc. You can also download movies, games, songs, TV Serial, etc., easily from the internet.

Advantages of the Internet

1. **Online Banking and Transaction:** The Internet allows us to transfer money online by the net banking system. Money can be credited or Debited from one account to the other.
2. **Education, online jobs, freelancing:** Through the Internet, we are able to get more jobs via online platforms like Linkedin and to reach more job providers. Freelancing on the other hand has helped the youth to earn a side income and the best part is all this can be done via INTERNET.
3. **Entertainment:** There are numerous options of entertainment online we can listen to music, play games can watch movies, web series, listening to podcasts, youtube itself is a hub of knowledge as well as entertainment.
4. **New Job roles:** The Internet has given us access to social media, and digital products so we are having numerous new job opportunities like digital marketing and social media marketing online businesses are earning huge amounts of money just because the internet being the medium to help us to do so.
5. **Best Communication Medium:** The communication barrier has been removed from the Internet. You can send messages via email, Whatsapp, and Facebook. Voice chatting and video conferencing are also available to help you to do important meetings online.
6. **Comfort to humans:** Without putting any physical effort you can do so many things like shopping online it can be anything from stationaries to clothes, books to personal items, etc. You can books train and plane tickets online.
7. **GPS Tracking and google maps:** Yet another advantage of the internet is that you are able to find any road in any direction, areas with less traffic with the help of GPS in your mobile.

Disadvantages of the Internet

1. **Time wastage:** Wasting too much time on the internet surfing on social media apps and doing nothing decreases your productivity rather than wasting time on scrolling social media apps one should utilize that time in doing something skillful and even more productive.
2. **Bad impacts on health**: Spending too much time on the internet causes bad impacts on your health physical body needs some outdoor games exercise and many more things. Looking at the screen for a longer duration causes serious impacts on the eyes.
3. **Cyber Crimes:** Cyberbullying, spam, viruses, hacking, and stealing data are some of the crimes which are on the verge these days. Your system which contains all the confidential data can be easily hacked by cybercriminals.
4. **Effects on children:** Small children are heavily addicted to the Internet watching movies, games all the time is not good for their overall personality as well as social development.
5. **Bullying and spreading negativity:** The Internet has given a free tool in the form of social media apps to all those people who always try to spread negativity with very revolting and shameful messages and try to bully each other which is wrong.

INTRANET

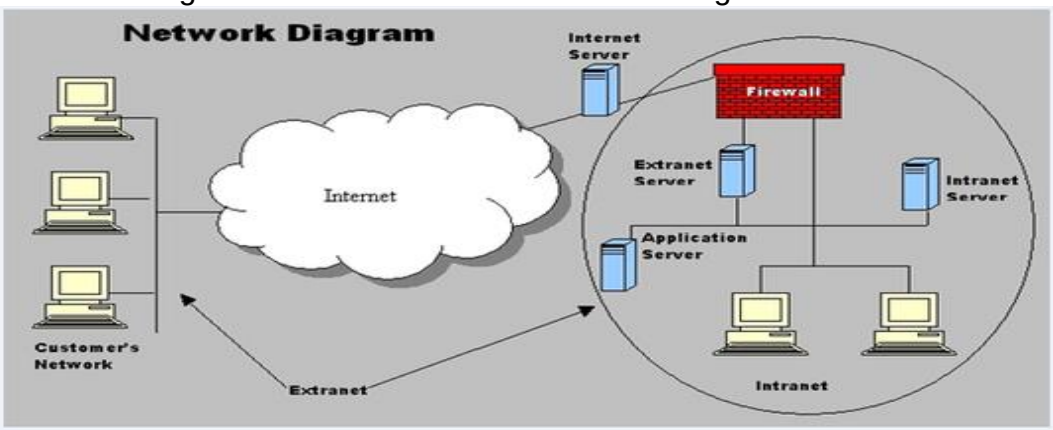
An intranet is a platform which works on the same principals as the internet but is not accessible to the outer world. It is unique to an organization such as universities which have information provided and can be viewed within the premises of the Institute. All the computer are connected with each other and have no connection with the outer world. When the intranet is connected to the internet, it will be protected with another level of security in the form of the firewall so that only particular people can reach it. To simplify it is a network on the computer which works without depending on the internet. There are files of intranet present inside the computer which help in gaining all the information without depending on the internet.

EXTRANET

An Extranet is best explained as a network which depends on the internet but is restricted to specific users. It is more accurate than intranet in a way that only a few people instead of a particular place can get access. It is protected by a firewall and if the intranet is accessed from the internet to send or receive information it becomes an extranet. It is mostly used by business and companies who have to share sensitive data with each other. The firewall is used to switch between internet and intranet and lets only the people who can log in with the help of passwords or by internet protocol addresses. It can be used by individuals or a group of folks depending on the level of requirement.

1. **Intranet** is shared content accessed by members within a single organization.

- **Extranet** is shared content accessed by groups through cross-enterprise boundaries.
- **Internet** is global communication accessed through the Web.



DIFFERENCE BETWEEN INTERNET, INTRANET, EXTRANET :

Internet	***Intranet***	***Extranet***
It is a **Global system** of interconnected computer network.	It is a **Private network** specific to an organisation.	It is a **Private network** that uses public network to share information with suppliers and vendors.
Not regulated by any authority.	It is regulated by an organization.	It is regulated by multiple organization.
Thus content in the network isaccessible to everyoneconnected.	Thus content in the network is accessible only to members of organization.	The content in the network is accessible to members of organization & external members with access to network.
It is largest in terms of number of connected devices.	It is small network with minimal number of connected devices.	The number of devices connected is comparable with Intranet.
It is owned by no one.	It is owned by single organization.	It is owned by single/multiple organization.
It is means of sharing information throughout the world.	It is means of sharing sensitive informationthroughout organization.	It is means of sharing informationbetween members and externalmembers.
Security is dependent of the user of device connected to network.	Security is enforced via a firewall.	Security is enforced via a firewall that separates internet & extranet.
Example: What we are normally using is internet.	Example: TCS using internal network for its business operations.	Example: HP and Intel using network for business related operations.
Users can access Internet anonymously.	Users should have valid username/password to access Intranet.	Users should have valid username/password to access Extranet.
Internet is unregulated and uncensored.	But Intranet is regulated by theorganization policies.	Extranet is also regulated by contractualagreements between organizations.

VIRTUAL PRIVATE NETWORK (VPN)

A **virtual private network** (**VPN**) is a **network** that is constructed using public wires — usually the internet — to connect remote users or regional offices to a company's **private**, **internal network**.

What Is a VPN?

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments**.**

HOW DOES A VIRTUAL PRIVATE NETWORK (VPN) WORK?

At its most basic level, VPN tunnelling creates a point-to-point connection that cannot be accessed by unauthorized users. To actually create the VPN tunnel, the endpoint device needs to be running a VPN client (software application) locally or in the cloud. The VPN client runs in the background and is not noticeable to the end user unless there are performance issues.

The performance of a VPN can be affected by a variety of factors, among them the speed of users' internet connections, the types of protocols an internet service provider may use and the type of encryption the VPN uses. In the enterprise, performance can also be affected by poor quality of service (QoS) outside the control of an organization's information technology (IT)
department.

OR

A VPN extends a corporate network through encrypted connections made over the Internet. Because the traffic is encrypted between the device and the network, traffic remains private as it travels. An employee can work outside the office and still securely connect to the corporate network. Even smart phones and tablets can connect through a VPN.

WHY VPN IS NEEDED?

- **Hide your IP address**

  Connecting to a Virtual Private Network often conceals your real IP address.
- **Change your IP address**

  Using a VPN will almost certainly result in getting a different IP address.
- **Encrypt data transfers**

  A Virtual Private Network will protect the data you transfer over public WiFi.
- **Mask your location**

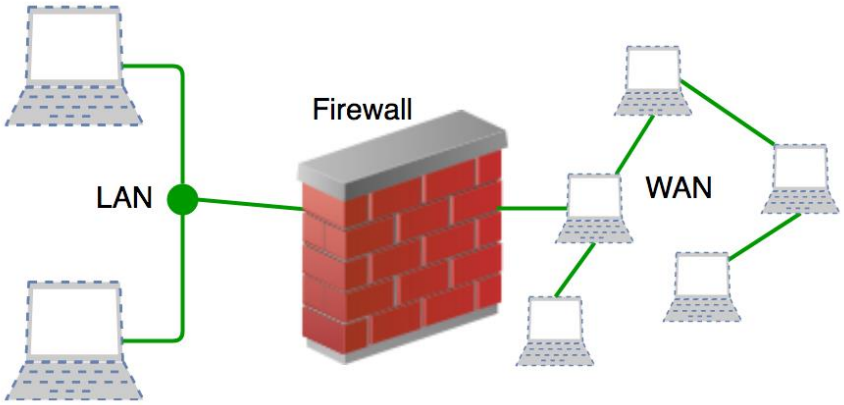
With a Virtual Private Network, users can choose the country of origin for their Internet connection.

- **Access blocked websites**

  Access government blocked websites with VPN.

FIREWALL

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.



HOW FIREWALL WORKS

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic.

For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department.

Rules can be defined on the firewall based on the necessity and security policies of the organization.
From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass.

Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

FIREWALLS CAN BE CATEGORIZED BASED ON ITS GENERATION.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly
   uses first 3 layers).
   Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

2. **Second Generation- Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.
3. **Third Generation- Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

   In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

4. **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

TYPES OF FIREWALL

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls:** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

CONCEPT OF CRYPTOGRAPHY

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

TECHNIQUES USED FOR CRYPTOGRAPHY:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

FEATURES OF CRYPTOGRAPHY ARE AS FOLLOWS:

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

TYPES OF CRYPTOGRAPHY:

In general there are three types of Cryptography:

1. **Symmetric Key Cryptography:**

   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. **Hash Functions:**

   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:**

   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Encryption – Process of converting electronic data into another form, called cipher text, which cannot be easily understood by anyone except the authorized parties.This assures data security.

Decryption– Process of translating code to data.

- Message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.
- When some message is to be kept secure like username, password, etc., encryption and decryption techniques are used to assure data security.

Types of Encryption

1. **Symmetric Encryption**– Data is encrypted using a key and the decryption is also done using the same key.
2. **Asymmetric Encryption**-Asymmetric Cryptography is also known as public key cryptography. It uses public and private keys to encrypt and decrypt data. One key in the pair which can be shared with everyone is called the public key. The other key in the pair which is kept secret and is only known by the owner is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Public key– Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone.
Private key– Key which is only known to the person who's private key it is.

Authentication-Authentication is any process by which a system verifies the identity of a user who wishes to access it.

Non- repudiation– Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Integrity– to ensure that the message was not altered during the transmission.

Message digest -The representation of text in the form of a single string of digits, created using a formula called a one way hash function. Encrypting a message digest with a private key creates a digital signature which is an electronic means of authentication..

DIGITAL SIGNATURE

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

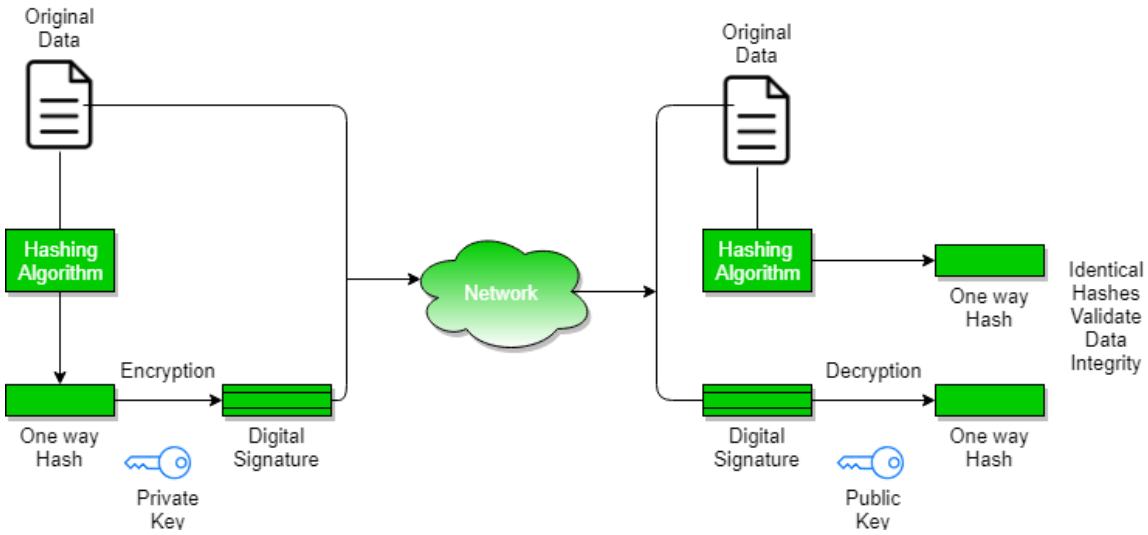
1. **Key Generation Algorithms** : Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.
2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.
3. **Signature Verification Algorithms** : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

THE STEPS FOLLOWED IN CREATING DIGITAL SIGNATURE ARE :

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity,as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).
4. The receiver now has the message digest.

5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



DIGITAL CERTIFICATE

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.
A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

DIGITAL CERTIFICATE CONTAINS:-

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Digital ceritifcate is also sent with the digital signature and the message.

DIGITAL CERTIFICATE VS DIGITAL SIGNATURE :

Digital signature is used to verify authenticity, integrity, non-repudiation ,i.e. it is assuring that the message is sent by the known user and not modified, while digital certificate is used to verify the identity of the user, maybe sender or receiver. Thus, digital signature and certificate are different kind of things but both are used for security. Most websites use digital certificate to enhance trust of their users.

Feature	**Digital Signature**	**Digital Certificate**

Basics / Definition	Digital signature is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.	Digital certificate is a file that ensures holder's identity and provides security.
Process / Steps	Hashed value of original message is encrypted with sender's secret key to generate the digital signature.	It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.
Security Services	**Authenticity** of Sender, **integrity** of the document and **non-repudiation**.	It provides security and **authenticity** of certificate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format

DIGITAL ENVELOPE:

A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication.

A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.

Rivest, Shamir and Adleman (RSA) Public-Key Cryptography Standard (PKCS) governs the application of cryptography to data for digital envelopes and digital signatures.

A digital envelope is also known as a **digital wrapper.**A digital envelope uses two layers for encryption: Secret (symmetric) key and public key encryption. Secret key encryption is used for message encoding and decoding. Public key encryption is used to send a secret key to a receiving party over a network. This technique does not require plain text communication.

Either of the following methods may be used to create a digital envelope:

- Secret key encryption algorithms, such as Rijndael or Twofish, for message encryption.
- Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

A digital envelope may be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data.

An example of a digital envelope is Pretty Good Privacy (PGP) - a popular data cryptography software that also provides cryptographic privacy and data communication authentication.

ELECTRONIC PAYMENT SYSTEM

An e-payment or Electronic Payment system allows customers to pay for the services via electronic methods. They are also known as online payment systems. Normally e-payment is done via debit, credit cards, direct bank deposits, and e-checks, other alternative e-payment methods like e-wallets, bitcoin, cryptocurrencies, bank transfers are also gaining popularity.

TYPES OF E-PAYMENT SYSTEM

E-payments can be done in the following ways,

- **Internet banking** – In this case, the payment is done by digitally transferring the funds over the internet from one bank account to another. Some popular modes of net banking are, NEFT, RTGS, IMPS.

- **Card payments** – Card payments are done via cards e.g. credit card, debit card, smart cards, stored valued cards, etc. In this mode, an electronic payment accepting device initiates the online payment transfer via card

- **Credit/ Debit card** – An e payment method where the card is required for making payments through an electronic device.

- **Smart card** – Also known as a chip card, a smart card, a card with a microprocessor chip is needed to transfer payments.

- **Stored value card** – These types of cards have some amount of money stored beforehand and are needed to make funds transfer. These are prepaid cards like gift cards, etc.

- **Direct debit** – Direct debit transfers funds from a customer's account with the help of a third party

- **E-cash** – It is a form where the money is stored in the customer's device which is used for making transfers.

- **E-check** – This is a digital version of a paper check used to transfer funds within accounts.

Alternate payment methods – As technology is evolving, e-payment methods kept evolving with it (are still evolving..) These innovative alternate e-payment methods became widely popular very quickly thanks to their convenience.

- **E-wallet** – Very popular among customers, an E-wallet is a form of prepaid account, where customer's account information like credit/ debit card information is stored allowing quick, seamless, and smooth flow of the transaction.

- **Mobile wallet** – An evolved form of e-wallet, mobile wallet is extensively used by lots of customers. It is a virtual wallet, in the form of an app that sits on a mobile device. Mobile wallet stores card information on a mobile device. The user-friendly nature of mobile wallets makes them easier to use. It offers a seamless payment experience making customers less dependent on cash.

- **QR payments** – QR code-enabled payments have become immensely popular. QR code stands for 'Quick Response' code, a code that contains a pixel pattern of barcodes or squares arranged in a square grid. Each part of the code contains information. This information can be merchant's details, transaction details, etc. To make payments, one has to scan the QR code with the mobile device.

- **Contactless payments** – Contactless payments are becoming popular for quite some time. These payments are done using RFID and NFC technology. The customer needs to tap or hover the payment device or a card near the payment terminal, earning it a name, 'tap and go'.

- **UPI payments** – NPCI (National Payment Corporation of India) has developed an instant real-time payment system to facilitate interbank transactions. This payment system is titled UPI(Unified Payment Interface). Payments via UPI can be made via an app on a mobile device.

- **Biometric payments** – Biometric payments are done via using/scanning various parts of the body, e.g. fingerprint scanning, eye scanning, facial recognition, etc. These payments are replacing the need to enter the PIN for making transactions making these payments more accessible and easy to use.

- **Payments are done via Wearable devices** – Wearable devices are rapidly becoming popular among customers. These devices are connected to the customer's bank account and are used to make online payments. An example of a wearable used for making an online payment is a smartwatch.

- **AI-based payments** – As machine learning and Artificial Intelligence is creating a revolution all around the world, AI-based solutions are becoming more popular. Payments based on AI such as speakers, chatbots, ML tools,

deep learning tools, etc are making it easier for businesses to maintain transparency.

How e-payment system works?

Entities involved in an online payment system
The merchant
The customer / the cardholder
The issuing bank
The acquirer
Payment Processor
Payment Gateway

Working of e-payments can be explained in the following three steps,

- **Payment initiation** – Customer finalizes the product/service and chooses the payment method to initiate the transaction. Depending on the payment method, the customer enters the required information like card number, CVV, personal details, expiration date, PIN, etc. The chosen payment method either redirects the customer to an external payment page or a bank's payment page to continue the payment process.

- **Payment authentication** – The information submitted by the customer along with other details like payment information, customer's account information is authenticated by the operator. The operator can be a payment gateway or any other solution involved. If everything gets authenticated positively, the operator reports a successful transaction. On the contrary, if there is any problem with any of the authentication checks, the transaction fails. After the successful transaction, the customer gets a payment confirmation.

- **Payment settlement** – After the successful authentication process, payment from the customer's bank gets transferred into the merchant's account by the online payment service provider.

BENEFITS OF E-PAYMENT SYSTEMS

People are almost comfortable with online shopping and e-payments. With this trend, accepting online payment is a must for any business.

E-payments are making shopping and banking more convenient. They are helping customers to reach more clients locally and globally.

E-payments are faster making the transactions efficient.

With e-payments, customers can pay online at anytime from anywhere, making them easily accessible and convenient for customers.

It’s easy to integrate online payment solutions with businesses as many payment processing solution providers offering different types of solutions.

Online payment solutions come with security and risk and anti-fraud tools making them reliable and secure not only for customers but also for merchants.

E-payments are proved to be highly effective for international transactions, as they are cheaper, easier, faster, and generally are real-time.

In conclusion, if you are running a business, accepting online payments is the need of current times. You need to find out what your target customers are preferring and accordingly you need to provide the most convenient and relevant online payment solutions.

RISKS ASSOCIATED WITH PAYMENT SYSTEMS

In any payment transaction, there will be a time lag between the time payment instructions are issued and final settlement of these claims (either on gross or net basis). This time lag exposes the entire system to various risks which are given below:

1. **Credit Risk:** the risk that a party within the system will be unable fully to meet its financial obligations within the system either when due or at any time in the future
2. **Liquidity Risk:** the risk that a party within the system will have insufficient funds to meet financial obligations within the system as and when expected although it may be able to do so at some time in the future
3. **Legal Risk:** the risk that a poor legal framework or legal uncertainties will cause or exacerbate credit or liquidity risks
4. **Operational Risk:** the risk that operational factors such as technical malfunctions or operational mistakes will cause or exacerbate credit or liquidity risks
5. **Systemic Risk:** the risk that the inability of one of the participants to meet its obligations, or a disruption in the system itself, could result in the inability of other system participants or of financial institutions in other parts of the financial system to meet their obligations as they become due. Such a failure could cause widespread liquidity or credit problems and, as a result, could threaten the stability of the system or of financial markets.

SECURE SOCKETS LAYER(SSL)

SSL (Secure Sockets Layer) is a standard security protocol for establishing an encrypted link between a server and a client. This ensures that all data transmission between a client and server remains confidential.

When data is transferred in non-encrypted form between a server and a client, cyber criminals can eavesdrop, intercept, modify and steal the data. Private, confidential data including personal information, login credentials, card details, banking data and

corporate communication must be transmitted securely, and this is achieved through SSL protocol.

Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message.

What Happens Between The Web Browser And Server

1. A browser attempts to connect to a web site secured with **SSL**. The browser requests that the web server identify itself.
2. The server sends the browser a copy of its **SSL certificate**.
3. The browser checks whether it trusts the SSL certificate. If so, it sends a message to the server.
4. The server sends back a digitally signed acknowledgement to start an SSL encrypted session.
5. Encrypted data is shared between the browser and the server.
   SSL Fundamentals

There are 3 essential elements at work in the process described above: a protocol for communications (SSL), credentials for establishing identity (the SSL certificate), and a third party that vouches for the credentials (the certificate authority).

- Computers use protocols to allow different systems to work together. Web servers and web browsers rely on the **Secure Sockets Layer (SSL) protocol** to enable encrypted communications. The browser's request that the server identify itself is a function of the SSL protocol.
- **Credentials** for establishing identity are common to our everyday lives: a driver's license, a passport, a company badge. An SSL certificate is a type of digital certificate that serves as a credential in the online world. Each SSL certificate uniquely identifies a specific domain (such as thawte.com) and a web server.
- Our trust of a credential depends on our confidence in the organization that issued it. **Certificate authorities** have a variety of methods to verify information provided by individuals or organizations. Established certificate authorities, such as Thawte, are well known and trusted by browser vendors. Browsers extend that trust to digital certificates that are verified by the certificate authority

BIOMETRICS

Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance.

The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits.

The term "biometrics" is derived from the Greek words "bio" meaning life and "metric" meaning to measure.

There are two main types of biometric identifiers:

- **Physiological characteristics:** The shape or composition of the body.
- **Behavioral characteristics:** The behavior of a person.

Examples of **physiological characteristics** used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor.

Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice. Certain biometric identifiers, such as monitoring keystrokes or gait in real time, can be used to provide continuous authentication instead of a single one-off authentication check.

Other areas that are being explored in the quest to improve biometric authentication include brainwave signals, electronic tattoos, and a password pill that contains a microchip powered by the acid present in the stomach. Once swallowed, it creates a unique ID radio signal that can be sensed from outside the skin, turning the entire body into a password.

Biometric verification becoming common

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics, and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry. Measuring someone's gait doesn't even require a contact with the person.
Biometric devices, such as fingerprint readers, consist of:

- A reader or scanning device.
- Software that converts the scanned information into digital form and compares match points.
- A database that stores the biometric data for comparison.

Accuracy of biometrics

The accuracy and cost of readers has until recently been a limiting factor in the adoption of biometric authentication solutions but the presence of high quality cameras, microphones, and fingerprint readers in many of today's mobile devices means biometrics is likely to become a considerably more common method of authenticating users, particularly as the new FIDO specification means that two-factor authentication using biometrics is finally becoming cost effective and in a position to be rolled out to the consumer market.

The quality of biometric readers is improving all the time, but they can still produce false negatives and false positives. One problem with fingerprints is that people inadvertently leave their fingerprints on many surfaces they touch, and it's fairly easy to copy them and create a replica in silicone. People also leave DNA everywhere they go and someone's voice is also easily captured. Dynamic biometrics like gestures and facial expressions can change, but they can be captured by HD cameras and copied. Also, whatever biometric is being measured, if the measurement data is exposed at any point during the authentication process, there is always the possibility it can be intercepted. This is a big problem, as people can't change their physical attributes as they can a password. While limitations in biometric authentication schemes are real, biometrics is a great improvement over passwords as a means of authenticating an individual.

E-COMMERCE - SECURITY SYSTEMS

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions −

- **Confidentiality** − Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
- **Integrity** − Information should not be altered during its transmission over the network.
- **Availability** − Information should be available wherever and whenever required within a time limit specified.
- **Authenticity** − There should be a mechanism to authenticate a user before giving him/her an access to the required information.
- **Non-Repudiability** − It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
- **Encryption** − Information should be encrypted and decrypted only by an authorized user.
- **Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

MEASURES TO ENSURE SECURITY

MAJOR SECURITY MEASURES ARE FOLLOWING −

- **Encryption** − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the same or a different secret code.
- **Digital Signature** − Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.
- **Security Certificates** − Security certificate is a unique digital id used to verify the identity of an individual website or user.

CURRENT TRENDS IN ELECTRONIC WORLD

ELECTRONIC WASTE

Electronics waste, also referred as e-waste, describes **"electronic products nearing the end of their 'useful life.'"** But, **"Many of these products can be reused, refurbished, or recycled."**

E-waste includes a huge variety of electronic devices, including:

- **Large appliances such as dishwashers and refrigerators**

- **Small appliances such as toasters and coffee makers**
- **Computers**
- **Televisions**
- **Stereo equipment**
- **Lighting equipment and bulbs**
- **Power tools**
- **Toys and sports equipment with electronic components**
- **Medical equipment systems**
- **Printers, scanners and photocopiers**
- **Personal care devices, such as electric toothbrushes and blowdryers**

Problems caused by E-waste

- Improper or incomplete waste disposal creates a huge environmental burden. **It affects air, soil, water and wildlife**, not to mention human health. That means trash in waterways and green spaces, cancer for animals and humans, species extinction, poisonous algae blooms and more.
- Failing to recycle is a *huge* waste of resources.

  "Recycling one million laptops saves the energy equivalent to the electricity used by 3,657 U.S. homes in a year," says Earth911, citing EPA studies. **"For every one million cell phones that are recycled, the EPA states that 35,274 pounds of copper, 772 pounds of silver, 75 pounds of gold and 33 pounds of palladium can be recovered."**

E-waste Can Be Hazardous Waste

Many electronic devices contain hazardous chemicals. If they aren't disposed of safely, those chemicals can pose a safety hazard to people, animals and the environment. In addition to contaminating soil, hazardous wastes can pollute the air and leach into water sources.

For example, in California, the law views non-functioning cathode-ray tubes (CRTs) from TVs and monitors as hazardous materials. These tubes are used to create images on a screen. They are considered hazardous because they also contain lead.

Here are a few other examples of the hazardous waste electronics hold.

- **Leaded glass:** Computers and television screens contain leaded glass, which is a poisonous heavy metal.
- **Cancer-causing elements:** Batteries carry explosive and cancer-causing elements such as cadmium, lithium and lead.

- **Mercury:** Some appliances like gas hot water heaters and chest freezers contain mercury switches. When mercury isn't properly disposed, it may create serious health issues such as respiratory and skin disorders.

Solutions to the E-waste Problem

1. Recycling

More consumers need to get into the habit of taking their used electronics to an experienced recycling firm that can disassemble them, separating and categorizing the contents by material and cleaning them, then shredding them mechanically for further sorting with advanced separation technologies.

An experienced recycling firm like Great Lakes Electronics Corporation will meet the highest standards for how they recycle our e-waste and ensure that nothing of value within any device gets wasted. By doing so, they're also able to meet the high demand for recycling metals from used electronics, which are then used to make new products.

2. Education

The second most important solution is to *educate* people about how important recycling is for e-waste. It can begin with setting an example, making a commitment on your own to take any electronic device you have that's no longer wanted or being used, and bring it to a recycling firm rather than throw it out with your regular trash or toss it in a desk drawer.

But then it's also important to be vocal about that with others: to note that out of concern for our environment, you adopted the practice of recycling each device.

Writing about the environmental benefits of recycling e-waste on social media sites is also a good place to start spreading the word.

3. Teach

It's important to spread that message to your family, friends, neighbours, and co-workers, but it's also important to get the message to our future leaders — our children.

we could start by asking your teacher if we could work on a project to have all the kids at school bring in the old cell phones their parents no longer want, and teach the students how to collect the devices and get them to a recycling firm.

And it isn't just schools that have a role to play here. Non-profit organizations, municipal governments and businesses in the private sector can also get involved in hosting community events that promote recycling and educating people about our e-waste challenge.

4. Keep Learning

Just as the technology that creates smart phones and other devices keeps changing, the same is true when it comes to e-waste. In the U.S., 25 states now have laws that aim to either prevent used electronics from being sent to landfills, or that promote recycling. The European Union has established new goals for increasing e-waste recycling rates. The United Nations has launched the Step-Initiative to introduce a comprehensive approach to handling E-Waste, while also preparing professionals to work in the field of E-Waste management.

E- SURVEILLANCE

Electronic surveillance is the act of recording, observing or listening to individuals in real-time with or without their knowledge. Electronic surveillance is typically conducted secretively and does not interfere with an individual's normal activities. Usually, a surveillance activity involves one or more individuals observing and documenting another individual's actions using cameras, long-range microphones and listening devices, as well as by monitoring cell, office, and home phone services.

Surveillance can be anywhere

Law enforcement and government agencies use electronic surveillance to collect information with the objective of identifying and preventing criminal activity or terrorist intentions. On the other hand, personnel security and the protection of property are the primary reasons large and small corporations employ electronic surveillance techniques. In either case, surveillance is an effective tool for crime prevention and identifying potential acts of espionage, theft and property damage.

Devices and Their Uses

The use of various electronic devices provides the opportunity to collect information on anyone at any time and with varying duration. Surveillance devices vary in size and use; listed below are several of the more prominent methodologies:

- **Wiretapping**: multiple wires connected internally to a target's communication device, such as a telephone enabling real-time monitoring and recording
- **Bugging**: requires the planting of a small electronic device on a person or in a strategic location, enabling individuals to listen in, copy and record real-time conversations

- **Pen register**: a device placed on a telephone line used to identify the telephone numbers of calls made from the surveilled phone
- **Photographic surveillance**: includes visual equipment such as closed-circuit television and digital cameras in various sizes used to photograph individuals
- **Wired agents and informers**: involves the planting of a recording or listening device on a single person while engaged in conversations with other individuals

SOME OF THE MAIN FEATURES OF THE E-SURVEILLANCE SOFTWARE

- Non-proprietary: Designed to support a wide range of quality CCTV products.
- Monitor an unlimited number of cameras and security devices across any number of sites.
- The system doesn't require any additional or proprietary hardware on site. It interfaces directly with a wide variety of devices including Adpro, Axis, Integral, SYAC, Panasonic, Dedicated Micros, Pixord, Pelco, lenel and Galaxy.
- Compliant with the British standard BS8418: Automatically monitors operator response times and creates a full audit trail of all actions taken.
- A truly scalable monitoring solution, available from a single standalone workstation to a server based central station with an unlimited number of operators and workstations.
- All alarms and events are intelligently prehandled, prioritised and routed immediately to available operators.
- Integrated incident reporting, problem management and extensive management information.
- All events, live cameras and other up to date site information and statistics are accessible through a customised website.
- No practical limit to the level of IP alarm traffic received and automatically handled. The software has been tested to over 10,000 unique alarms per second on standard PC server hardware.
- Certified by Microsoft through the 'Designed for windows' programme.

E-GOVERNANCE

E-Governance can be defined as the application of communication and information technology for providing government services, exchange of information, transactions, integration of previously existing services and information portals.

It makes the whole administrative process convenient, efficient, transparent, fully accountable and responsible. As a fast-growing economy and an emerging world leader, E-Governance is a must in a country like India, both in Government and corporate sector.

Some effective examples of successful implementation of E-Governance to the governmental function include projects like; e-Mitra project(Rajasthan), e-Seva project(Andhra Pradesh), CET(Common Entrance Test)

The objective of E-Governance is to bring about 'Simple, Moral, Accountable, Responsive and Transparent' (SMART) governance. The rationale of E-governance is in its need in reducing red tape; promotion of knowledge sharing to facilitate improvements in quality of governance; fulfilling expectations of the people from government; welfare of citizens, transparency and accountability; increase reach of service delivery by government; speeding up government processes and decision taking ability; equitable access to public service; internal efficiency; reducing costs and improving revenues; improving quality of services etc.

Elements of E-Governance:

Basic elements of e-governance are:

1. Government
2. Citizens
3. Investors/Businesses

Types of E-Governance:

E-governance is of 4 types:

1. **Government-to-Citizen(G2C):**

   The Government-to-citizen mentions the government services that are acquired by the familiar people. Most of the government services come under G2C. Similarly, the primary aim of Government-to-citizen is to supply facilities to the citizens. It also helps the ordinary people to minimize the time and cost to carry out a transaction. A citizen can retrieve the facilities anytime from anywhere.
   Similarly, spending the administrative fee online is also possible due to G2C. The facility of Government-to-Citizen allows the ordinary citizen to outclass time limitation. It also focuses on geographic land barriers.

2. **Government-to-business(G2B):**

   The Government-to-business is the interchange of services between Government and Business firms. It is productive for both government and business firms. G2B provides access to pertinent forms needed to observe. It also contains many services interchanged between business sectors and government.
   Similarly, the Government-to-business provides timely business information. A business organization can have easy and easy online access to government agencies. G2B plays a important role in business development. It upgrades the efficiency and quality of communication and transparency of government projects.

3. **Government-to-Government(G2G):**

   The Government-to-Government mentions the interaction between different government departments, firms and agencies. This increases the efficiency of government processes. In G2G, government agencies can share the same

database using online communication. The government departments can work together. This service can increase international discretion and relations.
G2G services can be at the local level or at the international level. It can convey with both global government and local government. It also provides safe and secure inter-relationship between domestic or foreign government. G2G builds a universal database for all members to upgrade service.

4. **Government-to-Employee(G2E):**

The Government-to-Employee is the internal part of G2G section. It aims to bring employees together and improvise knowledge sharing. It provides online facilities to the employees. Similarly, applying for leave, reviewing salary payment record and checking the balance of holiday. The G2E sector yields human resource training and development. So, G2E is also the correlation between employees and government institutions.

ADVANTAGES OF E-GOVERNANCE

- **Speed**

  Technology makes communication swifter. Internet, smartphones have enables instant transmission of high volumes of data all over the world.

- **Saving Costs**

  A lot the Government expenditure goes towards the cost of buying stationery for official purposes. Letters and written records consume a lot of stationery. However, replacing them with smartphones and the internet can saves crores of money in expenses every year.

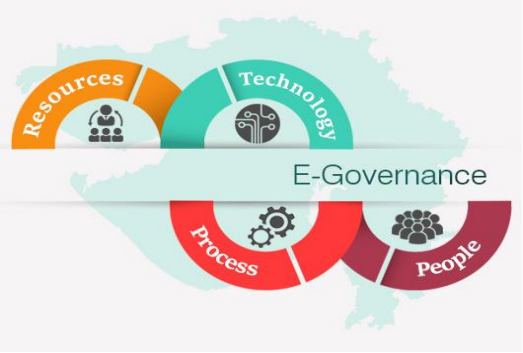
- **Transparency**

  The use of e-governance helps make all functions of the business transparent. All Governmental information can be uploaded onto the internet. The citizens access specifically access whichever information they want, whenever they want it, at the click of a mouse, or the touch of a finger.

  However, for this to work the Government has to ensure that all data as to be made public and uploaded to the Government information forums on the internet.

- **Accountability**

  Transparency directly links to accountability. Once the functions of the government are available, we can hold them accountable for their actions.



DISADVANTAGES OF E-GOVERNANCE

- **Loss of Interpersonal Communication**
  The main disadvantage of e-governance is the loss of interpersonal communication. Interpersonal communication is an aspect of communication that many people consider vital.
- **High Setup Cost and Technical Difficulties**
  Technology has its disadvantages as well. Specifically, the setup cost is very high and the machines have to be regularly maintained. Often, computers and internet can also break down and put a dent in governmental work and services.
- **Illiteracy**
  A large number of people in India are illiterate and do not know how to operate computers and smartphones. E-governance is very difficult for them to access and understand.
- **Cybercrime/Leakage of Personal Information**
  There is always the risk of private data of citizens stored in government serves being stolen. Cybercrime is a serious issue, a breach of data can make the public lose confidence in the Government's ability to govern the people.

E-CARE

e-care is an umbrella term referring to the automation of all aspects of the care delivery processes across administrative, clinical and departmental boundaries in the healthcare delivery system.

The beneficiary of the convergence of multiple technologies such as object-oriented and adaptive applications that leverage the web to link disperate system and enable automated, real time responses to inquires, clinical alerts etc.

BENEFITS OF E-CARE

- Request or schedule medical appointments.
- Request referrals.
- Request prescription renewals.
- View test results.
- View your health summary from your electronic health record.
- Communicate electronically and securely with your clinical team.