CS E63 E - BUSINESS

UNIT I

Electronic Commerce Environment and Opportunities: Background – The Electronic Commerce Environment – Electronic Marketplace Technologies – Modes of Electronic Commerce: Overview – Electronic Data Interchange – Migration to Open EDI – Electronic Commerce with WWW/Internet – Commerce Net Advocacy – Web Commerce going forward.

UNIT II

Approaches to Safe Electronic Commerce: Overview – Secure Transport Protocols – Secure Transactions – Secure Electronic Payment Protocol(SEPP) – Secure Electronic Transaction (SET)- Certificates for Authentication – Security on Web Servers and Enterprise Networks – Electronic cash and Electronic payment schemes: Internet Monetary payment and security requirements – payment and purchase order process - Online Electronic cash.

UNIT III

Internet/Intranet Security Issues and Solutions: The need for Computer Security – Specific Intruder Approaches – Security strategies – Security tools – Encryption – Enterprise Networking and Access to the Internet – Antivirus programs – Security Teams.

UNIT IV

MasterCard/Visa Secure Electronic Transaction: Introduction – Business Requirements – Concepts – Payment processing – E-mail and secure e-mail technologies for electronic commerce. Introduction – The Mean of Distribution – A model for message handling – Working of Email - MIME: Multipurpose Internet Mail Extensions – S/MIME: Secure Multipurpose Internet Mail Extensions – MOSS: Message Object Security Services.

UNIT V

Internet and Website Establishment: Introduction – Technologies for web servers – Internet tools relevant to Commerce – Internet Applications for Commerce – Internet charges – Internet Access and Architecture – Searching the Internet- Case study.

TEXT BOOK

1. Daniel Minoli and Emma Minoli, ―Web Commerce Technology Handbook‖, Tata McGraw-Hill, 2005.

REFERENCES

1. Andrew B. Whinston, Ravi Kalakota, K. Bajaj and D. Nag, ―Frontiers of Electronic Commerce‖, Tata McGraw-Hill, 2004.
2. Bruce C. Brown, ―How to Use the Internet to Advertise, Promote and Market Your Business or Website with Little or No Money‖, Atlantic Publishing Company, 2006.

UNIT I

Electronic Commerce Environment and Opportunities: Background – The Electronic Commerce Environment – Electronic Marketplace Technologies – Modes of Electronic Commerce: Overview – Electronic Data Interchange – Migration to Open EDI – Electronic Commerce with WWW/Internet – Commerce Net Advocacy – Web Commerce going forward.

UNIT-I

2 MARKS

1. What is E-Commerce? (Apr 2012)(Apr 2014)

Electronic commerce is the application of communication and information sharing technologies among trading partners to the pursuit of business objectives.

E-Commerce can be defined as a modern business methodology that addresses the needs of organizations, merchants, and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery.

2. What is meant by Information superhighway (I-Way)?

Any successful E-commerce application will require the I-Way infrastructure in the same way that regular commerce needs the interstate highway network to carry goods from point to point.

The I-Way is not a U.S phenomenon but a global one, as reflected by its various labels worldwide. The I-Way is quickly acquiring new on-ramps and even small highway systems.

3. Define Electronic Marketers? (Nov 2012)

Electronic marketers are defined as computers that market their products and services to other businesses or consumers through private online networks, commercial on-line services such as Prodigy and America Online (AOL); the internet, CD-ROMs, telecommunications-enhanced CD-ROMs, interactive television and web TV, and floppy disk media.

4. What are the Consumer oriented e-commerce applications?

The wide range of applications for the consumer marketplace can be broadly classified into

- **Entertainment**: Movies on demand, Video cataloging, interactive ads, multi-user games, on-line discussions.
- **Financial services and information**: Home banking, financial services, financial news.
- **Essential services**: Home shopping, electronic catalogs, telemedicine, remote diagnostics.
- **Educational and training**: Interactive education, video conferencing, on-line databases.

5. What are the building blocks in the infrastructure of e-commerce applications?

None of the applications would be possible without each of the building blocks in the infrastructure which are given as follows:

- Common business services, for facilitating the buying and selling process
- Messaging and information distribution, as a means of sending and retrieving information

- Multimedia content and network publishing, for creating a product and a means to communicate about it.
- The I-Way is the very foundation for providing the highway system along which all E-commerce must travel.

6. Some of the pillars supporting the e-commerce applications?

There are two pillars supporting all E-commerce applications and infrastructure. They are:

Public policy – To govern such issues as Universal access, privacy and information pricing.

Technical standards – To dictate the nature of information publishing, user interfaces, and transport in the interest of compatibility across the entire network.

7.What are the benefits of e-commerce? (Apr 2013)

Electronic Commerce can offer both short term and long-term benefits to the companies.

Not only can it open new markets, enabling you to reach new customers, but it can also make it easier and faster for you to do business with your existing customer base.

It can also reduce the paperwork involved in business-to-business transactions.

8. Explain about multimedia content for e-commerce applications.

Multimedia content can be considered both fuel and traffic for E-commerce applications. The technical definition of Multimedia is the use of digital data in more than one format, such as the combination of text, audio, video and graphics in a computer file/document.

Its purpose is to combine the interactivity of a user-friendly interface with multiple forms of content. The success of E-commerce applications also depends on the variety and innovativeness of multimedia content and packaging.

9. Explain the client-server architecture in e-commerce.

All E-commerce applications follow the client-server model. Clients are the devices plus software that request information from servers. Servers are the computers which server information upon the request by the clients.

Client devices handle the user interface. The server manages application tasks, handles storage and security and provides scalability (ability to add more clients as needed for serving more customers). The client-server architecture links PC's to a storage (or database) server, where most of the computing is done on the client.

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. Commercial users have only recently begun downsizing their applications to run on client-server networks, a trend that E-commerce is expected to accelerate.

10. What are the types of e-commerce?

The following three strategies are the focal points for E-Commerce

- Business-to-business E-commerce
- Business-to-consumer E-commerce
- Intra-company E-commerce

11. Explain about Business-to-business E-commerce.

The Internet can connect all businesses to each other, regardless of their location or position in the supply chain. This ability presents a huge threat to traditional intermediaries like wholesalers and brokers. Internet connections facilitate businesses' ability to bargain directly with a range of suppliers thereby eliminating the need for such intermediaries.

12. Explain about Business-to-consumer E-commerce.

One-way marketing. Corporate web sites are still prominent distribution mechanisms for corporate brochures, the push, and one-way marketing strategy.

Purchasing over the Web: Availability of secure web transactions is enabling companies to allow consumers to purchase products directly over the web. Electronic catalogs and virtual malls are becoming commonplace.

13. Explain about Intra-company E-commerce.

Companies are embracing intranets at a phenomenal growth rate because they achieve the following benefits:

Reducing cost - lowers print-intensive production processes, such as employee handbooks, phone books, and policies and procedures

Enhancing communications - effective communication and training of employees using web browsers builds a sense of belonging and community.

Distributing software - upgrades and new software can be directly distributed over the web to employees.

Sharing intellectual property - provides a platform for sharing expertise and ideas as well as creating and updating content - "Knowledge webs". This is common in organizations that value their intellectual capital as their competitive advantage.

Testing products - allows experimentation for applications that will be provided to customers on the external web.

14. What are the technologies of e-commerce? (Nov 2012)

While many technologies can fit within the definition of "Electronic commerce," the most important are:

- Electronic data interchange (EDI)
- Bar codes
- Electronic mail
- Internet
- World Wide Web
- Product data exchange
- Electronic forms

15. What is meant by Electronic Data Interchange (EDI)? (Apr 2012)(Apr 2014)

EDI is the computer-to-computer exchange of structured business information in a standard electronic format. Information stored on one computer is translated by software programs into standard EDI format for transmission to one or more trading partners. The trading partners' computers, in turn, translate the information using software programs into a form they can understand.

16. Explain Bar Codes.

Bar codes are used for automatic product identification by a computer. They are a rectangular pattern of lines of varying widths and spaces. Specific characters (e.g. numbers 0-9) are assigned unique patterns, thus creating a "font" which computers can recognize based on light reflected from a laser.

17. What is meant by Electronic Mail?

Messages composed by an individual and sent in digital form to other recipients via the Internet.

18. Explain Internet.

The Internet is a decentralized global network of millions of diverse computers and computer networks. These networks can all "talk" to each other because they have agreed to use a common communications protocol called TCP/IP. The Internet is a tool for communications between people and businesses. The network is growing very, very fast and as more and more people are gaining access to the Internet, it is becoming more and more useful.

19. Explain World Wide Web.

The World Wide Web is a collection of documents written and encoded with the Hypertext Markup Language (HTML).

With the aid of a relatively small piece of software (called a "browser"), a user can ask for these documents and display them on the user's local computer, although the document can be on a computer on a totally different network elsewhere in the world.

The World Wide Web is by far the most heavily used application on the Internet.

20. What is Product Data Exchange?

Product data refers to any data that is needed to describe a product. Sometimes that data is in graphical form, as in the case of pictures, drawings and CAD files. In other cases the data may be character based (numbers and letters), as in the case of specifications, bills of material, manufacturing instructions, engineering change notices and test results.

Product data exchange differs from other types of business communications.

21. What is Electronic Forms?

An electronic form is a technology that combines the familiarity of paper forms with the power of storing information in digital form.

To the user an electronic form is simply a digital analogue of such a paper form, an image, which looks like a form but which appears on a computer screen and is filled out via mouse, and keyboard.

22. What are the functions of EDI?

Some of the functions of EDI are,

- Integration of incoming and outgoing structured data into other applications (e.g., use of customer orders to schedule production)
- Lowers cost when transaction volume is high
- Eases communication with many different trading partners (customers, suppliers, vendors)

23. What are the functions of Bar Code?

Some of the functions of Bar Code are,

- Locate and identify material
- Integrate location and identification information with other applications and data bases (e.g., bar codes inserted at loading dock can be integrated into an advance ship notice EDI transaction).

24. What are the functions of Electronic Mail?

Some of the functions of Electronic Mail are,

- Free-text queries to individuals or groups
- Share information via simple messages
- Share complex information (via attachments)
- Collaboration across distance (by making it easier to communicate and share information)

25. What are the functions of World Wide Web?

Some of the functions of World Wide Web are,

- Present information about company
- Search for information from a large number of sources
- Electronic commerce -- buy/sell products and services
- Collaboration, information sharing among selected users within or without a company

26. What are the functions of Product Data Exchange?

Some of the functions of Product Data Exchange,

- Accurate product details transmitted to trading partners
- Oversight of trading partners design work
- Collaborative engineering across distance

27. What are the functions of Electronic Forms?

Some of the functions of Electronic Forms are,

- Managing processes when human oversight, approvals, or information input needs to be combined with standard elements of information (e.g., catalogue data)
- Tracking progress in a process where many people are involved doing different activities
- Integrating human input data with automated data bases or applications
- Electronic commerce (through integration with the WWW and internal systems)

28. Explain about implementation of e-commerce: a life cycle approach?

Proper implementation requires deliberate attention to seven stages of technology life cycle:

- Awareness Training
- Business Analysis
- Requirements Analysis
- Design
- Implementation
- Integration and Validation
- Maintenance

29. Explain about electronic shopping cart?

An electronic shopping cart works the same way a shopping cart does in the physical world. As you browse through an online store, you can place products in your virtual shopping cart, which keeps track of the products you have placed in it.

When you're ready to leave the store, you click a "check out" link that shows you what you've placed in your virtual shopping cart. You can usually remove items that you're no longer interested in purchasing and then enter your shipping and payment information to process your order.

30. What are the systems of payments in e-commerce? (Apr 2013)

E-commerce is rife with buzzwords and catchphrases. Here are some of the current terms people like to throw around:

- Credit card-based
- Smart cards
- Digital or electronic cash
- Electronic checks
- Electronic wallet

31. Explain CGI script.

Common gateway Interface is a scripting system designed to work with HTTP Web Servers. The scripts, usually written in the Perl coding language, are offer used to exchange data between a Web server and databases.

32. What is Joint Electronic Payments Initiative (JEPI)?

This initiative, led by the World Wide Web Consortium and Commerce Net, is an attempt to standardize payment negotiations. On the buyer's side (the client side), JEPI serves as an interface that enables a Web browser, and wallets, to use a variety of payment protocols.

On the merchant's side(the server side), JEPI acts between the network and transport layers to pass off the incoming transactions to the proper transport and payment protocols.

33. What is Microcash?

Small denomination digital tokens.

34. Explain about Smart cards.

A credit card-sized plastic card with a special type of integrated circuit embedded in it. The integrated circuit holds information in electronic form and controls who uses this information and how.

35. Explain Tokens.

Strings of digits representing a certain amount of currency. The issuing bank validates each token with a digital stamp.

36. What is Value added networks?

Networks that are maintained privately and dedicated to EDI between business partners.

37. What are the environments of e-commerce? (Apr 2015)

- The virtual corporation
- The Electronic Marketers
- The catalyst of electronic and web commerce
- Available communication apparatus

11 MARKS

1. Explain in detail about The Electronic Commerce Environment (Apr 2013) (Nov 2014)(Apr 2015)

1. The Virtual Corporation
2. The Electronic Marketers
3. The catalyst of Electronic and web commerce
4. Available communication apparatus
5. Application of Electronic / Web commerce
6. Benefits of Electronic/ Web commerce
7. Elements of a successful electronic marketplace
8. Security Issues and approaches related to web commerce
9. Size of Electronic Marketplace

- **The virtual corporation:**

  Electronic commerce goes hand in hand with changes that are occurring in corporations. The 1990s have

seen the rise of a new form of industrial organization-the networked firm, sometimes known as the Virtual Organization.

Information Technology (IT) has also undergone a significant change in the past quarter of a century. Electronic Commerce is the essence of the virtual corporation; it allows the organization to leverage information and communication resources with all its constituencies, including employees, customers, hankers, government agencies, suppliers, advertisement agencies, and the public.

Successful companies for turn-of –the-century environments

- Organizational structures of the past: Vertical corporations where every function was performed in-house.

- Organizational structures of late 1080s: horizontally integrated enterprises where core competencies were performed in-house and the rest were outsourced.
- Organizational structures of late 1990s: Corporations are moving toward being fully integrated and virtual.
- Aim at making all business functions world-class in order to enhance value (includes leveraging the world-class capabilities of strategic partners).
- Access to all the world's best of breeds, skills, knowledge, and resources.
- Use combination of in sourcing and outsourcing to create best-of-breed, end-to-end solutions.
- Overcome distance and time barriers.
- The future is a network-centric model, where the corporation is the network paradigm is supreme: as more intelligent functions are embedded in the network, the network is becoming the computer, and the corporation is becoming the network.
- Connectivity and bandwidth are becoming cheaper and easy to secure.

Network may be comprised of:

1. A traditional enterprise network(the physical foundation of the corporation's intra company communication facilities);
2. An intranet(an overlay on the enterprise network which is a way to build uniform application, clients, and servers having the look and feel of internet applications);
3. The internet, the inter enterprise network par excellence.
4. Other intercompany specialized networks(e.g., the NYCL banking network)- these are sometimes called as Extranets; and
5. International extensions.

It would be desirable if this fundamental, company-distinguishing synthesis of communication facilities-what can be called an Omninet- would also carry voice, video, image, and other media in addition to the traditional data objects.

What makes a virtual corporation successful is the scope, reach, compatibility, and transparency of the corporation's networking infrastructure. Networking and networking management are the critical enablers of e-commerce.

- **The electronic marketers:**

Electronic marketers are defined as computers that market their products and services to other businesses or consumers through private online networks, commercial on-line services such as Prodigy and America Online (AOL); the internet, CD-ROMs, telecommunications-enhanced CD-ROMs, interactive television and web TV, and floppy disk media.

Electronic commerce frees retailers and consumers from many store constraints. It changes the dynamic in terms of cost, reach, options, or speed. The cost of establishing, a transactional web site ranges from $3 to $25 million. The reach of the former is global, while the latter is local.

A web site can deliver products quickly (e.g., a software release) or in a few days (e.g., overnight mail); a retail store can supply products within a few hours (including the time to travel to the store and back) or within a few days (if the item has to be ordered).

- **The catalyst of electronic and Web commerce:**

The internet is an aggregation of networks connecting computer which is seen as one network by the user. It is the case where the whole is greater than the sum of the parts. There has really been no break-throughs in the internet of late. It relies on many protocols that are more than a decade old (some of the protocols are five years old).

What is new is the ability for the ensemble of the customer's browsers, local networks, backbone networks, and Web servers to internetwork harmoniously. This enables information (data, graphics, and video)
to flow freely and easily, at the click of a mouse. The WWW is one of the more well known applications of the internet to appear of late. Some of the key findings of recent surveys are as follows:

- 17 percent (37 million) of total persons aged 16 and above in the United States and Canada have access to the internet.
- 11 percent (24 million) of total persons aged 16 and above in the United States and Canada have used the internet in the past three months.
- Approximately 8 percent (18 million) of total persons aged 16 and above in the United States and Canada have used the WWW in the past three months.
- Internet users average 5 hours and 28 minutes per week on the Internet.
- Males represent 66 percent of Internet users and account for 77 percent of Internet usage.
- On average, WWW user are upscale (25 percent have income over $80,000/year), professional (%0 percent are professional or managerial), and educated (64 percent have at least college degrees).
- Approximately 14 percent(2.5 million)of WWW users have purchased products or services over the Internet
- More than 80,000 companies were using the Internet for distribution of critical company information, such as press releases.

- **Available communication apparatus**

Electronic commerce clearly depends on the availability of reliable, inexpensive, and ubiquitous connectivity. There are five relevant elements:

1. Organizations own enterprise networks which house appropriate information, usually beyond the organization's firewall apparatuses.
2. The public-switched telephone network. This is generally constituted of Local Exchange Carriers (LECs) and Competitive LEC (CLECs) at the local level and a multitude of Interexchange Carriers (IXCs) at the national backbone level.
3. The internet. As describes, this consists of ISPs and NSPs and provides a large enterprise infrastructure.
4. On-line networks such as America Online, which utilize their own communication and information (storage) facilities. They can be accessed by dial-up or private lines and now have access to the Internet.
5. Specializes industry networks, such as those to support EDI. Internet traffic routing rules are, generally, as follows:

   - If a user tries to reach a resource located on the same ISP's network to which the user is connected, the traffic is examined by the ISP router which in turn forwards it to the destination (this applies to both backbone providers and regional's).
   - If a user tries to reach a resource not located on the same ISP's network to which the user is connected, the traffic is examined by the ISP/NSP router, which in turn finds the nearest point at which it can hand off data to an exchange point (e.g., MAE-East). The traffic is then transferred to the appropriated target network.
   - Backbone ISPs, that is, NSPs, do not want to incur the cost of carrying traffic destined for another provider's network. So, they hand off the traffic to the nearest exchange point, destination network, or intermediate transit provider.

- **Application of electronic/Web commerce**

Electronic commerce combines the advantages of computer-based processing (speed, reliability, and relatively high volumes of data) with the advantages of people based insight.

Currently, there are three tires in the electronic market-place, offering opportunities for companies of all sizes:

- Tier 1. Electronic classified advertisements, which identify the item (or service) for sale, the price, and information necessary for contacting the seller. Electronic classifieds are analogous to print classifieds and are retrieved by the potential buyer.
- Tier 2. Includes the characteristics of the first tier, but adds decision-support materials to the information available which help the user reach a purchase decision. Such marketplaces may include such information as product reviews from an industry magazine.
- Tier 3. Includes the features of the first two tiers, but adds the ability to electronically match appropriate buyers and sellers. These electronic marketplaces may provide confirmation of a completed transaction through, such as that used to trade foreign exchange or software-based intelligent agents, are examples of technologies that can automatically match buyers and sellers.

❖ **Electronic funds transfer**:

Extending and completing the procurement process by providing buyers with the ability to rapidly and cost-

effectively make payments to sellers and shippers with less financial risk and fewer errors, while reducing paper-handling and storage requirements and banking networks.

❖ **Enterprise Integration**:

Extending integration throughout a company, including other trading partners. Business process reengineering can be employed to improve communication within a company or by outsourcing to other companies and using electronic commerce like tools to manage the relationship. The result is the virtual corporation.

❖ **Computer-supported collaborative work**:

Expanding collaborative activities, such as supporting joint development of requirements, maintenance documents, and so forth, within or across companies. The intent is to remove the barriers that inhibit creative interactions among people. Teaming may take place at either the company or individual level, creating a just-in-time virtual resource for delivery of the right human and business resources for a job.

This gives corporations the opportunity to increase changes of success, to share economic successes

More broadly, and to give the customers a mix of capabilities more exactly meeting their requirements.

❖ **Government regulatory data interchanges:**

Collecting data from various communities to enable the government to carry out its mandated responsibilities.

BENEFITS OF ELECTRONIC / WEB COMMERCE (2. Explain in detail about Benefits of electronic/web commerce. (Apr 2013))

❖ Reduced costs to buyers from increased competition in procurement, as more suppliers are able to complete in an electronically open marketplace.

❖ Reduced costs to suppliers by electronically accessing on-line databases of bid opportunities, by one-line abilities to submit bids, and by one-line review of awards.

❖ Reduced errors, time, and overhead costs in information processing by elimination requirements for reentering data.

❖ Reduced inventories, as the demand for goods and services are electronically linked through just-in-time-inventory and integrated manufacturing techniques.

❖ Increased access to real-time inventory information, faster fulfillment of orders, and lower costs due to the elimination of paperwork.

- Reduced time to complete business transaction, specifically reduced time from delivery to payment.
- Reduced overhead costs through uniformity, automation, and integration of management processes while enable flatter, wider, and more efficient processes.
- Better quality of goods as specifications are standardized and competition increases; also, better variety through expanded markets and the ability to produced customized goods.
- Creation of new markets, especially geographically remote markets, as the playing field becomes more even between companies of different sizes and locations.
- Faster time to market as business processes are linked, elimination time delays between steps and the engineering of each sub process within the whole process.
- New business opportunities, Businesses and entrepreneurs are continuously on the look-out for new and innovative ideas as viable commercial ventures; electronic commerce provides such opportunities.
- Optimization of resource selection as businesses build cooperative teams to better tailor capabilities, to work opportunities to increase chances of success more broadly, and to give the customer a mix of capabilities more precisely meeting the customer's requirements.
- Increased access to a client base, Identifying and location new clients and new markets is not a trivial task since it involves analysis, product marketing, and consumer-based testing.
- Improved product analysis as businesses are able to perform product analyses and comparisons and report their findings on the Internet and on-line.
- Improved market analysis. The large and increasing base of Internet users can be targeted for the distribution of surveys for an analysis of the marketability of a new product or service idea. Surveys can reach many people with minimal effort on the part of the surveyors. Once a product is already marketed, businesses can examine the level of customer's satisfaction.
- Wider access to assistance and to advice from experts and peers. Users can utilize the Internet to obtain expert adv ice and get help.
- Rapid information access. Accessing information on-line and over the Internet is faster (on most occasions) than transmissions via fax or transfers via courier services. Businesses can access information from countries around the world and make interactive connections to remote computer systems.
- Rapid interpersonal communications. Contacting other individuals through e-mail provides a new method of business communication. E-mail has both the speed of telephone conversations and the semi=permanence of regular mail. E-mail can be sent form nearly anywhere there is an Internet service or (dial-up) access. Businesspersons or travelers on the go can keep in touch with the office or site.
- Wide-scale information dissemination. One can place documents on servers on the Internet and make them accessible to millions of users. Creating Web documents and Web sites improves the availability of the documents to a client base larger than the circulation of many major newspapers.
- Cost-effective document transfer, transferring on-line documents over the Internet takes a short period of time, particularly if they are text-based (rather than multimedia-based); this can save money on regular

mail or courier services. Most, if not all, Internet access providers do not charge by the raw number of bytes transferred across their links, unlike other commercial information services.

ELEMENTS OF SUCCESSFUL ELECTRONIC MARKETPLACE (3.Explain in detail about Element of a successful electronic marketplace (Nov 2012))

The capabilities required for Internet/Web commerce are as follows:

- Enable buyers to inquire about products, review product and service information, place orders, authorize payment, and receive both goods and services on-line.
- Enable sellers to advertise products, receive orders, collect payments, deliver goods electronically, and provide ongoing customer support.
- Enable financial organizations to serve as intermediaries that accept payment authorization, make payment to sellers, and notify buyers that transactions are complete.
- Enable sellers to notify logistics organization electronically as to where and when to deliver physical goods/merchandise.

The following qualities characterize, in the view of industry experts, successful marketplaces.

- Utilizes an existing customer base. Magazine and newspaper publishers are example of electronic marketers that have capitalized on the relationships that exist with their customer bases (readers and print advertisers) to build loyalty and add value to their traditional products through electronic products.
- Makes an existing marketplace more effective. Consumers tend to be time deprived, the electronic marketplaces must be convenient, ordering must be fast, and delivery of the purchase must take place within 24 to 48 hours. Budget cuts and emphasis on the bottom line mean that business-to-business electronic marketplace must offer streamlined processes that eliminate paperwork and time-consuming telephone calls and voice messages.
- Brings together communities. The service must bring together buyers and sellers that are physically separated or scattered.
- Is easily accessible, has wide distribution. The electronic marketplace should encompass a number of formats to maximize effectiveness- Internet, interactive TV, online PC service, CD-ROMs, screen phones and kiosks.
- Offers decision-support information. Customers are comfortable with the manual way they currently shop. Electronic marketplaces must supply customers with reasons to use them, including cost-effectiveness, time savings, and faster delivery. Extensive information about products should be available on-line.
- Ability to close the sale. Customers need to be able to buy the advertised product through the electronic medium. In the view of some, if they have to walk to the telephone of fax an order form, the chance to create a successful transactional marketplace could be diminished.
- **Size of the electronic marketplace:** Market groups have estimated that the actual revenue generated from electronic transactions of tangible goods was $360 million in 1994 and $540 million in 1996.

Revenue was generated from several potential media-business on-line, consumer on-line, internet, CD-ROM, kiosks, screen phone, and interactive television.

- Business on-line, which includes such services as Data Transmission Network(DTN) services and

Auto info, represented the largest percentage of electronic transactions at press time.

SECURITY ISSUES & APPROACHES RETALED TO WEB COMMERCE(4.Explain in detail about Security issues and approaches related to web commerce (Nov 2012))

Many of the concerns about electronic commerce developments, particularly over open networks (e.g., the Internet), deal with the risks of possible fraud, security infractions, counterfeiting, and with consumer privacy issues.

Issues relate to:

(1) Secure payments via electronic cash (e-cash);

(2) Confidentiality (encryption) and authentication of financial transactions; and

(3) General confidentiality in the transfer of any document.

- The good news is that the technology to solve these problems is well developed and well understood. Many financial and technology companies are working to develop encryption software for the Internet.

- Encryption refers to the encoding of data so that it can only be decoded by the intended recipient who knows the key (code). Much of the software is based on RSA Data Security's public-key encryption, which uses a matched pair of encryption keys.

- Each key performs a one-way transformation of data—what on encrypts, only the other can decrypt. Encryption frustrates disclosure of information while in transfer. Strong host security for resident files is most critical when one understands how breaches usually occur.

- **Secure payments.** E-cash can be thought of as the minting of electronic money or tokens. In electronic cash schemes, buyers and sellers trade electronic value tokens which are issued or backed by some third party, be it an establishes bank or a new (Internet-based) institution.

- The effects of a system failure in an electronic cash scheme are much harder to anticipate; system failure could also occur through many means, not the least of which is insufficient funds (or paper money) to back up the new electronic money.

- **Secure transactions**. Agreements on standard Internet payment systems were getting closer at press time. During 1996, IBM/MasterCard and Microsoft/Visa respectively, agreed on a single industry standard for conducting credit card transactions over the Internet. The agreement was aimed at removing what had been the major obstacle in the emergence of large-scale electronic commerce applications for the Web.

- Such agreement resolves a long-standing struggle on standardized security technology. The issue has been which technology to use Microsoft's Secure Transaction Technology (STT) or IBM's SEPP; the breakthrough came when the four companies agreed to use SET (Secure Electronic Transfer); based on earlier SEPP work.

- SEPP is a protocol originally developed by MasterCard; IBM, Netscape, GTE and Cyber Cash have also signed on to further develop the protocol specification.
  - The development of electronic commerce is at a critical juncture at this time for the following reasons:
  - Consumer demand for secure access to electronic shopping and other service is high.
  - Merchants seek simple, cost-effective methods for conducting electronic transactions.
  - Financial institutions look for a level playing field for software suppliers to ensure quality products at competitive prices.
  - Payment card brands must be able to differentiate electronic commerce transactions without significant

    impact to the existing infrastructure.

  The solutions for achieving secure, cost-effective on-line transactions that will satisfy market demand is the development of a single, open industry specification.

- **Message transfer confidentiality and authentication**. Two different protocols have been developed for enhanced Web security: Secure Hyper Text Transfer Protocol (S-HTTP) and the Secure Sockets Layer (SSL).

- Besides confidentiality there are also issues of authentication: not only could a buyer masquerade for another buyer (in order to steal the payment instrument), but a fake Web-site merchant could put up a fraudulent storefront to steal payments (but never skip any goods).
- Companies such as VeriSign provide an authentication function by acting as a certificate authority. They provide two types of certificates: ID Class 1 and ID Class 2.
- S-HTTP is an extension of HTTP that provides a variety of security enhancements for the Web. Message protection is provided three ways: signature, authentication and encryption.
- S-HTTP is flexible in that it allows each application to configure the level of security required. A transmission from client-to-server or server-to-client can be signed, encrypted, both or neither.
- A secure HTTP message consists of a request or status line followed by a series of headers followed by an encapsulated content. Once the content has been decoded. it should either be another S-HTTP message, and HTTP message ,or simple data.
- Secure sockets layer(SSL) is a transport layer security technique that can be applied to HTTP as well as to other TCP/IP-based protocols. The SSL protocol is designed to provided privacy between two communicating applications, for example, a client and a server.SSL provides authentication, encryption, and data verification.
- The SSL protocol is actually composed of two protocols. Layered on top of some reliable transport protocol, is the SSL record protocol. the SSL record protocol is used for encapsulation of all transmitted and received data, including the SSL handshake protocol, which is used to establish security parameters.

The advantage of the SSL protocol is that it is application-protocol-independent. A higher-level application protocol (for example HTTP, FTP, and Telnet) can run transparently on top of the SSL protocol.

The SSL protocol can negotiate an encryption algorithm and session key, as well as authenticate a server before the application protocol transmits or receives its first byte of data. all of the application protocol data is transmitted encrypted, ensuring Privacy.

S-HTTP is an more flexible than SSL in that an application can configure the level of security it needs.

SIZE OF ELECTRONIC MARKETPLACE

Business online which includes such services as Data transmission Network (DTN) services and Auto Info, represented the largest percentage of electronic transactions at press time. Business on line services are proprietary or closed networks that connect manufacturers, suppliers, wholesalers and retailers.

Consumer online, which includes CompuServe's Electronic mall and other services delivered through proprietary (non Internet)networks.

Internet is just beginning to generate transactional revenue as of press time.

5.Explain in detail about Electronic Marketplace Technologies (Nov 2012)

1. Electronic Data Interchange
2. On-line Networks and services
3. The Internet: Web commerce
4. CD-ROM and Hybrids
5. Screen Phones
6. Kiosks
7. Interactive Television and Video Dial tone
8. Web TV
9. Interactive Banking

- **Electronic Data Interchange**
  - ❖ EDI is the exchange of well-defined business transactions in a computer-process able format.EDI provides a collection of standard message formats to exchange data between organizations computers via any electronic service.
  - ❖ In 1979, the American National standard Institute (ANSI) chartered the aggregated standards committee X12, electronic data interchange to develop uniform national standards for electronic interchange of business transactions.
- **On-line Networks and services**
  - ❖ On-line services provide access to information, entertainment, communications and transaction services. In general, this term refers to networks by companies such as America Online, Compu Serve and Prodigy.
  - ❖ The Public switched telephone network (PSTN) is the typical distribution system, cable networks, satellite, wireless networks and the unused, portion of FM Radio and broadcast TV signals may also be used. It also includes other specialized (Commercial) Networks.

- **CD-ROM and Hybrids**

  - The Multimedia and storage capabilities of CD-ROMs and the growth in the penetration of CD-ROM drives in both business and home PCs are the reasons why business-to-business and consumer marketers sought to use the CD-ROM as a marketing vehicle in the recent past.

  - CD-ROMs can store large amounts (650 MB or More) of data, in text and/or graphical form. In addition, the CD-ROM provides the ability to add sound, photos and full-motion video to a marketing interaction beyond what is offered by the On-line medium over the telecommunication links.

  - Because of their Cost-effectiveness, CD-ROM catalogue, with the products of either one or more multiple marketers, have become popular.

- **The INTERNET: Web Commerce**

  - The Internet is quickly becoming a popular commercial domain for business marketers, driven by the advent of low-cost commercial point – and- click internet software and WWW browsers.

  - The Fastest growing part of the internet at this time is the WWW. The web's ease of access, as well as its multimedia capabilities and downloadable applications (e.g. with Java), enable marketers to create compiling and enticing advertising and marketing environments.

  - The Internet offers an extensive and demographically attractive potential audience, especially for business-to-business marketers.

- **Screen phones**

Screen phones are similar to regular phones but have advanced features, such as credit card readers, small screens and keypads that can be used for variety of interactive, transactional and informative services.

Typical services include home banking, home shopping and electronic white Pages.

This technology is used more commonly in Europe, where consumers can get up-to-date information on many things from a list of specialty restaurants to train information.

The screen-phone's primary advantage for electronic commerce is that it is based on a device that consumers are familiar with and are comfortable using.

- **KIOSKS**

Kiosks are displays used to provide merchandise information in a remote location, such as a retail store or shopping mall.

Kiosks employ a variety of technologies to deliver multimedia marketing information.

Most kiosks allow the consumers to order product directly from the unit by using a magnetic credit card reader, touch screen, or keypad Kiosks' primary advantages are their large storage capacity and multimedia capabilities, including full-motion video, sound, graphics and text. However, kiosks have

not proven to be an Effective medium to support transaction-based interactions. It seems that consumers are not comfortable with the technology or the process of buying merchandise through a kiosk.

- **Interactive television and video dial tone**

The television is a ubiquitous electronic home appliance, interactive television, When Available, enables consumers to view advertising about specific products and place orders through the television screen using a remote control and a special set-top box attached to the Cable television line in to the home

There has been interest in bringing this technology to the market in recent years. The key Reason interactive television has generated interest among marketers, technology developers, Cable TV, and telephone companies is that it has a vast potential audience

- **Web TV**

A new technology, called Web TV by some and interacting by others, was seeing Deployment at press time. This approach is yet another vehicle for electronic commerce. Web TV illustrates the fusion or convergence of technologies, eliminating previous lines of demarcation.

Inter casting is a technology developed by Intel that intertwines WWW pages with TV Broad casts With it, video producers can backup their real-time broad casts with all the resources of the internet.

For example, a sports fan could call up batting averages to a window on the screen of a base Ball game; news programs could provide background analysis for those who want to go beyond A 2 to 3 minute story; advertisers could offer viewers the opportunity to purchase their products or obtain more information about them.

It can be considered a new medium; however, it is expected to complement rather than supplant existing media. It is being positioned as a medium that combines the digital power of the PC, the global interactivity of the internet, and the rich programming of television.

- **Interactive banking**

Many banks are offering another form of electronic commerce known as interactive banking. This generally refers to methods that allow their customers to conduct some of their bank business over the phone or with a PC. Using a Touch-Tone telephone, customers can check their account balance, pay bills, order statements and so forth.

PC finance software such as Intuit's Quicken also refers the links to blanks that can accomplish the same tasks. Home banking has been offered for over a decade with mixed results. Besides technology shock for the average user, users have had to contend with banking fees. The near-term future of home banking is unclear at this time.

At the other end of the spectrum, banks without branches are now becoming available on the internet. For example: Atlanta Internet Bank (AIB) offers interest-bearing checking, direct deposit, and

Electronic bill payment over the web. The bank uses applications behind the web server to hook into existing legacy systems to support the traditional banking functions.

The bank opened for business in late 1996 and had 200 initial customers. In general, however, most banks have been slow to offer all the elements of virtual banking, in part because few development tools exist.

To facilitate banks move toward web-based transaction processing and integration with personal finance management applications, portable toolkit-based CGI- like application must be developed by software houses to facilitate interworking with current software applications.

6.Explain in detail about Modes of Electronic Commerce. (Nov 2012)

What is electronic commerce?

- Commerce is the interchange of goods or services, especially on a large scale. In the past, trading typically took place face-to-face between parties. Over the centuries and decades, trading has continued to become more sophisticated. At this time, a large percentage of transactions are no larger done face to face, but are conducted over a telephone or via mail, with the exchange of new plastic money.
- The major difference between the way in which electronic commerce has been conducted until now and

  the way it is now proposed to operate relates to a paradigm shift: moving from Using a closed private network, in which two parties have previously established some type of agreement, to utilizing an open public network such as open public network such as the internet, without any prior knowledge of the buyer.

- In effect, that is how regular commerce takes place: anyone can walk into any store and buy something without having to be previously known by the store personnel. The internet and the Ancillary e-commerce software allow transactions between parties that do not previously know each other.

Some open issues

- Although there are traditional concerns about credit fraud and bank embezzlement, the potential for high-volume fraud and automated fraud is greater in e-commerce with the introduction of public network computerized transactions.
- In addition, protecting intellectual property rights becomes a problem when digital duplication is easy and fast, leading to the proliferation of pirated copies. Therefore, methods to ensure that cardholder's payments are safely made, that Merchants information is retained as confidential and that banks maintain a high degree of security over protected funds are issues that must be addressed and solved.

7.Explain in detail about Electronic Data Interchange. (Apr 2013) (Apr 2012)(Apr 2014)

1. EDI
2. EDI's Benefits
3. Status

4. System Approach
5. Communication Approach

- EDI is defined as the inter organization exchange of document in standardized Electronic form directly between computer applications.

- Examples of typical business documents include purchase orders, invoices, and Material releases. In basic terms, EDI can be thought of as the replacement of paper- Based purchase orders with electronic equivalents.

- EDI's goal is to enable easy and inexpensive communication of structured Information throughout the corporate community.EDI can facilitate integration among Dispersed organizations.

- Another of EDI's goals is to reduce the amount of data capture, and transcription: This results in a decreased incidence of errors, reduced time spent on exception handling, And fewer data-caused delays in the business and process.

- Benefits can be secured in inventory management, transport and distribution, Administration and cash management.

The key aspect of EDI are as follows

- The utilization of an electronic transmission medium(normally a VAN) Rather than the transfer of physical storage media such as paper, magnetic Tapes, and disks

- Use of structured, formatted messages based upon agreed standards(such That message can be translated, interpreted and checked for compliance with an explicit set of rules)

- Relatively fast delivery of electronic documents from sender to receiver (generally implying a receipt within hours or minutes)

- Direct communication between applications(rather than just between Systems)

EDI's benefits

- Businesses can secure many benefits when utilizing EDI. However, investment will be necessary in order to achieve lower costs and planning and control is needed to ensure that the savings actually realized. Monetary savings are obtained by Automating existing business procedures.

- The major benefit is the elimination of rekeying the data. With EDI, business Document transmit automatically from the sender's business application to the receiver's Application.

- The receiver need not reenter the information from a paper form; keypunching Errors are avoided and the accuracy of the data increases.

STATUS

- In recent years, the technologies underlying EDI have matured and the economics Of EDI application have improved to the point that an increasing number of Organizations are seeing opportunities for cost savings, improved service, and Competitive advantage. EDI has been growing in the recent past, although the penetration is still low.

SYSTEM APPROACH

- There are a number of ways in which computers can be set up to support EDI. A Single dedicated PC can be used as the company's link to the outside world. Alternatively, a group of computers which also support other desktop function can be utilized to dial up to the outside world via individual modems or modem pool.
- A more elaborate setup uses a server to act as the interface between the outside World and(set of) computers that process the business applications. The link to the EDI network can then be either dial-up or could have a dedicated link into the network's local hub point.
- The option selected usually depends on the scaled of EDI uses and its importance to the organization's operation. Types of software packages that would make up an EDI terminal on a PC include the following:
    - Application software
    - Message translator
    - Routing manager
    - Communication handler
- Using a PC with a dial-up modem is an easy way to start using EDI. Software is available that provides all the necessary EDI functions, such as the communications protocol and the EDI message translator. The function of the routing manager may be included in the software so that communication links are established automatically whenever a data exchange is required.

COMMUNICATION APPROACH

- Although dial-up is an entry-level mode approach to using this technology, sophisticated applications of EDI require a more elaborate communication infrastructure. But even beyond that, the VAN networks used by companied in a conventional EDI Environment are limited in functionality and scope. There are only a small number of companies one can reach and interact with.
- The Internet has had a high growth rare, averaging more than 12 percent every two months in the recent past; the VAN market has been growing at an annual rate of 12 percent per year.

8.Explain in detail about Migration to Open EDI.

- It appears that the Internet and the transition to what is called by some Open EDI will change the economics of EDI by reducing setup and rollout costs.
- To the extent that interoperability of networks increases the usability of EDI by making more potential trading partners available and accelerates the number of companies engaging in electronic commerce, it will directly stimulate the growth of EDI.

1. Approach
2. Benefits
3. Mechanics
4. Challenges
5. Examples

APPROACH

The development of Open EDI enables several types of rollout strategies. Generally, users can be classified into two groups. The first group is composed of users individuals or companies) who are not currently EDI users.

- The second group is composed of companies currently using EDI, generally through the services of either private networks or VAN's. This presents three migration paths to users:
  - A nonuser becoming a private network/VAN user. This is the most common migration when companies are considering additional use of EDI. Up to this time, this migration path has been the only route open to users.
  - A current EDI user who wishes to make a transition to Open EDI.
  - A non-EDI user who can make a direct transition to Open EDI. The factor driving migration is as follows:
  - The cost of using EDI service
  - The demands of customers
  - The opening up of market opportunities
- Migration from non-EDI to EDI operation is generally driven by the demands of dominant organizations.
- For example, subcontractors to major industrial establishments using EDI are at times forced to adopt the technology in order to continue doing business.

BENEFITS

- There are a number of benefits to supporting EDI on the Internet. The key benefit relates to the cost of transferring EDI messages on the Internet compared to transferring these messages on VAN.
- Internet access providers charge an average of about $30.00 per month for a SLIPP/PPP (Serial Line Internet Protocol/Point-to-Point Protocol) account that gives users an access number and unlimited (or at least a large number of) hours of Internet connect time.
- If a business needs higher throughput because it is sending large volumes of EDI data, then it can secure a dedicated 56-kpbs frame-relay connection to the Internet for about $450.00 per month.
- However, the introduction of Web technology to replace low-end EDI translators will greatly speed the introduction of small companies to electronic commerce.

MECHANICS

- Companies can send EDI transactions across the Internet in two ways. The first way is via the File Transfer Protocol (FTP) and the second is via e-mail. Most Internet EDI implementations use e-mail because it is relatively more secure and requires less administration.
- FTP requires the user to administer a login ID and password for each trading partner. The trading partners must also agree on directory names and files names before they can exchange EDI data via FTP. The overhead associated with FTP becomes significant when large numbers of trading partners are involved.

- With Internet e-mail, the sender and receiver do not log in to each other's computers. For some applications,

  FTP is a better choice than e-mail because some e-mail systems cannot handle large messages; however, most EDI business documents are much less than 500 KB.

- Another issue of using e-mail for EDI data concerns e-mail sent via the Simple Mail Transfer Protocol (SMTP). SMTP software can corrupt EDI data within an e-mail message since it treats the EDI data as printable text.

- EDI line-termination characters may be corrupted (if the line-termination character is a nonprintable character) and spaces may be added to or deleted from the EDI data.

- Multipurpose Internet Mail Extension (MIME) can solve this problem because it supports no text data by encoding it as text.

CHALLENGES

- There are several factors that may be keeping business form making the decision to send their EDI information over the Internet. There is the perception that the Internet is not secure enough for EDI applications.

- To address this issue, EDI users can utilize encryption and digital signatures to ensure secure EDI transmission across the Internet.

The use of EDI technologies over the Internet with the following goals:

- Define an architecture that links buyers, sellers, and service providers through the Internet as well as proprietary networks.
- Develop a set of electronic commerce services for use in the commercial and government sector.
- Enable the expansion of EDI technologies in ways that make it economical and practical for all type of organizations and individuals to use the EDI-based services.

EXAMPLES:

The cost of emerging EDI with in – house databases & paying for private value added networks, which ensure some level of secure transmission, has kept small businesses from using EDI.

9.Explain in detail about Electronic Commerce with WWW/Internet (Apr 2012)(Apr 2014)(Apr 2015)

- An evolving electronic commerce opportunity is WWW-based buying and selling through the Internet or through a VAN that provides gateways to the Internet. Web based electronic commerce includes the following:
  - Business-to-business
  - Business-to-consumer
  - Consumer-to-consumer
  - Revenue opportunities for Web commerce include:

- Technical and consulting services
- Merchandising products/information
- Transport services
- Directory services
- Content creation
- Subscriptions
- Access services
- Advertising services
- Hosting of web sites

❖ The web has the potential to seamlessly merge marketing and transaction mechanisms, to provide business with increased abilities to influence purchasing and facilities electronic commerce.

❖ Many corporations are using the internet for improved communication among employees and between employees and customers, suppliers and distribution channel partners

INTERNET/WEB STATISTICS

❖ The first commerce Net/Nielsen internet demographics survey was conducted in august 1995. The following statistics were measured among the person 16 years and older in United States and Canada,

- 16 percent as access to internet
- 10 percent had used the internet in last three months
- About 8 percent as used the World Wide Web (www) in the last 3 months.

❖ This research was a milestone in the measurement of the Internet and the World Wide Web usage.

❖ The following are some key statistics from the recon tact survey conducted in march/April 1996.for person 16 years or older in the United States and Canada

- 24 percent had access to the internet. This is a 50 percent growth in access to the internet from august 1995 to march1996.
- 17 percent has used the internet in last 6 months. Only 10%percent as used the internet in 3 months prior to august 1995. Of all persons using the internet in the 6 months between august 1995 and march 1996,55 percent had not used in three months prior to august 1995.
- 13% have used www in the last 6 months. Only 8% had used the www in the 3 months prior to august 1995.

INTERNET AND WWW TOOLS

❖ The internet is simply a network; that is a set of interconnected routers. It is a set of local, long-haul, and international links. Organizations that connect their servers to the internet and allow users to access them provide the content. Some companies specialize in content delivery.

- The key internet application of interest to electronic commerce is electronic mail, news group, FTP archives, telnet, WAIS, gopher, WWW and agents. These tools provide the building blocks for organizations.

- **Electronic mail:** the least expensive and still the most predominant of the internet information access mechanisms is e-mail. E-mail services allow companies to make information available to a large universe of recipients.

- Internet e-mail uses a number of internet protocols, including SMTP (RFC 8222), MIME (RFC 1767), and Post Office Protocol (POP).

- **Newsgroup:** newsgroup is discussion forums where articles get posted as topic and replies get posted to create a thread (a thread is the series of responses to a message in a news group).

- Articles can be posted to multiple newsgroups. A newsgroup can be established as moderated or read-only. Articles can be posted via e-mail, although many browsers now incorporate into their software abilities to view newsgroup.

- **File transfer protocol**: FTP is the way most internet users get files from other internet host (servers). FTP allows a user to log on a remote host (server), but restricts the user to a limited set of commands. Next to e-mail, FTP is the most commonly used internet service

- **Telnet:**telnet is a utility that allows users to log in to a remote system just as though they were logging in to a local system. Once logged in .the users have the same access to system as though they logged in form a terminal attached directly to the system. This method requires computer skills.

- **WAIS**: while the www is a user friendly interface for the browsing data, it has somewhat limited search capabilities. WAIS allows users to search for specific data they are interested in.

- **Gopher**: gopher is one of the information search and retrieval tools that preceded the widespread use of www. Gophers use is now only common integrated with the more sophisticated browser interfaces.

- Gopher is a simple tool and relatively easily implemented, but is an important capability it can be described as a document delivery tool; in fact, Gopher can deliver documents, list of documents and indexes.

- Gopher can offer not only textual information, but also organized browsing list of resources on the internet. Gopher transparently links groups of file server, each with their own accumulation of files and folders.

- **WORLD WIDE WEB:** The www is the newest and the most user friendly information's service on the internet. WWW as a ability to incorporate FTP, WAIS, Gopher, e-mail and FTP applications through one user interface.

- Before WWW application was available (they started to appear in the early 1990's) a user could need an

FTP client to connect to an FTP archive, a WAIS client to search a WAIS server, and a Gopher client to get

to a Gopher server.

❖ A web server provides access to all of these service to enable, among other things web based commerce. Website is referred to buy their uniform resources Locator (URL) addresses which specify an information object on the Internet such as an HTTP link or an FTP archive.

❖ All URLs indicate the type of object, a colon, then the address of the object, and any further information required. WWW documents are expressed in Hyper Text Markup Language (HTML). Web serves transfer HTML documents to each other through the Hyper Text Transfer Protocol (HTTP).

❖ ***Agent.*** Agents are becoming a useful tool for businesses and customers. An agent is a software program that is designed to automatically perform specific tasks. A customer's agent could search Web stores for the lowest price on a specific product (e.g., a book or a music CD) or check to see if certain URLs have been updated.

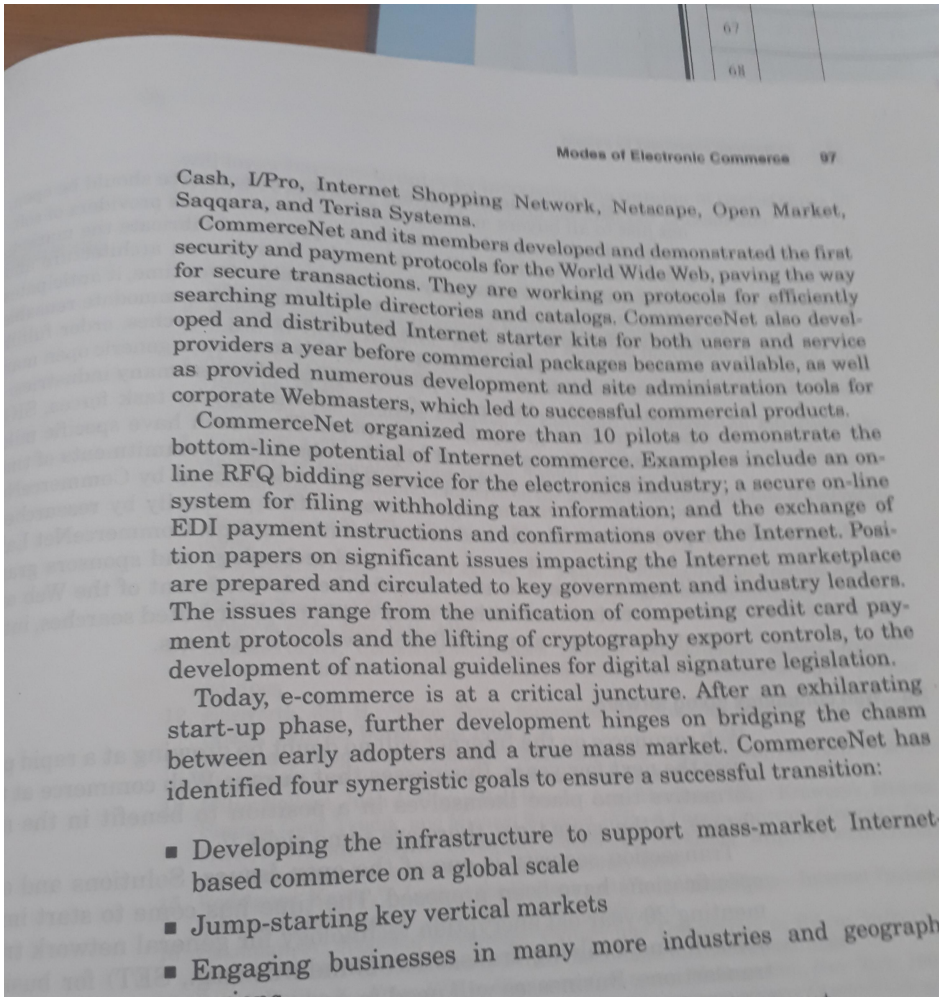
❖ A business might use an agent to look for competitors on the Internet. Agents are useful tools because they free organizations from laborious activities, like searching the Internet. They have the potential to revolutionize the way that customer and businesses gather information.

Bargain Finder (http://bf.cstar.ac.co/bf/) is an example of an agent that searches compact disc stores on the Internet. The user enters the name of an album and Bargain Finder searches for the best price available. This agent is limited in features, but it can be useful for a customer that wants a product at the lowest price possible.

10.Explain CommerceNet Advocacy.

COMMERCENET ADVOCACY

CommerceNet is the leading industry consortium, dedicated to accelerating the growth of Internet Commerce and creating business opportunities for members.



67

68

Modes of Electronic Commerce 97

Cash, I/Pro, Internet Shopping Network, Netscape, Open Market, Saqqara, and Terisa Systems.

CommerceNet and its members developed and demonstrated the first security and payment protocols for the World Wide Web, paving the way for secure transactions. They are working on protocols for efficiently searching multiple directories and catalogs. CommerceNet also developed and distributed Internet starter kits for both users and service providers a year before commercial packages became available, as well as provided numerous development and site administration tools for corporate Webmasters, which led to successful commercial products.

CommerceNet organized more than 10 pilots to demonstrate the bottom-line potential of Internet commerce. Examples include an on-line RFQ bidding service for the electronics industry; a secure on-line system for filing withholding tax information; and the exchange of EDI payment instructions and confirmations over the Internet. Position papers on significant issues impacting the Internet marketplace are prepared and circulated to key government and industry leaders. The issues range from the unification of competing credit card payment protocols and the lifting of cryptography export controls, to the development of national guidelines for digital signature legislation.

Today, e-commerce is at a critical juncture. After an exhilarating start-up phase, further development hinges on bridging the chasm between early adopters and a true mass market. CommerceNet has identified four synergistic goals to ensure a successful transition:

- Developing the infrastructure to support mass-market Internet based commerce on a global scale
- Jump-starting key vertical markets
- Engaging businesses in many more industries and geograph

CommerceNet sees itself as serving as the prototype for an open twenty-first-century Internet-based organization. CommerceNet and its members are developing elements of the infrastructure model for the future support of Web commerce. This is achieved through development, implementation, and expansion of the technical and institutional protocols required to impart electronic commerce to all worldwide markets. Launched in Silicon Valley in 1994, CommerceNet has grown to over 200 member companies and organizations worldwide. CommerceNet pioneered Web commerce by legitimizing the Internet as a place for business, developing key elements of the infrastructure such as security and payment, and fielding pilot demonstrations. Table 2.8 depicts the organization's activities and goals.

CommerceNet is a not-for-profit market and business development organization, with the mission of accelerating the growth of Internet commerce and creating business opportunities for its members. The organization focuses on precompetitive global and industrywide issues, so that members can benefit from economies of scale and avoid competing on an ineffective basis. The organization approaches issues from a multidisciplinary perspective encompassing technology, business processes, and regulatory policies. CommerceNet operates as a virtual organization, relying heavily on the expertise and resources of its members as well as other industry associations.[40]

Members of CommerceNet include leading U.S. computer companies, VANs, Telcos, on-line services, money center banks, and credit card processors. During 1996, in partnership with Nielsen, CommerceNet produced the first definitive survey documenting the explosive growth of the Internet marketplace; the recontact follow-up Nielsen/CommerceNet survey became available August 1996 (this study was quoted earlier). CommerceNet was involved, directly or indirectly, in the formation of many promising Internet startups, including Cyber-

ommerceNet Activities and Goals

Promoting a legal and regulatory environment that fosters global
CommerceNet engages businesses and

11.Explain Web commerce Going Forward

WEB COMMERCE GOING FORWARD

- Web commerce on the Internet will no doubt be growing at a rapid pace over the next few years. Businesses that pursue Web commerce at this formative time place themselves in a position to benefit in the near future: at the same time, there are some risks.

- Transaction security is one open issue. Businesses will need to use encryption and digital signature techniques to ensure that proprietary customer information is protected.

- Open EDI provides a loss-expensive alternative to electronic commerce than traditional EDI systems based on proprietary protocols and closed user groups.

PONDICHERRY UNIVERSITY QUESTIONS

2 MARKS

1. Define Electronic Marketers **(Nov 2012) (Ref.Qn.No.3)**
2. What are the technologies of e-commerce? **(Nov 2012) (Ref.Qn.No.14)**
3. Define the term E-Commerce.**(Apr 2012)(Apr 2014)(Nov 2014) (Ref.Qn.No.1)**
4. What is an EDI? **(Apr 2012)(Apr 2014) (Apr 2015)(Ref.Qn.No.15)**
5. Name any four e-payment provider **(Apr 2013) (Ref.Qn.No.30)**
6. What are the features of e-commerce? **(Apr 2013) (Ref.Qn.No.7)**
7. What are the environments of e-commerce? **(Apr 2015) (Ref.Qn.No.38, Ref Pg.no.10)**

11 MARKS

1. Briefly explain the Electronic Marketplace Technologies. **(Nov 2012) (Ref.Qn.No.5)**
2. Explain some open issues related to E-Commerce. **(Nov 2012) (Ref.Qn.No.4 & 6)**
3. Discuss the various activities and goals of Commerce Net. **(Nov 2012) (Ref.Qn.No.3)**
4. Discuss the applications of web and Electronic commerce. **(Apr 2012) (Ref.Qn.No.9)**
5. Explain the basics of EDI. **(Apr 2012)(Nov 2014) (Ref.Qn.No.7)**
6. Discuss in detail about EDI. **(Apr 2013)(Apr 2014) (Ref.Qn.No.7)**

7. Explore the basic concepts of e-commerce in detail. **(Apr 2013) (Ref.Qn.No.1)**
8. Explain in detail about Electronic Commerce with WWW/Internet **(Apr 2012)(Apr 2014)(Apr 2015) (Ref.Qn.No.9)**

9**.**Explain the E-Commerce Environment.**(Apr 2013)(Nov 2014)(Apr 2015) (Ref.Qn.No.1)**

UNIT-II

Approaches to Safe Electronic Commerce: Overview – Secure Transport Protocols – Secure Transactions – Secure Electronic Payment Protocol(SEPP) – Secure Electronic Transaction (SET)- Certificates for Authentication – Security on Web Servers and Enterprise Networks – Electronic cash and Electronic payment schemes: Internet Monetary payment and security requirements – payment and purchase order process - Online Electronic cash.

2 MARKS

1. Goals of Computer Security: (Apr 2012)

Computer security has several fundamentals goals.

- **Privacy-** Keep private documents private, using encryption, passwords, and access-control systems.
- **Integrity-** Data and applications should be sage from modification without the owner‟s consent.
- **Authentication-** Ensure that the people using the computer are the authorized users of that system.
- **Availability-** The end system (host) and data should be available when needed by the authorized user.

2. Secure Commerce Requirements:

Requirements	Description
Content security	The ability to send information across the Internet in a manner in which unauthorized entities are not able to read the contents.
Signature	The ability to specifically identify the entity associated with the information. Many things may be signed: contents, the message, and, frequently, several signatures may be imbedded in a single message or information unit.
Content integrity	The ability to identify modification to the covered information.

Non-repudiation of origin	The ability to identify who sent the information originally versus which intermediary forwarded it.
Non-repudiation of receipt	The ability to identify that the information was received by the final addressed destination in a manner that cannot be repudiated. The information has been opened and interpreted to some degree.
Non-repudiation of delivery	The ability to identify whether the information was delivered to an appropriate intermediary in a manner if cannot repudiate.
Key management	The functionality necessary to create, distribute, revoke, and mange the public/private keys.

3. What is secure Transport Protocol? (Nov 2014) (Nov 2012)

Netscape Communication‟s Secure Sockets Layer system and the Commerce Net„s Secure Hypertext Transfer Protocol offers security by means of transferring information through the Internet and the World Wide Web.

SSL and S-HTTP allow the client and servers to execute all encryption and decryption of Web transactions automatically and transparently to the end user. SSL works at the transport layer and it is simpler than S-HTTP which works at the application layer and supports more services.

4. Define S-HTTP.

S-HTTP is a secure extension of HTTP and it is developed by the Commerce Net Consortium. S-HTTP offers security techniques and encryption with RSA methods, along with other payment protocols.

S-HTTP supports end-to-end secure transactions by incorporating cryptographic enhancements in transferring the data at the application level for secured transport, but in HTTP authorization mechanisms, the client is required to attempt access and be denied before the security mechanism is employed.

S-HTTP incorporates public-key cryptography from RSA Data Security in addition to supporting traditional shared secret password and Kerberos-based security systems.

5. Define SSL.

It is a security protocol that provides privacy over the Internet. The data transmission in client/server applications to communicate cannot be altered or disclosed by using the SSL Protocol.

The authentication is permanent in Servers and clients are Optionally authenticated. The technology has support for key exchange algorithms and hardware tokens.

The strength of SSL is that it is application-independent. HTTP, Telnet, and FTP can be placed on top of SSL transparently.

SSL provides channel security (privacy and authentication) through encryption and reliability through the message integrity checks (secure hash functions).

Eg.: MasterCard and Visa.

6. What is Process in SSL?

SSL uses a three-part process.

- First, information is encrypted to prevent unauthorized disclosure.
- Second, the information is authenticated to make sure that the information is being sent and received by the correct part.
- Finally, SSL provides message integrity to prevent the information from being altered during interchanges between the source and sink.

7. Define Secure Electronic Transaction(SET). (Apr 2013)

SET is a protocol for allowing secure transactions to take place on the Internet. It is based on the idea that the merchant and the end-user don‟t directly transfer funds, but they

use a third party (payment gateway). It provides a set of protocols and formats that allow users to securely use the existing credit card payment infrastructure on the Internet.

Defined by the SET protocol is a series of messages with content and format as specified by the Abstract Syntax Notation One (ASN.1) for communication between each of the participants

8. Define Secure Transactions.

S-HTTP and SSL protocols provide secure transactions by transferring money from one location to another location in a secure and safe way. Netscape Communications Corporation and Microsoft Corporation have promoted three methods of payment protocols and installed them in WWW browsers and servers.

These three methods are as follows:

- Secure Electronic Payment Protocol (SEPP).
- Secure Transaction Technology (STT).
- SET.

9. What is SEPP?

SEPP is the electronic equivalent of the paper charge slip, signature, and submission process. SEPP takes input from the negotiation process and causes the payment to happen via a three-way communication among the cardholder, merchant, and acquirer.

It provides a standard for presenting credit card transactions on the Internet.

SEPP only addresses the payment process; privacy of nonfinancial data is not addressed in the SEPP protocol.

10. Mention the Elements in SEPP.

The SEPP system is composed of a collection of elements involved in electronic commerce.

- Cardholder.
- Merchant.
- Acquirer.
- Certificate management system
- Bank net.

11. Define Certificate For Authentication.

A digital certificate is a foolproof way of identifying both consumers and merchants.

The digital certificate acts like a network version of driver‟s license, it verifies the user‟s identity.

Digital certificates, includes the holder‟s name, the name of the certificate authority, a public key for cryptographic use, and a time limit for the use of the certificate.

The certificate typically includes a class, which indicates to what degree it has been verified.

12. Need for security of merchant host.

The need for security of the merchant host is necessary in order to protect

- Files containing buyer‟s information that might reside on the accessible web server.
- The overall information platform of the organization.

13. Methods for security on web servers.

Two general techniques are available:

- host- based security capabilities; these are means by which each and every computer on the system is made impregnable.
- Security watchdog systems which guard the set of internal inter-connected systems. Communication between the internal world and the external world must be funneled through these systems.

14. Define Enterprise Network Security.

A firewall supports communication-based security to screen out undesired communications which can cause havoc on the host. Firewalls act as a single focus for the security policy of the organization and support advanced authentication techniques such as smart cards and one-time passwords. They provide an identifiable location for logging alarms or trigger conditions.

15. Define Firewalls Configuration.

Firewalls are typically configured to filter traffic based on one of two design policies:

- Permit, unless specifically denied. This is weaker because it is impossible to be aware of all the numerous network utilities you may need to protect against. Specifically this approach does not protect against new Internet utilities.
- Deny, unless specifically permitted. This is stronger because the administrator can start off with a blank permit list and add only those functions that are explicitly required.

16. Define the term Electronic Cash interoperability?(Apr 2014)

Electronic cash (also known as e-currency, e-money, electronic cash) is money or scrip that is only exchanged electronically. Typically, this involves the use of computer networks, the internet and digital stored value systems.

Eg.: Electronic Funds Transfer (Eft), Direct Deposit, Digital Gold Currency And Virtual Currency . Also, it is a collective term for financial cryptography and technologies enabling it.

17. Advantages of Electronic Cash.

- Debit cards and online bill payments allow immediate transfer of funds from an account to a business‟s account without any actual paper transfer of money.
- Consumers will have greater privacy when shopping on the internet using electronic money instead of ordinary credit cards.

18. Disadvantages of Electronic Cash.

- E-cash and E-cash transaction security are the major concern. There are many other tricks including through phishing website of certain banks and emails.
- Money flow and criminal/terrorist activities are arder to be traced by government.
- Money laundering and tax evasion could be uncontrollable in e-cash systems as criminals use untraceable internet transaction to hide assets offshore.

19. Properties of Electronic Payment Schemes? (Apr 2014)

To purchase items over the Internet, people currently use credit cards as the prevailing form of Payment. These are the properties that would be necessary for such a scheme:

- Financial Infrastructure.
- No Double-Spending and Non-forgeability.
- Security.
- Persistence.
- Exclusive Ownership.
- Anonymity.
- Transferability.
- Amounts.
- Traceable to issuer.
- Divisibility and Combination.
- Compatibility with existing systems.
- E-Client for small amounts.
- Scalability.
- Competition between Issuers.

20. Types Of Electronic Payment Scheme.

There are 3 types in E-Payment scheme:

- Type 1: payment through an intermediary- payment clearing services.
- Type 2: payment based on EFT- national funds transfer.
- Type 3: payment based on electronic currency.

21. What are the transactions/processes that must occur for an electronic payment? (OR)Requirement For Electronic Payment Scheme: (Nov 2012)

The requirements of the electronic payment systems found in the literature are: identification, confidentiality, authentication, data integrity, non reputation, convertibility, anonymity, privacy, easy to use, user friendly, mobility…

1. **Technological Aspect:**

- Security.
  - Authentication (also referred to as Identification or Validity).

- Privacy (also referred to as Confidentiality).
- Data integrity (also referred to as Accuracy).
- Non-repudiation.
- Durability.

- Authorization type.
- Process speed.
- Flexibility.
- Trust.

2. Economic aspect

- Cost
  - Buyer cost
  - Merchant cost
- Liquidity (also referred to as convertibility or Multi currency).
- Atomic Exchange.
- User Reach (also referred to as Applicability or Acceptability).
- Value Mobility.
- Financial Risk.

22. Advantages Of E-Payment.

- E-payments have several advantages, which were never available through the traditional modes of payment. Some of the most important are:

  - Privacy.
  - Integrity.
  - Compatibility.
  - Good transaction efficiency.
  - Acceptability.
  - Convenience.
  - Mobility.
  - Low financial risk.
  - Anonymity.
  - convenience.

23. State the problems with traditional payment system (OR) Disadvantages of E-Payment scheme (Apr 2013)

- Lack of authentication.
- Repudiation of charges.
- Credit card fraud.
- No picture identification or signature.

24. Internet Monetary payment and Security Requirements.

For consumers and merchants to be able to trust one another, prevent transmitted payment information from being tampered with and complete transaction with any valid parts, the follows issues need to be addressed.

- Confidentiality of payment information.
- Integrity of payment information transmitted via public networks.
- Verification that an account holder is using a legitimate account.
- Verification that a merchant can accept that particular account.
- Interoperability across software and network problems.

25. Define Electronic Purchase Orders (POs).

An Electronic PO is a document that outlines the terms of an order, and outlines the agency‟s terms and conditions to which both parties must adhere.

Electronic PO‟s can be generated in a transactional e-procurement system, or directly from an FMIS or ERP system from a requisition, and then sent via electronic means to a supplier for direct upload into their system.

26. Creation Of Electronic Purchase Order.

Electronic POs are created through:

- Creating a PO through a FMIS or ERP system where the requisition and PO datais stored centrally and delivered to the supplier electronically Creating a PO through a standalone e–procurement system where the PO data is stored for procurement and accounts processing and delivered to the supplier electronically.

27. Types Of Electronic Purchase Order.

Types of Electronic POs include:

- Two–way PO match – where the payment is triggered by the invoice
- three–way PO match – where the payment is triggered by receipting the order of goods/services and then matched against the invoice.

28. Advantages Of Electronic PO's.

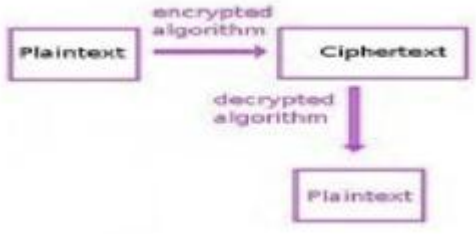
- **Maintain optimum stock levels:** No requirement to carry excess stock.
- **Improve on-shelf availability:** Ensure greater customer satisfaction and increased sales by stocking what your customers want.
- **Reduces costs:** Purchase order software that significantly reduces supply chain document management costs.
- **Improve on-shelf availability:** Ensure greater customer satisfaction and increased sales.
- **Supply chain management:** Increase competitiveness, reduces errors and dispute levels.
- **Reliability:** Speed and accuracy guaranteed for time critical orders.
- **Eliminate paper:** By automating the purchase order process you dispense with the requirement to print and manually post or fax purchase orders.

29. What does the term symmetric cryptography means? (Apr 2012)

Symmetric cryptography, or more commonly called secret-key cryptography, uses the same key to encrypt and decrypt a message. Thus, a sender and receiver of a message must hold the same secret or key confidentially. A commonly used secret-key algorithm is the Data Encryption Standard (DES).

30.How do you change plain text to cipher text? (Nov 2014)

The plaintext is commonly used as the input to a cipher or encryption algorithm. The output of these cipher‟s is normally referred to as ciphertext. The outputted text can be a result of one or many rounds of encryption employed on the plaintext depending on the specific algorithm in use.



31.What is meant by authentication? (Apr 2015)

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an **authentication** server. If the credentials match, the process is completed and the user is granted authorization for access.

32.What is secure transport layer? (Apr 2015)

- **Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network.
- Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP).
- Major web sites (including Google, YouTube, Facebook and many others) use TLS to secure all communications between their servers and web browsers.

11 MARKS

1. Explain In Detail About Approaches To Safe Electronic Commerce.

❖ As business activity grows on the Internet, security is becoming an important consideration to take into account ant to addresses, to the stakeholder‟s satisfaction. According to some sources, by the year 2000, commerce on the Internet could account for 9 billion payment transactions a year, representing an optimistic. In this context security relates to three general areas:

1. Secure file / information transfers
2. Secure transactions

3. Secure enterprise networks, when used to support Web commerce

❖ There is an extensive bibliography on the topic of network security going back several years. Perhaps the time has come to stop talking about it and start doing something about it. What some call the "chaotic landscape of electronic commerce primarily a hodgepodge of disparate, incompatible software solutions," is being leveled to some degree by initiatives such as digital certificates and SET.

❖ But even more needs to be done. Standards are expected to be established in the marketplace by way of actual products sometime in 1997 and beyond.

OVERVIEW

❖ Observers and proponents articulate the thesis that the security issue must be addressed quickly in order for companies to start investing in electronic commerce. There are indications that merchants are taking a wait-and-see attitude in electronic commerce on the Internet until either there is a dominant standard or there is universal software that will support a variety of encryption ant transaction schemes." The market is looking for a comprehensive solution (in a software product) that the merchants and banks can use to support all functions. Computer security has several fundamental goals.

1. **Privacy**: Keep private documents private, using encryption, passwords, and access control systems
2. **Integrity**: Data and applications should be safe from modification without the owner‟s consent
3. **Authentication**: Ensure that the people using the computer are the authorized users of that system.
4. **Availability**: The end system (host) and data should be available when needed by the authorized user.

❖ Another issue to be tackled is just plain fraud, where the buyer simply supplies out-of-date or incorrect credit card information.

❖ Web-based commerce is beginning to see penetration in the market, but security is critical to further penetration. For example, as of press time, 1-800-flowers had been doing business electronically for about three years. Approximately 10 percent of its $300 million in annual revenue comes from on-line purchases. The company has more than 15 preface of this book and chap.1, the Cisco Web site was discussed as an example of a successful and effective Web commerce site. Cisco‟s site. Cisco

Connection Online runs on Netscape Secure Commerce Servers. A firewall is used, presumably, to screen out unregistered customers.

2. Explain in detail about Secure Transport Protocols?(Apr 2012)

Introduction

- The secure sockets layer system from Netscape communications and the Secure Hypertext Transfer Protocol from Commerce Net offer secure means of transferring information through the internet and the WWW,SSL and S-HTTP allow the client and servers to execute all encryption and decryption of web transactions automatically and transparently to the end user.SSL works at the transport layer and it is simpler than S-HTTP which works at the application layer and supports more service (such as firewalls and generation and validation of electronic signatures.
    - S-HTTP
    - SSL
    - Alternatives

S-HTTP

- S-HTTP is a secure protocol used to encrypt and host sensitive information on the web. This is particularly important when dealing with financial and confidential information, Secure HTTP was developed by Enterprise Integration Technology(EIT)as part of the Commerce Net Project in Silicon Valley but has been released as a public specification, The system provides security enhancements to the web transport standard ,hypertext transfer protocol(HTTP).It allow clients and server to negotiate independently encryption, authentication, and digital signature methods, in any combinations in both directions. It
  supports a variety of encryption, triples DES, and others. The use of S-HTTO begins with an exchange of messages that specify security management information such as the encryption, hash, and signature algorithms to be used in each direction. These can be specified separately for header and content information.

- S-HTTP can provide confidentiality, authentication, integrity guarantees on an individual file basis. Web sites with security features are used when displaying information such as Credit card numbers, Personal information, passwords and Contact details. Security for Commerce on the Internet One of the main problems for retailing electronically on the Internet is the lack of security. Two general-purpose approaches that are broadly representatives and probably the most important

as well: the Secure Socket Layer (SSL) from Netscape and Secure HTTP(S-HTTP) from Enterprise Integration Technology. For payment systems that provide strong security for Internet purchases of goods and services two are SET, proposed for bank card transactions by MasterCard and Visa or a more sophisticated payment particularly in anonymity, is E-cash developed by DigiCash.

SSL (SECURE SOCKET LAYER) : (3.Explain in detail about Secure Socket Layer)

SSL OVERVIEW

❖ Communicating data over a network always implies a possible loss of confidentiality, message integrity or endpoint authentication. These are the major aspect one as to consider when speaking of data security:

- **Confidentiality:**

  We want to be sure that our data is kept secret from unintended listeners.

- **Message Integrity:**

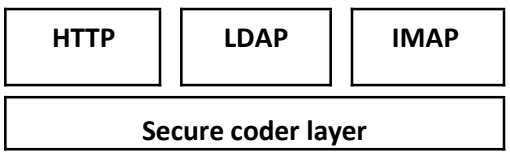
  We want to be sure that any message we receive is a exactly the one the sender sent.

- **Endpoint Authentication:**

  We want to be sure that our communicating partner is the one we intend.

❖ SSL is a security protocol that provides necessary mechanism to achieve these security goals through the use of cryptography, certificates and digital signatures. It provides a secure channel between two machines, namely a client (usually a browser) and a server (usually a web server)… SSL can be used with several higher layer protocols including the Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP) and the Net News Transfer Protocol (NNTP) with only minimal modifications, which is very convenient.

❖ SSL is not a single protocol, but consists of four sub-protocols which operate on top of TCP/IP(SSL Record Protocol) on the network layer and on the application layer(SSL Handshake Protocol, SSL Change Cipher Spec Protocol and the SSL Alert Protocol), where we find other higher layer protocols, such as HTTP(fig.1)



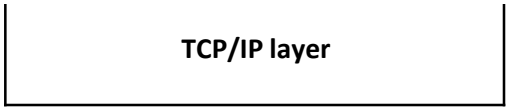


Figure.1 SSL layer above TCP/IP and below high-level application protocols.

- Netscape developed secure courier digital envelope. Information us encrypted at the same time it leaves the user‟s computer and remains so until it reaches the financial institution.

  Secure Courier also can verify the authenticity of inputted financial account information.

THE HISTORY OF SSL

- SSL was originally developed by NETSCAPE COMMUNICATIONS, intending to allow secure communication between a browser and a web server. Due to some major drawbacks mainly missing support for credit transaction over the internet, the first version of SSL was never released.

- After an abortive draft of SSLv2.1, which was supposed to be a modification of SSLv2, NETSCAPE eventually started all over and hired a well known security consultant to join the team and developed a completely new version of SSL. This project came to an end in late 1995 with the release of SSLv3 providing strengthened cryptographic algorithms and an important number s of solutions to previous security problems.

- In May 1996 the Internet Engineering Task Force (IETF) started a try to standardize an SSL-like protocol by chartering the Transport Layer Security (TLS) working group. The TLS working group finished its work in January 1999 and finally published TLS as RFC 2246 over two years late, because of backward compatibility problems with SSLv3 and several disagreements with the Internet Engineering Steering Groups (IESG), which must approve

  any document before its being allowed to be published as a Request For Comment(RFC). As of this writing, both Internet Explorer and Netscape/Mozilla browsers support TLS and SSL.

ALTERNATIVES:

A related capability is a certification authority to authority to authenticate the public keys on which the RSA system relies. The goal is to assure users that a public key that seems to be associated with a company actually is and not a spurious key. The authority requires applicants to prove their identity . those passing the tests are issued a certificate in which the applicant’s public key is encrypted by the authority’s private key.

4. Explain in detail about Secure Transactions? (Apr 2013)(Nov 2012)

- Secure Web transactions are increasingly commonplace. If anyone has ever ordered a book, a CD, or any other product or service over the Web (say, through Amazon.com), he or she likely utilized a secure transactions system. The e-commerce company Amazon.com processes thousands of secure e-transactions daily. As do most secure e-commerce Websites, Amazon.com encrypts confidential information with the Secure-Sockets Layer(SSL) technology as it is transmitted between the consumer‟s Web browser and the online company‟s Web server.

- No computer system can be assumed to be completely secure. Therefore, one needs to understand that security in an e-commerce sense is best defined in terms of acceptable risk-meaning that the consumer must feel comfortable that his or her personal information will be relatively safe from inappropriate use after it is sent online as part of the transaction. Moreover, acceptable risk means that the company operating the server must be confident that it can defy internal and external exploits.

- Because of concerns regarding e-commerce secure transactions, on February 9, 2005, XRamp Technologies announced that it is now issuing 256-bit digital SSL technology certificates the function with browsers and servers capable of the 256-bit Advanced Encryption Standard (AES). Besides working with the frequently used Mozilla Firefox Web Browser, the SSL technology certificates are backward compatible-able to provide encryption for software not meeting this standard.

- Majorly there are 3 methods for Secure Transactions
  - **SEPP**
  - **STT**
  - **SET**

- SEPP has been championed by MasterCard and Netscape and by other supporters; the American National Standard Institute (ANSI) is fast-tracking SEPP as a standard for the industry.

- STT was developed jointly by Visa and Microsoft as a method to secure bankcard transaction over open networks. STT uses cryptography to secure confidential information transfer, ensure payment integrity, and authenticate both merchants and cardholders.

- SET will become the industry de facto standard. SET has a lot in common with SEPP.

- All e-commerce environments require support for security properties such as authentication, authorization, data confidentiality, and non repudiation. E-commerce protocols such as SSL, TLS, and SET offer security for e-transactions, but they are specific to the uncast (point-to-multipoint) sessions. Multicast data transmission provides significant network resource savings for applications such as audio/video streaming, news broadcast services and software distribution. However, security is required to prevent theft, and to ensure revenue generation from authorized recipients. We have designed the Secure E-Commerce Transactions for Multicast Services (SETMS) architectural framework, to secure ecommerce sessions for multicast environments. The SETMS framework provides authentication of host through the HIP protocol, authorization of subscriber and his/her e-payments through a variant of the

  2KP protocol, a procedure to account for the subscriber‟s resource consumption, and support for no repudiation of principal parties through PKI. The SETMS framework has been formally validated using the AVISPA tool.

- The following are the some of the companies that support secure transactions:

  Commerce Net-> http://www.Commerce.Net

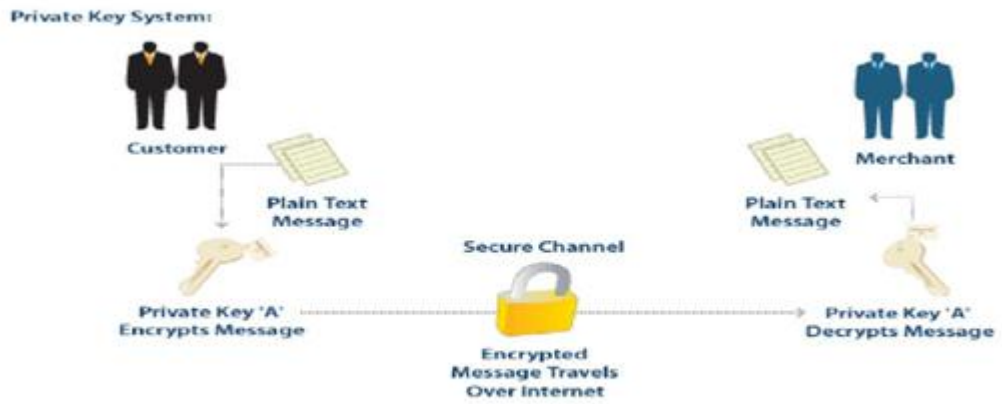
  CyperCash-> http://www.CyperCash.com

  DigiCash-> http://www.DigiCash.com

5. Explain in detail about Secure Electronic Transaction (set). (Nov 2012) (Nov2014) (Apr 2015)

- Secure Electronic Transaction (SET) is a standard protocol for sending credit card transactions over insecure networks, specifically, the Internet. SET is not itself a payment system, but rather a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion.

1. SET was developed by VISA and MasterCard starting in 1996.SET was said to become the de facto standard of payment method on the Internet between the merchants, the buyers, and the credit-card companies. When SET is used, the merchant itself has to know the credit-card numbers being sent from the buyer, which provide a benefit for e-commerce.



SET(Secure Electronic Transaction) purchase using public-key cryptography

Cardholder requests purchase

2. Merchant contacts payment gateway
3. Payment is authorized
4. Cardholder is notified of authorization
5. Merchant requests payment capture from gateway
6. Token is issued to merchant
7. Merchant redeems token for transfer into its bank account

❖ SET offers buyers more security then is available in the commercial market. Instead of providing merchants with access to credit card numbers, SET encodes the numbers so only the consumer and financial institution access to them. Cardholders, merchants, and the financial institution each retain SET certificates that identify them and the public keys associated with their digital identities.

❖ SET is a combination of an application-level protocol and recommended procedures for handling credit card transactions over the internet. SET does not use full-text encryption because it would require too much processing time.

In the SET protocol, two different encryption algorithms are used-

- **DES**
- **NSA**

❖ DES 56-bit key is used to encrypt transactions. This level of encryption, using DES, can be easily cracked using modern hardware.

❖ It is believed by some that the National Security Agency (NSA) were responsible for reducing its key size from the original 128-bits to 56.

❖ SET makes use of Netscape‟s Secure Sockets Layer (SSL), Microsoft‟s Secure Transaction

Technology (SST), and Terisa System‟s Secure Hypertext Transfer Protocol (SHTTP). SET uses some but not all aspects of a public key infrastructure (PKI).

❖ The following are the key functions of the specification

- Provide confidentiality of payment and ordering information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a credit card account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
- Create a protocol that neither depends in transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability among software and network providers.

IMPORTANCE OF SET :(6.Explain In Detail About Importance Of Secure Transactions.)

❖ Secure electronic transactions will be an important part of electronic commerce in the future. Without such security, the interests of the merchant, the consumer, and the credit or economic institution cannot be served. Privacy of transactions, and authentication of all parties, is important for achieving the level of trust that will allow such transactions to flourish. However, it is important that the encryption algorithms and key-sizes used will be Robust enough to prevent observation by hostile entities (either criminal or foreign powers). The ideal of the secure electronic transactions protocol (SET) is important for the success of Electronic commerce. However, it remains to be seen whether the protocol will be widely used because of the weakness of the encryption that it uses.

❖ **SET works:** Assume that a customer has a SET-enabled browser such as Netscape or Microsoft‟s Internet Explorer and that the transaction provider (bank, store, etc,) has a SET-enabled server.

1. The customer opens a MasterCard or Visa bank account. Any issuer of a credit card is some kind of bank.
2. The customer receives a digital certificate. This electronic file functions as a credit Card for online purchases or other transactions. It includes a public key with an Expiration

date. It has been through a digital switch to the bank to ensure its validity.

3. Third-party merchants also receive certificates from the bank. These certificates include the merchant‟s public key and the bank‟s public key.
4. The customer places an order over a Web page, by phone, or some other means.
5. The customer‟s browser receives and confirms from the merchant‟s certificate4 that the

   Merchant is valid.
6. The browser sends the order information. This message is encrypted with the Merchant‟s public key, the payment information, which is encrypted with the bank‟s Public key (which can‟t be read by the merchant), and information that ensures the Payment can only be used with this particular order.
7. The merchant verifies the customer by checking the digital signature on the customer‟s

   Certificate. This may be done by referring the certificates to the bank or to a third-party Verifier.
8. The merchant sends the order message along to the bank. This includes the bank‟s Public key, the customer‟s payment information (which the merchant can‟t decode), and the merchant‟s certificate.
9. The bank verifies the merchant and the message. The bank uses the digital signature On the certificate with the message and verifies the payment part of the message.
10. The bank digitally signs and sends authorization to the merchant who can then fill the Order.

7. Explain in detail about Certificates For Authentication.

A digital certificate is a foolproof way of identifying both consumers and Merchants. The digital certificate acts like a network version of driver‟s license- it is not Credit, but used in conjunction with any number of credit mechanisms, it verifies the User‟s identity. Digital certificates, which are issued by certificate authorities such as VeriSign and Cyber Trust, include the holder‟s name, the name of the certificate Authority, a public key for cryptographic use, and a time limit for the use of the certificate (most frequently, six months to a year).

- The certificate typically includes a class, which indicates to what degree it has Been verified. For example, VeriSign‟s digital certificates come in three classes. Class 1 Is the easiest to get and includes the fewest checks on the user‟s background: only his or Her name and e-mail address are verified. For class 2, the issuing authority checks the User‟s driver‟s license, Social Security number, and date of birth. Users applying for a Class 3 certificate can expect the issuing authority to perform a credit check using a Service such as Equifax, in addition to requiring the information required for a class 2 Certificates.

- It is now becoming easier for vendors and for consumers to get digital certificates. VeriSign and Cyber Trust, the two primary commercial issuers of digital certificates, can Issue certificates via the Web. Users of Microsoft Corporation‟s Internet Explorer 3.0 or Netscape Communications Corporation‟s Navigator 3.0 can take advantage of VeriSign‟s Offer for a free six-month class 1 certificate. Both Hewlett-Packard Company and IBM Have announced their intentions to use Entrust with their electronic commerce and Security products.

- One of the issues affecting the industry, however, is interoperability. The Document Certificate Practice Statement issued by VeriSign proposes interoperability Approaches, but the outcome was unknown at press time.

- DDoS attacks. It has become easy to the launch attacks today, with sophisticated tools being freely available on the Internet.

PHISHING:

- This is emerging as big threat to information security especially in the financial sector. Phishing (pronounced fishing) is the set of sending an e-mail to a user falsely claiming that it is from an established, legitimate enterprise. Such mails usually ask for private Information from the addressee, information that will be used for identity theft. Also referred to as brand spoofing, phishing tricks consumers into disclosing personal and/or Financial information. The e-mails appear to come from companies with whom Consumers may regularly conduct business (e.g., banks, credit-card companies). These Mails often contain links to fake websites of the established companies. When users go to the website, they come across

  trademarks of familiar brands they often deal with. The Website then instructs the

  consumer to re-enter their credit card numbers. ATM PINs or Other personal information.

SPYWARE:

❖ According a survey conducted by Watch Guard amongst 2000 IT managers globally,

Two-thirds of those surveyed believed spyware will be the number one threat to network Security in the coming months. Spyware is a growing category of malware that installs on A computer without the user‟s knowledge and it can secretly gather information about a Person or organization. It ranges from adware to tracking agents to software designed to hijack a Web browser to a different destination.

KEY CHALLENGES

❖ Most enterprises today have deployed one or more security products on their network. However the core issue is to first build the information security guidelines in accordance With their business needs. Once the guidelines are formulated, they should be translated into a framework of policies and processes. The network security architecture can then be developed in accordance with these. The architecture must be based on open standards And be flexible and scalable. It should also allow integration of new security Technologies, which the organization may want to leverage in order to gain business Advantage.

Gray Areas

- Spam filtering
- Patch management
- Managing the security logs of various products
- Plethora of best-of-breed products
- Lack of security management (it‟s expensive)
- Quality manpower for security operations.

❖ While the internet offers tremendous value by opening up new levels of integration with Partners, suppliers and customers-it also expose business systems to new forms of malicious attacks. In the era of unbounded networks, security boundaries have blurred where data flows across the information value chain. In addition to that, new threats have emerged as also quantity and virulence of attacks. As long as technology continues to Evolve, malicious code

will be right behind. The nature of viruses, Trojans, and worms Makes it virtually impossible to stop infiltration completely, though there are ways to Reduce, if not eliminate them.

- Operations are a constant challenge. Controls are easy to implement and easy to get Budgets for, operationally keeping a readiness state 24*7 will be a challenge. This means keeping track of all vulnerabilities, threats, and even legislations. This means Applying the myriad patches releases by vendors without increasing the windows of Exposure, keeping check of all DAT files, and turning on firewalls and IPS etc. these are Daily tasks as are employee awareness, password security, access controls, etc. the IT Team has to scan systems and applications for vulnerabilities, monitor the firewall and Traffic on networks for intruders, scan files for viruses, monitor mail and Web access for Inappropriate content, and notify when key system files have been modified. This is a Herculean task. Indeed, keeping up with the thousands of IT security threat alerts (most of Which are probably irrelevant) is one of the biggest sources of information overload.

8. Explain in detail about Security On Web Service And Enterprise Network.

- Network performance, high availability, and uptime are must for not only running the day – to-day operation of an enterprise, they are also critical for a successful business. Network downtime not only costs money and loss of precious time, it also mars an enterprise‟s reputation among its business partners and customers. Many times, the entire business strategy of an enterprise depends on how its network performs. So, when the network is business for an enterprise, nothing can be more nightmarish than an insecure network. On the other hand, enterprises today have many more users (both internal and external) accessing their network than they had in the past. Most of these networks are connected to several more networks, including the Internet, and many of these networks are accessed remotely.

- Networks are expanding in one more sense-they are running myriad applications that in turn drive many of the business that these enterprise deal in. This growth and expansion of enterprise networks, and increasing reliance of business on them, has given rise to new challenges of securing these networks. As the security environment worsens due to a complex set of threats and vulnerability, networks security must be deal with at different levels and in much more comprehensive manner than it is being done today.

- However security a network and thereby guaranteeing its high performance, availability, and uptime isn‟t a difficult task provided security managers do the right thing. The challenge is to know what those right things are.

KEY THREATS

- Growing frequency of attacks: According to latest SANS statistics, the average time between worm infection attempts is 13 minutes. This means that if you‟ve just installed an operating system on your computer, you have 13 minutes to fully patch it or protect it ever increasing threats to their networks in the form of new worms, viruses, DoS and most companies do not have sufficient IT staff to keep patch levels up-to-date, thereby allowing even kno0wn vulnerabilities to remain exposed. Security is a moving target-it is physically impossible for any organizations tom monitor, analyze threats, manage, and act upon them on a 24*7*365 basis. Signature, patches, and DAT files must be updated regularly to: eliminate false positives, eliminates vulnerabilities, and ensure detection of the latest intrusions and exploits.

- These tasks are not just time consuming but also require highly skilled security analysts who must stay apprised of any new threats and techniques. In addition to being expensive and often ineffective, providing constant vigilance in-house is a very management intensive exercise and can distract an organization from its core business.

- Enforcing the security posture of the organizations is a big challenge. Many organizations today have well-written security policies and procedures but they are not implemented and enforced properly. While a lot of this is related to people and processes, it is equally important to enforce these policies through use of technology.

- Building and sustaining high-quality resources for deploying and efficiently managing network security infrastructure.

- Managing the day-to-day network security operations and troubleshooting can be very daunting as well. Therefore, it is important to adopt technologies that are easy and cost effective to deploy and maintain in the long run.

- ❖ Ensuring a fully secure networking environment without degradation I the performance of business applications On a day-today basis, enterprises face the challenge of having to scale up their infrastructure to a rapidly increasing user group, both from within and outside of the organizations. At the same time, they also have to ensure that performance is not compromised.

- Enterprise sometimes has deal with the number of point products in the network. Securing all of them totally while ensuring seamless functionality is one of the biggest challenges they face while planning and implementing a security blueprint.

- Conceptualizing and implementing a security blueprint is a challenge. Security is an amalgamation of people, processes, and technologies; while IT managers are traditionally tuned to address only the technology controls.

- Security cuts across all functions and hence initiative and understanding at the top is essential. Security is also crucial at the grassroots level as your security is as good as the weakest link. Employee awareness becomes a big concern. Management Skepticism is a sure spoilsport.

- Keeping abreast of the various options and the fragmented market is a challenge for all IT mangers. In the security space, the operational phase assumes a bigger importance.

- Compliance also plays an active role in security; hence the business development team, finance, and the CEO office have to matrix with IT to deliver BLUEPRINT.

WHAT ENTERPRISE MUST DO?

- Enterprises should be prepared to copy with the growth of the organization, which in turn would entail new enhancement in the network both in terms of applications and size. They should plan security according to the changing requirements, which may grow to include various factors like remote and third-party access.

- Threats are no longer focused on network layer; application layer is the new playground of Hackers. Attack protection solution must protect network, service and application provide secure office connection, secure remote employee access, resilient network availability, and controllable internet access.

    - Conventional security products are not the ideal solution to internal security challenges. Internal security solutions must contain the threats (like WORMS), compartmentalize the network, not disturb legitimate traffic, protect the desktop, protect the server and secure the data center. About 90% of new attackers target Web-enabled application and their number is growing. Enterprises should, therefore, deploy web-security solution that provide secure Web access as well as protect web server applications. The security solutions must be easy to deploy, and they should also provide integrated access control

TECHNOLOGY OPTIONS

- **END-to-END SECURITY SOLUTIONS:** Leading security vendors offer end-to-end solution that claim to take care all aspect of network security. End-to-End solution usually offer a combination of hardware and software platforms including a security management solution that perform multiple function and take care of the entire gamut of security on a network. An integrated solution is one that encompasses not only a point-security problem (like WORMS/intrusion) but one that also handles a variety of network and application layer security challenges

- **ASIC based appliances: The** move is from software-based security products that run on open platforms to purpose-built, ASIC-based appliance, just like the path the routers have followed in the last decade.

- **SSL-VPN:** Greater awareness of encryption on the wire in the form SSL and IP-VPNs. People are increasingly aware of the security risks in transmitting data over the wire in clear text. To address this, SSL-VPN has acceptance of VPNs for end users and IT department alike.

9. Explain in detail about Electronic Cash And Electronic Payment Schemes (Nov 2012)

INTRODUCTION

- For Many Years Internet was just a place browser for information, but with a growing numbers of consumers getting access to the internet each and every day, business are beginning to accept the internet as a visible medium through which to market and sell products and services.

- Because of this, the business purposes they introduced the Electronic Cash and Electronic Payment Schemes. This plays a vital role to all kind of business and it reduce the time of both consumer as well as Company. Here both consumer and merchants must be able to identify and trust one another, prevent transmitted financial information from being tamped with, and easily complete transaction with any valid party.

- Some merchants have discovered that so far too many credit card numbers used by would-be buyers were canceled, stolen, over the limit, or just plain fictitious. These merchants need to find a way to reduce the number of bad numbers they are receiving.

- For this they implement two ways, That is,

    1. Account Based
    2. On-Line Electronic Cash

ACCOUNT BASED

❖ This Transaction may be equated to Credit cards, prepaid cards, ATM cards, Checking Accounts, or any type of financial medium where an account must be verified before a monetary transaction occurs.

ON-LINE ELECTRONIC CASH

❖ Beyond the account-based transaction is the concept of On-Line Electronic Cash

10. Explain in detail about Internet Monetary Payment And Security Requirement(Apr 2014)

❖ For consumers and merchants to be able to trust one another, prevent transmitted payment information from being tempered with, and complete transaction with any valid party, the following issues need to be addressed:

- Confidentiality of payment information
- Payment Information Integrity
- Account Holder and merchant Authentication
- Interoperability

CONFIDENTIALITY OF PAYMENT INFORMATION

❖ Payment information must be secure as it travels across the internet. Without Security, Payment information could be picked up by hackers at router, communication-line or host level, possibly resulting in the production of counterfeit cards of fraudulent transaction. To provide security, account information and payment information will need to be encrypted. This technology has been around for decades. Cryptography protests sensitive information by encrypting it using number theoretic algorithms parameterized on keys (bit string). The

resulting hypertext can then be transmitted to receiving party that decrypts the message using a specific key to extract the original information. There are two encryption methods used: symmetric cryptography and asymmetric cryptography.

❖ Symmetric cryptography, or more commonly called secret-key cryptography, uses the same key to encrypt and decrypt a message. Thus, a sender and receiver of a message must hold the same secret or key confidentially. A commonly used secret-key algorithm is the Data

Encryption Standard (DES). See Fig. Asymmetric cryptography, or public-key cryptography, uses two distinct keys: a public and a private key.

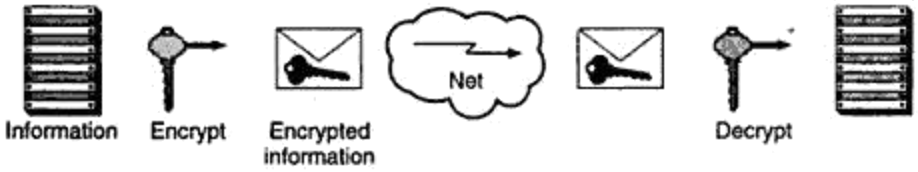


Fig: Symmetric/Secret key Cryptography

❖ Data encrypted using the public key can only be decrypted using the corresponding private key. This allows multiple senders to encrypt information using a public key and send it securely to a receiver, who uses the private key to decrypt it. The assurance of security is dependent on the receiver protecting the private key. See below fig.

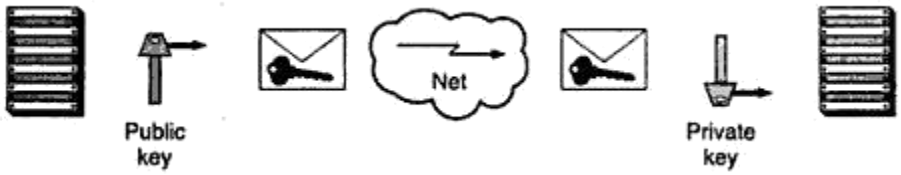


Fig: Asymmetric/Secret key Cryptography

❖ For merchants to use secret-key cryptography, they would each have to administer individual secret key to all their customers and provide these keys through some secure channel. This approach is complex form an administrative perspective. The approach of creating key pair using public key cryptography and publishing the public key is easier. This would allow customers to send secure payment information to merchants by simply efficiency, public-key cryptography a be used with secret-key cryptography without creating a cumbersome process

for the merchant. To institute; this process, the customer corresponding DES key is then encrypted using the public key of the merchant. To decrypt the payment information, the merchant first decrypts the DES key then uses the DSE key to decrypt the decrypt the payment information see fig

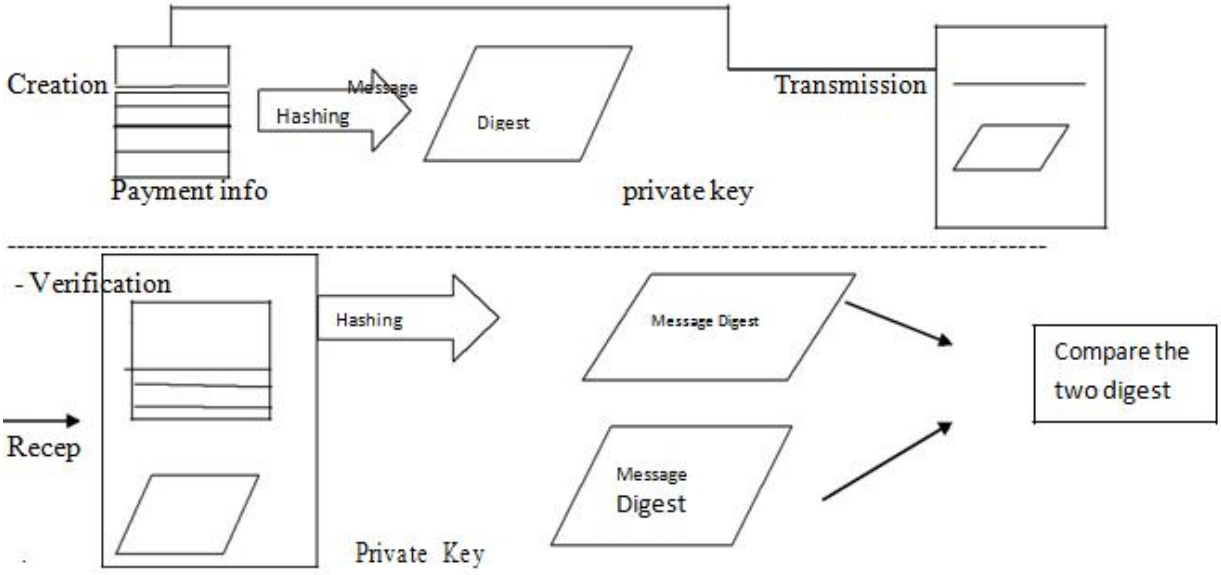
PAYMENT INFORMATION INTEGRITY (11.Explain in detail about Payment information integrity)

❖ Payment information sent from consumers to merchants includes order information, personal data, and payment instructions. If any piece of the information is modified, the transaction may no longer be accurate. To eliminate this possible source of error or fraud, an, arithmetic algorithm called hashing, along with the concept of digital signatures is employed. The hash algorithm generated is called a hash value or message di9gest. A helpful way to view a hash algorithm is as a one-way public cipher, in that:

- It has no secret key
- Given a message digest, there is no way to reproduce the original information.
- It is impossible to hash other data with the same value.

❖ To ensure integrity, the message digest is transmitted with the payment information. The receiver would then validate the message digest by once payment information is received. If the message digest does not the some value sent. The payment information is assumed to be corrupted is therefore Discarded. The hash algorithm however is the public information, therefore anyone may be able to alter the data and recalculate a new "correct" message digest to rectify the situation, the message digest is encrypted using a private key of the sender (customer). This encryption of the moving digest is called a digital signature. See Fig.

❖ Because a digital signature is created by using public-key cryptography, it is possible to identify the sender of the payment information. Since the encryption is done by using the private key of a public/private key pair, this means only the owner of that private key can encrypt the message digest calculated by the receiver, then the payment information could not have come from anyone but the owner of the private key.



Digital Signature

Note that the roles of the public/private key pair in the digital signature process are the reverse of that used in ensuring information confidentiality. In the digital signature process, the private key is used to encrypt (sign) the information and the public key is used to decrypt (verify the signature).

ACCOUNT HOLDER AND MERCHANT AUTHENTICATION(12.Describe Account Holder And Merchant Authentication)

❖ Similar to the way card accounts are stolen and used today, it is possible for a person to use a stolen account and try to initiate an electronic commerce transaction. To protect against this, a process that links a valid account to a customers digital signature needs to be established.

❖ In any instance, the best way for a third party to validate the public key and account is by issuing the items to the customer together under the digital signature of the third party. Merchants would then decrypt the public key of the customer (using the public key of the third party) and, by definition of public-key cryptography, validate the public key and account of the customer. For the preceding to transpire, however, the following is assumed:

- The public key(s) of the third party(ies) is widely distributed.
- The public key(s) of the third party(ies) is highly trusted on face value.

- The third party (ies) issue public keys and account after receiving some proffer of an individual‟s identity.

❖ So far, it has been assumed that error or fraud takes place only on the customer end of payment information transport. However the possibility exits that a fraud agent may try and pose as a merchant for the purpose of gathering account information to be used in a criminal manner in the future.

❖ To combat this fraud, the same third party process is used for merchants. For a merchant to be valid, the merchant‟s public key would need to be issued by a third party under the third party‟s digital signature. Customers would then decrypt the public key of the merchant, using the public key of the third party. Again, for this process to occur, the assumption previously identified would apply.

INTEROPERABILITY

❖ For E-commerce to take place, customers (acc holders) must be able to communicate with any merchant. For this reason, Security and process standards must support any hardware or software platform that a customer or merchant may use and have no preference over another.

❖ Interoperability is then achieved by using a particular set of publicity announced algorithms and process in support of E-commerce. The rest will assume that these algorithms and processes are in place and are being utilized.

13.Describe Payment And Purchase Order Process? (Apr 2013) (Apr 2014)

- Account holder Registration
- Merchant Registration
- Account Holder (Customer) ordering
- Payment Authorization

ACCOUNT HOLDER REGISTRATION

❖ Account holders must register with a third party(TP)that corresponds to a particular Account type in fore they can impact with any maximum in order creator the account Holder must have a copy of the TP‟s public key of the public/private key set. The manner in which the account holder receives the public key could be through various methods such as e-mail, web-page download, disk, or flashcard .once the account holder receives the public key of the TP. The registration process can be to register his or her account for internet use. To register, the account holder will most likely be required to fill out a form requesting

information such as name, address, account number, and other identifying personal information. When the form is completed. The account holder‟s software will do the following

- Create and attach the account holder‟s public key to the from
- Generate a message digest form the information
- Encrypt the information and message digest using a secret key
- Encrypt the secret key using the TP‟s public key
- Transmit all items to the TP

When the TP receives the account holder‟s request, it does the following

- Decrypts the secret key
- Decrypts the information, message digest, account holder public key
- Computes and compares message digests

❖ Assume the message digests compute to the same value, the TP would continue the verification process using the account and personal information provided by the requesting account holder. It is assumed the TP would use it existing verification capabilities in processing personal information. If the information in the registration is verified the TP certifies the account holder‟s public key and other pertinent account information by digitally singing it with the private key. The certified documentation is then encrypted with the account holder‟s public key. The emis Response is then transmit to the customer.

❖ Upon receipt of the TP‟s response the account holder‟s software would necessary decryption to emblem is certified documentation the created documentation would be held by the account holder‟s software for future use in electronic commerce transaction.

MERCHANT REGISTRATION

❖ Merchant must register with TP‟s that correspond to particular account types that they wish to honor before transacting business with customer who share the same account types. For example, if a merchant wishes to accept visa and master card, that merchant may have to register with two TP‟s or find a TP that represents both. The merchant register is

similar to the account holder‟s registration process. Once merchant information is validated, certified

documentation (CD) is transmitted to the merchant from the TP(s). The certified documentation is then stored to the merchant‟s computer for future use in electronic transactions.

ACCOUNT HOLDER (CUSTOMER) ORDERING

- To send a message to a merchant the customer (account holder) must have a copy of the merchant‟s public key a copy of the TP s public key that corresponds to the account type to be used. The order process starts when the merchants send a copy of its CD to the customer. At some point prior to sending the CD, the merchants must request the customer to specify what type of account will be used so that the appropriate CD will be sent. After receipt of the appropriate merchant CD, the customer software verifies the CD by applying the TP‟s public key, thus verifying the digital signature of the TP. The software then holds the merchant‟s CD to be used later in the ordering process at this points the customer is allowed to shop in the online environment provided by the merchant.

- After shopping, customer fills out an order form that lists the quantity, description and price of the goods and service they wish to receive. once the order form is completed the customer software does the following

1. Encrypts account information with the TP‟S public key.
2. Attaches encrypted account information to the order form.
3. Create a message digest of the order form and digitally signs it with the customer private key.
4. Encrypts the following with the secret key: order form (with encrypted account information), digital signature and customers CD-ROM.
5. Encrypts secrets key with the merchant‟s public key from the merchant‟s cd.
6. Transmits the secret key encrypted message and encrypted secret key to the merchants.

When the merchant software receives the order, it does the following:

1. Decrypts the secret key using the private key of the merchant.
2. Decrypts the order form, digital signature, and customer‟s cd using the secret key.
3. Decrypts the message digest using the customers public key obtained from the customers cd(and thus verifies the digital signature of customer).

4. Calculates the message digest from the order form and compares with the customers decrypted message digest.

❖ Assuming that the message digests math, the merchant continues processing the order according to its own pre established order fulfillment processes. One part of the order process however, will include payment authorization which is discussed in the next section. After the order as been processed , the merchant‟s host should generate an order confirmation or receipt of purchase notifying the customer that the order has been processed this receipt also serves as a proof of purchase equivalent to a paper receipt as currently received in stores. The way in which a customer receives the electronic receipt is similar to the encryption and digital signature processes previously described.

Payment authorization:

❖ During the processing of an order, the merchant will need to authorize the transaction with the TP responsible for the particular account. This authorization assures the merchant that the necessary funds or credit limit is available to cover the cost of the order. Also note that the merchant as no access to the customer‟s account information since it was encrypted using the TP‟S public key thus, it is required that this information be sent to the TP so the merchant can receive payment authorization from the TP and that the proper customer account is debited for the transaction. It is assumed that the eventual fund transfer from some financial institution to the merchant and the debit transaction to the customer account takes places through an existing an pre established financial process.

❖ In requesting payment authorization, the merchant software will send the TP the following information using encryption and the digital signature processes previously described.

- Merchant‟s cd
- Specific order information such as amount to the authorized, order number , date.
- Customer‟s cd.
- Customer‟s account information.

After verifying the merchant, customer and account information, the tp would then analyze the amount to be authorized. Should the amount meet some established criterion, the TP would sent authorization information back to the merchant? Again, the way this information would be sent in similar to the encryption and digital signature processes previously described

14.Describe in detail about online electronic cash.

E-cash works in the following way:

- A consumer opens an account with an appropriate bank. The consumer shows the bank some form of identification so that the bank knows who the consumer is, when cash is withdrawn, the consumer goes directly to the bank or accesses the bank through the internet and present proof of indent.
- Once the proof is verified, the bank gives the consumer some amount of e-cash. The e-cash is the stored on a PC‟s hard drive or possibly a PCMCIA card for later use.

- Problems with simple Electronic cash
- Creating Electronic Cash Anonymity
- Preventing Double spending
- E-cash Interoperability
- Electronic payment schemes

PROBLEMS WITH SIMPLE ELECTRONICCASH:

- A problem with the e-cash example just discussed is that double spending cannot be detected or prevented, since all cash would look the same. Both the bank and merchant must check the serial number each and every transaction correctly.
- Beyond the prevention of double-spending, e-cash with serial number is still missing a very important characteristic associated with real cash it is not anonymous. When the bank sees e-cash from a merchant with a certain serial number, it can trace back to the consumer who spent it and possibly deduce purchasing habits. This frustrates the nature of privacy associated with real cash.

CREATING ELECTRONIC CASH ANONYMITY:

- To allow anonymity, the bank and the consumer collectively create the e-cash and associated serial number, whereby the bank can digitally sign and thus verify the e-cash,

but not recognize it as coming from a particular consumer. To do this requires a complicated algorithm on behalf of the consumer or consumer‟s software.

- That is, instead of sending the generated serial number to the bank, however, the consumer applies a multiplier algorithm to the serial number and sends the new multiplied serial number to the bank. The multiplier is also a randomly generated number.

- When the bank receives the multiplied serial number, it digitally signs it with its private key and sends it back to the consumer. The bank never knows what the original serial number or the multiplier used digital signature of the bank. The double spending is prevented only by using two-part lock. The encrypted identity and encrypted secret key is attached to the e-cash. The property of the two-part lock is such that if the e-cash is double spent, the two parts of the lock are opened revealing the secrete key, and thus the identity of the individual who double-spent the cash.

E-CASH INTEROPERABILITY:

- Consumers must be able to transact with any merchant or bank. Hence, process and security standards must exist for all hardware and software used in e-cash transactions. Interoperability can only be achieved by adherence to algorithms and processes in support of e-cash-initiated commerce. Since e-cash it theory, can become the near equivalent of real cash, e-cash takes on many of the same economy driving properties.

- Because of this, it would seem necessary for some government control over e-cash transactions and the process and security standards associated with them. **While only a single bank is mentioned in the e-cash** examples, it is likely that the bank becomes a network of banks under the direct control of the Federal Reserve or similar institution outside of the United States.

ELECTRONIC PAYMENT SCHEMES:

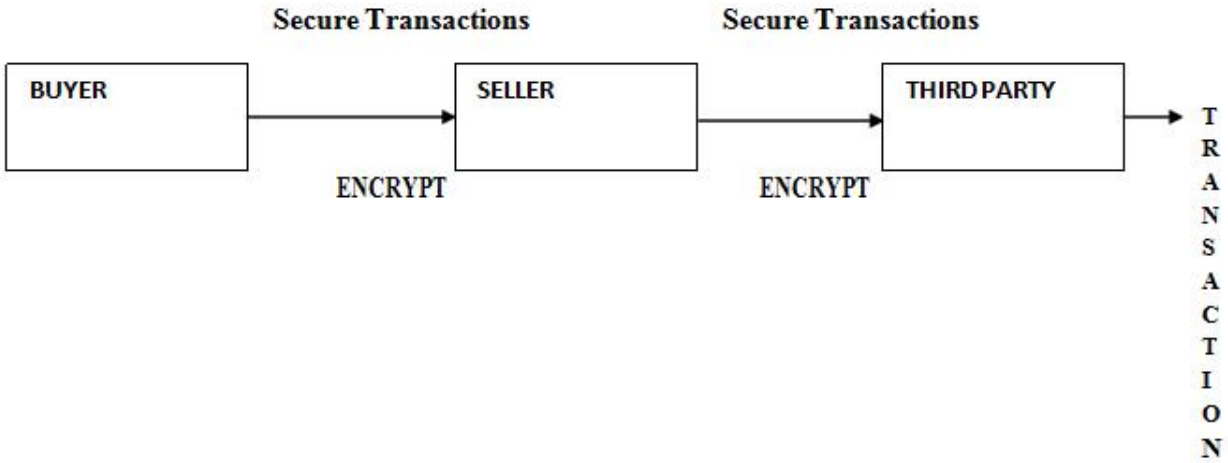
Some of the commercial electronic payment schemes that have been proposed in the past few years are,

- **Netscape**
- **Microsoft**
- **Check free**
- **Cyber cash**
- **Verisign**
- **Digicash**

- **First virtual holdings**
- **Commerce net**
- **Net cash**
- **Joint electronic payment initiative (JEPI)**

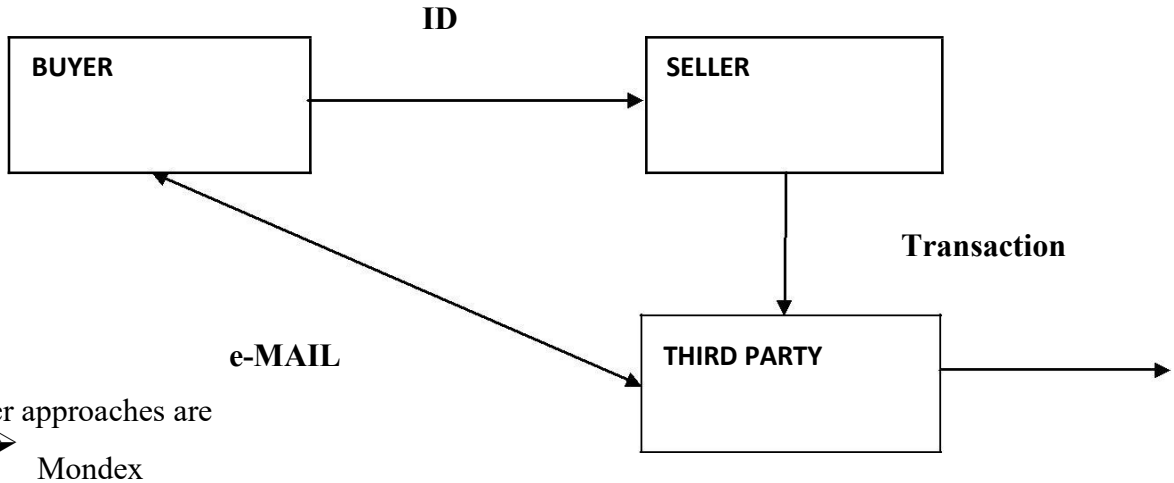
Cyber cash:

❖ This combines features from checks and cash. It is a digital cash software system which is used like a money order payment. It provides a secure solution for sending credit card information across the internet.



First virtual holdings:

❖ It is targeting individuals and small businesses that want to buy and sell on the internet.



Other approaches are

- Mondex
- Netmarket
- Open market
- Global on line

- Click share corporation

15. Explain Secure Electronic Payment protocol(SEPP)

3.4 Secure Electronic Payment Protocol (SEPP)

IBM, Netscape, GTE, CyberCash, and MasterCard have cooperatively developed SEPP—an open, vendor-neutral, nonproprietary, license-free specification for securing on-line transactions. Many of its concepts were rolled into SET (http://www.mastercard.com/set/set.htm# Windows), which is expected to become the de facto standard. Because of its development importance, SEPP is discussed briefly in this section.

There are several major business requirements addressed by SEPP:

1. To enable confidentiality of payment information
2. To ensure integrity of all payment data transmitted
3. To provide authentication that a cardholder is the legitimate owner of a card account
4. To provide authentication that a merchant can accept MasterCard-branded card payments with an acquiring member financial institution

SEPP is the electronic equivalent of the paper charge slip, signature, and submission process. SEPP takes input from the negotiation process (payment amount, order description, payment method, etc.) and causes the payment to happen via a three-way communication among the cardholder, merchant, and acquirer.[19,31] SEPP only addresses the payment process; privacy of nonfinancial data is not addressed in the SEPP protocol—hence, it is suggested that all SEPP communication be protected with encryption at a lower layer, such as with Netscape's SSL. Negotiation and delivery are also left to other protocols.[19,31]

SEPP features have been folded into SET, as discussed in Chap. 6, with the collaboration of Microsoft and Visa.

3.4.1 SEPP process

SEPP assumes that the cardholder and merchant have been communicating in order to negotiate terms of a purchase and generate an order. These processes may be conducted via a WWW browser; alternatively,

this operation may be performed through the use of electronic mail, via the user's review of a paper or CD-ROM catalog or other mechanisms. SEPP is designed to support transaction activity exchanged in both interactive (on-line) and noninteractive (off-line) modes.[12–18]

The SEPP system is composed of a collection of elements involved in electronic commerce (see Fig. 3.1):[31]

- *Cardholder.* This is an authorized holder of a bankcard supported by an issuer and registered to perform electronic commerce.
- *Merchant.* This is a merchant of goods, services, and/or e-products who accepts payment for them electronically and may provide selling services and/or electronic delivery of items for sale (e.g., e-products).
- *Acquirer.* This is a (MasterCard member) financial institution that supports merchants by providing service for processing credit-card-based transactions.
- *Certificate management system.* This is an agent of one or mor bankcard associations that provides for the creation and distributio of electronic certificates for merchants, acquirers, and cardholders.

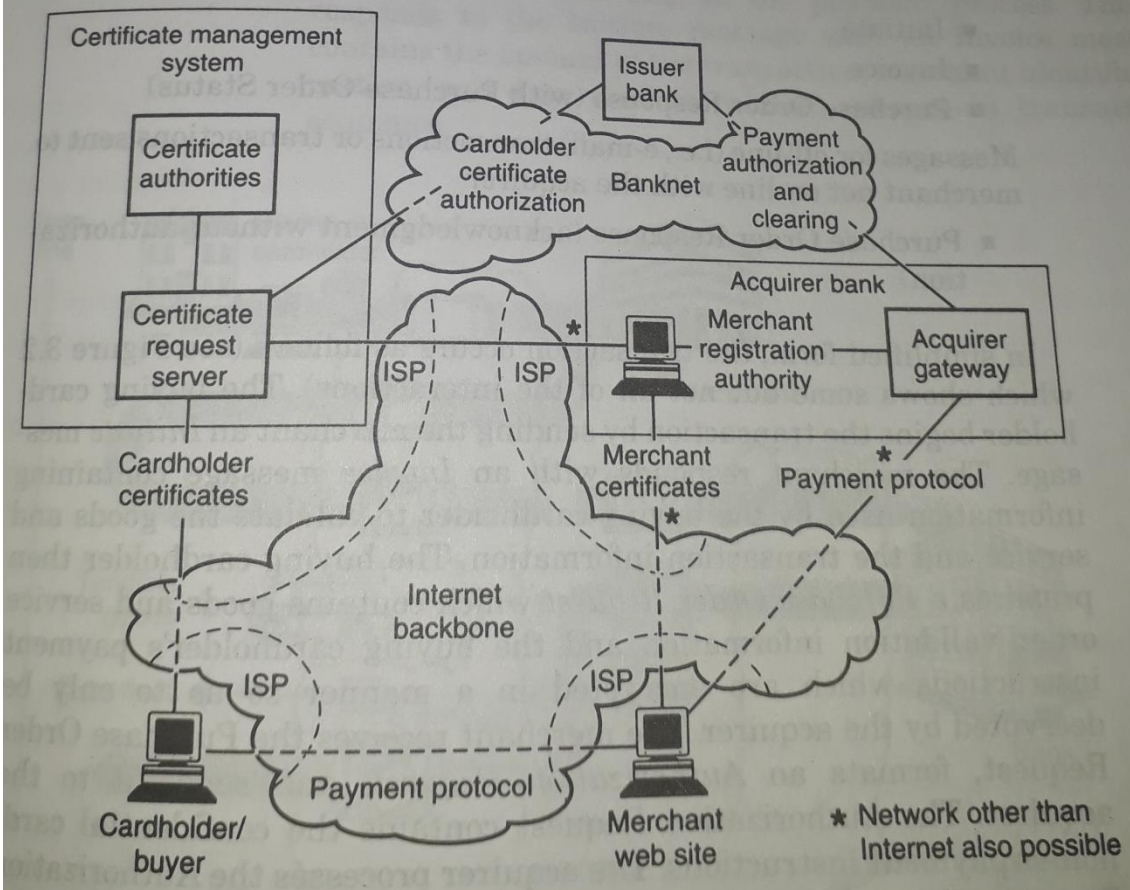


Figure 3.1 SEPP architecture.

- *Banknet.* This represents the existing network which interfaces acquirers, issuers, and (now) the certificate management system.

These elements for Web commerce exist today and interact through existing mechanisms, with the exception of the certificate management system. In the SEPP systems, these components acquire expanded roles to complement existing functionality into the electronic commerce context.

Several basic transaction messages are required in a SEPP-based environment; when variations to the canonical flow occur, additional data will be required in the supplementary messages (see the following list).

Messages for SEPP-compliant processing of payment transactions

- Purchase Order Request
- Authorization Request
- Authorization Response
- Purchase Order Inquiry
- Purchase Order Inquiry Response

Additional messages for on-line customer

- Initiate
- Invoice
- Purchase Order Response (with Purchase Order Status)

Messages for off-line (i.e., e-mail) transactions or transactions sent to merchant not on-line with the acquirer

- Purchase Order Response (acknowledgment without authorization)

In simplified form, the transaction occurs as follows (see Figure 3.2 which shows some but not all of the interactions). The buying cardholder begins the transaction by sending the merchant an *Initiate* message. The merchant responds with an *Invoice* message containing information used by the buying cardholder to validate the goods and service and the transaction information. The buying cardholder then prepares a *Purchase Order Request* which contains goods and service order validation information and the buying cardholder's payment instructions which are encrypted in a manner so as to only be decrypted by the acquirer. The merchant receives the Purchase Order Request, formats an *Authorization Request*, and sends it to the acquirer. The Authorization Request contains the confidential cardholder payment instructions. The acquirer processes the Authorization Request. The acquirer then responds to the merchant with an *Autho-*

rization Response. The merchant will respond to the buying cardholder with a *Purchase Order Response* if a Purchase Order Response message was not previously sent. At a later time, the buying cardholder may initiate a *Purchase Order Inquiry* (this transaction is used to request order status from the merchant) to which the merchant will respond with a *Purchase Order Inquiry Response.*[12–18,31]

The process of shopping is merchant-specific. The process of transaction capture, clearing, and settlement of the transaction is defined by the relationship between the merchant and the acquirer. In certain scenarios (e.g., shopping via a browser/electronic mall), the buying cardholder may have already specified the goods and services before sending a Purchase Order Request message. In other scenarios (e.g., merchandise selection from paper or CD-ROM-based catalogs), the order may be placed with the payment instructions in the Purchase Order Request message.

In an interactive environment, SEPP activities start when the buying cardholder sends a message to the merchant indicating an initiation of a SEPP payment session. This message is referred to as an Initiate message; it is used to request that the merchant prepare an invoice as the first step in the payment process. The merchant responds to the Initiate message with an Invoice message which contains the amount of the transaction, merchant identification information, and data used to validate subsequent transactions in the sequence.

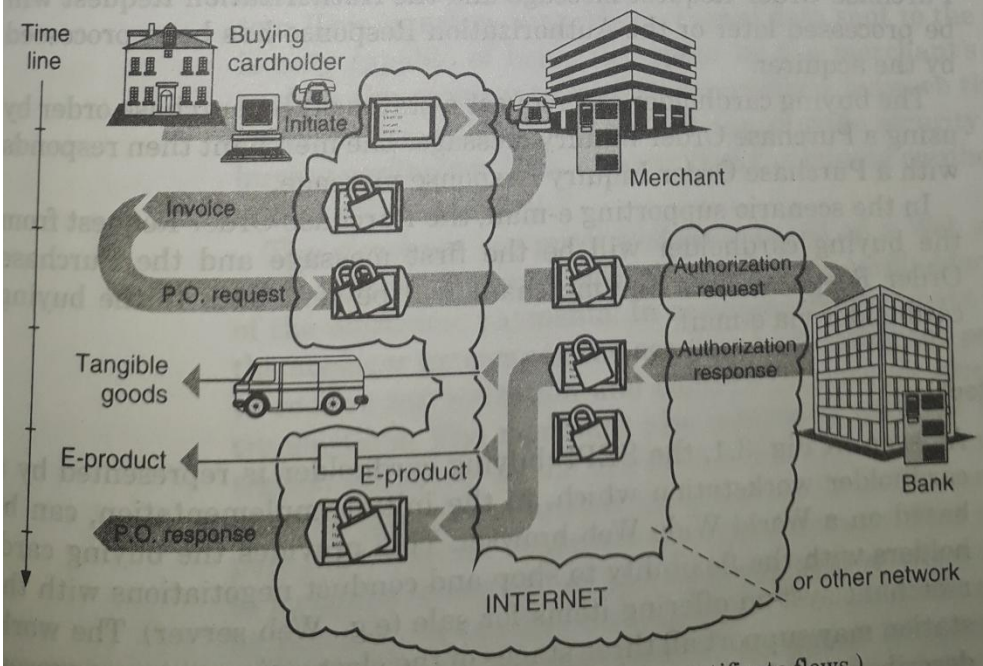


Figure 3.2 Simplified SEPP process. (Note: Does not show certificate flows.)

The next transaction is initiated by the buying cardholder. The transaction is the Purchase Order Request. This message contains the payment instructions of the buying cardholder. This information is protected in such a manner as to provide a high level of confidentiality and integrity. The payment instructions are encrypted so that they can only be read by the acquirer.

The merchant sends an Authorization Request to the acquirer. The acquirer performs the following tasks:[12–18,31]

- Authenticates the merchant
- Verifies the acquirer/merchant relationship
- Decrypts the payment instructions from the buying cardholder
- Validates that the buying cardholder certificate matches the account number used in the purchase
- Validates consistency between merchant's authorization request and the cardholder's payment instruction data
- Formats a standard authorization request to the issuer and receives the response
- Responds to the merchant with a validated authorization request response

The merchant responds to the buying cardholder with a Purchase Order Response indicating that either the merchant has received the Purchase Order Request message and the Authorization Request will be processed later or the Authorization Response has been processed by the acquirer.

The buying cardholder can request a status of the purchase order by using a Purchase Order Inquiry message. The merchant then responds with a Purchase Order Inquiry Response message.

In the scenario supporting e-mail, the Purchase Order Request from the buying cardholder will be the first message and the Purchase Order Response from the merchant will be sent back to the buying cardholder via e-mail.

3.4.2 SEPP architecture

As seen in Fig. 3.1, the SEPP buying cardholder is represented by a cardholder workstation which, in the initial implementation, can be based on a World Wide Web browser. This provides the buying cardholders with the flexibility to shop and conduct negotiations with the merchant system offering items for sale (e.g., Web server). The workstation may support all three stages of the electronic commerce process described in the previous section.[12–18,31] Two designs of cardholder

workstations are supported. Integrated electronic commerce workstations include WWW browsers that have been designed to support electronic payments in an integrated fashion. As an alternative design, "bolt-on" payment software may be provided alongside an independent browser to implement the payment process. The protocols have been designed to ensure that such independent software may be invoked from the browser at the appropriate times by particular data elements in the protocol exchange. Off-line operation using e-mail or other non-interactive payment transactions are also supported by the protocol. Functions added to traditional WWW browsers to support electronic payments include encryption and decryption of payment data, certificate management and authentication, and support for electronic payment protocols.[12–18]

To obtain a certificate, the buying cardholder's PC software interfaces with the certificate request server in the certificate management system. The certificate management system generates the certificates needed to identify the buying cardholder. The interface to the certificate request server is based on HTTP interactions; the certificate request server includes a WWW server to which the buying cardholder interfaces.

As noted in Fig. 3.1, the buying cardholder's second and primary interface is with the merchant system. This interface supports the buying cardholder's segment of the payment protocol, which enables the buying cardholder to initiate payment, perform inquiries, and receive order acknowledgment and status. The buying cardholder also has an indirect interface to the acquirer gateway through the merchant system. This interface supports encrypted data sent to the merchant that is only capable of being decrypted by the merchant's acquirer. This enables the acquirer to mediate interactions between the buying cardholder and merchant, and by so doing, provide security services to the buying cardholder. This ensures that the buying cardholder is dealing with a valid merchant.[31]

The merchant computer system is based on a Web server that provides a convenient interface with the buying cardholder for the support of the electronic payments. In addition, the merchant interfaces with the acquirer gateway in the acquirer bank using the payment protocol to receive authorization and capture services for electronic payment transactions. The merchant also interfaces with the merchant registration authority in the acquirer bank. This is the interface through which a merchant requests and receives its public certificates to support the electronic commerce security functions. This interface may be to a computerized server; alternatively, this interface and service may be provided by manual means. The merchant needs to support SEPP protocols for the capture and authorization of electronic commerce

PONDICHERRY UNIVERSITY QUESTIONS

2 MARKS

1. What is SET? **(Apr 2013) (Ref.Qn.No.7)**
2. State the problems with traditional payment system.**(Apr 2013) (Ref.Qn.No.23)**
3. List the various Secure Transport Protocols. **(Nov 2012) (Ref.Qn.No.3)**
4. What are the transactions/processes that must occur for an electronic payment? **(Nov 2012) (Ref.Qn.No.21)**
5. Mention the goals of computer security. **(Apr 2012) (Ref.Qn.No.1)**
6. What does the term symmetric cryptography means? **(Apr 2012) (Ref.Qn.No.29)**
7. Define the term Electronic Cash interoperability. (**Apr 2014) (Ref.Qn.No.16)**
8. Properties of Electronic Payment Schemes.(**Apr 2014) (Ref.Qn.No.19)**
9. What is secure Transport Protocol? (**Nov 2014) (Ref.Qn.No.3)**
10. How do you change plain text to cipher text? (**Nov 2014) (Ref.Qn.No.30)**
11. What is meant by authentication? (**Apr 2015) (Ref.Qn.No.31)**
12. What is secure transport layer? (**Apr 2015) (Ref.Qn.No.32)**

11 MARKS

1. Discuss about how to carry out secured transaction in e-commerce. **(Apr 2013) (Ref.Qn.No.4)**
2. Explain about payment and purchase order process. **(Apr 2013)(Apr 2014)) (Ref.Qn.No.10)**
3. Describe in detail the Secure Electronic Payment Protocol. **(Nov 2012) (Ref.Qn.No.4 & 5)**
4. Discuss briefly the various the Electronic Payment Schemes. **(Nov 2012/ Nov 2014) (Ref.Qn.No.9)**
5. State and Illustrate the usage of Secure transport protocols. **(Apr 2012) (Ref.Qn.No.2)**
6. Discuss the basics of Electronic payment and purchase order process. **(Apr 2012) (Ref.Qn.No.13)**
7. Discuss about Internet monetary payment and security requirements**(Apr 2014) (Ref.Qn.No.13)**
8. Briefly Explain the secure Electronic Transaction SET**(Nov2014)(Apr 2015) (Ref.Qn.No.5)**
9. Illustrate on the electronic payment techniques in detail.**(Apr 2015) (Ref.Qn.No.9)**

UNIT III

Internet/Intranet Security Issues and Solutions: The need for Computer Security – Specific Intruder Approaches – Security strategies – Security tools – Encryption – Enterprise Networking and Access to the Internet – Antivirus programs – Security Teams.

2 MARKS

1. What is meant by File transfer?

- Using FTP and HTTP, users can request and send a variety of bulk data including databases, files in all formats, documents, software, images and voice.
- While useful and convenient, file transfer can be insecure both in terms of confidentiality and virus threats.

2. Define IP Spooling(Apr 2014)

- IP spooling is a technique that can lead to root access on a system.
- It is the tool that intruders often use to take over open terminal and login connections after they get root access.
- Because of IP spooling, no address-based authentication is possible.

3. Define Password guessing:

- Most host administrators have improved their password controls, but group accounts still abound, and password-dictionary and password-cracking programs can easily crack at least 10 percent of the passwords users choose.
- The deterrent is enforcement of good passwords

4. Describe about Password sniffing:

- CERT estimates that, in 1994, thousands of systems were the victims of password sniffers.
- On LANs, any internal machine on the network can see the traffic for every machine on that network.
- Sniffer programs exploit this characteristic, monitoring all IP traffic and capturing the first 128 bytes or so of every encrypted FTP or Telnet session.
- The deterrent is to utilize programs that provide on-time passwords.

5. What is meant by Telnet: (Apr 2014)

- Telnet enables users to log on to remote computers.
- Telnet does little to detect and protect against unauthorized access.

- Telnet is generally supported either by using an application gateway or by configuring a router to permit outgoing connection using something such as the established screening rules.

6. Discuss about Viruses: (Nov 2012)

- Viruses do not necessarily give intruders access to a computer system, but may be a way to copy and forward information or otherwise create denial-of-service problems
- A virus is a program that can infect other programs by modifying them to include a copy of itself.

7. Lists of various computer virus infractions:

- Alter data in files.
- Change disk assignments.
- Create bad sectors.
- Decrease free space on disk.
- Destroy FAT (FILE Allocation Table).
- Erase specific programs.
- Format specific programs
- Hang the system.
- Overwrite disk directory.
- Suppress execution of RAM resident programs.
- Write a volume label on the disk.

8. Define SATAN:

- SATAN (Security Administrator Tool for Analyzing Networks) is a vulnerability detection application designed to hack into Internet-connected hosts.
- It is a UNIX program that checks both local and remote hosts for vulnerabilities.
- SATAN is a program freely available via the Internet.

9. List out the various Components of SATAN:

- HTTP server that acts as dedicated SATAN Web server.
- Magic cookie generator that generates a unique 32-bit magic cookie that includes a session key.
- Policy engine that defines which hosts are allowed to be probed and to what degree.
- Target acquisition that decides exactly which probes to run on various hosts when performing data acquisition.
- Data acquisition to gather security-related facts about the targeted hosts.
- Inference engine that is driven by a set of rule bases and input from data acquisition.

- Report and analysis, based on its findings.

10. What is meant by Encrypted data:

- Encrypted data is binary data, which cannot be sent by standard electronic mail.
- The ASCII Armor encoding actually uses four ASCII characters to represent three binary characters.

11. Discuss about Standard file extensions

- .txt- is attached to files created by a text editor or word processor before the file is encrypted.
- .pgp- is attached to an encrypted binary file. It is also used for key rings.
- .asc- is attached to an ASCII-armored encrypted file.
- .bin-is created when you use PGP's key-generate option.

12. Define Anti-virus software: (Nov 2014)

It consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

13. What is meant by Encryption:

- Encryption is used to protect the message from the eyes of others.
- Cryptographically secure ciphers are designed to make any practical attempt of breaking infeasible.
- Symmetric-key ciphers are suitable for bulk encryption using shared keys, and public-key encryption using digital certificates can provide a practical solution for the problem of securely communicating when no key is shared in advance.

14. Define Firewalls:

Firewalls are systems that help protect computers and computer networks from attack and subsequent intrusion by restricting the network traffic that can pass through them, based on a set of system administrator-defined rules.

15. Define Honey pots:

Honey pots are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.

16. What is meant by Intrusion-detection systems: (Apr 2013)

Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.

17. Define Pinging

The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer, they can try a port scan to detect and attack services on that computer.

18. Discuss about Social engineering

Social engineering awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.

19. Define S-HTTP

- S-HTTP is an extension of HTTP that provides a variety of security enhancements for the web.
- S-HTTP provides independently application security services for transaction confidentiality, authenticity/ integrity, and non-reputability of origin.

20. Define Secure Socket Layer (SSL)

- It is a transport layer security technique that can be applied to HTTP as well as to other TCP/IP-based protocols.
- The SSL protocol is designed to provide privacy between two communicating applications.

21. Define Electronic data interchange (EDI)

- EDI is defined as the inter-organization exchange of documents in standardized electronic form directly between computer applications.
- The ability to transmit EDI over the Internet has the potential to improve the penetration rate of this technology.

22. Define CERT

- Computer Emergency Response Team is a name given to expert groups that handle computer security incidents.
- The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

23. Define FIRST

- Forum of Incident Response and Security Teams (FIRST) is a collection of organizations modeled on the computer emergency response team idea.
- It is a voluntary umbrella organization that mainly offers help to systems administrators who find their systems under attack from intruders.

24. What are the two types of Anonymous remailers? (Nov 2012)

Anonymous remailers are of two types

1. Remailers that mask the sender's return address
2. Remailers that provide anonymity for both the sender and destination addresses.
   - **Privacy Enhanced Mail**
   - **Pretty Good Privacy**
   - **Multipurpose Mail Extension**

25. Define Network Security? (Apr 2012)

Network Security can be defined as the protection of network-connected resources against unauthorized disclosure, modification, utilization, restriction, incapacitation, or destruction. Hundreds of thousands of system are now connected to the internet. There is no accurate way of measuring the threat that may be launched by an inimical agent.

25. What are called as passive threats? (Apr 2012)

Passive threats involve monitoring the transmission data of an organization. The goal of the attacker is to obtain information that is being transmitted. In general, this is not the easiest task to undertake.

Two types,

- Release of message
- Traffic analysis

26. Difference between visa card and master card.(Nov 2014)

Visa's two levels. Visa offers two levels of benefits: base level and Visa Signature. Most of the company's base-level cards come with auto rental collision damage coverage, extended purchases warranties, unauthorized purchase coverage, emergency assistance and urgent card replacement.

MasterCard's three tiers. MasterCard offers three tiers of benefits: base, World and World Elite.MasterCard offers one notable service that Visa does not: price protection. If you buy an item with a MasterCard and the price is reduced within 60 days, MasterCard will cover the difference, though there are exclusions.

27. Define key and list out the keys.(Apr 2015)

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. In encryption, a key specifies the particular transformation of plaintext

into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

28. What is the use of anti virus software? (Apr 2015)

Antivirus (or anti-virus) software is used to safeguard a computer from malware, including viruses, computer worms, and Trojan horses. Antivirus software may also remove or prevent spyware and adware, along with other forms of malicious programs.

11 MARKS

1. **Explain in detail about internet /intranet security issues and solutions (or) Explain need for computer security (Nov 2014)(Apr 2015)**

NEED FOR COMPUTER SECURITY:

- A debate has taken place over the past decade whether security should be the burden of the host or of the network. To say that security is the responsibility of the internet is surely wrong. Both hosts and networks must be secure; the responsibility is at least equally shared, if not more slanted toward the hosts. Some believe that, pragmatically, given how information is actually hacked today, the major burden lies with the end system.
- Security addressed here relates to three general areas:
    1. Secure file/information transfers, including secure transactions.
    2. Security of information as stored on internet-connected hosts.
    3. Secure enterprise networks, when used to support web commerce.

❖ Implementing security involves assessing the possible threats to one's network, servers, and information. Security in an internet environment is important because information has significant value: information can be bought and sold directly or can be used to create new products and services that yield high profits. Security on the internet is challenging, prima, facie, because security involves understanding when and how participating users, computers, services, a and networks can trust one another, as well as understanding the technical details of network hardware and protocols.

REASONS FOR INFORMATION SECURITY:

❖ The requirements of information security in an organization have undergone two major changes in the last several decades.

❖ Computer and network security can be defined as the protection of network-connected resources against unauthorized disclosure, modification, utilization, restriction, incapacitation, or destruction. Hundreds of thousands of system are now connected to the internet. There is no accurate way of measuring the threat that may be launched by an inimical agent. However, as a gauge, internet security systems (ISS) made the following list from actual recent computer security breaches and news releases:

- The FBI estimated that American companies lose $ 7.5 billion annually to electronic attacks.
- There were over a half-million attacks against government computer just in 1995.
- It has been reported that the department of defense has found 88 percent of its computers are penetrable. In 96 percent of the cases where hackers got in, their intrusions went undetected.
- In recent year(1993), the Computer Emergency Response Team(CERT) found a 73 percent increase in security breaks.
- Russian computer hackers successfully breached a large number of Citicorpcoprorate accounts, stealing $400,000 and illegally transferring an additional $11.6 million (wall street journal, august 21, 1995).
- In April of 1995, SATAN was freely distributed on the internet.
- "The security of information systems and networks is the major security challenge of this decade and possible the next century", says scot charnel, chief, computer crimes unit, u.s.
- Nearly half of the respondents lost valuable information in the last two years;
- At least 20 respondents lost information worth more than $1 million.

PROTECTING RESOURCES:

- The term computer and network security refers in a broad sense to confidence that information and services available on a network cannot be accessed by unauthorized users. Security implies safety, including assurance of data integrity, freedom from unauthorized access, freedom from snooping or wiretapping, and
- Freedom from disruption of service, of course, just as no physical property is absolutely secure against crime, no host is absolutely secure.
- Data integrity is crucial, so is data availability. Because information can in prevent unauthorized read/write/delete. That is, network security must include a guarantee of privacy.

TYPES OF RISKS:

- The internet increases, the risk of security violations increases with it. Computer and security have evolved with computer technology, but the issues remain similar.
  - In the 1960s, computer security was not a significant issue. Dumb terminals attached to mainframe computers in effect fostered data security.
  - The 1970s saw the emergence of the ARPAnet, the internet of the academic world that interconnected several different defense contractors, defense agencies, and universities.
  - In the 1980s, enter the age of PCs, distributed networks and viruses, Researches stated that to show interest in confidentiality, integrity and availability of data.
  - With extensive use of the internet, today's enterprise networks and web servers are open to attack.

SECURITY THREATS:

- Some of the threats that simulated the upsurge of interest in security include the following
  - Organized and internal attempts to obtain economic or market information from completive organizations in the private sector.
  - Organized and intentional attempts to obtain economic information from government agencies.
  - Inadvertent acquisition of economic or market information
  - Inadvertent acquisition of information about individuals
  - International fraud through illegal access to computer respositories including acquisition of funding data, economic data, law enforcement data, and data about individuals.
  - Government intrusions on the rights of individuals
  - Invasion of individuals rights by the intelligence community.

PASSIVE THREATS:

- Passive threats involve monitoring the transmission data of an organization. The goal of the attacker is to obtain information that is being transmitted. In general, this is not the easiest task to undertake.

Two types,

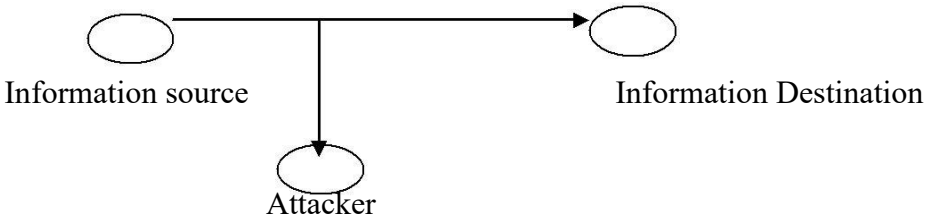
- Release of message
- Traffic analysis

Release of message:

❖ Is clearly a concern. A telephone conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information.

Traffic Analysis:

❖ Is more subtle and often is more applicable to military situations.

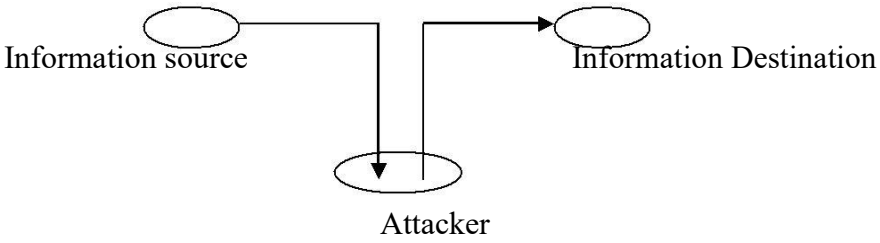


PASSIVE THREAT.

Active threats:

The second major category of threats is active threats . These involve some modification of the data stream to the creation of a false stream. One can clarify these into three categories:

- Message-stream
- Modification
- Denial of message service and masquerade



ACTIVE THREAT

❖ **Message –stream modification means** that some portion of a legitimate message is altered or that messages are delayed, replayed, or reordered to produce an unauthorized effect.

❖ **Denial of service prevents or inhibits** the normal use or management of communication facilities.

❖ **Masquerade** takes place when an attacker pretends to be someone else. A masquerade attack usually includes one of the other two forms of active attack.

2. Explain In Detail About Specific Intruder Approaches.

❖ The intruder approaches covers more detail in the following.

- Bulletin boards
- Electronic mail
- File transfer

- Ip spoofing
- Password guessing
- Password sniffing
- Telnet
- Viruses and SATAN

Bulletin boards:

❖ These internet services provide a clearinghouse for information and correspondence about a large variety of subjects. Many commercial organizations, especially technology houses, use them to provide customer service. Bulletin boards have been notorious hangouts for hackers and other antisocial types. A lot of pirated and virus-laden software appears on bulletin boards.

Electronic mail:

❖ This store-and-forward mail service allows users to communicate throughout the network, requiring only a target address and a point of access currently, e-mail is one of the most commonly used services and is all some organization use. E-mail poses fewer security problems than other forms of internet communication but is subject to interception(at he communication or gateway level), if it is unencrypted. However, an organization should be careful about what it sends and accepts. For example , unsolicited , executable code sent via e-mail could be a virus . (viruses remain generally harmless in message form until and useless executed)

File transfer:

❖ Using FTP and HTTP, users can request and send (download and upload) a variety of bulk data including databases, files in all formants, documents, software, images, and voices. While useful and convenient, file transfer can be insecure both in terms of confidentiality and threats. The network administrator must control how outsiders gain access to internal files and protect the files from misuse or unauthorized use. Normally, this requires a dedicated and isolated server(e.g. a bastion).

IP spoofing:

❖ IP spoofing is a technique that can lead to root access on a system. It is the tool that includes often use to take over open terminal and login connections after they get root access. Intruders create packets with spoofed or impersonated source IP addresses. Other types of ip attacks include user-in-the middle attacks and source-routing attacks.

Password guessing:

❖ Most host administrators have improved their password controls, but group accounts still abound, and password-dictionary and password-cracking programs can easily crack at least 10 percent of the passwords users choose. The deterrent is enforcement of good passwords.

Password sniffing:

❖ CERT estimates that, in 1994, thousands of systems were the victims of password sniffers. On LANs, any internal machine on the network can see the traffic for every machine on that network. Sniffer programs exploit this characteristic, monitoring all IP traffic and capturing the first 128 bytes or so of every encrypted FTP or telnet session. The deterrent is to utilize programs that provide on-time passwords.

Telnet:

❖ Telnet enables users to log on to remote computers. Telnet does little to detect and protect against unauthorized access. Fortunately, telnet is generally supported either by using an application gateway or by configuring a router to permit outgoing connection using something such as the established screening rules.

Viruses:

Viruses do not necessarily give intruders access to a computer system, but may be away to copy and forward information or otherwise create denial-of-service problems. A virus is a program that can infect other programs by modifying them to include a copy of it. It is possible infected with the virus. Virus attack humans, computer viruses can grow, replicated, travel, adapt and learn, attack and defend, camouflage them, and consume recourses. The following lists various computer virus infractions.

- Alter data in files
- Change disk assignments
- Create bad sectors
- Decrease free space on disk
- Destroy FAT(file allocation table)
- Erase specific programs
- Format specific tracks or entire disk
- Hang the system
- Overwrite disk directory
- Suppress execution of RAM resident programs
- Write a volume label on the disk

SATAN:

- In 1995, Dan Farmer, a software programmer for silicon graphics released a program named SATAN (security administrator tool for analyzing networks). The designer unleashed SATAN as a warning to companies and administrators that can thoroughly scan systems and entire networks of system for a number of common critical security holes. SATAN can be used by administrators to check their own networks; unfortunately, it is also used by hackers trying to break into a host. SATAN is a program freely available via the internet. its primary components include,
  - HTTP server that acts as the dedicate SATAN web server.
  - Magic cookie generator that generates a unique 32-bit magic cookie that include a session key.
  - Policy engine that decides exactly which probes to run on various hosts when performing data acquisition.
  - Target acquisition that decides exactly which probes to run on various hosts when performing data acquisition.
  - Data acquisition to gather security-related facts about the targeted hosts.
  - Inference engine that is driven by a set of rules bases and input from data acquisition.
  - Report and analysis , based on its findings.
  - More general information about SATAN and obtaining SATAN is available for anonymous FTP at fttp://ftp.win.tue.nl/pub/security/and ftp://mcs.anl.gov/pub/security/. It should be noted that security-auditing tools are now becoming available to analyze patterns of analyze patterns of attack. These are called network sniffers.

3. Explain in detail about security strategies.

- There are basic security strategies that can be utilized to combat the threats discussed so far: access control, integrity, confidentiality, and authentication.

a. Policy issues
b. Mechanisms for internet security.

POLICY ISSUES:

- Although the need for a policy is obvious, many organization attempt to make their network secure without first defining what security means. Before an organization can enforce security, the organization must access risks and develop an unambiguous policy regarding information access and protection.
- The policy needs to specify which parties are granted access to each element of the information to others, and a statement of how the organization will react to violations. The policy should also address details such as information entrusted to the organization by

clients in the normal course of conducting business and information that can be deduced about clients from their orders for goods and services.

- Establishing an information policy and educating employees is critical because humans are usually the most susceptible point in any security scheme. A worker who is careless or unaware of an elaborate mechanisms that may be in place.

- After an information policy has been established, achieving the desired level of security Can be daunting because doing so means enforcing the policy throughout the organization. Difficulties arise when dealing with external organization, when polices may conflict. For example, consider organizations A, B and C. Suppose the policy at A allow information to be exported to B, not to C. If the policy at B permits export to c, information can flow from A to C thought B. More importantly, although the end effect might compromise security, no employee at any organization would violate the organization's policy.

POLICY GUIDELINES:

- When a system administrator sets security policies, he or she is developing a plan for how to deal with computer security. One way to approach this task is to do the following.
  - Look at what it is you are trying to protect
  - Look at what you need to protect these data/resources from
  - Determines how likely the threats are
  - Implement measures which will protect your assets in a cost-effective manner.
  - Review the process continuously and improve processes when a weakness is found.

- There are a number of issues that need to be addressed when developing a security Policy, some of these issues are as follows:
  - **Who is allowed to use the resources?** The policy should explicitly state and Explain who should have access to what parts of the system, and who is authorized to use which resources.
  - **What is the proper use of the resources?** One needs to establish guidelines for the acceptable use of the resources. Those guidelines could be different if there is more Than one category of users.
  - **Who is authorized to grant access and approve usage?** The policy should clearly state who is authorized to use the resources furthermore, it must state what type Of access those users are permitted to give. A system administrator, who has no control Over who is granted access to his/her system, has no control over that system.
  - **What are user's rights and responsibilities?** The policy should incorporate a Statement on the user's rights and responsibilities concerning the use of the organization's computer systems and services. It must state what type of access those users are responsible for understanding and respecting the security rules of the system they are using.

What should be covered in the policy? The following is a list of topics that should Be covered in this area of the policy:

- What guidelines you have regarding resource use
- What might constitute abuse
- Whether users are permitted to share accounts or let others use their accounts.
- How users should keep their password secret.
- How often users should change their passwords and any password restrictions of requirements
- Restrictions on disclosure of information that may be proprietary
- Statement on electronic mail privacy
- Policy on electronic communications, mail forging, and so on
- The organization's policy concerning controversial mail or postings to mailing lists or discussion groups.

INADEQUATE MANAGEMENT:

❖ Related to the topic of policy is the topic of rational resource management. Solid Procedures and good management of computer systems as related to software are Critically important.

Installing untested software or incorporating unproved hardware has the potential to debilitate your business. Application and software changes open up the possible for bugs to be exploited to an attacker's advantage.

MECHANISM FOR INTERNET SECURIY (4.Explain in detail about Mechanisms for internet security)

❖ Mechanisms that help make internet based communication secure can be divided into three broad categories.

- Set focuses on the problems of authorization, authentication and integrity
- Set focuses on the problem of privacy
- Set focuses on the problem of availability by controlling access.

AUTHENTICATION AND INTEGRITY MECHANISMS.

❖ Authentication mechanisms address the problem of identification of individuals and entities requesting service or access. Many servers, for example, are configured to reject a request unless the request originates from an authorized client. When a client makes contact, the server must verify that the client is authorized to undertake the specific task before granting service.

There are three categories of authentication

- User-to-host: a host identifies a user before providing services
- Host-to-host: hosts validate the identity of other hosts

- User-to-user: users validate that data is being transmitted by the true sender and not an impostor posing as the sender.

❖ In **user-to-host** authentication, a host identifies users in order to provide services for which users are authorized and to deny those services for which they are not authorized. These services may include interactive login sessions, access to a network file system, or access to particular devices. There are a variety of implemented user-to-host authentication techniques. The most popular method, although not all the strongest, is based o password.(for example account name)

The following list provide some corrective suggestions,

Password don'ts

- Do not use a portion or variation of your account name or another account name.
- Do not use a portion or variation of your real name, office or home address, or phone number.
- Do not use words or variation of words found in any dictionary, especially /usr/dict words.
- Do not use pairing of short words founds in any dictionary (such as dogcat).
- Do not use dictionary words or names spelled backward (such as leinad).
- Do not use syllables or words from a foreign language.
- Do not use repeated character strings (such as AAAABBBB or CCAATT).
- Do not use passwords containing o0nly number digits (such as 123456).

Password dos:

- Run a password generator to generate one-time-only passwords. This ensures the passwords are constantly changing and are less likely to be guessed.
- Engage password aging by requiring users to reset passwords on a regular basis, such as once a week or once a month.
- Run a password guesser to test security of your own system password. This is a good way of determining weak passwords that may allow an intruder to enter.
- Prevent unsecured password at least seven characters long, if possible.

❖ **Host-to –host** authentication is concerned with the verification of the identify of computer systems. This method is employed by hosts on the internet.

❖ **User-to-User:** Authentication establishes proof of one user's identify to another user. This can be employed as a form of digital signature with electronic mail.

PRIVACY CONTROL

❖ Confidentiality is the assurance of privacy, often achieved on the internet through the use of encryption as previously discussed in the context of the integrity. An e-mail message that is sent via the internet can be compared to a postcard sent via the U.S.mail. Confidentially can

be achieved much like data integrity with the usage of encryption. This includes digital encryption, public keys, and ciphers.

ACCESS CONTROL

- Access control relates to who or what may have access to a certain service or system. Access control, essentially, is a form of authorization. A user's or service's privilege and rights dictate what services what services or objects (file and file systems, etc) may be accessed.

USER-ORIENTED ACCESS CONTROL

- An example of user access control on a time-sharing system is the user logon, which requires both a user identifier (ID) and a password.
- User access control can be either centralized or decentralized. In a centralized approach, the network provides a logon service, determining who can use the network and to who the user can connect, Decentralized user access control treats the network as a transparent communications link, and the usual logon procedure is carried out by the destination host.

DATA-ORIENTED ACCESS CONTROL

- The database management system, however, much control access to specific records or even portions of records. For example, anyone in administration may be able to obtain a list of company personnel, but only selected individuals may be access to salary information.
- The network considerations for data-oriented access control parallel those for user-oriented access control. If only certain users are permitted to access certain items of data, encryption may be required to protect those items during transmission to authorized users.
- Typically data access control is decentralized, that is it is controlled by host-based management systems. If a network database server exists on a network, data access control becomes a network functions.

5. Explain in detail about Security Tools(Apr 2014)

- Secure Transport Stacks
- Kerberos
- Secure Transactions over the Internet
- UNIX Security
- Password Security Systems
- Electronic Mail
- Server Security
- Trusting Binaries

Secure Transport Stacks

❖ The Internet uses the TCP/IP protocol as the primary network protocol.

- Each IP packet contains the data that is to be sent to destination. The IP packets consist of a 32-bit source and destination address optional bit flags, a header checksum, and data itself. There is no guarantee at the network layer that the IP Protocol data units will be

received and even they are received ,the data may not be received in a particular order in which they are sent from the source system.

- TCP provides retransmission of lost or corrupted protocols data units.

The acknowledgement number is the sequence number of the last packet transmitted.

❖ There are various network protocol encryption schemes that offer secure information being transmitted. Two most prominent Secure Transmission protocol for web communication are,

- **Secure Sockets Layer**
- **Secure-HTTP**

❖ **SECURE SOCKETS LAYER**

- This Secure Socket Layer was advanced by Netscape Communications Corporation.
- It is used to encrypt communication within higher-level protocols, such as HTTP, NNTP and FTP.

❖ The SSL Capable to Perform

- Server Authentication (verifying the server to the client)
- Data Encryption
- Client Authentication (verifying the client to the server).

❖ SSL employs RSA Cryptographic techniques to implement data encryption.

- RSA uses variable – length public key Cryptographic algorithm which uses mathematical formula to encrypt the data.
- The larger the key, the harder it is to decrypt.

Secure-HTTP

- S-HTTP is an encryption algorithm advanced by commerce net.
- S-HTTP is a higher-level protocol that currently only works with the HTTP protocol.

KERBEROS

❖ Kerberos uses a trusted third-party authentication scheme, in which users and hosts rely on the third-party to bear the burden of trust- both the hosts and the users trust the third party and not each other. The model postulates that the third party (also called the key distribution center, KDC) verifies the identity of users and hosts, based on a shared cryptographic key.

- This key enables the third-party to decrypt an encrypted password and thus prove the identity of a user or host without revealing its password.
- Some of the design principles of Kerberos are as follows:
  - Both one-way and two-way authentications are supported.
  - Authentication should be achieved without transmitting unencrypted passwords (clear text) over a network.
  - No unencrypted passwords should be stored in the KDC(trusted host)
  - Clear text passwords entered by client users should be retained in memory for the shortest time possible, and then destroyed.
  - Authentication compromises that might occur should be limited to the length of the user's current login session.
  - Each authentication should have a finite lifetime, lasting about as long as atypical login session. During this lifetime, the authentication may be reused as often a s needed
  - Network authentication should be nearly unnoticed by users: the only time users should be aware that authentication is occurring is when entering a password at the time of login.
  - Minimal effort should be required to modify existing applications that formerly used other, less-secure authentication schemes.
- The following is a brief example of the Kerberos protocol as it applies to a user accessing a network service in a client\sever environment.
- A user wishes to use a certain network services. The client sends two items to the server: a session key and a service ticket. The ticket contains four things:

  1. The name of the user it was issued to,
  2. The address of the workstation that the person was using when he or she acquired the ticket
  3. A session key, and
  4. An expiration date in the form of a lifespan and a timestamp
- All this information has been encrypted in the network service's password.

  - User sends [session key | ticket]
  - The network service decrypts the ticket with the session key so the ticket resembles this: { session key : username: address: service name: lifespan: timestamp}
  - Authenticator{Username: address}is encrypted with session key

KERBEROS AUTHENTICATION PROCESS

- Client sends a request to the authentication server requesting credentials for a giver server. Authentication server responds with these credentials, encrypted in the client's key. The credentials consist of the following.

    1. A ticket for the server
    2. A temporary encryption key (often called a session key)

- The Kerberos system relies on the premise of mutual authentication via an encrypted to. It is not, however, without its limitations. Among them are the following.

    - Vulnerability of passwords and encryption keys when presented to or maintained by the workstation
    - The need for synchronized clocks
    - No support for authenticated messages to multiple recipients
    - Weak assurances against repudiation

Secure Transactions over the Internet

- Secure transaction mechanisms for transaction processing across the internet. Business customers digitally sign encrypted credit card information; merchants then pass this information to the banks. The banks then decrypt and process information. An authorization is then returned to the merchant.

- As an alternative to the use of credit cards over the Internet is the use of e-cash. E-cash allows users to transfer electronic money over the Internet for the purchase of goods and services with relative ease.

- Digit cash is a system that provides the service of electronic cash to the Internet community; the computer system which stores the digital cash is protected by a series of passwords, access restrictions, and encryption.

UNIX SECURITY

- UNIX provides various built-in security features, such as user passwords, file access, directory access, file encryption, and security on password files.
- A UNIX system can be used for web support or more generally for FTP or related support.
- Password security on UNIX systems provides eight-character passwords for users.
- Passwords are not displayed on the screen when they are typed in, to prevent anyone else from reading them. User passwords are generally encrypted using DES algorithm.
- Once a password has been encrypted, it cannot be decrypted back to its text format; this helps to prevent hackers from reading the password file and stealing passwords.
- Users have the responsibility for the maintenance of their passwords

PASSWORD SECURITY SYSTEMS

❖ Passwords are the most widely-used security measures in existence today. Login attempts should be limited to three or less tries. Password security is only as good as the password itself.

❖ Attackers today have sophisticated password breaking tolls, which will keep trying different combinations of numbers and characters until the password has been breached.

- **One-time passwords**
- **Smart Cards**

One-time passwords

❖ There are several ways to implement one-time passwords:

One of the most common involves the use of an internal clock, a secret key and a handheld display. The current time and the secret key are processed thought some function and are displayed on the screen. The displayed value will change about once per minute, so that the value will not be repeated. The host processor proceeds to validate the user by matching the user's output to the hosts calculated output

Smart Cards

❖ A smart card is a portable device that contains some non-volatile memory and a microprocessor. This card contains some kind of an encrypted key that is compared to a secret key contained on the user's processor. Some smart cards allow users to enter a personal identification number (PIN) code.

ELECTRONIC MAIL

❖ Electronic mail or E-mail is one of the most widely used forms of communication over the Internet today. The simple Mail Transfer Protocol (SMPT) provides inter-machines e-mail transfer services.

❖ Anonymous retailers provide a service that forwards a user's mail message onto The destination address but without disclosing the return address of the sender. This protects the sender of a message from intruders learning the sender's e-mail address.

Anonymous remailers are of two types

1. Remailers that mask the sender's return address
2. Remailers that provide anonymity for both the sender and destination addresses.
   - **Privacy Enhanced Mail**
   - **Pretty Good Privacy**
   - **Multipurpose Mail Extension**

Privacy Enhanced Mail

❖ PEM describes formats and techniques for encryption and authenticating message senders. PEM allows users to send e-mail and have automatically encrypted.PEM supports confidentiality, originator authentication, message integrity, and no repudiation of origin

There are three types of PEM message

- MIC(Message Integrity Code)-CLEAR, message integrity checked in clear text has a digital signature affixed to its unencrypted content
- MIC-ONLY. Message integrity checked is encoded to protect the message's content.
- ENCRYPTED messages are also integrity checked and contain cipher text.

Pretty Good Privacy

PGP utilize the

- International Data Encryption Algorithm (IDEA)
- RSA
- MD5 algorithm to provide message encryption .

- PGP incorporates features such as digital signature and allow user to choose the size of the encryption key
- PGP also provides compression of data prior to applying the encryption algorithm

Multipurpose Internet Mail Extension

❖ MIME is a standard that defines the format of textual messages exchanged on the internet.

Its purpose is to standardize the format of message bodies in the way that enables them to carry many types of recognizable non-ASCII data.

❖ MIME-encoded message are tagged with content types

SERVER SECURITY

❖ Many of the web browsers allow user to save the html source code used to create the web pages that are viewed.

❖ The source code, once save on a user's pc is capable of recreating html formatted text. the source code contains all the designation and file name of the respective graphic video , programs and hyperlinks that would be executed clicking on the web page item.

❖ There is a security risk if a hacker were to save the web page source code and access the associated file and also they can modify or they can perform any destructive action.

❖ To overcome this, a Netscape corporation provides a web servers encrypt the communication links between pc and the server by using RSA public key cryptographic technology which is transparent to the user.

Some of the security techniques used by the commerce server include

- Data Encryption over the Communication Link.
- Server Authentication
- Message Authentication – which verify the message received are in the fact the messages that were sent.

TRUSTING BINARIES

- Security does not end with the various firewall and browser security products available. These products may not take into account the issue of trusting executables. Effective security, especially if the Internet is to become the "marketplace of the future", must be end to end. This means that not only must the protocol layer be secure to communication over an insecure network, but the binaries at both ends must be secure as well.

- Based on a security Web page, "Basic Flaws in Internet Security and Commerce," the Web page authors attempted various IP spoofing attacks to prove that security could be compromised. The results of their testing showed that they could spoof NFS (Network File System) to patch binaries on the fly, as long as they were on some subnet between the client running NFS and the NFS server itself. Being able to patch binaries, they were able to patch the Netscape executable so that it used a fixed key that was only known to the authors.

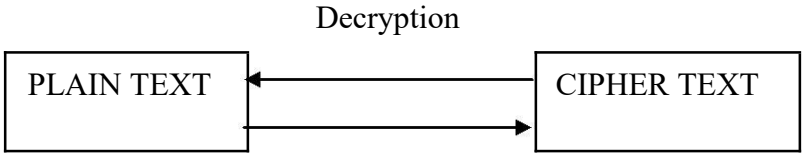
6. Explain in detail about Encryption(Apr 2014)

- Most effective way of securing the contents of electronic data i use of encryption.

- Encryption involves the scrambling of data by use of a mathematical algorithm. The term cryptography mean secret. In the simple words, cryptography is the science of disguising message so only the writer and the intended receivers are able to read them.

- Caesar was one of the first to use cryptography because of his distrust in his messengers; he used the shift-by-three method each letter of the alphabet replaced by the third letter ahead of it, for example the word “GOOD” when encrypted would become “JRRG”.

  Today's encryption is much more sophisticated.



Encryption Process

- Encryption methodologies are being used by many financial, communications, software, and credit card companies to secure the integrity of incoming and outgoing messages as well as to authenticate that messages received are actually from the persons who sent.

- Encryption is a process where the cryptographer puts an input plaintext into a codified algorithm and a key to get an output cipher text.

- Decryption on the other hand, is the reversing of encryption with the cipher text as the input and the plaintext as the output.

- The function involves both an algorithm and a key, because it would be difficult and time-consuming to keep coming up with new effective algorithms every time one wants to send a secure message.

- In most cases, the algorithm is known to all parties, since the algorithm - is useless without the key.

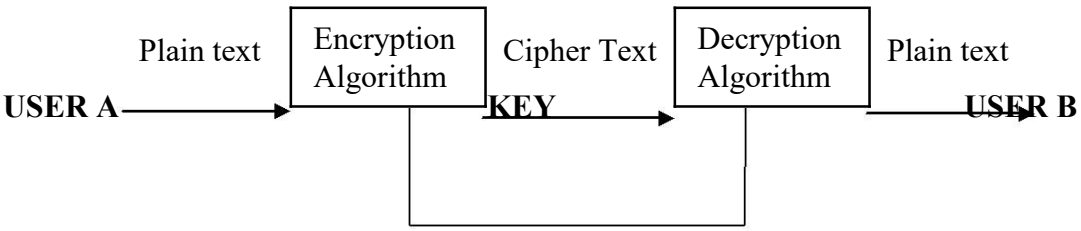
- The ease of figuring out the key depends on its length. The shorter, in number of bits, the key is easier it is to figure out. Therefore, cryptographic algorithms should have variable-length keys.
- The key is short, say 4 bits, the scheme would not be secure, for it would be easy to try all possible keys to find the corresponding plaintext.
- If the length of the block is too long, it would be inconvenient and complex. Usually the practical length is 64 bits because it is not too easy or too hard to manipulate.
- The following lists the highlights of encryption.
- Encryption is a process that conceals meaning by changing messages into unintelligible messages.

Uses a code or a cipher.

- Code system uses a predefined table or dictionary to substitute a in word or phrase for each message or part of a message.
- Cipher uses a computable algorithm that translates any stream of message bits into an unintelligible cryptogram.
- There are three kinds of cryptographic functions:
- **Hash functions (involve the use of no keys).** .
- **Secret-key functions (involves the use of one key).**
- **Public-key functions (involves the use of two keys).**

Conventional Encryption

- The encryption process consists of an algorithm and a key. The key is a relatively short bit string that controls the algorithm. The algorithm produces output depending on the key used: changing the key radically changes the output of the algorithm.
- After the cipher text is produced, it is transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.



Conventional Encryption

- It's also known as conventional cryptography or symmetric cryptography. Involves the use of a single key.

❖ Given a message (plaintext) and the key; encryption produces unintelligible data (ciphertext), which is about the same length as the plaintext.

- If two parties agree on a shared key, then by using secret -key cryptography they can send messages to one another on a medium that can be tapped, without worrying about eavesdroppers.
- Also used for securely storing data on insecure media: you can encrypt data using your own secret key and store it anywhere you want, since nobody knows the key.

❖ Decryption, which is the reverse process, uses the same key as encryption.

❖ The security of conventional encryption depends on several factors.

❖ The encryption algorithm must be powerful enough so that it is impractical to decrypt a message on the basis of the ciphertext alone. Beyond that, the security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm.

❖ With the use of conventional encryption, the principal security problem is maintaining the secrecy of the key.

❖ Authentication is another benefit of secret-key cryptography. The term strong authentication means that someone can prove knowledge of a secret without revealing it. Strong authentication is possible utilizing cryptography. It is useful when two computers are attempting to communicate over an insecure network.

❖ For secret-key cryptography is integrity checking. A secret-key scheme can be used to generate a fixed-length cryptographic checksum associated with a message.

❖ A traditional checksum protects against accidental corruption of a message. The sum is sent along with the message. The receiver checks the sum. If the sum does not match the sum sent, the message is rejected. To provide protection against malicious changes to a message, a secret checksum algorithm is required, such that an attacker not knowing the algorithm cannot compute the right checksum for the message to be accepted as authentic.

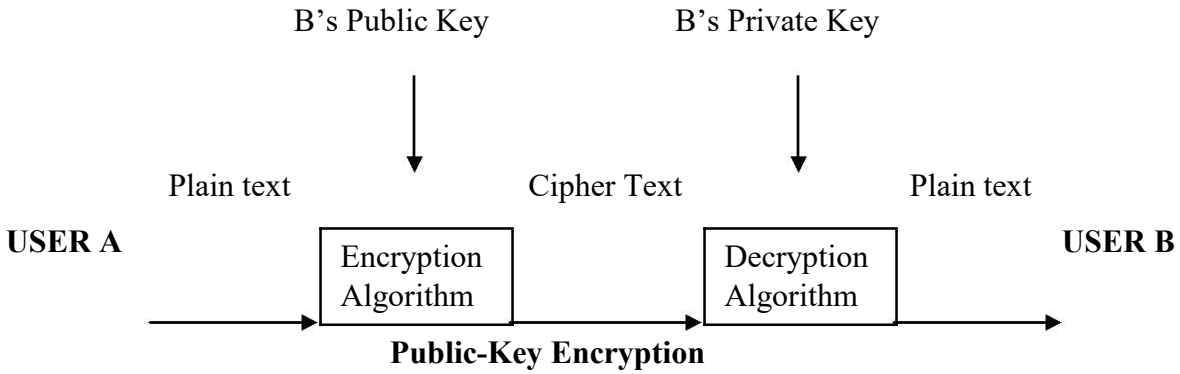
Public-Key Encryption

❖ One of the major difficulties with conventional encryption schemes is the need to distribute the keys in a secure manner.

❖ Public-key encryption, first proposed in 1976, does not require key distribution.

❖ For conventional encryption schemes, the keys used for encryption and decryption are the same. But it is possible to develop an algorithm that uses one key for encryption and a companion but different key for decryption.

❖ Furthermore, it is possible to develop an algorithm such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key.



Public-Key Encryption

Thus the following technique will work.

- Each end system in a network (say Emil and Gabrielle) generates a pair of keys to be used for the encryption and decryption messages that it will receive.
- 2 Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

  If Emil wants to send a message to Gabrielle, he encrypts it using Gabrielle's public key.

  When Gabrielle receives the message, she decrypts it using Gabrielle's private key. No other recipient can decrypt the message because only Gabrielle knows Gabrielle's private-key.

Public-key encryption solves the distribution problem because there are no keys to distribute. All participants have access to public keys, and private keys are generated locally by each participant

Public-key cryptography is sometimes also referred to as asymmetric cryptography. Using public-key technology, one can generate a digital signature on a message, called message integrity code or message authentication code.

A digital signature is a number associated with a message, like a checksum. However, unlike a checksum, which can be generated by anybody, a digital signature can only be generated by someone knowing the private key.

A public key differs from a secret key because verification of a MIC requires knowledge of the same secret as was used to create it.

Application of encryption:

The strength of cryptographic system rest with the key distribution technique, term that refers to the mean of delivering a key to two parties that want to exchange data without allowing other to see key. Key distribution can be achieved in number of ways.

Two keys are identified.

Session key: When two end system want to communicate, they establish a logical connection for the duration of that logical connection, all user data in encrypted with a one time session key.

Permanent Key: A permanent key is used between entities to distribute session key.

The configuration consist of following elements:

Access control center: The access control center determines which system can communicate with each other.

Key distribution center: The network interface unit performs end to end encryption and obtain session key on behalf of its host terminal.

Breaking an encryption scheme:

There are 2 basic attacks.

1. Ciphertext only, known plain text

2. Ciphertext only, chosen plain text

Known plain text is an attack using old pairs of to decipher new ciphertext messages.

Chosen plaintext attack, hackers choose any plaintext they want and have the system give them corresponding encrypted version.

Data Encryption Standard(DES):

DES has also been the subject of much controversy as to how secure it is. The main concern is in the length of the key, which some observe consider too short.

Commercial Communication security endorsement program:

The replacement is family of algorithm developed under NSA commercial COMSEC(Commercial Security Endorsement Program(CCEP). CCEP is a joint NSA and industry effort to produce a new generation of encryption devices that are more secure than DES algorithm.

Government Security Levels:

The features and capabilities of a secure operating system require significant amount of processing power and disk space.In low end servers one may find that enabiling the security features seriously affects the number of users a server can support.

The Clipper Chip:

The Clipper chip uses key escrow which is type of private key encryption that allows user for two parties to hold the secret key. the encryption algorithm is based on NSA's Skipjack algorithm.

Commercial outlook encryption:

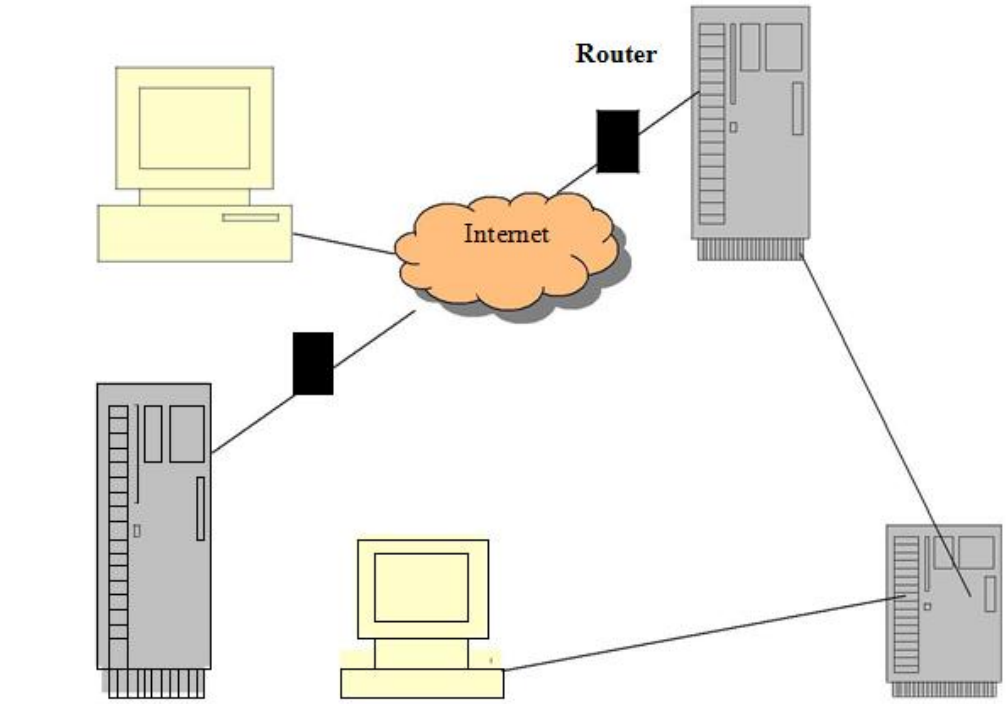
Security experts recommend layering security because no single layer of encryption is sufficient

7. Explain In Detail About Enterprise Networking And Access.

Many companies, including electronic merchants, have their employees working off of LAN-based PCs and servers. Generally, LANs am interconnected with other LANs within a company over a local or wide area network (WAN) internetworking infrastructure. With the Internet increasingly becoming a useful corporate tool (e.g., World Wide Web, e-mail, etc.), company

users are requesting access to the Internet. In addition, companies may have exposed sites to draw surfers and customers. All of this opens the enterprise-based hosts up to the outside world

Access to the Internet is accomplished in a number of ways. Access can be attained through company's LAN-resident Internet gateway by using modem



Example of VPN

- When the system is connected to the internet there may be a lot of insecurity for the data to handle that we may use firewall.

- Firewalls that control Internet access handle the problem of screening a particular network or an organization from unwanted communication. Such mechanisms can help prevent outsiders from obtaining information, changing information, or disrupting communication organization's enterprise network.

Approaches for Enterprise-Level Security

- A firewall is a security device that allows limited access out of a one's network from the Internet. So, a firewall is a piece of hardware is connected to a network to protect it from agents reaching re: on the network via public open networks .In effect, permits approved traffic in and out of one's local site. This type security measure allows an administrator to select applicable service

- Firewalls operate at the application layer of the protocol stack .They can also operate at the network and transport layers; in this case, they examine the IP and TCP headers of incoming and outgoing packets and reject and pass packets based on the programmed packet filter rules Security concerns go beyond the headquarters location. If a company has a corporate-wide backbone that connects corporate sites in several cities or countries, the network manager at a given site may choose to connect the site to a local ISP The organization must form a security perimeter by installing a firewall at each external connection. It needs an Internet firewall at the access (boundary) point of the network to be protected.

❖ Firewall are classified into three main categories

- Packet filter
- Application –level Gateway
- Proxy server

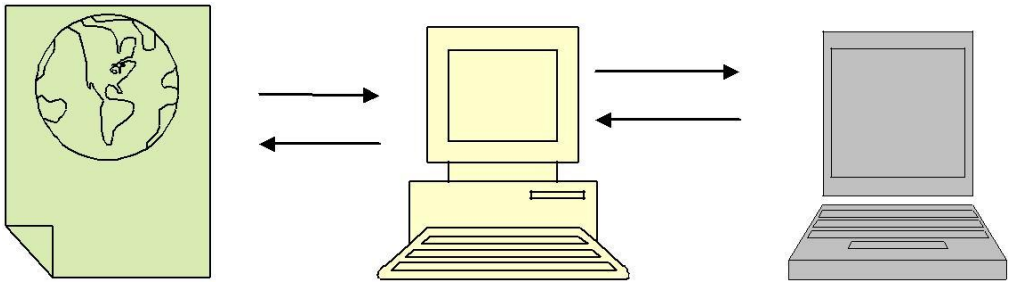
PACKET FILTER

❖ Packet filtering at the network layer can be use first defense.

❖ Filtering can occur on incoming packets, outgoing packets, or both. Limitations may exist on one's router as to where one can apply a filter. Filtering of incoming packets may protect the router from becoming compromised by an attacker.

❖ Firewalls are generally a good way of protecting an organization against attacks through the Internet.

❖ Some security issues may come in the form address spoofing. IP address spoofing is defined as sending pa from an outside host that allege to be sent from an internal Attacks using IP address spoofing are difficult to detect unless logging is performed and activities are correlated against legitimate. Hence, though filtering helps in the fight against security threats does not by itself prevent attacks from address spoofing. A threat could still be realized by an attacker portraying a trusted host that may be on an internal network.



The Global Internet The Fire wall The corporate Network

Use of Firewall

APPLICATION –LEVEL GATEWAY

An application-level gateway provides mechanism for filtering traffic for various applications. The administrator defines and implements code specific to applications or service. Services or users that can compromise the network security then be restricted . To counter some weaknesses associated with filtering routers, firewalls utilize software applications to forward filter connections for services such as Telnet, FTP, and HTTP

❖ A key distinction between a packet-filtering router application-level gateway is the ability to filter and log at the application level rather than just the IP level.

❖ In this way, administrators do not have to worry about security holes in foreign hosts which may only invoke simple measures. Another advantage to an application -level gatewa3 they

control all traffic going in and out of the network and allow logging. Utilizing a gateway provides a central point for monitor logging activity, which means administrators have the ability to all data being passed through the gateway, which could be used to look for suspected illegal activity."

- Application gateways have a number of advantages over filtering routers, including logging, hiding of internal host names and IP addresses, robust authentication, and simpler filtering rules. FTP gateway might be configurable to permit incoming FTP outgoing FTP, a particularly useful combination in main secure firewall.

PROXY SERVER

- A proxy server terminates a user's connection and sets up a new connection to the ultimate destination on behalf of the user, proxying for the user. A user connects with a port on the proxy; the connection is routed through the gateway to a destination port, which is routed to the destination address. Logging can be set up to track such transmission information as number of bytes sent, inbound IP address, and the outbound destination IP address. Usually, if a proxy is used, the proxy server provides most of the Internet connectivity. An example of a proxy is a Web services proxy server (HTTP).

- As for the disadvantages, most proxy servers require two steps to connect inbound or outbound traffic and may require modified clients to work correctly.

Variation and combinations:

a. **Dual homed host:** In TCP/IP networks, the term multihomed host describes a host that ha multiple network interface connections.
b. **Dual homed gateways:** The dual homed gateway is an alternative to packet filtering routers. It consist of an application gateway with two network interfaces and with the host's forwarding capability disabled.
c. **Screened host firewall:** The screened host firewall is more flexible than the dual homed gateway; however the flexibility is achieved with the some cost to security.
d. **Screened Subnet Firewall:** It is a variation of dual homed gateway and screened host firewall. It can be used to locate each component of the firewall on separate system, thereby achieving greater throughput and flexibility, although cost to simplicity.
e. **Bastion host:** It is any host subject to criterical security requirement. Because of this, the bastion host must be well fortified. This means that the bastion host is closely monitored by network administrators.

Design Consideration:

a. Deployment approach
b. The consequences of restricted access for clients
c. Bastion deployment approach
d. Monitoring and logging

8. Explain In Detail About Antivirus Programs.

Viruses and Worms

- A new thread has arisen in the past few years to cause concern among data processing and data communications manger – the virus and its relative worms
- These entities range from harmless to the destructive.
- A virus is a program that can affect other programs by modifying them; the modified program includes a copy of the virus program, which can then go on to infect other programs.

❖ A worm is a program that makes use of networking software to replicate itself and move from system to system. The worm performs some activity on each system it gains access to, such as consuming processor resources or depositing viruses.

Nature of Viruses

❖ A computer virus carries in its instructional code the capability for making copies of itself.

❖ Lodged in a host computer, the typical virus takes temporary control of computer disk operating system. Then, whenever a computer comes in contact with an uninfected piece of software, a fresh copy of the virus passes into a new program. Thus the infection can be spread through one computer to another computer.

❖ A virus can do anything that other program do; the only difference is that it attaches itself to another program and executes secretly every time the host program run. If after a virus program is executed it can perform any function, such as erasing files and programs.

How the infected program might works

- Find the first program instruction
- Replace it with a jump to the memory location following the last instruction in the program
- Insert a copy of the virus code at that location
- Have the virus stimulate instruction replaced by the jump
- Jump back to the second instructions of the host program
- Finish executing the host program

❖ Every time the host program is run the virus would infect another program and then execute the host program.

Countering the Threat of Viruses

❖ The best solution for the threat of viruses is prevention; do not allow a virus to get into the system

❖ The next approach is to do following steps

- **Detection:** After infection has occurred, determine that it has occurred and locate the virus.
- **Purging:** Remove the virus from all infected systems so that the disease cannot spread further.
- **Recovery:** Recover any lost data or program.

There is no universal remedy for protecting the system from the viruses even many number of program are provided for protection.

9.Explain the Security Teams. (Nov 2012)
SECURITY TEAMS

- The issues of network and internet security have become increasingly more important as more business and people go on-line.
- Teams of people have been formed to assist in solving hackers attacks and to disseminate information on security attacks and how to prevent them.
- Two such teams are

  - **Computer Emergency Response Team(CERT)**
  - **Forum of Incident Response and security Teams(FIRST)**

Computer Emergency Response Team (CERT)

- Computer Emergency Response Team (CERT) exists as a point of contact for suspected security problem related to the internet.
- CERT can help determine the scope of the threat and recommend an appropriate response.
- A World Wide Web page supplied by the software Engineering Institute post CERT advisories.

Forum of Incident Response and security Teams (FIRST)

- Security threats are a problem that affects computer and networks around the world.
- FIRST is made up of a variety of computer emergency response teams including teams from the government, business and academic sectors.
- FIRST plans to cultivate cooperation and coordination between teams in an attempt to decrease reaction time to security incidents and promote information sharing among team members.

FIRST is made up of following teams

- AUSCERT
- CERT Coordination center
- DFN-CERT
- CERT-NL
- CIAC
- NASIRC
- NAVCIRT
- PCERT
- SUNSeT
- SWITCH-CERT
- ANS
- VA

PONDICHERRY UNIVERSITY

2 MARKS

1. Name any three intrusion detection approaches. **(Apr 2013) (Ref.Qn.No.16)**
2. State the need for security features in e- commerce. **(Apr 2013)**
3. What are the two types of Anonymous remailers? **(Nov 2012)(Ref.Qn.No.24)**
4. What is a virus? **(Nov 2012) (Ref.Qn.No.6)**
5. Define: Network security. **(Apr 2012)(Ref.Qn.No.25)**
6. What are called as passive threats? **(Apr 2012)(Ref.Qn.No.26)**
7. Write a note on IP Spoofing**?(Apr 2014)(Ref.Qn.No.2)**
8. What is meant by Telnet**(Apr 2014)(Ref.Qn.No.5)**
9. List out some antivirus software.**(Nov 2014)(Ref.Qn.No.12)**
10. Difference between visa card and master card.**(Nov 2014)(Ref.Qn.No.26)**
11. Define key and list out the keys.**(Apr 2015)(Ref.Qn.No.27)**
12. What is the use of antivirus software?**(Apr 2015)(Ref.Qn.No.28)**

11 MARKS

1. Discuss the need and concept of antivirus software in detail. **(Apr 2013)(Ref.Qn.No.8)**
2. Explain about security tools for e-commerce. **(Apr 2013) (Apr 2012)(Apr 2014) (Ref.Qn.No.5)**
3. Explain the Specific Intruder approaches. **(Nov 2012) (Apr 2012) (Ref.Qn.No.2)**
4. a. Discuss the various security Teams. **(Nov 2012) (Ref.Qn.No.8)**
5. b. Explain the three main categories of firewalls. **(Ref.Qn.No.7)**
6. Discuss about Encryption?(**Apr 2014) (Ref.Qn.No.6)**
7. Describe the different security issue. (**Nov 2014) (Ref.Qn.No.1)**
8. Discuss about the security protection and recovery. (**Nov 2014)**(**Apr 2015) (Ref.Qn.No.1)**
9. Describe the antivirus program.(**Apr 2015) (Ref.Qn.No.8)**

UNIT IV

MasterCard/Visa Secure Electronic Transaction: Introduction – Business Requirements – Concepts – Payment processing – E-mail and secure e-mail technologies for electronic commerce. Introduction – The Mean of Distribution – A model for message handling – Working of Email - MIME: Multipurpose Internet Mail Extensions – S/MIME: Secure Multipurpose Internet Mail Extensions – MOSS: Message Object Security Services.

2 MARKS

1. Write the Role of payment Systems.

Payment systems and their financial institutions will pays a significant role by establishing open specification for payment card transactions that:

- Provide for confidential transmission.
- Authenticate the parties involved.
- Ensure the integrity of payment instruction for goods and services order data. And

Authenticate the identity of the card holder and the merchant to each other.

2. Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Master card, Visa, Microsoft, Netscape, and others.

3. Features of SET

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

4. Payment processor

A **payment processor** is a company (often a third party) appointed by a merchant to handle credit card transactions for merchant banks. They are usually broken down into two types: front-end and back-end.

5. List the objective of Payment Security. (Nov 2012)

The objectives of payment security are to:

- Provide authentication of cardholders, merchants and acquirers.
- Provide confidentiality of payment data.
- Preserve the integrity of payment data and

Define the algorithms and protocols necessary for these security services.

6. List the objective of Market Acceptance:

The objectives of market acceptance are to:

- Achieve global acceptance, via ease of implementation and minimal impact on merchant and cardholder end users,

- Allow for ―bolt-on‖ implementation of the payment protocol to existing client applications.
- Minimize change to the relationship between acquirers and merchant and cardholders and issuers,
- Allow for minimum impact to existing merchant, acquirer and payment system applications and infrastructure and
- Provide an efficient protocol viewed from the financial institution perspective.

7. Write the Feature of the specification.

These requirements are addressed by the following features of these specifications

- Confidentiality of information,
- Integrity of data,
- Cardholder account authentication
- Merchant authentication.
- Interoperability.

8. Write the Motivation for secure payment.

The primary motivation for the backend associations to provide specifications for secure payment is:

- To have the backend community take a leadership position in establishing secure payment specifications and in the process, avoid any cost associated with future reconciliation of implemented approaches,
- To respect and preserve the relationship between merchants and acquirers and between cardholders and issuers,
- To facilitate rapid development of the market place.
- To respond quickly to the needs of the financial services market and
- To protect the integrity of bankcard brands.
-

9. List the objectives of Interoperability.

The objectives of interoperability are to:

- Clearly define detailed information to ensure that applications developed by ont vendor will interoperate with applications developed by other vendors.
- Create and support an open payment card standard.
- Define exportable technology throughout, in order to encourage globally interoperable software,
- Build on existing standards where practical,
- Ensure compatibility with and acceptance by appropriate standards bodies, and

Allow for implementation on any combination of hardware and software platforms such as Power PC, Intel, Sparc, Unix, MS-DOS,OS/2,Windows and Macintosh

10. Describe privacy enhanced mail.

PEM describes formats and techniques for encryption and authenticating message senders. PEM allows users to send e-mail and have automatically encrypted.PEM supports confidentiality, originator authentication, message integrity, and no repudiation of origin.

11. What are all the types of PEM message?

There are three types of PEM message

- MIC(Message Integrity Code)-CLEAR, message integrity checked in clear text has a digital signature affixed to its unencrypted content
- MIC-ONLY. Message integrity checked is encoded to protect the message's content.
- ENCRYPTED messages are also integrity checked and contain cipher text.

12. Define MIME. (Apr 2012)

MIME is a standard that defines the format of textual messages exchanged on the internet. Its purpose is to standardize the format of message bodies in the way that enables them to carry many types of recognizable non-ASCII data.

13. Define Front-end processors.

Front-end processors have connections to various card associations and supply authorization and settlement services to the merchant banks' merchants.

14. Define Back-end processors.

Back-end processors accept settlements from front-end processors and, via The Federal Reserve Bank, move the money from the issuing bank to the merchant bank.

15. What is Electronic mail? (Nov 2014)(Apr 2015)

Electronic mail, commonly known as **email** or **e-mail**, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks.

16. List Components of an E-mail?

An email message consists of three components, the message envelope, the message heade*r*, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses.

17. What is Secure Email service?

The Secure Email service is designed for faculty and staffs that need to use email to send Prohibited, Restricted, or Confidential Data—in particular, Protected Health Information (PHI) in accordance with the HIPAA guidelines, as defined by the Information Security Office.

18. Features of secure Email services.

- Uses reliable technology to encrypt email messages sent to off-campus addresses.
  Easy to use for busy medical employees who must comply with HIPAA guideline.

19. **Define Multipurpose Internet Mail Extensions (MIME).**

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support:

- Text in character sets other than ASCII
- Non-text attachments

- Message bodies with multiple parts
- Header information in non-ASCII character sets

20. Define MIME-Version.

The presence of this header indicates the message is MIME-formatted. The value is typically "1.0" so this header appears as MIME-Version: 1.0

21. What is Content-Type of MIME?

This header indicates the Internet media type of the message content, consisting of a *type* and subtype, for example:

Content-Type: text/plain

22. Define S/MIME (Secure/Multipurpose Internet Mail Extensions).

S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption).

23. Define MIME Object Security Services (MOSS).

MIME Object Security Services (MOSS) is a protocol that uses the multipart/signed and multipart/encrypted framework to apply digital signature and encryption services to MIME objects.

24. What exactly is MIME?

MIME is an extension to the Internet mail standard, known as Simple Mail Transfer Protocol (SMTP) that allows mail messages containing different type of multimedia information to be sent across the network this includes, but is not limited to, word-processor documents, spreadsheets, programs, graphics, audio, and motion picture files, as well as links that enable users to retrieve information from remote databases from within a mail message.

25. How MIME works?

The developers of MIME found a clever way to work around the limitation. It packages different data types into a 7-bit ASCII format. That way, all e-mail, regardless of the data it contains, appears as standard e-mail messages to the internet's SMTP servers. The beauty of the solution lies in the fact that SMTP didn't have to change to handle such data.

26. What is New MIME headers?

Required fields

- MIME - Version
- Date - Time

Optional fields

1. Content- type

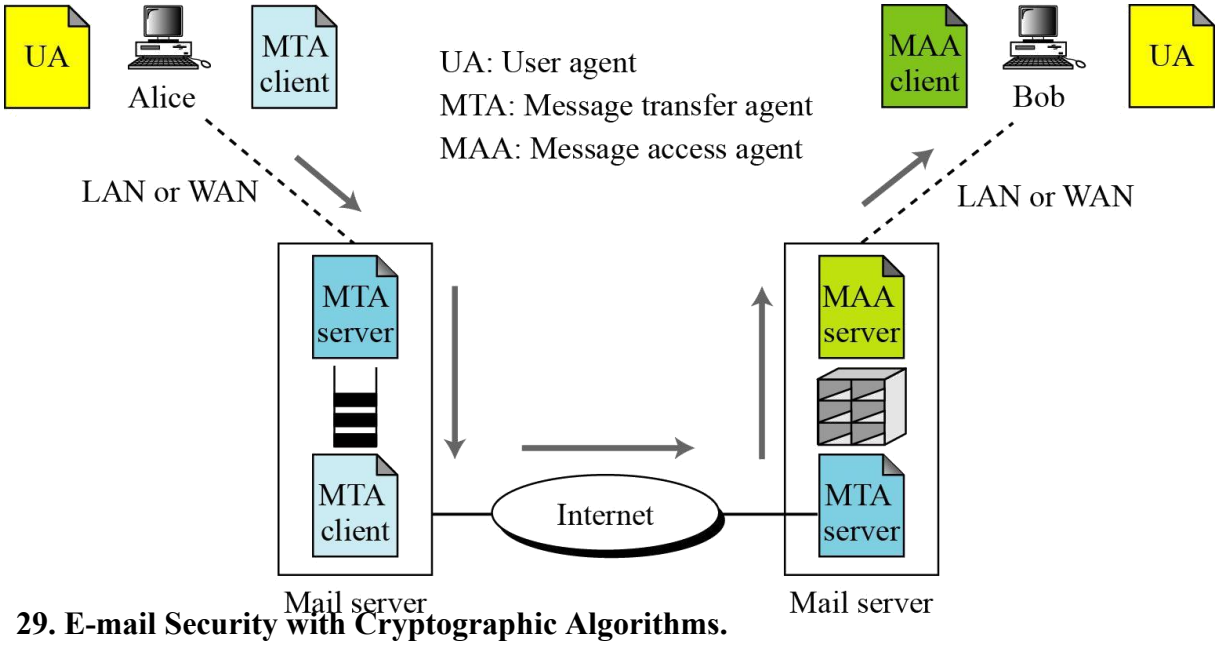
2. Content-transfer encoding
3. Content-ID
4. Content-description
5. Content-disposition

27. The Content-type Applications of MIME. (Nov 2014)(Apr 2015)

Subtypes:

- Postscript
- Octet-Stream-Unidentified binary data
- Many others will be added

28. E-mail architecture



29. E-mail Security with Cryptographic Algorithms.

In e-mail security, the sender of the message needs to include the name or identifiers of the algorithms used in the message.

30. Define E-mail Security with Cryptographic secrets.

In e-mail security, the encryption/decryption is done using a symmetric-key algorithm, but the secret key to decrypt the message is encrypted with the public key of the receiver and is sent with the message.

31. Define Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) can be used to create a secure e-mail message or to store a file securely for future retrieval.

32.Write note on uudecode((Apr 2014)

Uuencode (also called Uuencode/Uudecode) is a popular utility for encoding and decoding files exchanged between users or systems in a network

33.Writa not on cryptography?(Apr 2014)

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. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).

34.What are the key pairs used in SET? (Apr 2012)

- Certificates: need for authentication
- Certificates: need for trusted third party

35.List the internet protocols related to mail specific applications. (Nov 2012)

Simple Mail Transfer Protocol(SMTP)
Post Office Protocol(POP)
Network News Transfer Protocol(NNTP)
Domain Name System(DNS)

36. Difference between master and visa card. (Apr 2013)

Visa and **MasterCard** are both payment systems, not **credit cards** in themselves. They rely on providers to issue **credit cards** using their system. Both exist to set rules and standards for the way in which card transactions are accepted, authorised, and processed.

11 MARKS

1. **Explain objectives of business cards(Master card, Visa card) April 2012**

BACKGROUND

Impact of electronic commerce

- There is no question that electronic commerce as exemplified by the popularity of the internet is going to have an enormous impact of the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce.
- The number of payment card purchases made through this medium will grow as internet based on line ordering systems are created.
- Many banks are planning to support this new form of electronic commerce by offering card authorizations directly over the Internet.
- Several trials with electronic currency and digital cash are already underway.

Projected use

- With more than 30 million user in 1998 and 90 million projected to come on board in the next two years the internet is a new way for businesses to establish computer based resources that can be accessed by consumers as well as business partners around the world.

Internet

- The internet is changing the way we access and purchase information communicate and pay for services and acquire and pay for goods Financial services such as bill payment brokerage insurance and home banking are now or soon will be available over the Internet.

World Wide Web

- The web can display text sound images and even video allowing merchants to transmit information directly to potential consumers around the world around the clock.

Consumer payment devices

- With open networks payment will increasing be made by consumer driven devices. As advanced technologies become more practical and affordable the marketplace will move from brick and mortar to more convenient locations such as the home or office. As financial services evolve consumers will consolidate their payment needs into one multi functional relationship product that enables widespread around the clock access.

Publicity

Internet and the possibilities for consumers and merchants to create a new type of shopping called electronic commerce. The publicity has focused on three areas:

- Marketing opportunities to develop new ways to browse select and pay for goods and services to on- line consumers.
- New products and services and
- Security risks associated with sending unprotected financial information across public networks.

Role of payment systems

Payment systems and their financial institutions will play a significant role by establishing open specifications for payment card transactions that:

- Provide for confidential transmission,
- Authenticate the parties involved,
- Ensure the integrity of payment instructions for goods and services order data and
- Authenticate the identity of the cardholder and the merchant to each other.

Procedures needed

- Because of the anonymous nature of communications networks procedures must be developed to substitute for existing procedures used in face to face or mail order /telephone order (MOTO0 transactions including the authentication of the cardholder by the merchant.

Use of payment card products

- Financial institutions have a strong interest in accelerating the growth of electronic commerce. Although electronic shopping and ordering does not require electronic payment a much higher percentage of these transactions use payment card products instead of cash or checks.

Purpose of secure electronic transaction

To meet these needs the secure electronic transaction (SET) protocol uses cryptography to:

- Provide confidentiality of information
- Ensue payment integrity and
- Authenticate both merchants and cardholders.

OBJECTIVES

Motivation

The primary motivations for the bankcard associations to provide specifications for secure payments are:

- To have the bankcard community take a leadership position in establishing secure payment specifications and in the process avoid any cost associated with future reconciliation of implemented approaches

- To respect and preserve the relationship between merchants and acquirers and between cardholders and Issuers,
- To facilitate rapid development of the marketplace,
- To respond quickly to the needs of the financial services a market and
- To protect the integrity of bankcard brands.

Payment security

The objectives of payment security are to

- Provide authentication of cardholders merchants and acquires,
- Provide confidentiality of payment data
- Preserve the integrity of payment data and
- Define the algorithms and protocols necessary for these security services.

Interoperability

The objectives of interoperability are to:

- Clearly define detailed information to ensure that applications developed by one vendor will interoperate with applications developed by other vendors.
- Create and support an open payment card standard,
- Define exportable technology throughout, in order to encourage globally interoperable software,
- Build on existing standards where practical
- Ensure compatibility with and acceptance by appropriate standards bodies and
- Allow for implementation on any combination of hardware and software platform such as power PC, Intel, spare, UNIX, MS-DOS, OS/2, WINDOWS and MACINTOSH.

Market acceptance

The objectives of market acceptance are to:

- Achieve global acceptance via ease of implementation and minimal impact on merchant and cardholder end users,
- Allow for ―bolt-on‖ implementation of the payment protocol to existing client applications,
- Minimize change to the relationship between acquirers and merchant cardholders and issuers,
- Allow for minimum impact to existing merchant, acquirer and payment system applications and infrastructure and
- Provide an efficient protocol viewed for the financial institution perspective.

2. Explain about business requirements and scope, features. (Nov 2012)

BUSINESS REQUIREMENTS

Introduction:

The business requirements for secure payment processing using payment processing using payment card products over both public networks (such as the Internet) and private networks.

Security issues noncompetitive

Security issues regarding electronic commerce must be viewed as noncompetitive in the interests of financial institutions, merchants and cardholders.

Seven business requirements

There are seven major business requirements addressed by SET:

- Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
- Ensure integrity for all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a branded payment card account.
- Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties of an electronic commerce transaction.
- Ensure the creation of a protocol that is neither dependent on transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability across software and network providers.

FEATURES

Features of the specifications

These requirements are addressed by the following features of these specifications.

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Interoperability

For the sake of clarity, each of these features has been described as a distinct component. It should be noted, however, that these elements do not function independently; all security functions must be implemented.

Confidentiality of information

- The cardholder, account and payment information must be secured as it travels across the network, preventing interception of account numbers and expiration dates by unauthorized individuals.
- ***On-line shopping***: In today's on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open network with little or no security precautions.
- ***Fraud***: while it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high volume fraud, automated fraud the potential
- For ―mischievous fraud‖ that appears to be characteristic of some hackers. In addition, the transmission of account information in a relatively unsecure manner has triggered a great deal of negative press.
- The specifications must guarantee that message content is not altered during the transmission between originator and recipient.
- Payment information sent form cardholders to merchants includes order information, personal data and payment instructions. If any component is altered in transit; the transaction will not be processed accurately.

Cardholder account authentication

- Merchant need a way to verify that a cardholder is a legitimate user of a valid branded payment card account number. A mechanism that uses technology to link a cardholder to a specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing.

- These specifications define the mechanism to verify that a cardholder is a legitimate user of a valid payment card account number.

Merchant authentication

The specifications must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce.

Interoperability

The specifications must be applicable on a variety of hardware and software platforms and must include no preference for one over another. And cardholder with compliant software must be able to communicate with any merchant software that also meets the defined standard.

SCOPE

Use of payment cards

The SET specifications address a portion of the message protocols that are necessary for electronic commerce. It specifically addresses those parts of the protocols that use or impact the use of payment cards.

Electronic shopping experience

The electronic shopping experience can be divided into several distinct stages.

Stage	Description
1	The cardholder browses for items. This may be accomplished in a variety of ways, such as: Using a browser to view an on-line catalog on the merchants world wide web page; Viewing a catalog supplied by the merchant on a CD-ROM; or Looking at a paper catalog.
2	The cardholder selects items to be purchased.
3	The cardholder is presented with an order form containing the list of items, their prices, ant a total prices including shipping, handling and taxes. This order form may be delivered electronically from the merchant's server or created on the cardholder's computer by electronic shopping software.
4	The cardholder selects the means of payment.
5	This cardholder sends the merchant a completed order along with a means of payment.
6	The merchant request payment authorization from the cardholder's financial institution.
7	The merchant sends confirmation of the order.
8	The merchant ships the goods or performs the requested services from the order
9	The merchant request payment from the cardholder's financial institution.

Within the scope:

The following are within the scope of these specifications:

- Application of cryptographic algorithms
- Certificate message and object formats
- Purchase messages and object formats
- Authorization messages and object formats

- Message protocols between participants

Outside the scope:

The following are outside the scope for the set specifications:

- Message protocols for offers, shopping, delivery of goods, etc.
- Operational issues such as the criteria set by individual financial institutions for the issuance of cardholders and merchant certificates
- Screen formats including the content, presentation and layout of order entry forms as defined by each merchant
- General payments beyond the domain of payment cards
- Security of data on cardholders, merchant. And payment gateway systems including protection from viruses, Trojan horse programs, and hackers.

3. Explain about concept of payment system.

CONCEPTS

1. Payment System Participation
2. Cryptography
3. Certificate Issurance
4. Kinds of shopping

PAYMENT SYSTEM PARTICPATION

Interaction of participants

SET (Secured Electronic Transaction) changes the way the participants in the payment system interact. In a face-to-face retail transaction or a mail order transaction, the electronic processing of the transaction begins with the merchant or the acquirer. However, in an SET transaction, the electronic processing of the transaction begins with the cardholder.

Cardholder

In the electronic commerce environment, consumers and corporate purchasers interact with merchants form personal computers. A cardholders uses a payment card that has been issued by an issuer, SET ensures that the interactions the cardholders has with a merchant keep the payment card account information confidential.

Issuer

An issuer is the financial institution that establishes an account for a cardholder and issues the payment card. The issuer guarantees payment for authorizes transactions using the payment card in accordance with payment card brand regulations and local legislation.

Merchant

A merchant offers goods for sale or provides services in exchange for payment. SET allows a merchant to offer electronic interactions that cardholders can use securely.

Acquirer

An acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Payment gateway

A payment gateway is a device operated by an acquirer or a designated third party that processes merchant payment messages

Brand

Financial institutions have founded bankcard associations that protect and advertise the brand, establish and enforce rules for use and acceptance for their bankcards, and provide networks to interconnect the financial institutions.

Third parties

Issuers and acquirers sometimes choose to assign the processing of payment card transactions to third party processors. This document does not distinguish between the financial institution and the processor of the processor of the transactions.

CRYPTOGRAPHY(4.Explain various secure e-payment system Or Explain various secure e-payment systems and its certificate issuance. Or What are the technique used for secure e-payment system and explain.)

Protection of sensitive information

- Cryptography has been used for centuries to protect sensitive information as it is transmitted from one location to another.
- In a Cryptography graphic system, a message is encrypted using a key. The resulting cipher text is then transmitted to the recipient where it is decrypted using a key to produce the original message.
- There are two primary encryption methods in use today: secret-key encryption and public key Cryptography. SET uses both methods in its encryption process.

Secret key Cryptography

Secret key Cryptography also known as symmetric Secret key Cryptography, use the same key to encrypt and decrypt the message. Therefore, the sender and recipient of a message must share a secret, namely the key. A well known secret key Secret key Cryptography algorithm is the data encryption standard which is used by financial institutions to encrypt PINs.

Public key Cryptography

- Public key Cryptography, also known as asymmetric cryptography, uses two keys: one key to encrypt the message and the other key to decrypt the message.
- The two keys are mathematically related such that data encrypted with either key can only be decrypted using the other. Each user has two keys: a public key and private key. The user distributes the public key. Because of the relationship between the two keys, the user and anyone receiving the public key can be assured that data encrypted with the public key and sent to the user can only be decrypted by the user using the private key.

Encryption

Confidentially is ensured by the use of message encryption

- **Encryption: relationship of keys**

  When two users want to exchange messages securely, each transmits one component of their key pair, designated the private key. Because messages encrypted with the public key can only be decrypted using the private key, these messages can be transmitted over an insecure network without fear that an eavesdropper can use the key to read encrypted transmissions.

  Encryption: use of symmetric key

  SET will rely on cryptography to ensure message confidentially. In SET, message data will initially be encrypted using a randomly generated symmetric encryption key. This key, in turn, will be encrypted using the message recipient's public key. This is

referred to as digital envelope; the recipient decrypts it using his or her private key to obtain the randomly generated symmetric key and then uses the symmetric key to unlock the original message.

Digital Signatures

Integrity and authentication are ensured by the use of digital signatures.

Digital Signatures: relationship of keys

Because of the mathematical relationship between the public and private keys, data encrypted with either key can only be decrypted with the other. This allows the sender of a message to encrypt it using sender's private key. Any recipient can determine that the message came from the sender by decrypting the message using the sender's public key.

Digital Signature: using message digests

When combined with message digests, encryption using the private key allows users to digitally sign messages. A message digest is a value generated for a message that is unique to that message. A message digest is generated by passing the message through a one way cryptographic function i.e., one that cannot be reversed. When the digest of a message is encrypted using the sender's private key and is appended to the original message, the result is known as the digital signature of the message.

Digital Signature: Example

For example, Alice computes the message digest of a property description and encrypts it with her private key yielding a digital signature for the message. She transmits both the message and the digital signature to Bob. When Bob receives the message, he computes the message digest of the property description and decrypts the digital signature with Alice's public key. If the two values match, Bob knows that the message was signed using Alice's private key and that it has not changed since it was signed.

Two key pairs

SET uses a distinct public/private key pair to create the digital signature. Thus, each SET participant will possess of encryption and decryption, and a ―signature‖ pair for the creation and verification of digital signatures.

Certificates: need for authentication

Before two parties use public-key cryptography to conduct business, each wants to be sure that the other party is authentication. Before Bob accepts a message with Alice's digital signature, he wants to be sure that the public key belongs to Alice and not to someone masquerading as Alice on an open network. One way to sure that the public key belongs to Alice is to receive it over a secure channel directly from Alice. However, in most circumstances this solution is not practical.

Certificates: need for trusted third party

An alternative to secure transmission of the key is to use a trusted third party to authenticate that the public key belongs to Alice. Such a party is known as a Certificate Authority (CA). The certificate authority authenticates Alice's claims according to its published policies.

SET authentication

The means that a financial institution uses to authenticate a cardholder or merchant is not defined by these specifications. Each payment card brand and financial institution will select an appropriate method.

ENCRYPTION SUMMARY

Encryption

The encryption diagram consists of

1. Alice runs the property description through one-way algorithm to produce a unique value known as the message digest.
2. She then encrypts the message digest with her private signature key to produce the digital signature.
3. Next, she generates a random symmetric key and uses it to encrypt the property description, her signature and a copy of her certificate. Which contains her public signature key? In order to decrypt the property description, bob will require a secure copy of this random symmetric key.
4. Bob's certificate which Alice must have obtained prior to initiating secure communication with him contains a copy of his public key-exchange key. To ensure secure transmission of the symmetric key, Alice encrypts it using bob's public key-exchange key. The encrypted key referred to as the digital envelope is sent to bob along with the encrypted message itself.
5. Finally, she sends a message to bob consisting of the following: the symmetrically encrypted property description, signature and certificate as well as the asymmetrically encrypted symmetric key.

Decryption

6. Bob receives the message from Alice and decrypts the digital envelope with his private key exchange key to retrieve the symmetric key.
7. He uses the symmetric key to decrypt the property description, Alice signature and her certificate.
8. He decrypts Alice digital signature with her public signature key, which he acquires from her certificate. This recovers the original message digest of the property description.
9. He runs the property description through the same one-way algorithm used by Alice and produces a new message digest of the decrypted property description.
10. Finally he compares his message digest to the one obtained from Alice digital signature.

Introduction of dual signature

SET introduces a new application of digital signatures, namely the concept of dual signatures. To understand the need for this new concept, consider the following scenario: Bob wants to send Alice and offer to purchase a piece of property and an authorization to his bank to transfer the money if Alice accepts the offer, But bob does not want the bank to see the terms of the offer nor does he want Alice to see his account information.

Generation of a dual signature

A dual signature is generated by creating the message digest of both messages concatenating the two digests together; computing the message digest of the result and encrypting this digest with the signer's private signature key. The signer must include the message digest of the other message in order for the recipient to verify the dual signature.

Uses of dual signatures

Within set, dual signatures are used to link an order message sent to the merchant with the payment instructions containing account information sent to the acquired. When the merchant sends an authorization request to the acquirer, it includes the payment instruction sent to it by the cardholder and the message digest of the order information.

Import/export issues

A number of governments have regulations regarding the import or export of cryptography. As a
General rule these governments allow cryptography to be used when:

- The data being encrypted is of a financial nature;
- The content of the data is well defined
- The length of the data is limited ; and
- The cryptography cannot easily be used for other purposes

CERTIFICATE ISSUANCE

- Cardholder certificates function as an electronic representation of the payment card. Because they are digitally signed by a financial institution they cannot be altered by a third party and only the financial institution can generate one. A cardholder certificate does not contain the account number and expiration date.
- A certificate is only issued to the cardholder upon approval of the cardholder's issuing financial institution. By requesting a certificate a cardholder has indicated the intent to perform commerce via electronic means.

Merchant certificates

Merchant certificates function as an electronic substitute for the payment brand decal that appears in the store window. (The decal itself is a representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand)

- A merchant must have at least one pair of certificates in order to participate in the SET environment but there may be multiple certificate pairs per merchant. A merchant will have of certificates for each payment card brand that it accepts

Payment gateway certificates

- Payment gateway certificates are obtained by acquires or their processors for the systems that process authorization and capture messages. The gateway's encryption key which the cardholder gets form this certificate is used to protect the cardholder's account information
- Payment gateway certificates are issued to the acquirer by the payment brand

Acquirer certificates

- An acquirer must have certificates in order to operate a certificate Authority that can accept and process certificate requests directly from merchants over public and private networks. Those acquirers that choose to have the payment card brand process certificate requests on their behalf will not require certificate because they are not processing SET messages. Acquirers receive their certificates from the payment card brand

Issuer certificates

- An issuer must have certificates in order to operate a certificate authority that can accept and process certificate requests directly from cardholders over public and private

networks. Those issuers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Issuers receive their certificates from the payment card brand.

HIERARCHY OF TRUST

- SET certificates are verified through a hierarchy of trust. Each certificate is linked to the signature certificate of the entity that digitally signed it. By following the trust tree to a known trusted party one can be assured that the certificate is valid. For example a cardholder certificate is linked to the certificate of the Issuer (or the association on behalf of the issuer).

Root key validation

- Software can confirm that it has a valid root key by sending an initiate request of the certificate authority that contains the hash of the root certificate. In the event that the software does not have a valid root certificate, the certificate authority will send on in the response.

Root key replacement

- When the root key is generated a replacement key will also be generated. This replacement key is stored securely until it is needed.
- The self signed root certificate and the hash of the replacement key are distributed together.
- Software will be notified of the replacement through a message that contains a self signed certificate of the replacement root and the hash of the next replacement root key.
- Software validates the replacement root key by calculating its hash and comparing it with the hash of the replacement key contained in the root certificate.

KINDS OF SHOPPING (5.Describe about different types of shopping)

Variety of experience

- There are many ways that cardholders will shop. This section describes two ways. The SET protocol supports each of these shopping experiences and should support others as they are defined.

Online catalogues

- The growth of electronic commerce can largely be attributed to the popularity of the World Wide Web. Merchants can tap into this popularity by creating virtual storefronts on the Web that contain on line catalogues. These catalogues can be quickly promotions.
- Cardholders can visit these web pages selecting items for inclusion on an order.

Electronic catalogues

- Merchants may distribute catalogues on electronic media such as diskettes or CD-ROM. This approach allows that cardholder to browse through merchants off-line. With an on-line catalogue the merchant has to be concerned about bandwidth and may chose to include fewer graphics or reduce the resolution of the graphics. By providing an off-line catalogue such constraints are significantly reduced.

6.Explain Different type e-payment processing. Or Describe about e-payment processing with protocol description. (Nov 2014)(Apr 2015)

PAYMENT PROCESSING

OVERVIEW

Transaction described

This describes the flow of transaction as they are processed by various system.

SET defines a variety of transaction protocols that utilize the cryptographic concepts.

This action describes the following transactions:

- Cardholder registration
- Merchant registration
- Purchase request
- Payment authorization
- Payment capture

Other transactions

The following additional transactions are part of these specifications,

- Certificate query
- Purchase inquiry
- Purchase notification
- Sale transaction
- Authorization reversal
- Capture reversal
- Credit
- Credit reversal

A guide to the diagrams

Initial	participant
C	Cardholder
M	Merchant
P	Payment Gateway
GA	Certificate Authority

The following symbols are used in the detailed diagram

The teeth of the key indicate the key's owner.
Keys with ―PV‖ on the handle are private keys
Keys with ―PB‖ are public keys.
Keys with a diamond ( ) are signature keys
Keys with small key ( ) are key-exchange keys.
Dual signature, initial indicates which private key was used to create the signature
Certificates. The initial in the ―seal‖ indicates which private key was used to sign the certificate.
Symmetric key used to encrypt data.
Payment card used to indicate when the cardholder's account number is being transmitted.
Protected data used to represent account information sent in the digital envelope of registrations
Encrypted message including the digital envelope.

The data in the shaded region has been encrypted using a randomly generated symmetric key.

Protocol description

The description of the processing differ from the formal protocol definition, the formal protocol definition take precedence.

Certificate Authority functions

The primary authorities are to:

- Receive registration requests;
- Process and approve/decline requests; and
- Issue certificates.

Payment card brands and individual financial institutions will review their business needs for these functions to select a solution for implementation. The selected solution may be to implement a single server device that provides the Certificate Authority functions or multiple devices that distribute the processing. Payment card brands and financial institutions will select an appropriate solution based on their individual business needs.

Optional cardholder certificates

Payment card brands at their option may allow cardholders to process transactions without a certificate as a temporary measure to facilitate implementation of these specifications.

No digital signature

When a cardholder does not possess a signature certificate, no digital signature is generated. In place of the digital signature, the cardholder generates the message digest of the data and inserts the message digest into the digital envelope.

Assurance of integrity

The recipient of data from the cardholder uses the message digest from the digital envelope to confirm the integrity of the data.

Strength of cardholder certificates

The strength depends on the methods employed by the payment card brand and the payment card issuer to authenticate the cardholder prior to the certificate being issued.

Cardholder authentication

If a cardholder signature certificate is not present, authentication of the cardholder must be performed by other means where SET uses cardholder certificate to confirm.

CARDHOLDER REGISTRATION (7.Briefly discuss about cash holder registration)

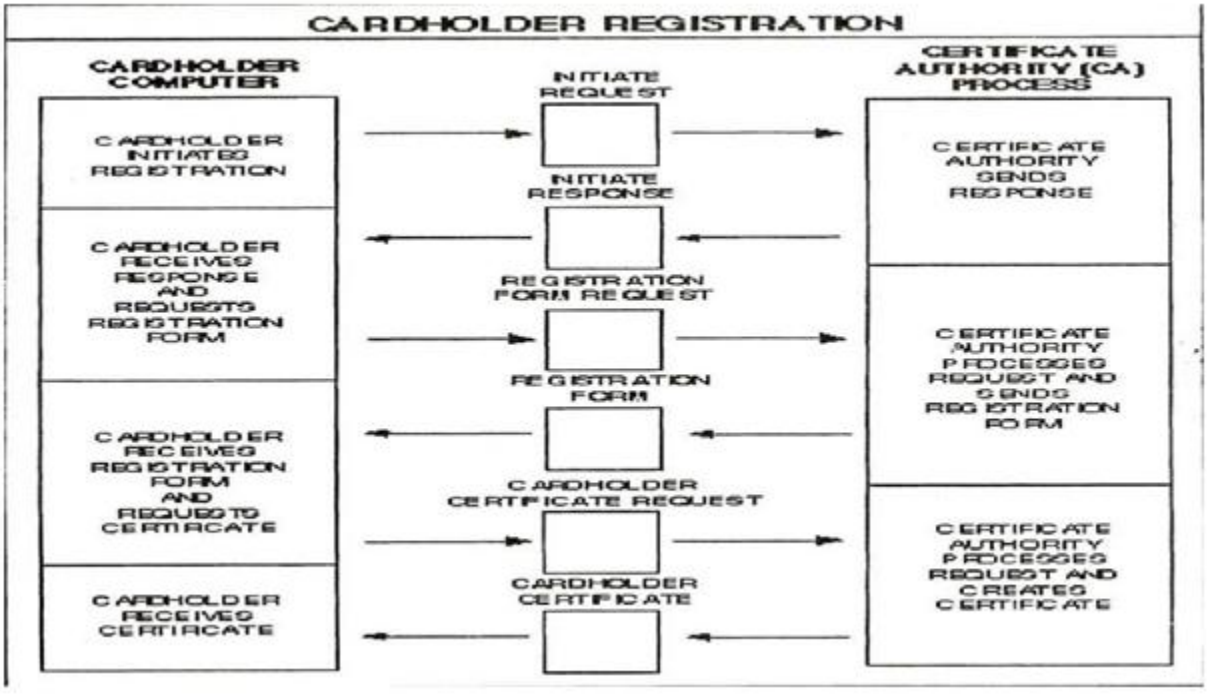
This scenario is divided into its seven fundamental steps.

Cardholder must register with a Certificate Authority (CA) before they can send SET messages to merchants.

For sending SET messages to CA the cardholder must have copy of the CA public key-exchange key, copy of the registration form from the cardholder's financial institution.

The CA provides the registration form, for this it requires two exchanges between the cardholder software and the CA.

The registration process is started when the cardholder software requests a copy of the CA's key-exchange certificate.



- **Cardholder initiates registration**

CARDHOLDER COMPUTER

INITIATE REQUEST

1. Cardholder software sends initiative

Request to CA → REQ

C INIT

C INIT REQ

C INIT REG

2. CA receives initiative request

INITIATE RESPONSE

3. CA generates response and digitally signs it by generating a msg digest of the response & encrypting it with the CA private signature key.

4. CA sends response along with the CA certificates to cardholder

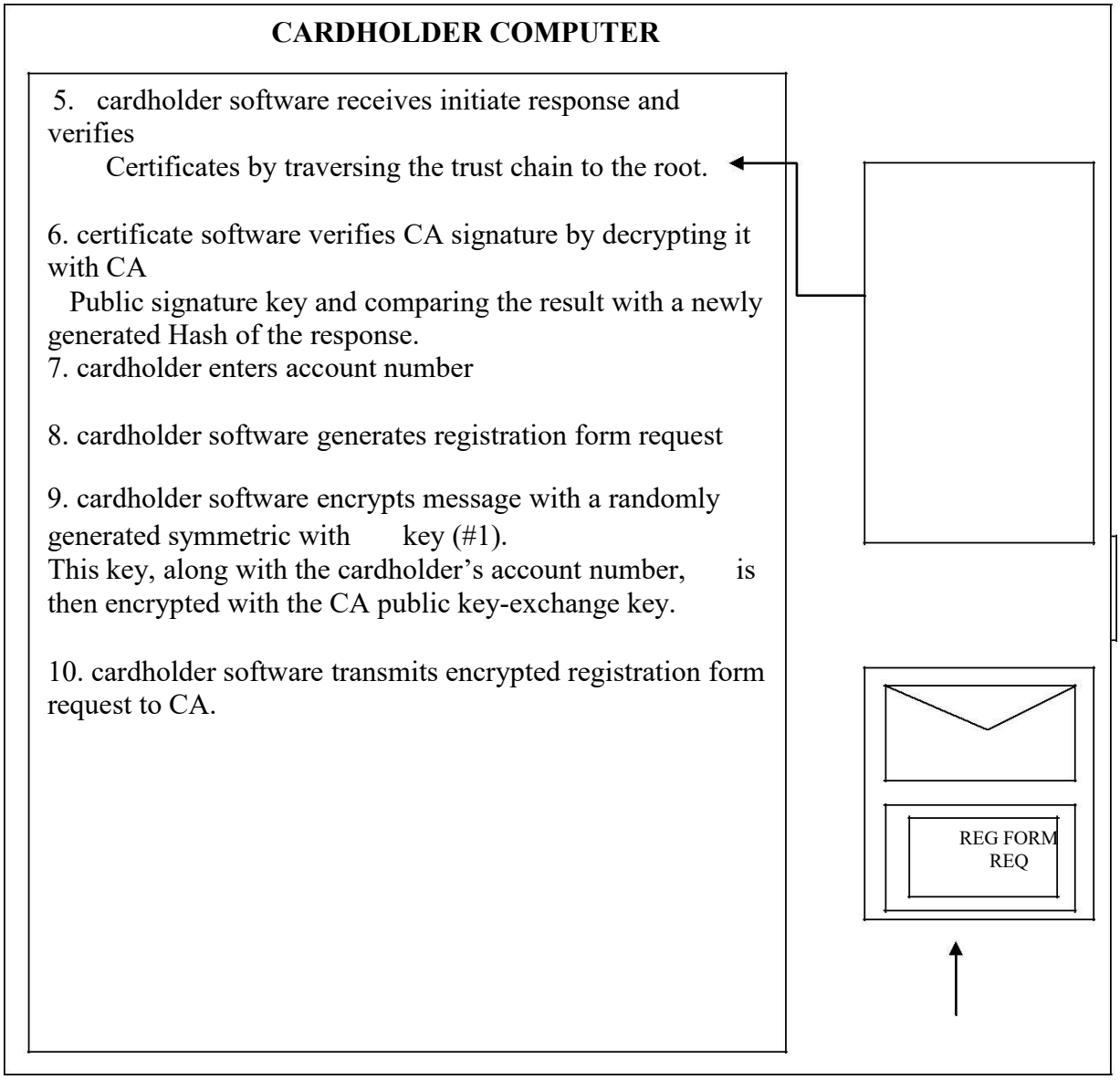
CAP RBG

Once the software has a copy of the CA key-exchange certificate, the cardholder can request a registration form. The cardholder software creates a registration form request message then it generates a random symmetric encryption key. This random key is used to encrypt the registration form request message, which is then encrypted along with the account number into the digital envelope using the CA public key-exchange key. Finally the software transmits all of these components to the CA.

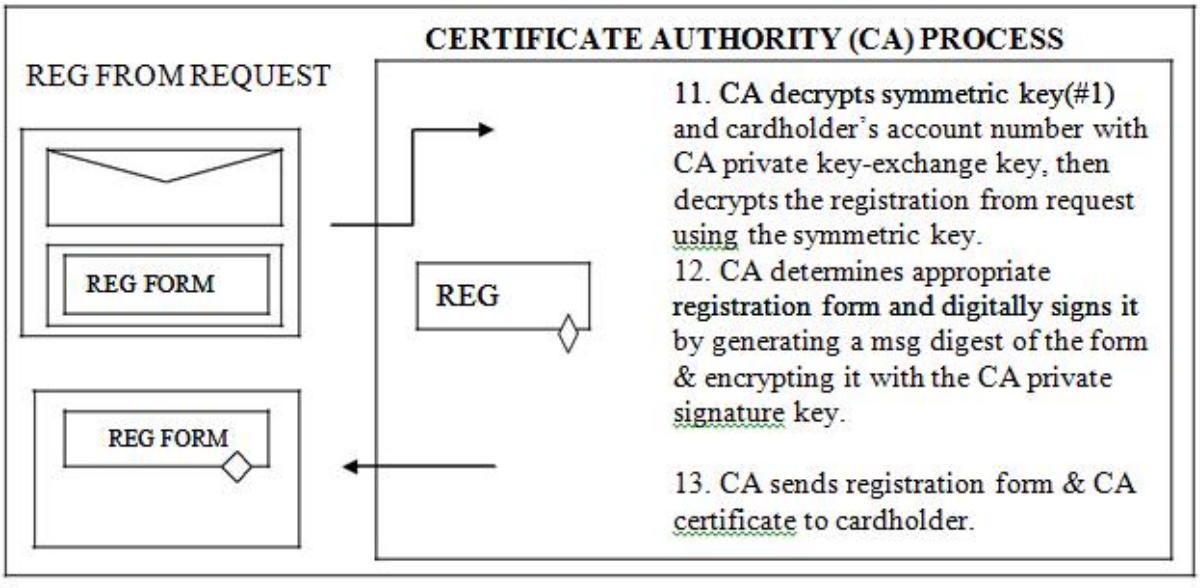
Cardholder receives response and requests registration form

The CA identifies the cardholder's financial institution and selects the appropriate registration form.

It digitally signs and then returns this registration form to the cardholder. The CA may not have a copy of the registration form but can inform the cardholder software.



The cardholder needs a signature public/private key pair for use with SET. The cardholder software generates this key pair if it does not already exist.



To register an account, the cardholder fills out the registration form that was returned by the CA with information such as the cardholder's name, expiration date, account billing address, and any additional information the issuing financial institution deems necessary to identify the certificate requester as the valid cardholder.

The cardholder software generates a random number that will be used by the CA in generating the certificate, which is combining with the public key in the registration message.

The software digitally signs the registration messages, and generates two random symmetric encryption keys. It places one random key inside the message; the CA will use this key to enc the response. It uses the other random key to encrypted the registration message. This key is then encrypted along with the acc number, expiration date, and the random number into the digital envelope using the CA public key-exchange key. Finally the software transmits all of these components to the CA.

Cardholder receives registration form and requests certificate

When the CA receives the cardholder's request, it decrypted the digital envelope to obtain the symmetric encrypted Key, the account Information And the random number generated by the cardholder Software.

- It uses the symmetric key to decrypted the registration request.
- If signature Is verified, the message processing continues; otherwise, the message is rejected and an appropriate response message is returned to the cardholder
- The CA must verify the information from the registration request using the cardholder's account Information
- If the information In the registration request is verified, a certificate will be issued. First the CA generates a random number that is combined with the random number created by the cardholder Software to generate a secret value, which is used to protect the account Information In the cardholder Certificate.

- The value are encoded using one way hashing algorithm, the result is placed into the cardholder Certificate.
- A response message containing the random number generated by the CA and the other information Is then generated and encrypted Using the symmetric key sent by the cardholder Software in the registration message the response is then transmitted to the cardholder.

Certificate authority processes request and creates certificate

When the cardholder Software receives the response from the CA, it verifies the certificate By traversing the trust chain to the root key, then cardholder Software decrypted the registration response using the symmetric encrypted Key that it sent to the CA in the registration message, combines the random number returned by the CA with the value that it sent in the registration message to determine the secrete value.

MERCHANT REGISTRATION

Merchants must register with a certificate Authority (CA) before they can receive the SET payment instructions from cardholder Or process SET transactions through a payment gateway. To send the merchant mush has a copy of the CA public key-exchange key, a copy of registration form from the merchant's financial institution. The merchant software must identify the Acquirer to the CA. The registration process Is started when the merchant software request a copy of the CA's key-exchange certificate And the appropriate registration form.

Merchant requests registration form

The CA identifies the merchant's financial institution and selects the approved egistration form. It returns third registration form alone with a copy of its own key-exchange certificate to the merchant.

Certificate authority processes request and sends registration form

- The merchant software verifies the CA certificate By traversing the trust chain to the root key, it must hold a CA certificate
- The merchant can register to accept SET payment instructions and process SET transactions. The merchant needs two public/private key pairs for use with SET key-exchange and signature the merchant Software generates these key pairs if they do not already exist.
- To register, the merchant Fills out the registration form, the merchant Software takes this registration form and combines it with the public keys in a registration message the software digitally signs the registration message. The software generates a random symmetric encryption key, which is used to encrypt the message finally the software transmits all of these components to the CA.

Merchant receives registration form and requests certificates

When the CA receives the merchant's request, it decrypts the digital envelope to obtain the symmetric encryption key, which it uses to decrypt the registration request.

If signature is verified, the message processing continues; otherwise, the message is rejected and an appropriate response message is returned to the merchant

The CA must verify the information from the registration request using known merchant Information

If the information in the registration request is verified, the CA creates and digitally signs the merchant Certificate

The certificate Are then encrypted Using a randomly generated symmetric key, which in turn is encrypted Using the merchant Public key-exchange key. the response is then transmitted to the merchant.

Certificate authority processes request and creates certificate

When the merchant software receives the response from the CA, it decrypted the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypted the registration response containing the merchant Certificate

After the merchant Software verifies the certificate by traversing the trust chain to the root key, it stores the certificates on the merchant's computer.

PURCHASE REQUEST

The SET protocol is invoked after the cardholder has completed browsing, selection and ordering. The cardholder will have selected a payment card as the means of payment. In order to send SET messages to merchant, the cardholder must have a copy of the merchant public key-exchange key as well as the payment gateway's key-exchange keys. When cardholder software requests a copy of the merchants and gateway's certificates. The message from the cardholder indicates which payment card brand will be used for the transaction.

Cardholder initiates request

When the merchant receives the request, it assigns a unique transaction identifier to the message. It then transmits the merchant and gateway certificates that correspond to the payment card brand indicated by the cardholder along with the transaction identifier to the cardholder.

Merchant sends certificate(s)

The cardholder software verifies the merchant and gateway certificates. It creates the order Information (OI) and Payment Instruction (PI).

It places the transaction identifier assigned by the merchant in the OI and PI, for linking the OI and PI together when the merchant requests authorization. This information is exchanges between the cardholder and merchant software during the shopping phase before the first SET message.

The cardholder Software generates a dual signature For the OI and PI by computing the msg. digests of both, concatenating the two digests, computing the msg. digest of the result and encrypting that using the cardholder private signature Key.

Then the software generates a random Symmetric encryption key & uses it to encrypt the dual signed PI. The software then encrypts the cardholder Account No. as well as the random Symmetric Key used to encrypted The PI into a digital envelope using the payment gateway's key-exchange key. Finally the software transmits a msg. consisting of the OI and the PI to the merchant.

Cardholder Receives response and sends request

When the merchant software receives the order, it verifies the cardholder signature Certificate By the traversing the trust chain to the root key. The merchant Software then processes the order including the payment authorization. After the OI has been processed, the merchant software generates & digitally signs a purchase response message. If transaction was approved, the merchant will perform the services indicated in the order.

Merchant processes request message

When the cardholder Software receives the purchase response message from the merchant, it verifies the merchant Signature Certificate and uses merchant Public signature Key to check the merchant Digital signature, and then it takes some action based on the contents of the response message. The cardholder can determine the status of the order by sending an order inquiry msg.

PAYMENT AUTHORIZATION

During the processing of an order from a cardholder, the merchant will authorize the transaction. The merchant software generates and digitally signs an authorization request, which the amount to be authorized, the transaction identifier from the OI and the other information about the transaction. The request is then encrypted using the public key-exchange key of the payment gateway. Then the authorization request and the cardholder payment instructions are transmitted to the payment gateway.

Merchant requests authorization

When the payment gateway receives the authorization request, it decrypts the digital envelope of the authorization request to obtain the symmetric encryption key.

- It uses the symmetric key to decrypt the request. It then verifies the merchant signature certificate by traversing the trust chain to the root key; it also verifies that the certificate has not expired.
- It uses the merchant public signature key to ensure the request was signed using the merchant private signature key.
- Then the payment gateway decrypts the digital envelope of the payment instructions to obtain the symmetric encryption key and the account information by using symmetric key.
- It verifies the cardholder signature certificate by traversing the trust chain to the root; it also verifies that the certificate has not expired.
- The payment gateway verifies that the transaction identifier received from the merchant matches the one in the cardholder payment instructions. Then it is formatted and sends a authorization request to the issuer via a payment system.
- After authorization, the payment gateway generates and signs a response message. It is encrypted using a new randomly generated symmetric key, which is again encrypted using the merchant public key-exchange key. Finally the response Is transmitted to the merchant.

Payment gateway processes authorization request

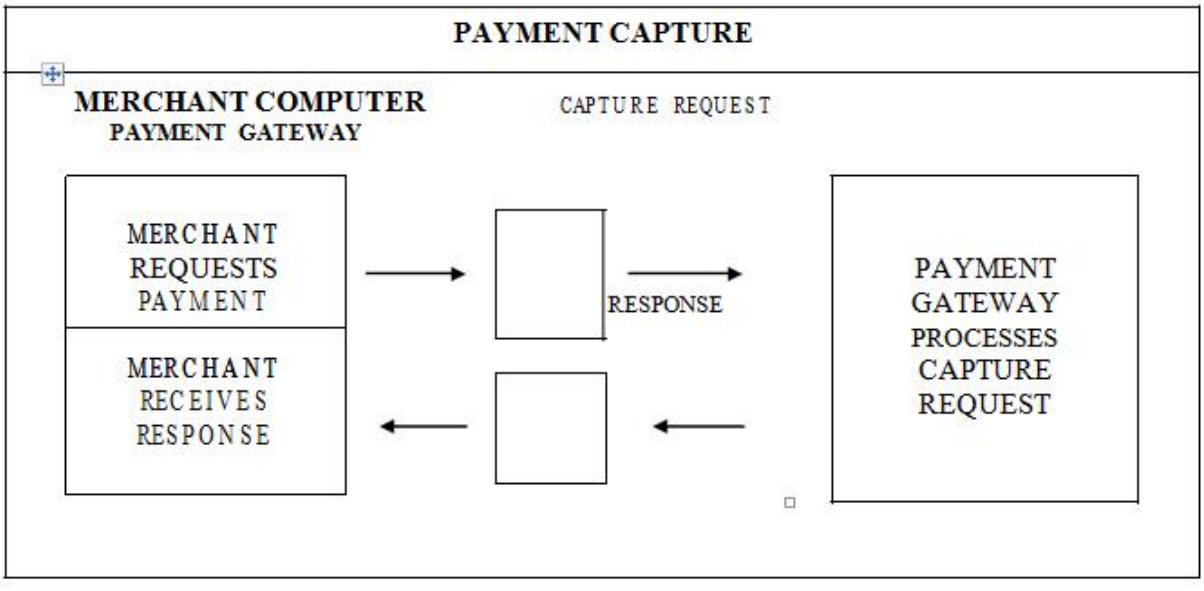
When the merchant software receives the authorization response message from the payment gateway, it decrypts the digital envelope to obtain the symmetric encryption key.

- Uses symmetric key to decrypt the response message, then verifies the payment gateway signature certificate by traversing the trust chain to the root key.
- It uses the payment gateway public signature key to check the payment gateway digital signature
- The merchant software will store the authorization response and the capture token to be used when requesting payment through a capture request.
- The merchant then completes processing of the cardholder's order by shipping the goods or performing the services indicated in the order.

PAYMENT CAPTURE

The diagram provides a high level overview of a merchant's payment capture process.

Payment capture



It is divided into its three fundamental steps.

After completing the processing of an order from a cardholder the merchant will request payment.

The merchant software generates and digitally signs a capture request, the request is then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the public key-exchange key of the payment gateway.

The capture request is then transmitted to the payment gateway.

When the payment gateway receives the capture request, it decrypts the digital envelope of the capture request to obtain the symmetric encryption key.

It uses the symmetric key to decrypt the request. It then uses the merchant public signature key to ensure the request was signed using the merchant private signature key.

The payment gateway decrypts the capture token and then uses the information from the capture request and the capture token to format a clearing request, which it sends to the issuer via a payment card payment system.

This then generates and digitally signs a capture response message, which includes a copy of the payment gateway signature certificate. The response is then encrypted and transmitted to the merchant.

Payment gateway processes capture request

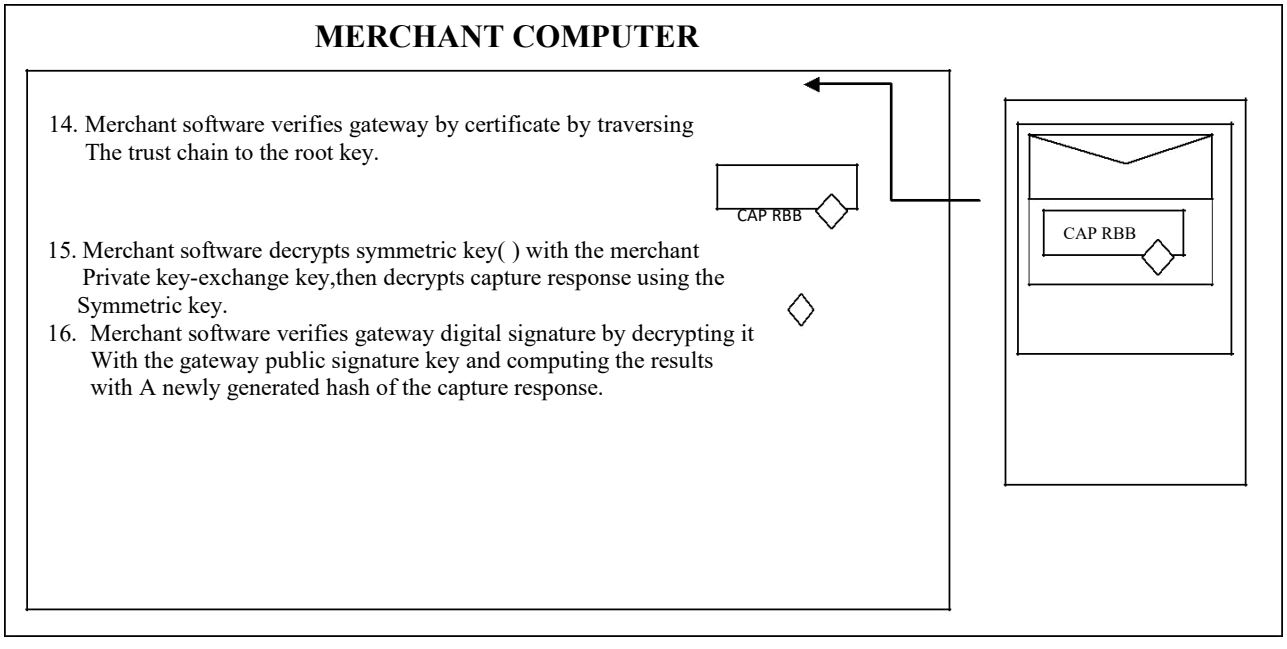
When the merchant software receives the capture response message from the payment gateway, it decrypts the digital envelope to obtain the symmetric encryption key.

It uses the symmetric key to decrypt the response message. It then verifies the payment gateway signature certificate by traversing the trust chain to the root key.

It uses the payment gateway public signature key to check the payment gateway digital signature.

The merchant software will store the capture response to be used for reconciliation with payment received from the acquirer.

Merchant receives response



Purchase inquiry

Cardholders can check the status of the processing of an order after the purchase response has been received by sending an order inquiry.

It does not include status of back ordered goods but indicate the status of authorization, capture and credit processing.

Authorization reversal

- This message allows a merchant to correct previous authorization requests.
- If part of the order will not be completed, the merchant will reverse part of the amount of the authorization.

Capture reversal

This message allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.

Credit

This message allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping.

Payment gateway certificate request

This message allows a merchant to query the payment gateway and receive a copy of the gateway's current key-exchange and signature certificates.

Batch Administration

This message allows a merchant to communicate information to the payment gateway regarding merchant batches.

8. Explain about email and secure e-mail technologies for E- Commerce.

THE MEANS OF DISTRIBUTION:

Electronic mail and messaging systems are an increasingly important part of an enterprise's computing and communications strategy. E-mail can be distributed over a private enterprise network, on-line networks (such as AOL), and the Internet. The growth in the subscriber population of Internet-based services for both individuals and businesses, makes Internet e-mail a pervasive tool.

- Most companies using the Internet for electronic commerce or EDI use mail communications with customers and business partners; they also use FTP for accessing public archives and for delivering software patches. As described elsewhere, the Internet provides a variety of capabilities for e-commerce/EDI use, including e-mail, file transfer, World Wide Web, and remote logins.
- TCP/IP provides the underlying transport protocol; the applications support different protocols, dependent on function. For example, a business application may need to utilize SMTP for mail, FTP for file transfer, HTTP for Worldwide Web access, and Telnet for remote logins. Each of these protocols supports different capabilities with respect to use and value-added functions
  such as security, encryption, and non repudiation.

- The Internet Engineering Task Force (IETF) meets regularly to discuss operational and technical issues impacting the Internet community. Capabilities related to security are under development or have recently been developed by the IETF.

- Working groups are set up for further investigation of important issues. Anyone can attend either of these meetings and become a member of a working group. Each working group has the responsibility of producing documentation and deciding how issues should be handled. The reports are called RFCs (Requests for Comments).

- To obtain an RFC, one can send a mail message to rfc-info@isi.edu with a message body of Retrieve: RFC
- Doc-ID: RFCxxxx
- where xxxz is the number of the RFC.
- The original RFCs that define how Internet e-mail messages are transmitted and how the format of the e-mail messages should appear are RFC-821' and RFC-822;8 these have been made obsolete by RFC-1123.
- SMTP performs the message transmission function, but only supports seven-bit American Standard Code for Information Interchange (ASCII) transmissions and limits the maximum message size.
- Modifications to SMTP were needed to address the needs of e-commerce/EDI. Some of these modifications came in the form of Multipurpose Internet Mail Extensions (MIME), as described in RFC-15219.
- MIME defines mail body part structure and content types that pro-vided an SMTP-compatible way to encapsulate documents in e-mail messages, while supporting multipart content types including text, audio, image, video, and even application data.

- MIME also provides support for several content-transfer encodings including base64, which enables incorporation of 8-bit binary data as 7-bit ASCII data.
- Further refinements were introduced in RFC-1767 to specifically address the encapsulation of EDI objects within MIME. This permitted the transmission of EDI transactions through Internet mail supporting both EDIFACT and ANSI X12 EDI standards as MIME content types and ensured that EDI objects retained their syntax and semantics during transmission'-'.

A MODEL FOR MESSAGE HANDLING:

ITU-T model:

- In 1971, the International Federation for Information Processing, a prestandards organization, developed a model for message handling. This model was eventually adopted and expanded by the International Telecommunication Union-Telecommunication (ITU-T), which developed the X.400 series recommendations, Message Handling System (MHS).

- Although Internet mail is not based on ITU-T standards, it is useful to look at this abstraction.
- E-mail messages are transported by a message transfer system (MTS), which is

  composed of one or more message transfer agents (MTAs). At the borders of the system, a user agent (UA) acts on behalf of a user and interfaces to its local message transfer agent.10-" From the perspective of the message transfer system, the e-mail message being sent is called the content, and all delivery information associated with the message is the envelope.

- In theory, the MTS is not aware of the structure of the content it transports; the UAs bilaterally agree as to what this structure is. Although there are no strict requirements as to the structure, there are usually two types of content in each e-mail message: control information (often called the headers) and data information (often called the body). A way of thinking about all these terms is as follows:
    - The envelope is meaningful to the message transfer agents.
    - The headers are meaningful to the user agents.
    - The body is meaningful to the users (people or programs).
- When an e-mail message is sent from one user to another, the following activities occur: the originating user indicates to the UA the address of the recipient; the UA places the destination address and the sender's address into the envelope and then posts the message through a posting slot to a message transfer agent, which involves a posting protocol in which the validity of those addresses and the syntax of the e-mail message are considered.
- Upon successful completion of the submission protocol, the MTA accepts the responsibility to deliver the e-mail message or, if delivery fails, to inform the originating user of the failure by generating an error report.
- After accepting responsibility to deliver the e-mail message, an MTA must decide if it can deliver the message directly to the recipient; if so, it delivers the e-mail message through a delivery slot to the recipient's UA, using a delivery protocol. If not, it contacts an adjacent MTA that is closer to the recipient and negotiates transfer of the e-mail message. This process repeats until some MTA is able to deliver the e-mail message or some MTA determines that the message is undeliverable. Given this model for e-mail, one realizes that:10, 11.
- E-mail transfer is third-party in nature: once an e-mail message passes through the posting slot, the user agent has no claims on the message. The MTS takes responsibility for the e-mail message at posting time and retains that responsibility until delivery time.

- E-mail transfer is store-and-forward in nature: the UAs for the originator and recipient need not be on-line simultaneously for mail to be submitted, transported, and delivered. In fact, only the node currently responsible for the
  e-mail message and the "next hop" taking responsibility for the 'message need be connected in'\\ order for the message to be transferred.

To summarize, there are three general protocols involved in the model:

- A messaging protocol used between two UAs
- A relaying protocol used between two MTAs
- A submission/delivery protocol used between an MTA and a UA

INTERNET APPARATUS:

We can view the Internet suite of protocols used for generic transmission as having four layers:

1. The interface layer describes physical and data-link technologies used to realize the transmission at the media (hardware) level.
2. The internet layer describes the internetworking technologies used to realize the internetworking function; this is realized with a connectionless mode network service, provided by the Internet Protocol (IP), originally defined in 1981 in RFC-791.
3. The transport layer describes the end-to-end technologies used to realize reliable communications between end systems; this is realized with a connection-oriented transport service provided by the Transmission Control Protocol (TCP), originally defined in 1981 in RFC-793.

4. The application layer describes the technologies used to provide end-user services.

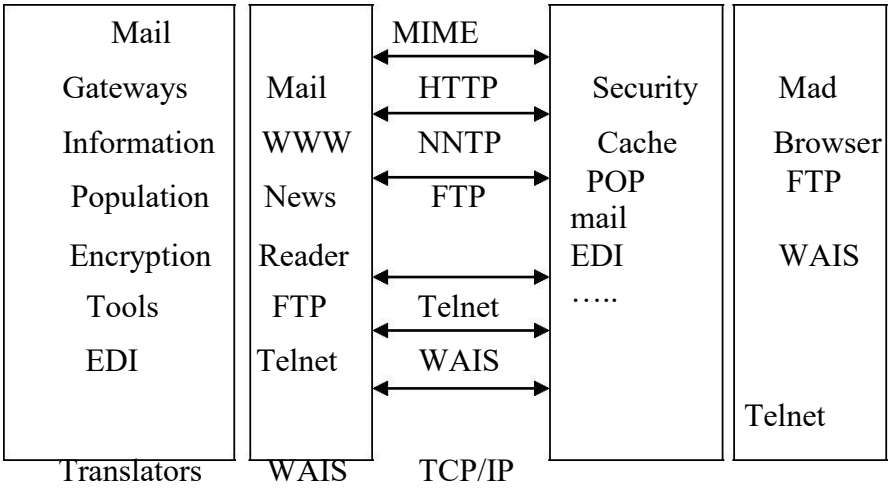
The Internet protocols related to mail-specific applications are as follows:

- The Simple Mail Transfer Protocol (SMTP), defined in RFC-821 (August 1982) and RFC-974 (January 1986), which provides store-and-forward service for textual e-mail messages, and RFC822 (August 1982), which defines the format of those messages.

- The Pbst Office Protocol (POP), defined in RFC-1225 (May 1991), which provides a simple mailbox retrieval service.
- The Network News T ansfer Protocol (NNTP), defined in RFC-977 (February 1986), which provides store-and-forward service for news messages.
- The Domain Name System (DNS), defined in RFC-1033 (November 1987) ,and RFC-1034 (November 1987), which provides map-ping between host names and network addresses.

In terms of the generic protocols described earlier, RFC-822 corresponds to the messaging protocol and SMTP corresponds to the relaying protocol. In the Internet suite, submission and delivery are local matters.

Shows how different business applications support different protocols depending on usage."



Business applications Vs Different protocols.

9. How does e-mail work? Explain. (Apr 2013)

Figure depicts how e-mail works. Basically, two architectures are involved in this diagram. The first architecture is commonly referred to as a file-based system. In this architecture, the mail client creates a file containing the message header, text, and pointers to attachments and posts it to a directory on a post office server.

Next, message-transport software, usually hosted on another PC, uses TCP/IP transport capabilities to route messages from post office to post office, as needed. The recipient's e-mail client periodically polls the local post office server's directory and notifies

the user when new mail arrives. The second example is the more popular client/server architecture.

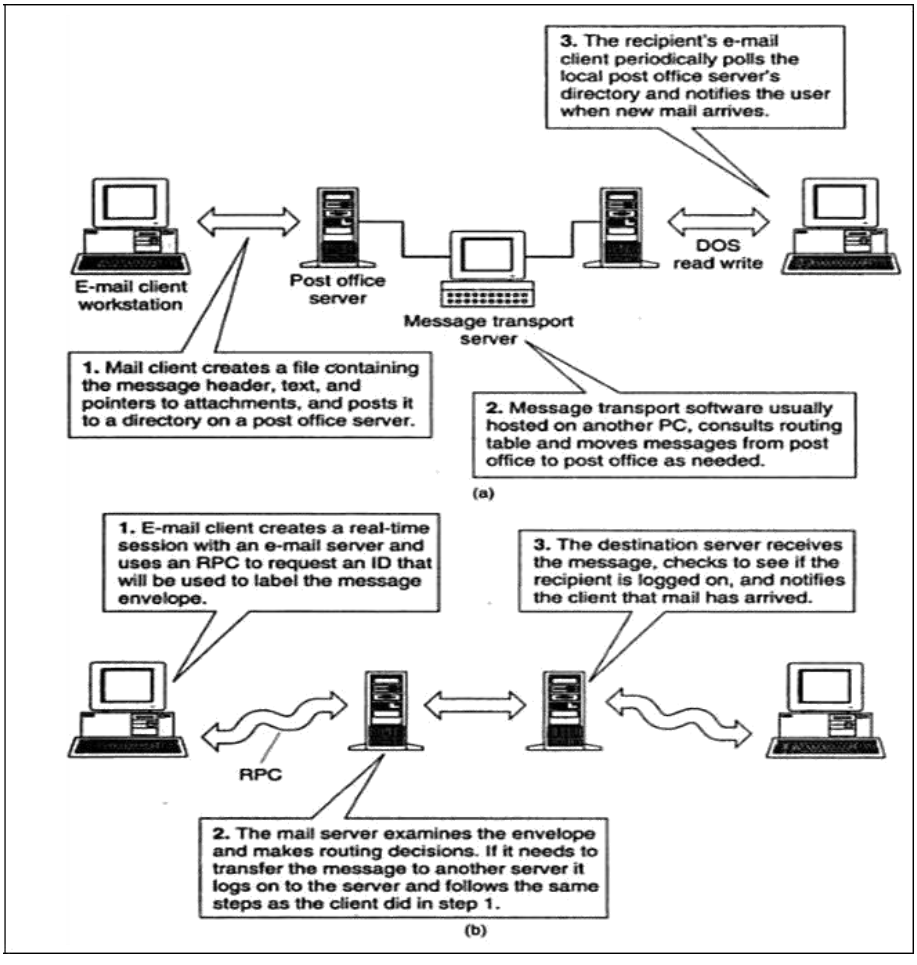
Here, the first step involves the e-mail client workstation creating a real-time session with an e-mail server and using a remote procedure call (RPC) to request an ID that will be used to label the message envelope. Next, the mail server examines the envelope and makes routing decisions. If it needs to transfer the message to another server, it does. The destination server receives the message, checks to see if the recip - ient is logged on, and notifies the client that mail has arrived. "Two basic components of an Internet e-mail message are the header and the body. The header requires the following lines:1z"

- **Delivery-Date:** This line shows the date and time the message was received in the mailbox.
- **Return-Path:** This line shows the reply address of the original sender.
- **Received:** Every entry in the header starting with Received represents a computer/gateway that has transferred the message, also referred to as a hop. If there are too many hops, the message will be bounced, or returned, to the original sender. A message will also bounce if the person is no longer found at that mail system.
- **Date:** This line shows the date and time the message left the sender. This will vary by several seconds or minutes from the delivery date line.
- **From:** This line specifies the full name and e-mail address of the original sender.
- **Message-ID:** This line serves as a unique identifier of each mail message. It includes the name of the machine sending the message, the date, time, and file name.
- **To:** Each person receiving the message will appear on this line. If there is more than one address, the addresses will be separated by a comma.
  - Some e-mail systems may add these lines at the Internet gateway and may not be transparent to the sender. Most e-mail systems will also add the following lines, even though they are not required: subject, content type, and priority status.
  - Internet e-mail addresses are made up of two parts: the user name and domain name. The user name is the account from which a message is sent. Some systems use the person's last name, while others use an alias which shields the name from the recipient. The domain name is an alphabetical mnemonic.
  - Machines use the IP number assigned by the InterNlC to every machine or network connected to the Internet. (Note: The InterNIC assigns and organizes domains and addresses, maintains directories of Internet users, and provides information for connection to the Internet.) A special (set of) computer(s), known as the Name Server, uses DNS (Domain Naming System) to convert the domain name into the proper IP address.
  - For example, an Internet address is denise_derkacs@merck.com. The user name is denise derkacs. The domain name is merck.com.

The last identifier in the domain name, .com, identifies this address as an ad-dress on a commercial organization's mail system. Other classical domain identifiers are

- .edu for educational institutions
- .gou for federal governmental offices or organizations
- .org for any other address that does not fall into the previous identifiers-usually nonprofit organizations

Figure: How E-Mail works three staps to mail delivery: (a) File-Based systems; (b) Client/Server-Based systems.



- Addresses outside the United States will append a two-letter country identifier, such as.ca (Canada).
- To send a message on a mail system, one needs to specify where the message is being sent. Let us take, for example, a message one sends to a user on the Rutgers University mail system, thatch@eden. rutgers.edu.

After the message has been written and the address is entered, the sender's MTA starts the sending process.

- The MTA first spools/queues the message to a directory on the machine that is running the transfer. This is to prevent the loss of the message, in case the machine is busy and one needs to try again. (Spooling messages is the same concept used in spooling print jobs on a busy public printer: the print job stays in the queue until the printer is ready to handle it.)

- This entire process takes place in only a few seconds. The protocol that allows these two machines to talk to one another about e-mail is SMTP. This protocol is often used on large systems, but can also be used by an MTA to connect smaller LANs to the Internet.
- SMTP gateways are typically referred to as Internet gateways. The SMTP gateway software allows users on a LAN-based mail system to send and receive Internet mail. The gateway software allows the transmission of Internet messages, transparent to the sender.
- The SMTP gateway translates the message to the acceptable RFC-822

format and then transfers the message to the TCP/IP transport system which will send the message to its final destination.12^{-2}2 The SMTP gateway also listens to the Internet for messages being sent to its LAN-based e-mail system. It translates the incoming message from the RFC-822 format to the format recognized by the local e-mail system. There are several ways in which attachments are handled. Some SMTP gateways support UUEncoded files and/or MIME attachments.

- In the early 1990s, the RFC-1425 (1993) extended the SMTP protocol to become ESMTP (Extended SMTP). The main reason for this extension was to allow the transmission of 8-bit binary files in addition to the 7-bit ASCII in e-mail messages. This allows programs, word processor files, and other application files to be transmitted over e-mail systems. SMTP will sometimes clear the eighth bit off every character to reduce it to an acceptable 7-bit format.

UUENCODE/UUDECODE:

- UUEncoding was created as a simple program to be used between a small group of users exchanging information on UNIX systems. The most common way to accomplish the transferring of 8-bit binary files to the •7-bit format was to use UNIX-to-UNIX Encoding (UUEncode).
- Some mail systems support UUEncoding and will automatically trans-late the data for the recipient. To avoid confusing and wasting the time of an e-mail recipient, one should include a statement letting the recip-ient know the attachment is UUEncoded.

10.Explain about MIME and data encoding techniques (Apr 2014)

MIME: Multipurpose Internet Mail Extensions

Multipurpose Internet Mail Extensions (MIME) (RFC-1521) provides Internet e-mail support for messages containing formatted text, sound images, video, and attachment. MIME is backward-compatible with SMTP messaging specifications and is easier to implement.

- Common way in which binary files are sent as e-mail on the internet.
- Content types are
  1. Primary type – indicates general content of the material
  2. Subtype – indicates the specific format
- Five basic primary MIME content-types are text, image, audio, video, and application.
- Composite MIME content types:
  1. Message – one can send the message inside another message, labeling it message/rfc822.
  2. Multipart – allows more than one piece of MIME to be included in a message.
     Eg: multiple objects, multipart/parallel, and multi-part/alternative.

- **MIME encoding:**
  - Uses many different encoding methods, depending on the file type it is sending.
  - MIME provides the ability to encapsulate different content types within the body of the message. With the MIME specification, RFC-1351, the internet was only able to transmit and receive ASCII type data. If one wants to send binary data, one had to convert it to ASCII-type data.

- The RFC-1521 version of MIME added the ability of Internet e-mail to handle binary and text data, as well as multiple body parts without conversion to ASCII.

An internet electronic mail message consists of two parts:

- The header
- The body

The header form a collection of field/value pairs structured is defined according to MIME.

The multipart/signed content type contains two body parts:

- The first body part is the body part over which the digital signature was created, including its MIME headers. It may contain valid MIME content type.
- The second body part contains the control information necessary to verify the digital signature.

Message Integrity Check (MIC)

The Message Integrity Check (MIC) is the name given to the quantity computed over the body part with a message digest or hash function, in support of the digital signature service.

The framework is provided in RFC-1847 by defining two new security subtypes of the MIME multipart content type: signed and encrypted.
In each of the security subtypes, there are two related body parts:

1. One for the protected data and
2. One for the control information.

The multipart/signed content type specifies how to support authentication and integrity services via digital signature. The control information is carried in the second of the two required body parts.
When creating a multipart/signed body part, the following sequence of steps describes the processing necessary:

1. The content of the body part is prepared according to a local convention. The content is then transformed into a MIME body part in canonical MIME format, including MIME headers.
2. The body part to be digitally signed is prepared for signature according to the value of the protocol parameter. The headers are included in the signature to protect the integrity of the MIME labeling of the data that is signed.
3. The body part is made available to the signature creation process, which made available to a MIME implementation two data streams:

- The control information necessary to verify the signature.
- The digitally signed body part.

When receiving a multipart/signed body part, the steps describes the processing to verify signature.

1. The first body part and the control information in the second part must be prepared for the signature verification process according to the value of the protocol parameter.
2. The prepared body parts must be made available to signature verification, then to the MIME implementation of the signature verification and the body part that was digitally signed.
3. The result is made available to the user and the MIME implementation continues processing with the verified body part.

When creating a multipart/encrypted body part, the following steps are required

1. The contents are prepared and transformed into a MIME body part in canonical MIME format, including MIME headers.
2. Then the body part is prepared for encryption according to the value of the protocol parameter.
3. The prepared body part is made available to the encryption process according to local convention, then to MIME implementation two data streams

   - The control information necessary to decrypt the body part
   - The encrypted body part.

When receiving a multipart/encrypted body part, the following steps are required.

1. The second body part and the control information in the first body part must be prepared for the decryption process according to the value of the protocol parameter.
2. The prepared body must be made available to the decryption process according to a local convention. The decryption process must make available to the MIME implementation.
3. The result is made available to the user and the MIME implementation continues processing with the decrypted body part.

MIME body parts

MIME specifications currently support seven body types:

1. Text,
2. Multipart,
3. Application,
4. Message,
5. Image,
6. Audio,
7. Video.

I) Text:

The text body part enables a message to contain simple message data such as ASCII and can be transported using the current 7-bit message content specified within MIME.

The richtext subtype is used to handle simple text format protocols that support boldfacing, italicizing, indenting, and so on. The richtext protocols are a reduced subset of the Standard Generalized Markup Language(SGML) commands. Two categories of character set are supported:

1. Charsert=US-ASCII
2. ISO-8859-1 through ISO-8859-9.

AI) Multipart:

This part consists of several body parts containing unrelated data. The contents are divided into subtypes.

The four initial subtypes are mixed, alternative, parallel, and digest. Only 7-bit, 8-bit, or binary may be used for the content type encoding.

Mixed: It ensures that a number of very different message content types, such as text, graphics, or images, can be transmitted in the same message.

Alternative: This subtype presents the same data in different formats, such as a word processing document in three representations such as ASCII, word for windows, and word perfect. **Parallel:** This subtype contains body parts that must be viewed at the same time.

Digest: This subtype is used when all the body parts are messages in their own right. It is important that an e-mail gateway interpret that the message body is a nested message as opposed to a video image or graphic.

- **Message:** It contains other messages, such as forwarded or transferred messages. It is the most basic body part in MIME and its subtypes are as follows:
- **RFC-822:** primary and most frequently used subtype, is the specification for a complete standard Internet e-mail message.
- **Partial:** It allows messages to be sent in parts through the e-mail networks. It is necessary when the message has exceeded the 64-KB.
- **External-Body:** It is for specifying larger data files, such as text, video, audio, or others that are not contained within the message.

- **Image:** It contains time varying images or images that contain movement-like motion picture and full motion video.

The current subtypes are

1. MPEG motion picture experts group – standard for digitally compressing movies.
2. GIF – compuServ's Graphic Image Format.

- **Audio:** It contains sound data such as voice or music. The basic subtype indicates 8-bit, integrated services digital network(ISDN), with a sample rate of 8000Hz.
- **Application:** It contains spreadsheets, calendar information, word processing documents, and presentation formats such a word perfect or Microsoft word. Its current subtypes are ODA-Office Document Architecture.
- **Postscript:** It defined by Adobe Systems and supports high-quality postscripts printer output. It should not be used with nonprinter interpreters.

MIME data encoding techniques:

The current SMTP network only supports 7-bit ASCII, up to 1000 characters per line of data, and a normal message length of 64KB.

ESMTP supports binary data exchange.

The RFC-821(SMTP) –compliant networks will not handle binary data contained in the MIME structure.

RFC-1521 specifies that the body of the message can be encoded in a form that will be transportable by the SMTP network. A new field called Content-Transfer-Encoding has been added to the header of the RFC-822 message. It may have one of the following six different encoding values:

Base64

It is for any series of octets and is used in Private Enhanced Messaging(PEM), specified in RFC-1113. Binary input strings are converted to a series of 65 ASCII characters which are the only ones that are represented the same in ISO 646, US ASCII, and EBCDIC.

8-bit

Eight bit means that lines are of the same form as they are in 7-bit encoding. It also means that the body has not been encoded.

Binary

Binary means that there is not a line length limit within the message. It also means that the body has not been encoded.

Quoted printable encoding

This encoding value is for data that generally uses an ASCII character set. It allows unsophisticated MTAs to convey data, the format of which may be a little off, readable by the end user.

7-bit:

Seven-bit is the default value when the Content-Transfer-Encoding header field is not present in the header. This means that the data is of the type specified in RFC-821,7-bit US ASCII code, and has not been encoded.

x-token

This value is for defining a nonstandard encoding which has been put in place by mutual agreement between the parties to the transfer.

Address directory

The SMTP architecture does not define an address directory. Users find names by enrolling in distribution lists, using a utility program called FINGER to search on their system and a query facility called WHOIS to find addresses. ITU-T X.500 directory services are also expected to become available.

11.Explain S/MIME (Apr 2013)

S/MIME was designed to add security to e-mail messages in MIME format. The security services offered are authentication (using digital signatures) and privacy (using encryption).

S/MIME joins crypto-graphic constructs with standard e-mail practices and was designed to be interoperable, so that any two packages that implement S/MIME can communicate securely.

S/MIME is a specification for secure electronic mail. S/MIME was designed to add security to e-mail messages in MIME format. The security services offered are authentication using digital signatures and privacy using encryption.

Need for S/MIME:

There is a growing demand for e-mail security. S/MIME melds proven cryptographic constructs with standard e-mail practices. More importantly, it was designed to be interoperable, so that any two packages that implement S/MIME can communicate securely.

How does SIMIME compare with PGP and PEM?

S/MIME PGP, and PEM all specify methods for securing electronic mail. All offer privacy and authentication services. Since PGP and PEM are all different, they need to be compared with S/MIME individually.

PGP can be thought of as both a specification and an application. PGP relies on users to exchange keys and establish trust in each other.

Cryptographic Algorithms In S/MIME

Hybrid approach to providing security often referred to as envelope. The bulk message encryption is done with a iq cipher, and a public-key (asymmetric encryption) algorithm key exchange.

A public-key algorithm is also used features. S/MIME recommends three symmetric encryption DES,32 Triple-DES, and RC2.

Does S/MIME use digital certificates?

S/MIME does use digital certificates. The X.509 format is used due to its wide acceptance as the standard for digital certificates.19 VeriSign has set up a hierarchy specifically to support the S/MIME effort.

Does S/MIME only work on the Internet?

S/MIME is not specific to the Internet and can be used in any electronic mail environment. This is accomplished by making the implementation guidelines flexible and scalable.

Is a public domain implementation of S/MIME available?

A free version of S/MIME was planned to be available soon. A future version of the popular public domain mailer RIPEM will implement S/MIME.

RIPEM is a program developed by Mark Riordan that enables Internet e-mail. RIPEM provides both encryption and digital signatures. RIPEM is free for noncommercial use.

12.Expalin MOSS: Message Object Security Services

- MIME Object Security Services (MOSS), defined in RFC-1848,37 is a protocol used to apply digital signature and encryption services to MIME objects.
- The services are offered through the use of end-to-end cryptography between an originator and a recipient, at the application layer. This protocol is needed since MIME itself does not provide for the application of security services.

- MOSS is a protocol that uses the multi- part/signed and multipart/encrypted framework to apply digital signature and encryption services to MIME objects2-20 MOSS can be thought of as a framework rather than a specification, and consider-able work in implementation profiling has yet to be done. MOSS is new at the time of this writing.

- MOSS uses a framework of security services defined in RFC-1847 to be applied to MIME body parts.
- In each of these subtypes, there are two related body parts: one for the protected

- data and one for the control information.
- MOSS is based in large part on the Privacy Enhanced Mail protocol. PEM is message encryption and message authentication for text based electronic mail messages. It uses a certified key management procedure Several specifications of PEM are supported by MIME.
- **For example**, the transfer encoding operation and the content- domain header
- The private key is used to digitally sign MIME objects. The recipient of the message uses the stored originator as public key to verify the digital signature. The recipient's public key is used to encrypt the data-encrypting key that is used to encrypt the MIME object; a recipient uses the corresponding private key to decrypt the data-encrypting key in order to decrypt the MIME objects.

MOSS services-overview

- The MOSS digital signature service. The MOSS digital signature service requires two components the data to be digitally signed and the private key of the originator.
- The digital signature is created by generating a hash of the data and encrypting the hash value with the private key of the message originator.
- The digital signature, some supplemental information, and the data are incorporated into a multipart/signed body part. This multipart/ signed body part may be

processed further when transferred to the recipient-it may become encrypted. To apply the digital signature service, the following sequence of events must take place.

1. The body part to be signed must be converted to a canonical form that is uniquely and unambiguously represented in both the environment in which it was created and the environment in which it will be verified.

The canonicalization transformation takes place in two steps: (1) the body part must first be converted to a form that is unambiguously representable on many different host computers; (2) the body part must have its line delimiters converted to a unique and unambiguous form. The digital signature service requires the originator and the recipient to use the same line delimiter.

2. The digital signature and other control information must be generated. Some control information that is generated by the digital signature service is a version of the MOSS protocol, originator-ID and the MIC header.

3. The control information must be incorporated in an appropriate MIME content type. The application/moss-signature content type is used on the second body part of an enclosing multipart/signed. It must include the digital signature of the data in the first body part of the enclosing multipart/signed and the other control information required to verify the signature.

4. The control information body part and the data body part must be incorporated in a multipart/signed content type. The multipart/ signed content type is created as follows:

a. the value of its required parameter protocol is set to application/moss-signature;

b. the signed body part becomes its first body part;

c. its second body part is labeled application/moss-signature and is filled with the control information generated by the digital signature service; and

d. the value of its required parameter micalg is set to the same value used in the MIC-Info: header in the control information.

The MOSS encryption service

The MOSS encryption service requires three components:

The data to be encrypted, a data encrypting key to encrypt the data, and the public key of the recipient.

The originator creates a data-encrypting key and encrypts the data.

The recipient's public key is used to encrypt the data-encrypting key.

To apply the encryption service, the following events must take place:

1. The body part to be encrypted must be in MIME-compliant form.

2. The data-encrypting key and other control information must be generated. The application of the encryption service generates control information which includes the data-encrypting key used to encrypt the data itself. The syntax of the control information is that of a set of RFC-822 headers, except that the folding of header values onto continuation lines is forbidden.

3. The control information must be incorporated into an appropriate MIME content type. The application/moss-keys content type is used on the first body part of an enclosing multipart/encrypted. Its content is comprised of the data encryption key used to encrypt the data in the second body part and other control information required to decrypt the data.

4. The control information body part and the encrypted data body part must be incorporated into a multipart/encrypted content type. The definition of the multipart/encrypted body part in RFC-1847 specifies three steps for creating the body part:

a The body part to be encrypted is created according to a local convention, for example, with a text editor or a mail user agent.

b. The body part is prepared for encryption according to the protocol parameter; in this case, the body part must be in MIME canonical form.

c. The prepared body part is encrypted according to the protocol parameter.

The multipart/encrypted content type is constructed as follows:

- The value of its required parameter protocol is set to application/moss-keys.
- The first body part is labeled application moss-keys and is filled with the control information generated by the encryption service.
- The encrypted body part becomes the content of its second body part, which is labeled application/octet-stream.

Definition of security subsystem:

Multipart/Signed – this type specifies how to support authentication and integrity services via digital signature. There are three required parameters: boundary, protocol and micalg. The content type contains two body parts: the first one contains the body over which the digital signature was created, including its MIME headers, and the second body part contains the control information necessary to verify the digital signature. The second body part is labeled according to the value of the protocol parameter.

In support of the digital signature service there is a quantity computed over the body part with a message digest or hash function. It is called MIC and is part of the definitions of RFC1421, Privacy-Enhanced Mail.29

Creating process of multipart/signed. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The content of the body part to be protected is prepared according to a local convention (i.e., text editor or local user agent) and is then transformed into a MIME body part in canonical format, including the appropriated MIME headers. In addition, the body is constrained to 7 bits, considering the restrictions of the standard Internet SMTP infrastructure. Binary material must be encoded
using quoted-printable or base64 encoding.

2. The body part (headers and content) to be digitally signed is prepared for signature according to the value of the protocol parameter.

3. The signature is created according to a local convention, and the process must make available to a MIME implementation two data streams: the control information necessary to verify the signature, which will be placed in the second body part, and the digitally signed body part, which will be used as the first body part.

Receiving and verifying process of multipart/signed. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The first body part and the control information in the second body part must be prepared for the signature verification process according to the value of the protocol parameter.

2. The prepared body parts must be made available to the signature verification, process according to a local convention. The signature verification process must make available to the MIME implementation the result of the signature verification and the body part that was digitally signed.

3. The result of the signature verification process is made available to the user and the MIME implementation continues processing with the verified body part, that is, the body part returned by the signature verification process.

Multipart/encrypted: This type contains two body parts.

i) The first one contains the control information necessary to decrypt the data in the second body part and is labeled according to the value of the protocol parameter.

ii) The second body part contains the data which was encrypted and is always labeled application/octet-stream.

It has two required parameters: boundary and protocol.

Creating process of multipart/encrypted. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The contents of the body part to be protected is prepared according to a local convention. The contents are then transformed into a MIME body part in canonical MIME format, including an appropriate set of MIME headers.

2. The body part (headers and content) to be encrypted is prepared for encryption according to the value of the protocol parameter. The MIME headers of the encrypted body part are included in the encryption to protect from disclosure the MIME labeling of the data that is encrypted.

3. The prepared body part is made available to the encryption process according to a local convention. The encryption process must make available to a MIME implementation two data streams: the control information necessary to decrypt the body part, which the MIME implementation will place in the first body part and label according to the value of the protocol parameter, and the encrypted body part, which the MIME implementation will place in the second body part and label application/octet-stream.

Thus, when used in a, multipart/encrypted, the application/octet-stream data is comprised of a nested MIME body part.

Receiving and verifying process of multipart/encrypted. The following sequence is descriptive of the activities involved and is an amplification of the description in the previous section.

1. The second body part and the control information in the first body part must be prepared for the decryption process according to the value of the protocol parameter.

2. The prepared body parts must be made available to the decryption process according to a local convention. The decryption process must make available to the MIME implementation the result of the decryption and the decrypted form of the encrypted body part.
3. The result of the decryption process is made available to the user and the MIME implementation continues processing with the decrypted body part, that is, the body part returned by the decryption process.

APPLICATION (13.Discuss about Application of MIME Object Security Services.(Apr 2014))

MOSS is based in large part on the Privacy Enhanced Mail protocol as defined by RFC-1421/1422/1423, which defines message encryption and message authentication procedures for text-based electronic mail messages using a certificate-based key management mechanism.

In order to make use of the MOSS services, a user is required to have at least one public/private key pair. The public key must be made available to other users with whom secure communication is desired.

An originator's private key is used to digitally sign MIME objects; a recipient would utilize the originator's public key to verify the digital signature. A recipient's public key is used to encrypt the data encrypting key that is used to encrypt the MIME object; a recipient would utilize the corresponding private key to decrypt the data encrypting key so that the MIME object can be decrypted. The ownership of the public keys used in verifying digital signatures and encrypting messages should be verified. A stored public key should be protected from modification.

The framework defined in RFC-1847 provides an embodiment of a

MIME object and its digital signature or encryption keys. When used by MOSS, the framework provides digital signature and encryption services to single and multipart textual and non-textual MIME objects.

LDigital signature service:

The verification of the MOSS digital signature service requires the following components:

- A recipient to verify the digital signature
- A multipart/signed body part with two body parts: the signed data and the control information
- The public key of the originator

The digital signature is verified by recomputing the hash of the data decrypting the hash value in the control information with the originator's public key, and comparing the two hash values. If the two hash values are equal, the signature is valid.

The definition of the multipart/signed body part in RFC-1847 specifies three steps for receiving it:

1. The digitally signed body part and the control information body par are prepared for processing.
2. The prepared body parts are made available to the digital signature verification process.
3. The results of the digital signature verification process are made available to the user and processing continues with the digital, signed body part, as returned by the digital signature verification process.

Encryption service:

The decryption of the MOSS encryption service requires the following components:

- A recipient to decrypt the data

- A multipart/encrypted body part with two body parts: the encrypt data and the control information
- The private key of the recipient

The data-encrypting key is decrypted with the recipient's private key and used to decrypt the data. The definition of the multipart/encrypted body part in RFC-1847 specifies three steps for receiving it:

1. The encrypted body part and the control information body part prepared for processing.

2. The prepared body parts are made available to the decrypted process.

The results of the decryption process are made available and processing continues with the decrypted body part and key by the decryption process. Identifying originators, recipients, and their keys. In the PEM specifications, public keys are required to be embodied in certificates, objects that bind each public key with a distinguished name.

In MOSS, a user is not required to have a certificate. The MOSS ser-vices require that the user have at least one public/private key pair.

The MOSS protocol requires the digital signature and encryption services to transmit the Originator-ID: and Recipient-ID: headers, as appropriate.

MOSS allows other identifiers in Originator-ID: header and Recipient-ID: header. These other identifiers are comprised of two parts:

1. a name form and
2. a key selector.

Since a user may have more than one public key and may wish to use the same name form for each public key, a name form is insufficient for uniquely identifying a public key. Hence, a unique key selector must be assigned to each public key. The combination of a name form and the key selector uniquely identifies a public key. This combination is called an identifier.

With a public/private key pair for a user and software that is MOSSaware, an originating user may digitally sign arbitrary data and send it to one or more recipients.

Key management content types:

RFC-1848 defines two key management content types: one for requesting cryptographic key material and one for sending cryptographic key material.

Key management functions are based on the exchange of body parts. Two content types are used:

- application/mosskey-request Content Type:

A user would use this is content type to specify needed cryptographic key information. The application/mosskey-request content type is an independent body part because it is entirely independent of any other body part. One possible response to receiving an application/mosskey-request body part is to construct and return an application/mosskey-data body part.

- application/mosskey-data Content Type:

The principal objective of this content type is to convey cryptographic keying material from a source to a destination. This might be in response to the receipt of an application/mosskey-request content type.

Pretty Good Privacy (PGP) :

Pretty Good Privacy (PGP), is a public key encryption system in circulation. PGP uses the RSA (Rivest, Shamir, and Andleman) public-key cryptosystem. PGP supports the following functions:

- Generates public/private RSA keys
- Encrypts messages to be transmitted using the destination's public key
- Decrypts messages received using the recipient's private key
- Authenticates messages with digital signatures
- a Manages key rings that keep track of destination's public keys

All encryption systems security is based on a cryptographic key or the key to the cryptography's electronic lock. Private-key encryption systems, or conventional cryptography, use a single or private key. This private key is used for both encryption and decryption. The sender and recipient of the mail message must share the same key. Public-key systems generate two mathematically related keys. A message encrypted with one key can be decrypted only with the other.

Cryptography is the science of using mathematics to hide or code the meaning of messages. The goal behind cryptography is to make it impossible to take a ciphertext and reproduce the original plaintext without the corresponding key.

The secret key is used to decrypt messages that have been encrypted with an organization's public key. The key is called the secret or private key, since the organization must keep it a secret.

The session key is randomly generated for every message encrypted with PGP's public-key encryption system following is a simplified description of how PGP is used to send an e-mail message:

1. PGP creates a random session key for the message being sent.
2. PGP uses the IDEA (International Data Encryption Algorithm) private-key algorithm to encrypt the message with the session key. This is because encrypting in software the entire message would take extraordinary amounts of computing power. IDEA is an iterated block cipher with 64-bit input and output blocks, with a 128-bit key (DES only has a 56-bit key32).

3. PGP then uses the recipient's public RSA key to RSA-encrypt the session key (not the message itself, as noted in the previous point).
4. PGP bundles the IDEA encrypted message and the RSA-encrypted session key together.

The message is now ready to be sent.

If someone has the organization's public key, that person can send e-mail but cannot read the organization's e-mail. A key certificate is created each time a public key is stored. It contains the public key, one or more user IDs for the key's creator, the creation date, and sometimes a list of digital signatures. The digital signatures would be used to verify that a message was sent by the person who matches the digital signature. These public keys are kept in a single file called the key ring (pubring.pgp); the public key ring is like an address book.

The organization also has a secret key ring that contains the organization's secret Key.

Problem with the public key:

The availability of public keys has one problem. If someone were to replace the organization's listed public key, with his or her own public key, that person would be able to intercept and read any messages sent to the organization. The intruder could then reply to the messages and re-encrypt the messages with the organization's public key.

The only way to prevent such a problem is to use a digital signature. The digital signature encrypts a special number into the information of the file. The number is checked against the original message and the public key of the sender. If the numbers match, the message has not been modified since it was signed and transmitted. If the numbers do not match, the message has been modified and the recipient is notified.

Encrypted data is binary data, which cannot be sent by standard electronic mail. The ASCII Armor encoding actually uses four ASCII characters to represent three binary, characters.

Some of the standard file extensions are as follows:

.txt - is attached to files created by a text editor or word processor before the file is encrypted.

.Pgp - is attached to an encrypted binary file. It is also used for key rings.

.asc - is attached to an ASCII-armored encrypted file.

.bin - is crated when you use PGP's key-generate option. It is used for the randseed.bin file, which stores the seed for PGP's random number generator.

Pondicherry University Questions

2 MARKS

1. What are the key pairs used in SET? **(Apr 2012) (Ref.Qn.No.34)**
2. What is a MIME? **(Apr 2012) (Ref.Qn.No.12)**
3. Mention the objectives of payment security. **(Nov 2012) (Ref.Qn.No.5)**
4. List the internet protocols related to mail specific applications. **(Nov 2012) (Ref.Qn.No.35)**
5. Difference between master card and visa **(Apr 2013) (Ref.Qn.No.36)**
6. What is S/MIME? **(Apr 2013) (Ref.Qn.No.22)**
7. Write a short note Uudecode?**(Apr 2014) (Ref.Qn.No.32)**
8. Write a note on cryptography?(**Apr 2014) (Ref.Qn.No.33)**
9. Define Email?(**Nov 2014)(Apr 2015) (Ref.Qn.No.15)**
10. What is the use of MIME? (**Nov 2014)(Apr 2015) (Ref.Qn.No.27)**

11 MARKS

1. Discuss the objective of bank card associations. **(Apr 2012) (Ref.Qn.No.1)**
2. Explain in detail about MIME. **(Apr 2012)(Apr 2014)(Nov 2014) (Nov 2012)(Apr 2015) (Ref.Qn.No.10)**
3. Discuss about the business requirements. **(Nov 2012) (Ref.Qn.No.2)**
4. Explain about S/ MIME in detail. **(Apr 2013) (Ref.Qn.No.10)**
5. How does e-mail work? Explain in detail. **(Apr 2013) (Ref.Qn.No.9)**

6. Describe the message object security services in detail**.(Apr 2014)(Ref.Qn.No.12)**
7. Explain the basic aspects of payment processing.**(Nov 2014)(Apr 2015)(Ref.Qn.No.6)**

UNIT V

Internet and Website Establishment: Introduction – Technologies for web servers – Internet tools relevant to Commerce – Internet Applications for Commerce – Internet charges – Internet Access and Architecture – Searching the Internet- Case study.

2 MARKS

1. List the web browser features.

- Forms completion.
- E-mail support.
- Date inquiry.
- Customize by user.
- Rapid integration with other applications.
- Hypertext.

2. List the internet application for commerce.

- Direct selling or marketing of a company's existing products and services.
- Selling advertising space.
- Charging fees for the actual content accessible on a web site.
- Charging fees for online transaction or links.

3. Mention the 3 ways to provide information as home pages on the web.

Roll on your own- It is a low cost entry level strategy to create your own WWW pages and post them on the web.

Outsource- for many business working with a commercial web services provider is a good choice. You can create pages, get the assistance of a consultant or an market agent, then lease commercial web pages.

In-house development- Business with the resources to hire or train the necessary personnel can set up web servers within their business. It provides the best control over access, design, and content.

4. What is a routing arbiter?

A Routing Arbiter (RA) is an element that is introduced into the NAP architecture. RA organization implements the concept of policy-based network routing that enables routing of traffic between different network operators.

5. List the effects of Routing Arbiter.

The effects of the RA as follows:

- Route servers
- Network management systems
- Routing arbiter database
- Routing engineering

6. Mention the processing components of gathering information.

The process consists of 3 main components:

- Sourcing information
- Index, catalog, or database creation
- The search engine

7. What is a search engine spider?

A spider also known as a robot or a crawler is actually just a program that follows or crawls links throughput the internet, grabbing content from sites and adding it to search engine indexes.

8. List the uses spiders. (Nov 2012)

A spider is a program that autonomously explores the Web and newsgroups and takes some action upon the information it finds. This action may be as counting the number of web links found or as complex as indexing the entire text of a Web page or newsgroup.

The primary uses of spiders are as follows.

- Link validation
- HTML validation
- "What's new" monitoring
- Indexing

9. Define Multithreading?

Multithreading is a sophisticated and refers to the ability to support paths of execution within a single address space. Older operating systems achieve multitasking by creating multiple processes, which creates a great deal of overhead.

10. Describe the benefits of Frame relay?

Frame relay has two benefits:

- **Speed:** It is no longer necessary to carryout error controls and corrections between each node due to the improvements in transmission media.
- **Sharing costly bandwidth:** Frame relay allows users to share costly, high throughput channels over a single access line, and it uses a "hubbing" approach to distribute traffic over a wide area.

11. Define Multiprocessing?

Multiprocessing is defined as the ability to support the concurrent execution of several tasks on multiple processors. This implies that ability to use more than one CPU for executing programs. The processors can be tightly or loosely coupled.

12. Define multitasking?

Multitasking means that the server operating systems can run multiple programs and give the illusion that they are running simultaneously by switching control between them.

Two types of multitasking are used:

- Preemptive
- No preemptive

13. List some services of the internet?

Some services of the internet are:

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

14. What are all the key search features in search engine?

The following lists key technology features that should be included in search engines.

- Free-text search
- Automatic morphology
- Word indexing
- Lexical affinity search
- Ranking and relevance scoring

15. What is InfoSeek?

The search engine accepts natural language questions, such as, “What is a good restaurant in New York City that serves fresh morels?”But also provides keyword search capability. InfoSeek returns the most relevant matches.

16. What is WebCrawler?

WebCrawler is faster than InfoSeek and lets the user view more matches on the screen simultaneously. It does not screen its matches for relevance as much as InfoSeek does; hence users may find matches that InfoSeek omitted.

17. What is Lycos?

Lycos is the slowest of the “big three,” but it is also the most detailed. The Lycos robot indexes not only the sites that it visits, but also every link on those sites.

18. What is Savvy Search?

One can search the entire previously mentioned database simultaneously using a tool called Savvy Search. It is not a search engine itself rather; it is a client that executes searches on several engines in parallel.

19. What is USENET?

If you are searching for something current, then Usenet is an excellent resource. Usenet is not a network and Usenet does not even need the Internet. Rather, what drives Usenet is akin to an agreement set up between those who want to distribute and those who want to read newsgroups.

20. What is Veronica?

Veronica is a self-updating database of Gopher documents. Veronica allows users to search all of the Gopher sites in the world. By entering a word or words, directories, programs, and articles with those words in them will show up in a menu for users to browse. For purposes of a Veronica search, the title is the name of the resource as listed on its home Gopher server.

21.What is meant by NAP access?(Apr 2014)

NAP access:

Sprint supports access from an NSP's router located at Sprint's physical NAP facility. The NSP can supply and maintain the router which interfaces directly with Sprint's NAP, or it can choose a sprint-supplied router.

22.Write a note on internet browser?(Apr 2014)

Although **browsers** are primarily intended to use the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems. The major web **browsers** are Firefox, **Internet**Explorer, Google Chrome, Opera, and Safari.

23. Define the term Internet. (Apr 2012)

A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide.

24. What are the two most common publishing systems? (Nov 2012)

The electronic publishing process follows a traditional publishing process but differs . Ink-jet or laser printer or via a print on demand system. Three attributes of digital technology: XML tags to define content, style .The most common file format is .epub, used in many e-book .A desktop publishing system allows you to use different typefaces, specify various margins.

25.Write about electronic payment system. (Apr 2013)

An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. Also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

26.What is SOA GOVERNANCE? (Apr 2013)

SOA governance is a concept used for activities related to exercising control over services in service-oriented architecture (SOA) solutions. One viewpoint, from IBM and others, is that SOA governance is an extension (subset) of IT governance which itself is an extension of corporate governance.

27. Write short notes on Internet & Intranets.(Nov 2014)

Internet

A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Intranet

A local or restricted communications network, especially a private network created using World Wide Web software.

28.Mention Some Internet Tools.(Nov 2014)(Apr 2015)

- **Telnet**
- **E-Mail**
- **FTP**
- **Gopher**
- **World Wide Web**

29. Comparison between Website & Webpage.(Apr 2015)

Website

A site (location) on the World Wide Web. Each Web site contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files. Each site is owned and managed by an individual, company or organization.

Webpage

A web page *or* webpage is a document commonly written in HyperText Markup Language (HTML) that is accessible through the Internet or other network using a browser. A web page is accessed by entering a URL address and may contain text, graphics, and hyperlinks to other web pages and files.

11 MARKS

1. Describe about Browsing and providing Information. (or) Internet Charges.

INTERNET CHARGES:

Browsing for information:

A user needs to get the computer server and software choose and ISP, and obtain a suitable connection. A machine is required for the user to access the internet the machine could be an internet terminal a PC or a high speed server depending on what type of info. A person needs , and how much the person is willing to pay.

With a PC a user the user can be connected and configured as a client on the internet by a low or high speed connection. Depending on power and capacity the user wants the cost of the PC ranges from a couple hundred dollars to a couple thousand dollars. There are many options to choose for internet connections.

Browsing and providing information:

There are three ways to provide information as home pages on the web. They are

Roll on your own- It is a low cost entry level strategy to create your own WWW pages and post them on the web.

Outsource- for many business working with a commercial web services provider is a good choice. You can create pages, get the assistance of a consultant or an market agent, then lease commercial web pages.

In-house development- Business with the resources to hire or train the necessary personnel can set up web servers within their business. It provides the best control over access, design, and content.

Settlements:

The financial settlement between internet providers is an important issue. This is clear when you understand that the internet is no more than a set of local and long distance networks. The internet is WWW and many we servers and internet hosts are outside of the united states. The settlements will require complex accounting mechanisms whose costs might be passed on the end user.

2. What is the internet architecture? Or Explain the Internet Access and Architecture with neat Diagram. Or Explain about E- Commerce and internet access in detail. (April 2013)

INTERNET ACCCESS AND ARCHITECTURES:

It is define a Meta network a constantly changing collection of thousands of individual networks intercommunicating with a common protocol.

The internet architecture is described in it name, a short from of the compound word inter-networking. This architecture is based in the very specification of the standard TCP/IP protocol designed to connect any two networks which may be very different in internal hardware,
software and technical design. Once two networks are interconnected communication with TCP/IP is enabled end-to-end, so that any node on the internet has the near magical ability to communicate with

any other no matter where they are. This openness of design has enabled the internet architecture to grow to a global scale.

Routing arbiters:

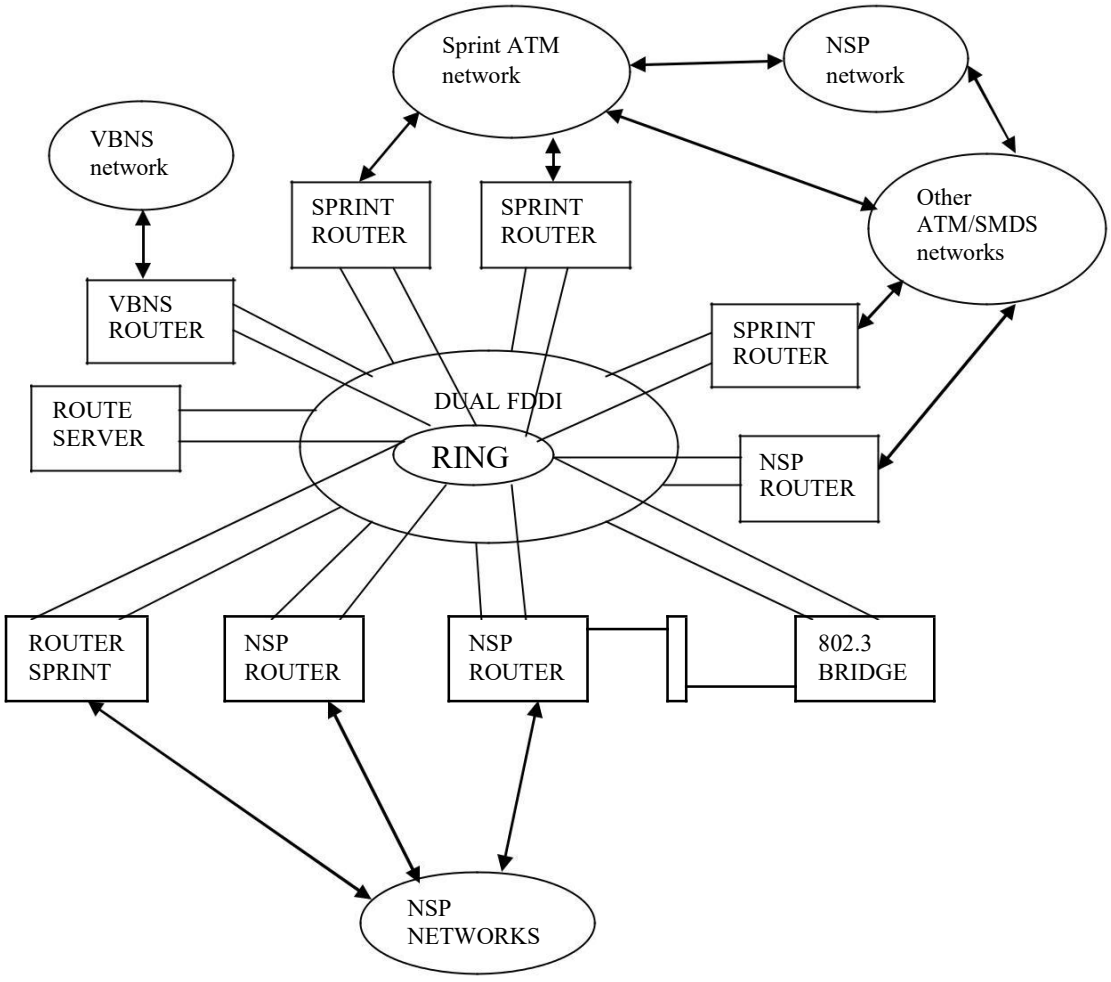
The routing arbiters to provide stable coherent routing in the internet with the internet doubling every 13 months this is not as easy to it might be. The problem is compounded by the withdrawal of the NFSNET service and the proliferation of internet service providers and exchange points. A brief view from the RA perspective is given with some attention to tools and techniques that will facilitate the contained growth of the internet in size, features and function.

The effects of the RA as follows:

- Route servers
- Network management systems
- Routing arbiter database
- Routing engineering

Example of NAP architecture

As an illustrate example, sprint chose FDDI as an initial architecture for its NAP; sprint has planned to upgrade to an ATM switch in the near future. In the interim, switched FDDI hubs may be deployed when the NAP loads are projected to exceed what the FDDI ring can support. An Ethernet interface is also available for use by any NSP that requires that type of interface.



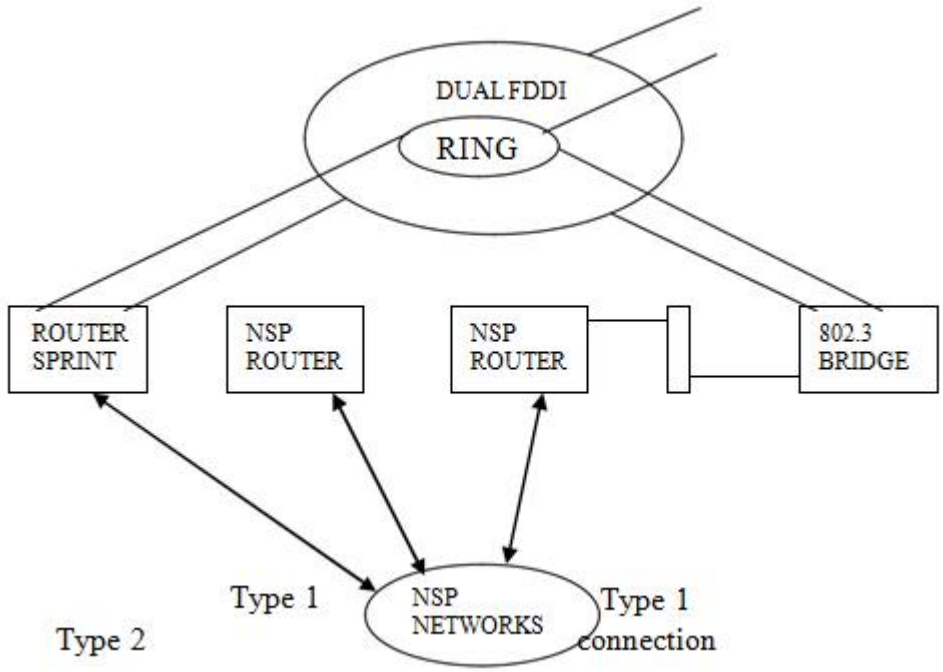
NAP access:

Sprint supports access from an NSP's router located at Sprint's physical NAP facility. The NSP can supply and maintain the router which interfaces directly with Sprint's NAP, or it can choose a sprint-supplied router. This approach allows NSPs to connect to the sprint NAP via a serial link or a switched service from dispersed locations using any type of WAN technology the NSP choose to use. WAN technologies supported include the following:

- Dedicated circuit access
- Switched service access

Dedicated circuit access:

For a dedicated circuit connection from an NSP to the Sprint NAP, the NSP can choose to provide the link via Sprint, a local exchange carrier (LEC), a competitive LEC (CLEC), or another interexchange carrier in conjunction with either a LEC or a CLEC.



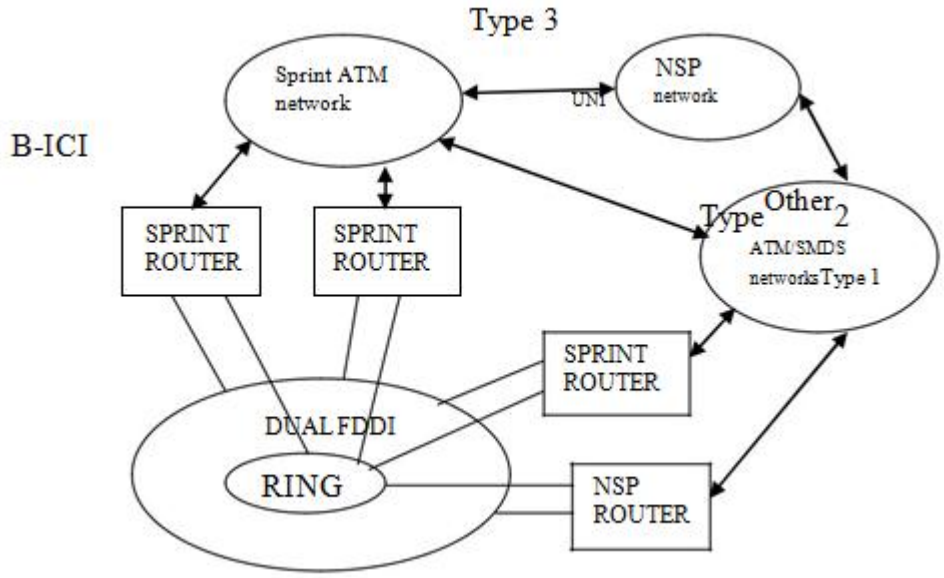
Switched service access:

The Sprint NAP may also be accessed by any one of three switched services: ATM, frame relay, or SMDS.

ATM- The NSP connects directly via a UNI to Sprint's ATM network. When broadband intercarrier interface (B-ICI) is available, an NSP may also use it to connect another carrier's ATM network to a sprint's network in order to reach the NAP.

Frame relay. The NSP connects directly via a frame relay link or a frame relay network to a Sprint-provided router. A NSP may also use B-ICI to connect another carrier's frame relay network to Sprint's ATM network.

SMDS (Switched Multi-Megabit Data Service). The NSP connects directly via an SMDS link or network to a sprint-provided router. An NSP may use B-ICI to connect another carrier's frame relay network to Sprint's ATM network.



3.Describe about searching operations in Internet and its Limitations.

SEARCHING THE INTERNET:

As the amount of content on-line increases, it becomes more and more difficult for users to find what they are looking for on the Internet.

Gathering information:

The process consists of 3 main components:

- Sourcing information
- Index, catalog, or database creation
- The search engine

SPIDERS AND SEARCH ENGINE:

A spider also known as a robot or a crawler is actually just a program that follows or crawls links throughput the internet, grabbing content from sites and adding it to search engine indexes.

Spiders only can follow links from one page to another and from one site to another. That is the primary reason why links to your site are so important links to your website from other website will give the search engine spiders more food to chew on. The more time they find links to your site the more times they will stop by and visit. Google especially relies on its spiders to create their vast index of listings.

Spider find web pages by following links from other web pages, but you can also submit your web pages directly to a search engine or directory and request a visit by their spider. In fact it a good idea to manually submit your site a human edited directory such as yahoo and usually spiders from other search

engines will find it and add it to the database. It can be useful to submit your URL straight to the various search engines as well, but search cheating.

Uses of spiders:

A spider is a program that autonomously explores the Web and newsgroups and takes some action upon the information it finds. This action may be as counting the number of web links found or as complex as indexing the entire text of a Web page or newsgroup.

The primary uses of spiders are as follows.

- Link validation
- HTML validation
- "What's new" monitoring
- Indexing

An advantage of using spiders is that databases can be updated automatically, allowing users to be reasonably sure they are receiving the latest information.

Limitations of spiders:

The information databases complied by spiders are useful; however, there are some limitations to spiders concerning resource discovery. The main limitation is that there is just too much information available through the Internet and the amount is growing all the time. Although spider-generated databases are generally more current in totality than manually complied databases, the fact that new information is being added every day precludes the spider-generated database from being completely up-to-date. Also, adding to the problem is the fact that a large portion of the data on the Internet is dynamic in nature.

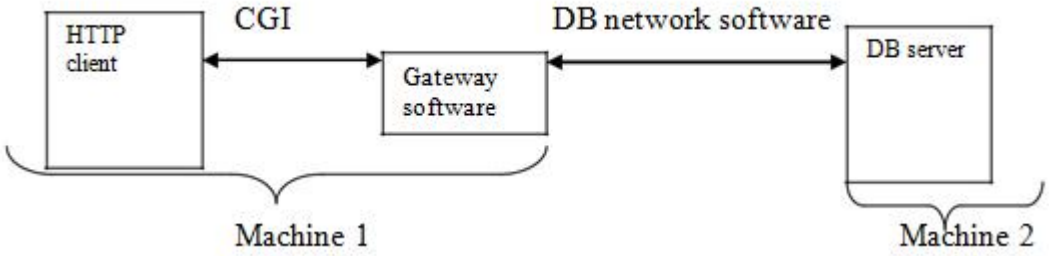
To address redundant and irrelevant database listing developed by spiders, a standard for spider exclusion has been developed. This standard describes the use of simple structured text files at an easily found place on a server to specify which parts of a URL space should be avoided by spiders.

This process can be used to give specific instructions to individual spiders, given that some behave more sensibly than others or are known to specialize in particular areas. Currently, this standard is voluntary, but there is pressure from various Internet agencies for users of spiders to comply.

Search engines

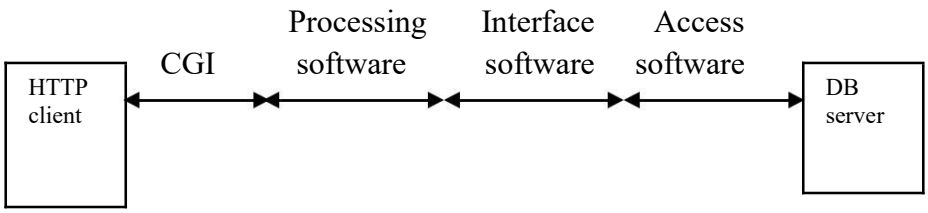
A search engine is a program that searches through a database. In the context of the Internet, search engine is most often equated to search forms that request programs to look through databases of HTML documents gathered by spiders or through manual data gathering processes.

Accessing the information databases- An HTTP server provides a method of running database searches from within an HTML document. This method is called the Common Gateway Interface (CGI). The server can pass information to the CGI program and get back any results returned by the database search.

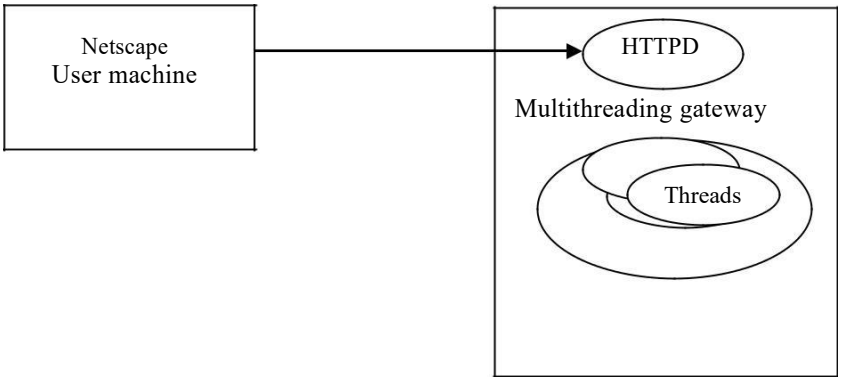


High-level details of using CGI and gateway software- Processing software is called directly from the HTML search document by the HTTP client. The processing software reads the query input passes to it via the CGI call.

CGI use:

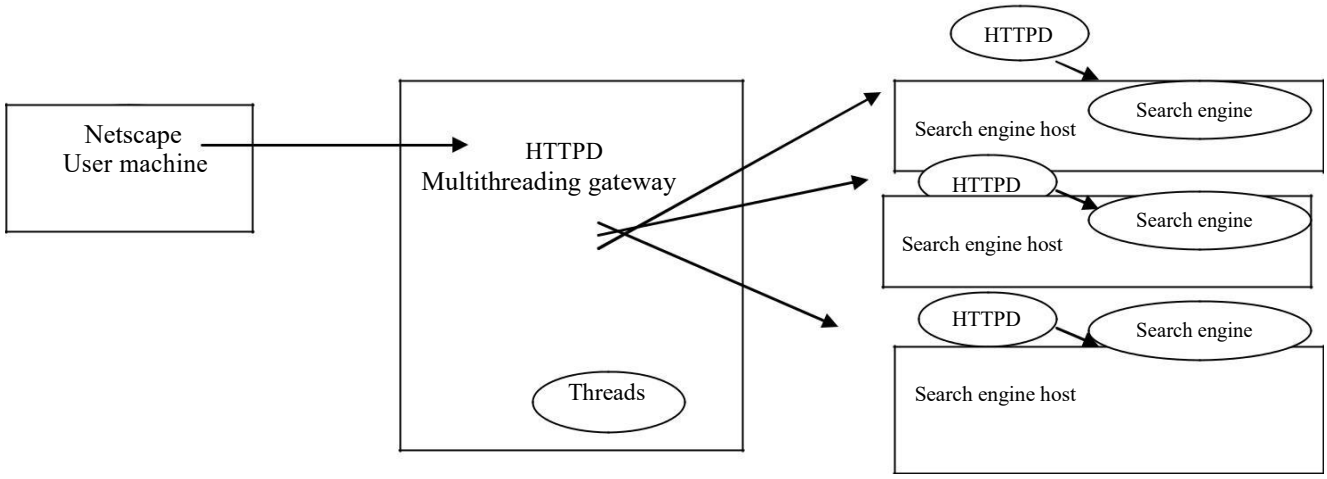


Multithread queries:



Multithreading queries are performed by using a gateway program which conforms to CGI. The program works with an HTML form describing the various search engines and the type of queries that can be performed. When users wish to perform a query, they retrieve the HTML form, select the desired search engines, fill in the query parameter, and submit the form. The query is then submitted to an HTTPD (HTTP daemon) process which starts the multi-threaded query gateway giving the query information.

When a multithreaded gateway receives the query, it creates a thread for each search engine. Each thread then sends the query to the gateways using HTTP and waits for the response. When responses have been received from all search engines, the multithreaded gateway creates an index bringing all responses into one document which is sent to the user.



What if a search engine was programmed to boost the ratings of sites with a particular political

inclination? People would for ex, see a lot of sites at the top of the list advocating a certain political stance which contrary pages could be ranked way down where most people would not see them.

The search terms entered by users also provide an immediate snap shot of people thoughts. Google has a whimsical feature that tracks how often different topics are searched for such information would be invaluable to adventures, politicians, newspaper reporters, commercial organizations etc because they would get a clue about what hot people use indexes of searches terms as indicators of frame is Madonna being searched for less often? Is Britney spears on the way up or down in her career? You can often get clues from the trends in search terms submitted to search engines.

Different search engines handle moral issues differently. Some reward sponsors by inserting their link into search results regardless of words used in the search terms. Often these sponsored links are not identified as such leaving people to wonder why bobs hardware appeared in the results of their search for Britney spears.

Other search engines pride themselves on more reputable behaviour. They only include sponsored links if they are relevant to a search Google goes further and keeps sponsored links separate links separate from search results and clearly identifies them as sponsored.

Many people try to work how different search engine calculate the positioning in search results. Most engines keep their formula secret to prevent people exploiting it to their sites popularity artificial inflated.

Tricks like including a lot of irrelevant keywords in the META tags have been popular with web authors. A site on a band for ex, would include irrelevant but popular keywords like Pamela Anderson, nude porn free. Many search engines now pay little attention to keywords for their reason. Google them completely.

Another trick is to repeat keywords many times on a page, often with the text made invisible by setting the text color to the page color. Again some search engines know this trick and will ignore blatant mass-listings.

Oddly Google will occasionally list page that don't have your search terms but other pages linked to that page with those words. This led to the Google bomb originally a fun trick but potentially a powerful technique to manipulate and distort Google results.

4. Briefly explain about search engine and its relevant ranking methods. (Nov 2014)

Social implications of search engines:

Sounds odd, doesn't? Social implications of search engines? You might as well talk about the social implications of screw drivers. They are just tools aren't they? In fact search engines have heavy moral and social responsibilities and can widely considerable influence. They believe that a person searching for info. On the church would be getting a satisfied and biased list of links. A bit of a controversy corrupted with people arguing that Google was censoring the internet.

Search engine relevance ranking methods:

Keyword matching: simply checks to see how many of the search terms appear on a page ex: if searching

for King Henry, a page with both the search terms would be judged more relevant than a page with only one of the terms.

Frequency: If a page mentioned king Henry frequently, it's a good sign the page is more valuable than another page a that just mentions him once.

Positioning:

Pages with king Henry n the page title or in a heading or formatted as hold would probably be more valuable than another page that did not emphasize the words or positioning them in a prominent place. A page that has the search terms near the beginning of the text would be more highly ranked than a page that had the search terms near the end of the text.

HTML web pages also have an invisible section, the head where META tags can be inserted by the pages author. If search terms appear in these tags it is a clue that the words are important to the page and it will tend to be ranked more highly.

There is a continuing battle to be the best search engine. While their services are free to users search engines make a great deal of money through advertising and sponsorship. Although they all do the same job, they use a variety if techniques to do it.

Some search engines also take into account whether as site is listed in prestigious listings. One ex is DMOZ a list of services selected by human editors. A sites inclusion in this list is an indicator of the quality of the site and search engine like Google take this us to account with TCP/IP is enabled end to end so that any node on the internet magical ability to communicate with any other no matter where they are.

The companies running the internet backbone operate very high bandwidth networks relied on by governments, corporations and large organizations and other internet service providers. As always a larger scale introduces new phenomena the no. of packets flowing through the switches on the backbones is so large that it exhibits the kind of complex non linear patterns found in natural analog systems like the flow of water or development of the rings of Saturn.

Key search features (in most search engines):

The following lists key technology features that should be included in search engines.

- Free-text search: The ability of the search engine to accept single words, phrases, or sentences. Common words are ignored, and the documents are elected based on the words in the query.
- Automatic morphology: Nouns and verbs in English occur in many tenses; the search process automatically generates the various forms of the words and uses in the query.
- Word indexing: Processing of collections of documents by building indexes which contain the location of every instance of every word. It is the indexes, not the documents that are searched.
- Lexical affinity search: Search on words that occur close to the text form of the query.
- Ranking and relevance scoring: Using a ranking algorithm, the search engine assigns every document that contains at least one of the queried words a numerical score.

These items do not by themselves guarantee a good search engine but assist users in better defining their informational requirements.

4.List the Search tools available in internet? (or) Internet Tools (Apr 2014).

Actual search tools:

Yahoo: This is currently considered the most complete directory resource on the WWW. It is a categorized, menu-driven directory of web resources.

InfoSeek: The search engine accepts natural language questions, such as, "What is a good restaurant in New York City that serves fresh morels?"but also provides keyword search capability. InfoSeek returns

the most relevant matches.

AltaVista: This is a search engine that is very likable. Often it may be all a user needs.

Open Text: This is a technically superior search engine on the Internet and produces fast, relevant responses.

WebCrawler: WebCrawler is faster than InfoSeek and lets the user view more matches on the screen simultaneously. It does not screen its matches for relevance as much as InfoSeek does; hence users may find matches that InfoSeek omitted.

Lycos: Lycos is the slowest of the "big three," but it is also the most detailed. The Lycos robot indexes not only the sites that it visits, but also every link on those sites.

Savvy Search: One can search the entire previously mentioned database simultaneously using a tool called Savvy Search. It is not a search engine itself rather; it is a client that executes searches on several engines in parallel.

Galaxy: Galaxy searches for resources on the Web, including Gopher and Telnet.

Usenet: If you are searching for something current, then Usenet is an excellent resource. Usenet is not a network and Usenet does not even need the Internet. Rather, what drives Usenet is akin to an agreement set up between those who want to distribute and those who want to read newsgroups.

Archie: If you are searching for computer software, then Archie is an excellent resource for navigating through the content on anonymous FTP archives throughout the world.

Veronica: Veronica is a self-updating database of Gopher documents. Veronica allows users to search all of the Gopher sites in the world. By entering a word or words, directories, programs, and articles with those words in them will show up in a menu for users to browse. For purposes of a Veronica search, the title is the name of the resource as listed on its home Gopher server.

Gopher: Gopher is a service that allows users to view and obtain files, programs, and software. When accessing Gopher information with a graphic browser, users are presented with a series of menu choices, much like the directory structure one sees in the Microsoft Windows File Manager.

Ftp: Anonymous FTP permits users to access remote systems without actually having user accounts on the systems. Users can FTP to any anonymous site in the world using hypertext interface.

Telnet: Telnet allows users to remotely log in to other computers and can give them access to databases and many information services.

WAIS: WAIS lets the user search indexed information to find articles containing groups of chosen words. WAIS is like Gopher in that it shields users from having to know on which computer the information resides; but unlike Gopher, WAIS does the searching for the user.

Internet Directory Services: There are a number of ways to create resources that provide access to e-mail addresses of individuals and institutions and contact information for Internet services. Directories to Internet addresses for people and services indexed by name are often referred to as white pages, while those directories that allow access to addresses of services by category are usually called yellow pages.

6.Explain in detail about internet applications for commerce?(Apr 2014)

A growing segment of the Internet is Electronic Commerceor E-Commerce. Consumers are looking for suppliers selling products and services on the Internet. Meanwhile,suppliers are looking for buyers to increase their market share.The vast amount of available information causes a great deal ofproblems for both ends. Searching, a task executed online, isnot only time consuming but boring as well. Intelligent Agents suited for this type of task.

A typical campus Internet Infrastructure is a collection of communication devices and networks of varying types and configurations connected together to form one network: the
"Internet". The tower and the high speed disk are used as a data warehouse for suppliers' products and consumers' needs and services. The remaining devices on the network provide user interface to the network clients.

Agents executing on such network will surf through the information on the Internet, resulting in the selection of specific information of interest to the user. Intelligent Agents provide a mechanism for conducting ECommerce. Using Intelligent Agents, the user composes the task offline, logs to the Internet to issue the task and logs off. At a later time the user can log to the Internet to collect the results of the task execution. Typical Internet Infrastructure

SIMULATION TEST

The NET-Computer was simulated in a network of three hosts: ainur, kira and yavanna connected. The hosts connected to networks A, B and C are located on different floors of the same building and run UNIX operating systems. Simulation test network The objective of the simulation test is to test the following Agents characteristics:

• Mobility: Agents navigate the network and reach destination address (host).
• Agency or task execution: Agents carry out useful work on behalf of the user.
• Intelligence: Agents follow a set of rules predefined by user.

1. Direct Selling
2. Selling and space
3. Charging for content
4. Charging for services

...for on-line transaction or links.

A gamut of companies has begun selling their products directly on the Web. The Web's reach can transform a small company into a global distributor. Large corporations that already have their distribution networks in place often find the Web to be a niche channel and many still think it is too early to be profitable. Some believe the reason is that "Internet selling is too new," others believe that people are not certain, and changing behavior takes some time.[31] Smaller companies and so-called cyberpreneurs are moving faster and getting more substantive results. For industries overrun by corporate chains, the Web may help smaller companies level the playing field. An information-rich Web site can help specialist retailers provide the same services as a fancy store in a big city.[30]

While the "no location" aspect of Web-based commerce can be advantageous, companies are also finding out that customers have a hard time discovering a particular site among the hundreds of thousands out there. As a result, more Web merchants are paying a sales commission as well as an advertising fee in exchange for prominent placement on high-traffic web sites, such as search engines and home pages of on-line service providers. For example, Amazon.com and 1-800-Flowers have entered into long-term exclusive agreements with America Online to gain access to the service's 8.5 million customers. These two 1997 agreements were valued at $44 million in revenue. In exchange, AOL will

provide premiere placement on AOL's orginal service or on its heavily trafficked Internet site. On-line users will be able to click on the ads and be connected to the Amazon.com or 1-800-Flowers sites. Stand-alone Web sites face challanges in attracting potential customers.

8.4.2 Selling ad space

Many companies have started advertising their products and services on the Web. It was estimated that companies spent $10 million to advertise on the Web in 1995 and the figure has been larger in recent years.[32] Companies selling ads on the Web say that this business model is a natural extension of their other lines of business. For instance, Career Mosaic functions as an on-line classified-ad and job database. Internet users going to the site can view ads organized by type of work and corporate profiles. The site lists several thousand jobs.[19] There is no standard rate structure yet emerged for Internet advertisements. DealerNet charges a flat $995 fee to put a car dealership on the Internet, plus a $500/month maintenance fee.[32]

4.3 Charging for content

Content providers charge for subscriptions and also count on advertising revenue from their sites. Observers believe that advertising drives business. Forrester expected companies would spend $2.2 billion advertising on the Web by year 2000.[32] A few daily newspapers have started charging for content. For instance, San Jose Mercury News began charging fees, ranging from about $1 to $5 per month, for its Mercury Center news site in 1995.[32]

.4 Charging for services

Another model involves charging for some type of services such as searching databases, providing space, linking, and other services on a Web site. *Industry.Net* offers business a place to shop for goods. It charges manufacturers and suppliers $3000 to $8000 a year to maintain an electronic storefront on its site. *Industry.Net* generated $30 million in 1995. The business not only allows users to access the data but also allows them to place orders by e-mail.[30]

7. What are the technologies used for web servers? Explain. (April 2012)(Nov 2014)(April 2015)

Designing a web presentation for a company or an organization requires or to sort out the content to present, set goals, decide on topics, then organize the layout and navigation of the web pages. As previously discussed, to publish documents on the web, a server that makes available documents and media to the browser that requests them in needed. Whenever the browser is pointing to a web documents, the browser communicates with the server to get at that document.

HTML:

General features: HTML is the markup language used to create web documents. It is loosely a subset of the SGML (standardized General Markup Language).SGML is used to describe the general structure of various kinds of documents. The primary focus of SGML, and therefore HTML, is the content of document, not its appearance. Browsers decode the HTML instructions and display the document on the requester's screen. The theory behind this is that most documents have common elements, for example, titles, paragraphs, or lists, and if these elements are defined, they can be labeled as the appropriate parts of the documents. The elements of the Web documents are labeled through the use of HTML tags. The following is a list of basic tags for HTML.

Tag	Use
<HTML>….<\HTML>	The entire HTML document
<HEAD>…..</HEAD>	The head, or prologue, of the HTML document
<CENTER>…</CENTER>	Center text
<TITLE>…..</TITLE>	The title of the document
<A>…..</A>	Illustrate reference and anchor portions
<B>…..</B>	Make word boldface
<I>…..</I>	Italicize word
<H4>…..</H4>	Fourth-level heading
<P>…….</P>	Paragraph
<!----…--->	Comment

HTML does little to describe the exact placement or appearance of any element on the page, since there is no way of knowing what platform in the document going to be viewed on, the size of the screen, the font that are installed on the platform, or if there are any fonts at all. In addition to the creating tabs, the user may also create links between documents, create list set page breaks Identify addresses and quotations and inserts any special characters and colors.

Editors and converters are the programs that can help publishers to write HTML pages. These Programs tend to fall into two categories: Editors, in which HTML is directly written, and The converters which convert the output of some other word processing program into HTML.

Most of the programmers are essentially text editors with extra menu items of buttons that insert Appropriate HTML tags into the text.HTML based text editors are useful and easy to use because publishers do not have to remember tags and do not have to type them all. Some examples of editors are as follows:

Editor	Description
• HTML editor	It is an application that allows the insertion of tags into a file and the result is in WYSIWYG fashion. The tags are shown in a lighter

color and the surrounding text. There are options to hide the tags in the documents to depict the full affect.

- Microsoft Internet Assistant — It is a plug in for words for windows 6.0 that allows user to create HTML files in the word and then save them as HTML.
- Template packages — For Microsoft word version 2.0 or 6.0 that allows user to assign for MS Word styles in a word document and select HTML features from a toolbar.
- WordPerfect Internet Publisher — It is plug in for word profile for windows. It include template for editing files for the web and a converter program that supports the ability to add links and convert the document to HTML.

These converters takes files from many popular word processing programs and convert them to HTML. Using these converters, a user may create documents in a program and then convert the results. Converters help put existing documents on the web quickly.

Tables are critical for summarizing information in a way that can be quickly and easily grasped. Tables are ranked high among some of the viewer's best information designs. They help structures the data so that viewers of the document can get in and out of the pages with ease.

Initially, support for tables was somewhat limited.

There are two ways to create home pages: do it yourself or hire a consultant who knows HTML and has the knowledge of HTML.As described, there are tools available to help the creation of home pages. These specialists can combine the text, image, audio, and video.

Some people argue that if an organization's pages are not attractive, well-designed, and user-Friendly, people will not be interested and the organization will not get much out of it.

HTML tools (partial list)

Tool	Type	platform
BBEdit HTML Extensions[a]	Template	BBEdit or for Mac
Fm2html[b]	MIF converter	UNIX
Hot Metal[c]	Editor	Mac, pc, UNIX
HTML Assistant[d]	Editor	PC
Web Maker[i]	MIF converter	UNIX
Web Weaver[j]	Editor	Mac

Given a pointer to a piece of information on the Internet, the browser has to able to access that Information or operate in some way based on the contents of that pointer. For hypertext web Documents, this means that the browser must be able to interconnect with the server using the HTTP protocol. Since the web can also manage information contained on FTP and gopher servers, in new postings, in mail, and so on, the browser has to support these tools as well. Each page that is loaded from the web to the single document, written in HTML that includes the text of the document, its structure, and any links to the other documents, images, and other media. The browser interprets the HTML markup code contained in that documents and formats and displays the document.

Hypermedia:

For graphical output, there are two kinds of images that a web browser can handle: inline image and external images. An inline image is a graphic on web page that does not contain a link to another place; it is there for illustration only. External images are not directly loaded on a web page; they are only downloaded at the request of the reader.

Inline images are specified using the<IMG> tag in the HTML file. An example of an image tag is <IMG SRG="danscat.gif"> which makes references to a GIF (Graphics Interchange Format) files containing scanned pictures of Dan's cat, Micio-Micio. However inline images and External images provide a design and presentation for a document that can be alluring to the Customer. Therefore, publishing on a web would be more attractive and beneficial if some image Formats were included to help capture the viewer's attention. Once an image is placed on the web, the publisher may then perform any text and image alignment, place any links on the image needed, place transparent backgrounds on the image, create borders, and so on. Some of the more newly introduced technologies include the interlacing effects. Interlacing a GIF image does not change the appearance of the image but rather changes the effect of how the image is saved and loaded. The image, as it is loading, has the appearance of fading-in line by line. To create these effects, publisher needs tools for creating interlaced GIF images.

Gif, is the most widely used graphics formats on the web today. GIF was developed by CompuServe to fill the need for a cross-platform image formats.GIF files are predominately used for logos, icons, line, art, and other simple images. The problems with GIF, at the moment, is that the form of compression it uses, LZW, is patented. Unisys, the owner of the patent, has requested that developers who use the GIF formats after 1994 pay a per-copy royalty for the use of LZW. Because of the problems with the patent on LZW and the possibility of it costing publishers to use the format, the GIF formats may fade away in the future to be replaced with some other, more freely available format.

The candidate likely to replace GIF is jpeg, named after the group that developed it the Progressive JPFG file format loads images up to three times more quickly than the previous GIF formats and provides faster intermediate image recognition, so users on slow connections can view color-rich images quickly. In facts, with Native Progressive JPEG decompression, less than 10 percent of the image needs to be loaded to be recognizable.

JPEG was designed for the storage of photographic images. Unlike GIF, JPEG images can have any number of colors, and the compression formula it uses works well for photographic patterns, so the files sizes it creates from photographs are considerably smaller than those that GIF produces. In addition, JPEG files have just begun to widely supported by browsers.

Including sound files on a web page can provide customers with important information. In addition, it may provide welcome messages for readers or sound clips of an organization. To include a link to a sound on a web page, the sound sample must first be in the correct format. Currently, the only cross-platform sound file format for the web is Sun Microsystems 'AU format. The following is an illustration of linking an AU format file:
(<A HREF="vivaldi.au">AIFF format, 357K)</A>

The current standard video format for the web is Motion Picture Expert Group (MPEG). Apple has also introduced the QuickTime format that has increasingly gained popularity. To include video files on the web pages, one must first have the correct file

extension.MPEG files have the extension .mpg or.mpeg while QuickTime has .move extensions. The following is an illustration of linking a video to an image:

<A HERP=”specialist.mpeg”><IMG SRC=”film.gif”(12Meg)</A>

- For graphical output, there are two kinds of images that a web browser can handle; inline images and external images.
- An inline image is a graphic on the Web page that does not contain a link to another place.
- External images are not directly loaded on a Web page; they are only downloaded at the request of the reader.
- Inline images are specified using the<IMG> tag in the HTML file.
- Eg. <IMG SRC=”danscat.gif”> which makes reference to a GIF(Graphics Interchange Format)
- Some of the more newly introduced technologies include the interlacing effect.
- Interlacing a GIF image does not change the appearance of the image but rather changes the effect of how the image is saved and loaded.
- GIF is the most widely used graphics format on the Web today.
- GIF files are predominately used for logos, icons, line art, and other simple images.
- The problem with GIF, at the moment, is that the form of compression it uses, LZW, is patented.

- The progressive JPEG file format loads images up to three times more quickly than the previous GIF format and provides faster intermediate image recognition, so users on slow connections can view color-rich images quickly.
- JPEG was designed for the storage of photographic images.
- Unlike GIF, JPEG images can have any number of color, and the compression formula it uses works well for photographic patterns.
- To include a link to a sound on a Web page, the sound sample must first be in the correct format.
- The only cross-platform sound file format for the Web is Sun Microsystem’ AU format.
- The following is an illustration of linking an AU format file:

(<A HREF=”Vivaldi.au”>AIFF format, 357K)</A>

- The current standard video format for the Web is Motion Picture Expert Group (MPEG).
- MPEG files have the extension .mpg and .mpeg while QuickTime has .mov extensions.
- To link the video files to a web page is similar to the functionality of linking a sound.
- The following is an illustration of linking a video to an image:

<A HERF=”specialist.mpeg”><IMG SRC=”film.gif”(12 Meg)</A>

Data collection:

- As many sites owners know by now, most web servers automatically create an access log of usage data, recording the domain name or IP address of sites accessing the file, dates and times of access, which files were viewed, and the sizes of those files.
- A three-digit return code indicates whether file requests were fulfilled or rejected, helping the web masters check the validity of links.
- The agent file records the brand and version of browser being used; the referrer file identifies the page from which a visitor is linking and where the visitor travels within the site.
- These log files can be linked to one another, run separately, or may not be used at all.

- Information on the visitor's travels through a site can identify underused pages and possibly suggest better navigational patterns.
- And attention to the error log can prevent visitors from being stopped by a broken link.

Publishing systems:

- There are many browsers/publishing systems that allow users to create Web documents.
- Companies are now beginning to understand the benefits of publishing their information on the WWW.
- Information about a company has always been available for anyone with the time, resources, and energy to collect it manually.
- The Web is shrinking the time it takes to gather this information and publish it: once it is published, the web increases the speed at which the information can be collected.
- Web/intranet publishing enables internal corporate departments to provide timely information on new product announcements or marketing videos and to help increase employee productivity, improve competitiveness, enhance customer service, and reduce internal publishing costs.
- Publishing on the web goes a long way in helping to acquire customers and maintain their loyalty.
- Two of the most common publishing systems are Netscape Publisher and Adobe PageMaker.
    - The following subsections highlight the features of each (systems from other vendors are also entering the market).

Netscape:

- Netscape Publishing System has allowed enterprises to distribute their own publications and services on the Internet by offering content providers flexible and integrated software for organizing, customizing, and delivering text, graphics, audio, or video documents to users around the world.
- Netscape Publishing System is an integrated solution that is easily customized and can deploy quickly.
- It can be used as a standalone solution or be integrated with current software systems.
- It has the ability to enhance existing systems to become Internet-enabled and to provide increased functionality to customers.
- In addition to storing and providing access to information, the Netscape Publishing System allows publishers to add value to information by tailoring it to the requirements of individuals.
- Netscape Publishing system automatically searches new documents for predefined keywords and create automatic hyperlinks.
- Netscape Public system features an easy-to-use graphical interface and the ability to work with content derived from multiple sources.
- It exploits the security capabilities of Netscape Commerce Server and the ease of use of Netscape Navigator to provide a system that is industrial strength yet easy to manage and develop standards, Netscape in the past has worked with the Internet Engineering Task Force and the World Wide Web consortium. Table 8.2 describes key features.

The following is a listing of some additional standards that Netscape Publisher complies with .These standards help existing software packages such as plug-ins, Internet servers, and also many platforms be compatible with one another.

- *Native support*. Available for HTML, HTTP, FTP, NNTP, SMTP, MIME, S/MIME, S/MIME, and POP3 standards.
- *Cross –platform support.* Provide a common interface and common behavior among the different platforms.
- *Open environments.* Works in environments that support HTTP compliant network clients, including Winsock.

Minimum platform requirements are shown in Table 8.3.

The following is a listing of support platform for the Publisher.

- Apple Macintosh — Macintosh system 7 or later; Mac OS; Power PC
- Intel (x86)-based — Window 3.1 and 3.11; Window for workgroups 3.11; Window 95; Windows NT (3.5 or higher)
- UNIX — Digital Equipment Corporation Alpha (OSF/12.0); Hewlett-Packard 700-series (HP-UK 9.03); IBM RS/600 AIX 3.2; Silicon Graphics (IRIX 5.2); Sun SPARC (Solaris 2.4, SunOS 4.1.3); 386/486/Pentium (BSDI)

Adobe PageMaker. AdobePageMaker is a Professional, cross-platform, desktop publishing program that allow the ability to design and pro-duce sophisticated publications. PageMaker combines text and graphics from a wide range of software application for printed or electronic delivery .PageMaker offers tools for producing professional-quality publications. PageMaker helps produce accurate color.

Registration	At time of registering, subscribers specify their interests. This information is used to filter through incoming documents for each subscriber. Subscribers scan their list and can then review the documents of interest.
Access Control	Access to documents can be controlled at the level of the entire publication or by the particular issue of a publication. Access controls can be applied to documents at various levels.
Document Managements	Electronic content such as text, graphics, audio and video can be created with a number of software tools or be imported to tag , convert the formats of, and load news and satellite feeds.
Simplified content Administration	A range of tools simplify the task of managing large document collections, including the ability to define searchable attributes, presentation formats, and profile.
Content Retrieval	A Natural Language Interface with support for dictionaries, synonyms and relevance ranking is providing to help users easily locate information.
An Open solution	The Publishing system is built on widely used Industry-standard technologies such as relational Database, text search engines , HTML,HTTP,SQL

Architecture	Modular system design to allow different modules to run on multiple systems, if necessary, to support high availability, scalability, security.
Document handling	Multiple media types supported, including text, graphics, audio and video incoming feeds can include satellite and electronic news feeds and several other formats.
Personalized Information access	Automatic filtering of information to generate personalized list of documents matching each subscriber's interests. Flexible number of Preferences can be stored per subscriber.
Text search	Full Boolean search Capability including AND, where document OR and NOT. Relevance ranking, retrieved as a result of a query are ranked in order of their relevance.
Flexible Billing Option	Support for both subscriptions and real time credit card purchases.

Table 8.3: Platform requirement

Platform	Processor (minimum)	Disk space (MB)	Memory (minimum, MB)	Memory (recommended, MB)
Window	386SX	2	4	8
Macintosh	68020	2	4	8
UNIX	N/A	3	16	16

Adobe PageMaker includes a build in word with a spell Checker and search and replace features. In addition PageMaker words with text, graphics, image, spreadsheets and data from all software application.

PONDICHERRY UNIVERSITY QUESTIONS

2 MARKS

1. Define the term Internet. **(Apr 2012) (Ref.Qn.No.23)**
2. What is the usage of a browser? **(Apr 2012) (Ref.Qn.No.22)**
3. What are the two most common publishing systems? **(Nov 2012) (Ref.Qn.No.24)**
4. Give the primary uses of Spider program. **(Nov 2012) (Ref.Qn.No.8)**
5. Write about electronic payment system. **(Apr 2013) (Ref.Qn.No.25)**
6. What is SOA GOVERNANCE? **(Apr 2013) (Ref.Qn.No.26)**
7. What is meant by Nap access?(**Apr-2014) (Ref.Qn.No.21)**
8. Write a note on internet browser?(**Apr-2014) (Ref.Qn.No.22)**
9. Write short notes on Internet & Intranets.(**Nov 2014) (Ref.Qn.No.27)**
10. Mention Some Internet Tools.(**Nov 2014(Apr 2015) (Ref.Qn.No.28)**
11. Comparison between Website & Webpage**.(Apr 2015) (Ref.Qn.No.29)**

11 MARKS

1. What are the technologies used for web servers? Explain. **(April 2012)**(**Nov 2014)(April 2015) (Ref.Qn.No7)**
2. Discuss the tools of WWW. **(April 2012) (Ref.Qn.No.5)**
3. Describe the various internet tools relevant to commerce. **(Nov 2012)(April 2014) (April 2015) (Ref.Qn.No.5)**
4. Discuss the key technology features that should be included in search engines.**(Nov 2012) (Ref.Qn.No.4)**.
5. Explain about various e-commerce considerations for internet applications. **(April 2013) (April 2014) (Ref.Qn.No.6)**
6. Explain about E- Commerce and internet access in detail. **(April 2013) (Ref.Qn.No.2, Pg.no.7)**
7. Explain the function of Search Engine.(**Nov 2014) (Ref.Qn.No.4)**