B.SC IV TH SEM COMPUTER SCIENCE

PAPER: 4.6 COMPUTER APPLCATIONS

2 marks

QUESTIONS AND ANSWERS

1. What is EDI? ? Give one advantage of EDI

Ans: Electronic Data Interchange (EDI) is the exchange of business documents between any two trading partners in a structured, machine – readable form. It can be used to electronically transmit documents such as purchase – orders, invoices, shipping bills, receiving advices, and other standard business correspondence between trading partners.

2. According to the EDI University, what is EDI?

Ans: "EDI stands for Electronic Data Interchange, a method of transporting all types of information, such as purchase orders, invoices, payments and even graphics, to another party electronically.

3. What is TCP/IP?

Ans: The term TCP/IP(transmission control protocol/internet protocol) refers to the protocols suite and a pair of the TCP and IP are the most important internet communication protocols. An internet protocol is a unique address or identifier of each computer or communication devices on the network and internet.

4. What is Ethernet?

Ans:This is the most widely used protocol. This protocol uses an access method called CSMA/CD(carrier sense multiple access/collision detection)

5. What is HTTP?

Ans: hypertext transfer protocol is a method of transmitting the information on the web. HTTP basically publishes and retrieves the HTTP pages on the World Wide Web .HTTP is a language that is used to communicate between the browser and web browser.

6. What is FTP?

Ans: FTP or file transfer protocol is used to transfer(upload/download) data from one computer to another over the internet or through or computer network.FTP is a most commonly communication protocol for transferring the files over the internet.

7. What is SMTP?

Ans: Simple message transfer protocol that is used to send the email messages between the servers. Most email systems and email clients use the SMTP protocol to send messages to one server to another.

8. What is POP3?

Ans: in computing, email clients such as ms outlook, outlook express and thunderbird use post office protocol to retrieve emails from the remote server over the TCP/IP connection. most email applications use POP protocol.

9.what is DHCP?

Ans: the DHCP or dynamic host configuration protocol is a set of rules used by a communication device such a router.

10.what is UDP?

Ans: the user datagram protocol is almost important protocol of the TCP/IP suite and is used to send the short messages known as datagram.

11. Expand OSI/ISO

Ans: OSI-Open systems interconnection and ISO-International organization for standardization.

12.What is DNS?

Ans: the Domain name system is a method of administering names by giving different groups responsibility for subsets of names. These are separated by periods.

13. What is router?

Ans: In reality packets are being passed from one system to another, the networks on the internet uses a hardware device called a Router.

14. What is IP address?

Ans: Each machine on the internet is assigned a unique address called an IP address.

15. What is m-commerce?

Ans: it is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants(PDA's).it is known as m-commerce.

16. what is E-commerce?

Ans: e-commerce commonly associated with information on buying and selling of products and services via computer networks using technologies like web,

E-mail, EFT, EDI etc..

Or

E-commerce is also defined as the process of using digital technology for transmitting information between organizations.

17. What is firewall?

Ans: firewall (software or hardware) protect a server, a network and an individual personal computer by viruses and hackers.

18. What is E-mail?

Ans: E-mail or electronic mail permits the transmission of electronic messages between computer users.

19. What is HTML?

Ans: Hypertext mark-up language used to create World Wide Web pages.

20. What is URL?

Ans: uniform resource locator is the address of a file or resource accessible on the internet. Ex: http://www.kckclg.org/

21. What is Cryptography?

Ans: Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

22. What is Encryption?

Ans: Encryption Means of hiding a message through substitution or rearranging.

23. What is Decryption?

Ans: Decryption is the process of converting encrypted data back into its original form, so it can be understood.

24.Expand NAP and ISP?

Ans: NAP—Network access point or network access provider

ISP—Internet service providers

25. Expand IPOP.

Ans: Internet point of presence

26. What is e-commerce?

Ans: E-commerce is a modern business methodology that addresses the needs of organization, merchants and consumers to cut costs while improvin the quality of goods and services and increasing the speed of service delivery.

27 What is I-way?

Ans: E-commerce is associated with the buying and selling of information, Products and services via computer networks today and in the future via any one of the myriad of networks that make up the information superhighway (I-way).

28. What is message passing?

Ans: The client-server model allows the client to interact with the server. Through a request –reply sequence governed by a paradigm known as message Passing.

29. List some challenges that each highway route provider faces?

Ans:
- Telecom-based
- Cable-based
- Computer Network-based
- Wireless

30. What is a Network Access Point?

A NAP is a high speed network or switch to which a number of routers can be connected for the purpose of traffic exchange and interoperation.

31. List some services of the internet?

Ans: Some services of the internet are:

- Individual to group communications
- Information Transfer and delivery services
- Information Databases
- Information processing services
- Resource-sharing services

32. What are the 3 types of electronic tokens?

Ans:
- Cash or real-time
- Debit or prepaid
- Credit or postpaid

33. What are the properties of e-cash?

Ans:
- E-cash must have a monetary value
- It must be interoperable
- It must be storable and retrievable
- It should not be easy to copy or tamper with while being exchanged

34. What are smart cards?

Ans: Smart cards are credit and debit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic stripe.

35. Mention the 2 types of smart cards.

Ans:
- Relationship-based smart credit cards
- Electronic purses

36. Mention some factors to be included for designing electronic payment systems.

Ans:
- Privacy
- Security
- Intuitive interface
- Database integration
- Brokers
- Pricing
- Standards

37. Specify the 4 layers of EDI architecture.

Ans:
- EDI semantic layer
- EDI standard layer
- EDI transport layer
- Physical layer

38. What are the 2 major EDI standards?

Ans:
- ANSI X.12
- EDIFACT

39. Give the uses of smart card.

Ans: A **smart card**, typically a type of chip **card**, is a plastic **card** that contains an embedded computer chip–either a memory or microprocessor type that stores and transacts data. This data is usually associated with either value, information, or both and is stored and processed within the **card's** chip.

40. why do you need Encryption of data?

Ans: The main purpose for **Encrypting your data and need** is to ensure your privacy, protect your data, and secure intellectual property. This is also known as endpoint encryption it can still be used to protect a user's identity and privacy.

41. What is digital signature?

Ans: A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature**.**

or

The digital signature is to the electronic world what the handwritten signature is to the commerce.

42. What is authentication?

Ans: The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from *authorization* , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

43. What is Mobile Commerce?

Mobile Commerce is any transaction, involving the transfer of ownership or Rights to use goods and services, which is initiated and/or completed by using mobile access to compute mediated networks with the help of an electronic device."

Five marks questions

1. Describe EDI applications used in business
2. Explain website design issues
3. Explain: 1)E-mail 2) Business to Business e-commerce
4. Explain the E-mail security?
5. Explain the internet industry structure with diagram?
6. Explain the follows:1.LAN 2.WAN
7. What is meant by security policy? Explain the security procedures?
8. Explain the follows:1.FTP 2 E-mail
9. Describe silent features of hypertext transfer protocol
10. Explain the concept of World Wide Web server.
11. Explain the transaction security in network?
12. . Explain the follows 1.Internet 2.DNS
13. Explain the Features of E-Commerce

Ten marks questions

1. Explain the types of Business models in E-Commerce
2. Explain the applications of E-commerce
3. Explain the conventional trading process?
4. Explain framework or architecture of E-commerce?
5. Explain the basic building blocks of an EDI system?
6. Describe TCP/IP reference model with diagram?
7. Explain framework or architecture of M-commerce?
8. What is firewall? Explain its types in detail?
9. Explain the protecting the network services?
10. Explain internet marketing in detail.
11. Explain web clients and web servers
12. Describe the credit card transactions process in detail.
13. Explain the follows: 1.cryptography 2.digital signature
14. Explain the transaction security in network
13. Explain the different types of online payment system.

2) The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.

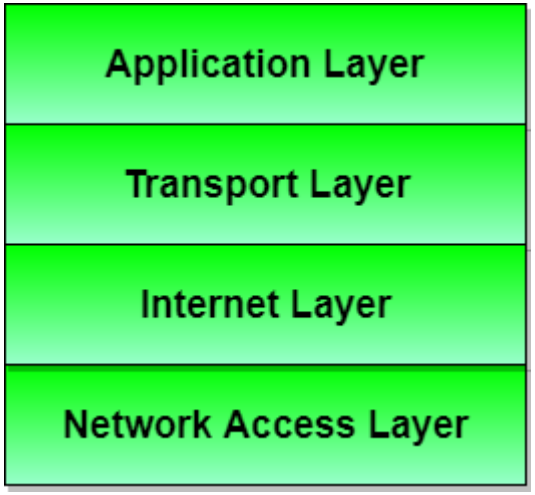
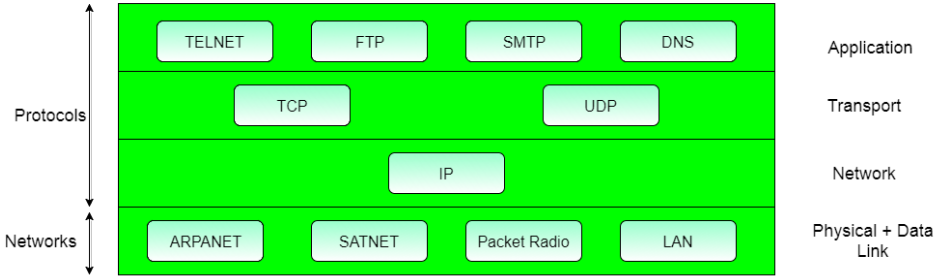


Diagram Tcp/ip model

Protocols and networks in the TCP/IP model:



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of **Defence's Project Research Agency** (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.

- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.

2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
    - **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
    - **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

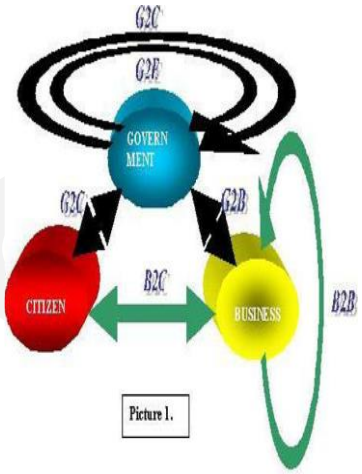
3) Application of E-commerce:

- Buying/selling a variety of goods and services from one's home or business
- Anywhere, anytime transaction
- Can look for lowest cost for specific goods or service
- Businesses can reach out to worldwide clients - can establish business partnerships
- Order processing cost reduced
- Electronic funds transfer faster
- Supply chain management is simpler, faster, and cheaper using ecommerce
- Can order from several vendors and monitor supplies.
- Production schedule and inventory of an organization can be inspected by cooperating supplier who can in turn schedule their work
- **Retail & wholesale**

4. ELECTRONICS COMMERCE BUSINESS MODELS CAN GENERALLY CLASSIFY IN FOLLOWING CATEGORIES.

Meaning: A plan for the successful operation of a business, identifying sources of revenue, the intended customer base, products, and details of financing.

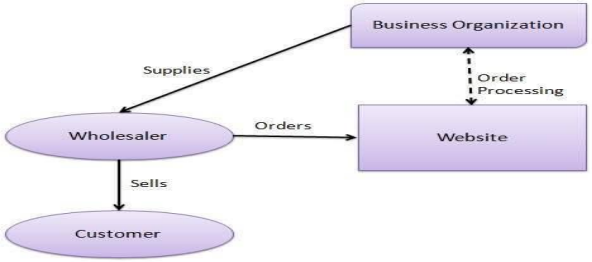
1. Business - to - Business (B2B)
2. Business - to - Consumer (B2C)
3. Consumer - to - Consumer (C2C)
4. Consumer - to - Business (C2B)
5. Business - to - Government (B2G)
6. Government - to - Business (G2B)
7. Government - to - Citizen (G2C**)**



Picture 1.

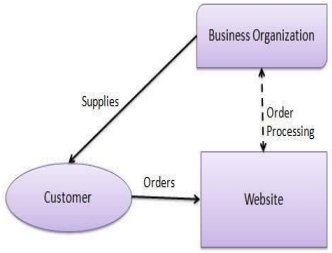
1) Business - to - Business (B2B)

Website following B2B business model sells its product 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 final customer who comes to buy the product at wholesaler's retail outlet.



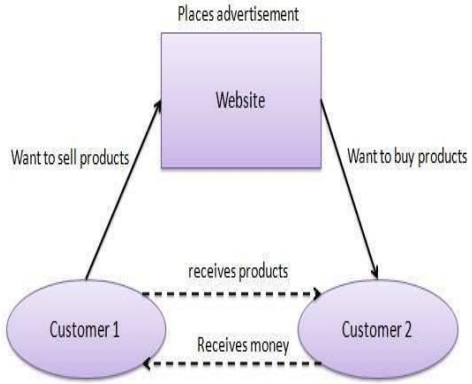
2) Business - to - Consumer(B2C)

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



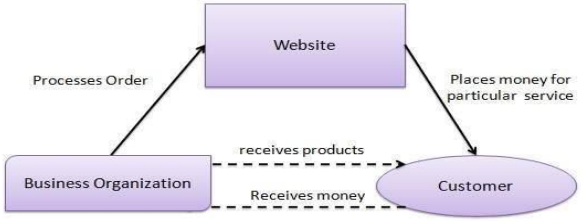
3) Consumer - to - Consumer (C2C)

Website following C2C business model helps consumer 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.



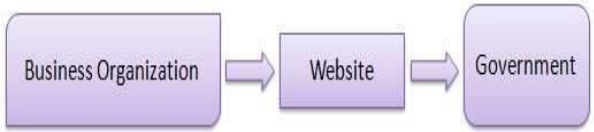
4) Consumer - to - Business (C2B)

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



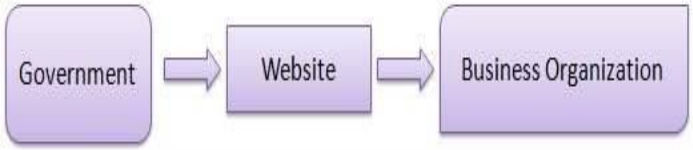
5) Business - to - Government (B2G)

B2G model is a variant of B2B model. Such websites are used by government 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.



6)Government - to - Business (G2B)

Government uses B2G model website to approach business organizations. Such websites support auctions, tenders and application submission functionalities.



7) Government - to - Citizen (G2C)

Government uses G2C model website 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. Main objectives of G2C website are to reduce average time for fulfilling people requests for various government services.

4. BUILDING BLOCKS OF EDI SYSTEMS: LAYERED ARCHITECTURE:

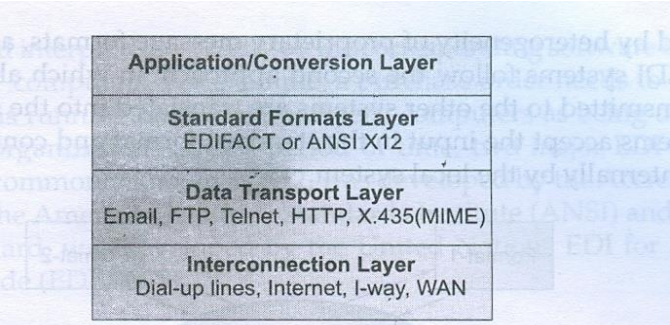


Fig. 3.2 Layered Architecture of EDI Systems

Application / Conversion Layer

The application layer consists of the actual business applications that are going to be connected through the EDI systems for exchange of electronic information. These applications may use their own electronic record formats and document formats for storing, retrieving, and processing the information within each company's systems. Since each company's system may have its own proprietary format, which would be used by their system(s), for EDI to operate, they need to convert the internal company document format to a format that can be understood by the system by the trading partner. When the trading partners are small in number, converters for various partner formats can be built. But, as the number of partners with different internal formats increase, the task of building converters for each proprietary format to other formats becomes overwhelming. The fig. below shows a number of converters for four trading partners with four different proprietary message formats.

The Standard Formats Layer

The application layer of EDI systems rely on common agreed formats for operation. Thus, the second important and critical building block of the EDI system is standards for business documents / forms. Since the sender and receiver in the EDI systems have to exchange business documents that can interpreted by all parties, it has necessitated the development of form standards in EDI. EDI form standards are basically data standards in that they lay down the syntax and semantics of the data being exchanged.

The grocery industry sector created the Uniform Communication Standards (UCS) for addressing the EDI standards requirement for their segment, which were later adopted by several other retail sectors.

. In Europe on the other hand, the industry developed and adopted yet another set of standards.

The shipping industry devised a set of standards called Data Interchange for Shipping (DISH), the automobile sector came up with a standard under the umbrella of Organization for Data Exchange by Tele Transmission in Europe (ODETTE).

The need for an industry-wide EDI standards was widely felt and this lead to the formation of a Standard Committee X12 under the auspices of American National Standards Institute (ANSI)

ANSI X12

The Accredited Standards Committee (ASC) X12 was set up by the American National Standards Institute (ANSI) in 1979 to develop cross-industry standards for exchanging electronic documents for use by all businesses in the United States. The committee developed ANSI ASC X12, commonly referred to as X12 standard. Today, EDI standards are firm but not static, because the development of EDI is a continuing effort. Specific industry groups are continuing to evolve new transaction sets that may be better suited to standardization. The X12 standard sets the framework and rules for electronic data interchange. It describes the format for structuring the data.

EDIFACT – An International Standard

In 1987, the United Nations announced an international standard called EDI for Administration, Commerce, and Transport (EDIFACT). The EDIFACT standard is promoted by the United Nations Economic Commission, which is responsible for the adoption and standardization of messages. The International Standards Organization (ISO) has been entrusted with the responsibility of developing the syntax and data dictionary for EDIFACT. EDIFACT serves the purpose of trans-border standardization of EDI messages. EDIFACT combines the efforts of American National Standards Institute's ASC X12, Trade Data Interchange (TDI) standards developed and deployed by much of Europe and the United Kingdom

The data transport layer consists of services that **automate the task of electronic transfer of messages**.

The Electronic Mail exchanged through the network infrastructure has emerged as the dominant means for transporting the EDI messages.

Data Transport Layer

The data transport layer consists of services that automate the task of electronic transfer of messages. In a typical purchase process, once a purchase order has been prepared and printed in the standard format, it is

placed in an envelope and dispatched through postal or courier services to the supplier

In order to achieve equivalence to the security control offered by the paper-based systems, it has three types of notifications.

- A positive notification – It indicates that the recipient has received the document and accepts the responsibility for it;
- A negative notification- It indicates that the recipient received but refused to accept the document. The reason for refusal is attached with the notification.

A forwarding notification- It indicates that the document was received, but

forwarded to another recipient

Inter Connection Layer

It refers to the network infrastructure that is used for the exchange of information between trading partners. In the simplest and most basic form it may consist of dial-up lines, where trading partners dial-up through modem to each other and connect to exchange the messages as illustrated in the following:

The leased lines and I-way, Internet or any reliable network infrastructure that can provide ability of interconnection can be used. Through the interconnection, the EDI partners are able to achieve document exchanges between themselves

5. Benefits and application of EDI

- **Reduces Lead Time**

In the EDI environment, the exchange of documents among trading partners happens electronically through interconnected computers. The process of transferring the documents is instantaneous, offering weeks of time savings compared to the traditional environment that used postal / courier based exchange of printed documents.

- **Improves Coordination with Supplies**

Traditional trading environments are often burdened with the problem of mismatched invoices, un-matching terms in quotations and purchase-orders, missing invoices even after the bill for payment is received and many similar inter-business problems.

- **Reduces Redundancy**

As all the documents exchanged between trading partners are stores in an electronic mailbox, documents can be accessed, retrieved, and examined at any point of time.

***Expands the Market Reach**

Most large manufacturers like General Motors deal with EDI-enabled suppliers only. In the process of streamlining the purchase process they often institute a value-added network. By being a part of their value-added network, many opportunities open up for supplying the material to some other larger supplies who are also a part of the network

6. Applications of EDI:

The ability to exchange documents electronically has been found to facilitate coordination between the partners, reduce the lead time and thus reduce inventory. Although, large manufacturing and transportation companies were the early birds who recognized the advantages, any of the other industry segments also stand to benefit from electronic document exchange. The health care, and financial sectors and cross-border trade facilitated through electronic document exchanges including customs service – have been some other sectors that adopted and derived the returns from EDI.

7.Architectural framework of Electronic Commerce:

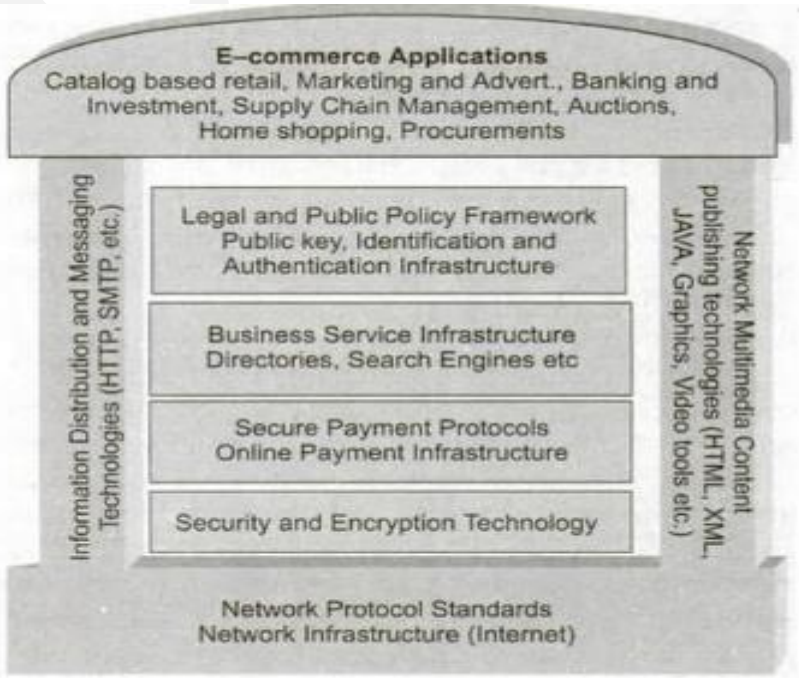


Fig. 4.1 Architectural Framework for Electronic Commerce

Apply computer technology to improve business process and information exchange both within the an organization and across the organization. E-commerce is used to devote proper exchange of business information using EDI,

E-mail, Electronic bulletin boards, EFT(electronic fund transfer) and other similar technologies.

E-Commerce is used to describe a new online approach to perform traditional function such as payment and fund transfer, order entry and processing inventory management involving cargo tracking, electronic catalogue etc. Advertising, marketing and customer support functions are also a part of E-commerce application. No single technology can provide the full potential of E-commerce. Therefore we require an integrated architecture which is revolving in the form of WWW as E-commerce is becoming more matured. Thus we need

To develop sophisticated applications on WWW.

Architectural framework of E-commerce:

A Frame Work is intended to define and create tools that integrate the information found in today's closed system and allows the development of E-commerce applications. Architectural framework should focus on synthesizing the diverse resources already in place incorporation to facilitate the integration of data and software for better use and application.

The E-commerce applications architecture consists of 6 layers of functionality or services. They are

1. Application Services
2. Brokerage Services
3. Interface support layer
4. secure messaging & EDI
5. Middleware, structured document interchange.
6. Network infrastructure and providing communication services.

1. Application services:

It will be composed of existing and future applications based on innate architecture. The three distinct classes of E-commerce applications can be distinguished as

a) Consumer to Business

(b) Business to Business

(c) Intra organization.

(a) Consumer to Business:

We call this enterprise market place transaction. In market place transaction customer learn about product differently through Electronic publishing by them differently using Electronic cash and secure payment and have themdeveloped differently.

(b) Business to Business:

This is called as market link transaction. Here business, govt and other organizations depend on computer to

computer communication as a fast, economical dependable way to conduct business transactions. They include the use of EDI and E-mail for Purchasing goods and services, buying information and consulting services, submitting requests for proposals and receiving proposals.

(c) Intra Organizational transactions:

This is called as market driven transaction. A company becomes market driven by dispersing throughout the firm information about his customers and competitors by spreading strategic and tactical decision making so that all units can participate and by continuously monitoring their customer commitment.

(i) Customer orientation through product and service customization

(ii) Cross functional coordination through enterprise integration, marketing and advertising.

(iii) Customer service.

2. Information Brokerage and management:

This layer provides service integration through the notion of information brokerages. Information brokerage is used to represent an intermediary which provides service integration between customer and information providers, given some constraints such as low price, fast service, profit maximization for a client. Information brokerage addresses the issue of adding value to the information that is retrieved. Brokerage function can support data management and traditional transaction services. Brokerage may provide tools to accomplish more sophisticated tasks such as time delay updates or feature comparative

3. Interface support service:

The third layer interface and support services will provide interface for e commerce applications such as interactive catalogues and will support directory services etc., functions necessary for information search and access. Interactive catalogues are customized interface to consumer applications such as home shopping.

4. Secure messaging and structure document interchange service:

The importance of fourth layer is secured messaging. Messaging is a software that sits between the network infrastructure and the clients or e-commerce applications.

Messaging services offer solutions for communicating non formatted data such as letters, memo, reports etc as well as formatted data such as purchase order, shipping notices and invoice etc. messaging support both for synchronous (immediate) and asynchronous (delay) messaging. When a message is sent work continuous (software does not wait for response).

5. Middleware services:

Middleware is a relatively new concept that emerged only recentlyIt solves all the interface, translation, transformation and interpretation problems that were driving application programmers crazy. To achieve data centric computing middleware services focus on three elements.

(1) Transparency

(2) Translation security management

(3) Distributed object management and services

8.INTERNET INDUSTRY STRUCTURE

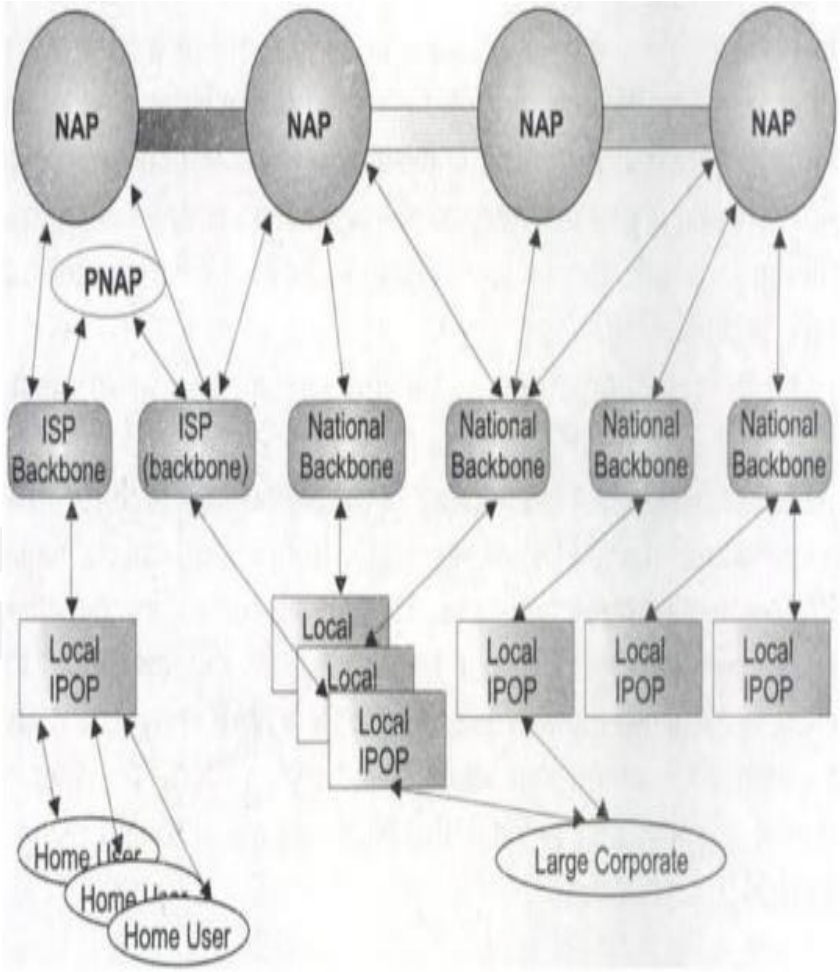


Fig. 5.21 Internet architecture

In 1986,the national science foundation(NSF) of USA created a nationwide backbone interconnecting the six supercomputer centres.the original backbone was handed over for five years to the leading communication company (MCI)for upgrading and operating it. moreover four network access providers(NAP)were created as central points to interconnect commercial backbones. These four NAPs are located in san Francisco,Chicago,Washington DC,and new jersey, operated by pacbell,amertitech,worldcom etc.. network access points(NAP'S) are central points, which interconnect many different national backbones and internet service providers(ISP'S).these ISP's offer connectivity through the local internet point of presence(IPOP)to other internet service providers who operate locally and thus have local IPOP.business organizations and home users connect to the local IPOP provider, which in turn is connected to the backbone and ultimately to NAP. The private network access points(PNAP) are technically identical to a NAP, but interconnect peer backbone ISPs are even peer local ISPs.

9. FIREWALL:

A firewall is a network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic.

A firewall acts as a barrier between a trusted network and and an entrusted network. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied. A Firewall is a controlled access point between domains, usually with different levels of trust. It acts as a gateway through which all traffic to and from the protected network and systems passes. It helps to build a wall between one part of a network and another part. For example placing limitations on the amount and type of communication that takes place can separate a company's internal network and the internet. Firewalls can be a highly effective tool in implementing a network security policy if they are configured and maintained correctly. They provide a certain level of protection and are, in general a way of implementing security policy at the network level.

History and types of firewalls

Computer security borrowed the term firewall from firefighting and fire prevention, where a firewall is a barrier established to prevent the spread of fire.

When organizations began moving from mainframe computers and dumb clients to the client-server model, the ability to control access to the server became a priority. Before firewalls emerged in the late 1980s, the only real form of network security was performed by access control lists (ACLs) residing on routers. ACLs determined which IP addresses were granted or denied access to the network.

The growth of the Internet and the resulting increased

1.Packet firewalls

The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination address, protocol, and destination port number are checked against the firewall's rule set. Any packets that aren't specifically allowed onto the network are dropped (i.e., not forwarded to their destination). For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for TCP port number 23, the port where a Telnet server application would be listening.

Packet-filter firewalls work mainly on the first three layers of the OSI reference model (physical, data-link and network), although the transport layer is used to obtain the source and destination port numbers. While generally fast and efficient, they have no ability to tell whether a packet is part of an existing stream of traffic. Because they treat each packet in isolation, this makes them vulnerable to spoofing attacks and also limits their ability to make more complex decisions based on what stage communications between hosts are at.

2. Stateful firewalls

In order to recognize a packet's connection state, a firewall needs to record all connections passing through it to ensure it has enough information to assess whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. This is what's called "stateful packet inspection." Stateful inspection was first introduced in 1994 by Check Point

Software in its FireWall-1 software firewall, and by the late 1990s, it was a common firewall product feature.

This additional information can be used to grant or reject access based on the packet's history in the state table, and to speed up packet processing; that way, packets that are part of an existing connection based on the firewall's state table can be allowed through without further analysis. If a packet does not match an existing connection, it's evaluated according to the rule set for new connections.

3. Application-layer firewalls

As attacks against Web servers became more common, so too did the need for a firewall that could protect servers and the applications running on them, not merely the network resources behind them. Application-layer firewall technology first emerged in 1999, enabling firewalls to inspect and filter packets on any OSI layer up to the application layer.

The key benefit of application-layer filtering is the ability to block specific content, such as known malware or certain websites, and recognize when certain applications and protocols -- such as HTTP, FTP and DNS -- are being misused.

Firewall technology is now incorporated into a variety of devices; many routers that pass data between networks contain firewall components and most home computer operating systems include software-based firewalls. Many hardware-based firewalls also provide additional functionality like basic routing to the internal network they protect.

4. Proxy firewalls

Firewall proxy servers also operate at the firewall's application layer, acting as an intermediary for requests from one network to another for a specific network application. A proxy firewall prevents direct connections between either sides of the firewall; both sides are forced to conduct the session through the proxy, which can block or allow traffic based on its rule set. A proxy service must be run for each type of Internet application the firewall will support, such as an HTTP proxy for Web services.

10.ELECTRONIC ONLINE PAYMENT SYSTEM ONLINE PAYMENT SYSTEM:

E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost. Being user friendly and less time consuming than manual processing, helps business organization to expand its market reach /expansion. Some of the modes of electronic payments are following.

1) Credit Card
2) Debit Card
3) Smart Card
4) E-Money
5) Electronic Fund Transfer *EFT*

Credit Card

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system. The card holder – Customer The merchant - seller of product who can accept credit card payments. The card issuer bank - card holder's bank The acquirer bank - the merchant's bank The card brand - for example , visa or MasterCard.

Credit card payment process

Step Description

Step 1 Bank issues and activates a credit card to customer on his/her request.

Step 2 Customer presents credit card information to merchant site or to merchant from whom he/she want to purchase a product/service.

Step 3 Merchant validates customer's identity by asking for approval from card Brand Company.

Step 4 Card brand company authenticates the credit card and paid the transaction by credit. Merchant keeps the sales slip.

Step 5 Merchant submits the sales slip to acquirer banks
and gets the service chargers paid to him/her.
Step 6 Acquirer bank requests the card brand company to clear the credit amount and gets the payment.

Step 6 Now card brand company asks to clear amount from the issuer bank and amount gets transferred to card brand company.

Debit Card

Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immediately and there should be sufficient balance in bank account for the transaction to get completed.

Smart Card

Smart card is again similar to credit card and debit card in appearance but it has a small microprocessor chip embedded in it. It has the capacity to store customer work related/personal information. Smart card is also used to store money which is reduced as per usage. Smart card can be accessed only using a PIN of customer. Smart cards are secure as they stores information in encrypted format and are less

expensive/provides faster processing.Mondex and Visa Cash cards are examples of smart cards.

E-Money

E-Money transactions refer to situation where payment is done over the network and amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient and save a lot of time. Online payments done via credit card, debit card or smart card are examples of e-money transactions. Another popular example is e-cash. In case of e-cash, both customer and merchant both have to sign up with the bank or company issuing e-cash.

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 same bank or different bank. Fund transfer can be done using ATM *AutomatedTellerMachine* or using computer.

Now a day, internet based EFT is getting popularity. In this case, customer uses website provided by the bank. Customer logins 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 amount to other account if it is in same bank otherwise transfer request is forwarded to ACH *Automated Clearinghouse* to transfer amount to other account and amount is deducted from customer's account. Once amount is transferred to other account, customer is notified of the fund transfer by the bank.

11.Explain the Internet Marketing in detail: (qp may 2015)

Internet marketing, also referred to as web marketing, online marketing, or e-marketing, is the marketing of products or services over the Internet. The Internet has brought media to global audience. The interactive nature of the Internet marketing in terms of providing instant responses and eliciting responses is the unique quality of the medium.

Internet marketing is sometimes considered to be broad in scope because it not only refers to marketing on the Internet but also includes marketing done via e-mail and wireless media. The management of digital customer data and electronic customer relationship management systems are also often grouped together under the Internet marketing.

Internet marketing ties together creative and technical aspects of the Internet, including design, development, advertising and sales.

Components of Internet Marketing:

Internet marketing evolves in a fast-phase manner. It is dynamic and requires every online business and marketers to keep updated with the changes in the system. There are two components of Internet marketing:

1. B-to-B (B2B):
It refers to business to business e-commerce, where business firms sell their products and services to other business firms using the Internet.

2. B-to-C (B2C): It refers to business to consumers, where business firms sell their products and services to the consumers using the Internet.

Effectiveness of Internet Marketing:

The effectiveness of Internet marketing can be enhanced if the following points are considered:
1. Build trust, because web site serves as the platform for selling/displaying products and services.

2. Web site should be simple, but professional in approach.

3. The content of the web site should be relevant and quantitative.

4. Every possible means should be taken into account to drive Internet traffic towards the web site.

5. Being an Internet marketer, requires discipline and perseverance.

Online Promotion:

It can be done through various means and strategies.

1. Firms can promote the products and services of the company by establishing an online presence. An entrepreneur can introduce the products of the organization by creating an official web site.

A web site gives an overview to the prospective customer about the corporation. This enables the firm to establish a global presence and reach global market.

2. E-mail marketing is another form of online promotion. In this kind of marketing, firms can reach the prospective customers directly through the means of an electronic mail. An advertiser can invite the customer for subscription of newsletters or alerts for special offers by the company. An electronic mail promotion generates sales and often repeats sales. It is an effective way to fetch new and retain present customers.

Advantages of Internet Marketing:

1. Internet marketing is relatively inexpensive when compared with the ratio of cost against the reach of the target audience.

2. Companies can reach a wide audience for a small fraction of traditional advertising budgets.

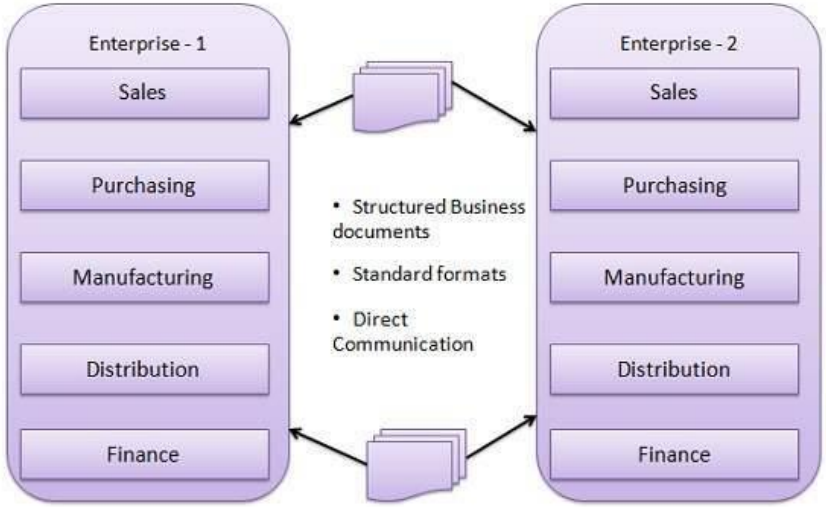
Disadvantages of Internet Marketing:

1. Internet marketing sometimes appear to be confusing and at times considered as a kind of virus.

2. The more you know, the more you realize the need to learn more.

12. Concept of electronic data interchange

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.

13.SECURITY POLICY , PROCEDURES AND PRACTICES:

SECURITY POLICY:

A security policy is a formal statement of the rules by which people with access to an organization's technology and information assets must abide, to ensure the security of these assets. It provides a framework for making specific decision such as which defense mechanisms to use and how to configure services . It is the basis for developing secure programming guidelines and procedures , for users and system administrators to follow .

A security policy generally covers the following aspects:

- High-level description of the technical environment of the site, the legal environment (governing laws),the authority of the policy , and the basic philosophy to be used when interpreting the policy .

- Risk analysis to identity the site's assets , the threats existing against those assets and the costs of assets loss
- Guidelines for system administrators on how to manage the systems
- Definition of acceptable use for users
- Guidelines for reacting to site compromise (e.g whether to trace intruder or shutdown and rebuild the system)

Technological support for the security policy includes options like :

- Challenge/response systems for authentication
- Encryption systems for confidential storage and transmission of data
- Network tools such as firewalls and proxy servers
- Auditing systems for accountability and event reconstruction

SECURITY RELATED PROCEDURES AND PRACTICES:

Procedures are specific steps to be followed, based on the security policy. Procedures address such as connecting to the site's system from home or while travelling, retrieving programs from the network using encryption, authentication for issuing accounts, configuration and monitoring.

SECURITY PRACTICES:

System administration practices play a key role in network security. some commonly recommended practices are:

- Implement a one-time password system,ensure that all accounts have a password and these passwords are difficult to guess.
- Use strong cryptographic techniques to ensure the integrity of system software on a regular basis.
- Use safe programming techniques when writing software.
- Make appropriate changes to the network configuration when vulnerabilities become known.
- Keep the system current with upgrade and patches.

- Check for security alerts and technical advice regularly
- Audit systems and networks,and regularly check logs for detecting an intrusion.

14.The essential requirements for secure safe e-payments/transactions

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.

Security Protocols in Internet

We will discuss here some of the popular protocols used over the internet to ensure secured online transactions.

Secure Socket Layer (SSL)

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements −

- Authentication
- Encryption
- Integrity
- Non-reputability

"https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.

Secure Hypertext Transfer Protocol (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiple security mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

Secure Electronic Transaction

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol. It has the following components −

- **Card Holder's Digital Wallet Software** − Digital Wallet allows the card holder to make secure purchases online via point and click interface.

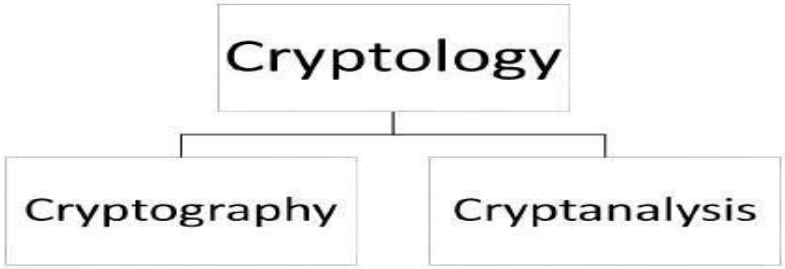
- **Merchant Software** − This software helps merchants to communicate with potential customers and financial institutions in a secure manner.
- **Payment Gateway Server Software** − Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.
- **Certificate Authority Software** − This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.

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.

15. CRYPTOGRAPHY:

Cryptology, the study of cryptosystems, can be subdivided into two branches −

- Cryptography
- Cryptanalysis



What is Cryptography?

Cryptography is the art and science of making a cryptosystem that is capable of providing information security.

Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

What is Cryptanalysis?

The art and science of breaking the cipher text is known as cryptanalysis.

Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Note − Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

Security Services of Cryptography:

The primary objective of using cryptography is to provide the following four fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

Confidentiality

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as **privacy** or **secrecy**.

Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

Data Integrity

It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants −

- **Message authentication** identifies the originator of the message without any regard router or system that has sent the message.
- **Entity authentication** is assurance that data has been received from a specific entity, say a particular website.

In 1976, a concept referred to as public key cryptography was introduced by Whitefield Diffie and martin Hellman, called the **Diffie-hellman** technique. The public-key method allows a sender and a receiver to generate a shared, secret key over an insecure telecommunications line.

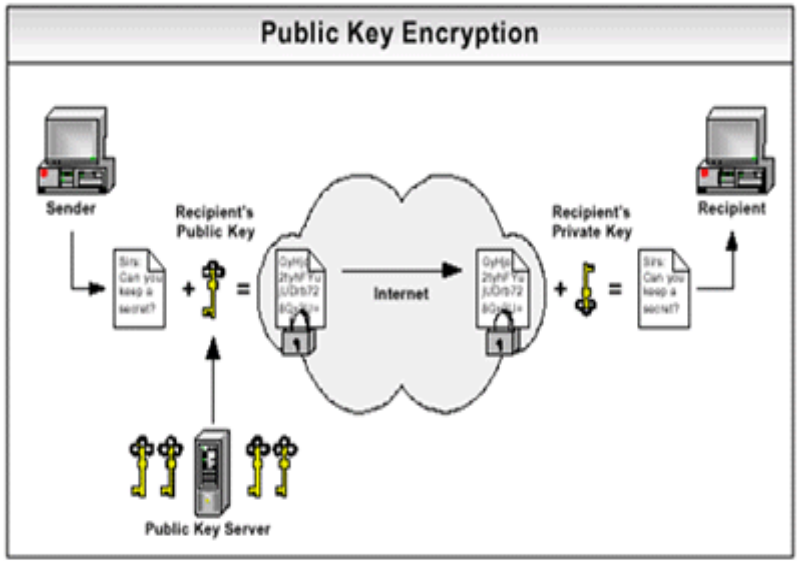


Figure 1

This process uses an algorithm based on the sender's and receiver's public and private information. The following steps are used

1. The sender determines a secret value a.
2. A related value, A, is derived from a. A is made public.
3. The receiver determines a secret value b.
4. A related value, B is derived from b. B is made public.

5. the Diffie-Hellman algorithm is used to calculate a secret key corresponding the

key pairs (a, B) and (b, A). the sender knows his private value, a and the receiver's public value, B. the receiver knows her private value, b , and the sender's public value, A. the secret key is generated from (a, B) and (b, A) by an algorithm that makes it computationally infeasible to calculate the secret key from solely knowing the two public values, A and B. In order to generate the secret key, one of the secret values must be known. The secret key is shared avoiding the problem of transmitting it over a insecure telecommunications line.

Good encryption practices:

The following are the few good encryption practices that foster stronger security.

1. Password maintenance: never share your secret password. A password can be used to protect your private key, and therefore your digital signature.

2. key length: use an appropriate key length whenever possible. The longer the key length, the greater the security. For domestic use a key length of at least 64-bits should be used .

3. compressed files: in order to reduce transmission time, data compression is frequently used to reduce the size of a file. Most loss less data compression techniques are based on removing redundancy from the file.