E-COMMERCE

SYLLABUS:

UNIT 1: Electronic Commerce: Overview, Definition, Advantages & Disadvantages of E-Commerce, Threats of E-Commerce, Managerial Prospective, Rules & Regulation for Controlling Commerce, Relationship Between E-Commerce & Networking, Different Types of Networking for E-Commerce, internet, Intranet, EDI Systems, Wireless Application Protocol: Definition, Hand Held Devices, Mobility & Commerce Model, Mobile Computing, Wireless Web, Web Security, Infrastructure Requirement for E-Commerce, Business Model of E-Commerce; Model Based on Transaction Type, Model Based on Transaction Party- B2B, B2C, C2B, C2C, E-Governance.

UNIT 2: E-Strategy: Overview, Strategic Methods for developing E-Commerce. Four C's (Convergence, Collaborative, Computing, Content Management & Call Center). Convergence: Technological Advances in Convergence - Types, Convergence and its implications, Convergence & Electronic Commerce. Collaborative Computing: Collaborative Product Development, contract as per CAD, Simulations Collaboration, Security. Content Management: Definition of Content, Authoring Tools and Content Management, Content Management, Content - partnership, repositories, convergence, providers, Web Traffic.

UNIT 3: Traffic Management: Content Marketing Call Center: Definition, Need, Tasks Handled, Mode of Operation, Equipment, Strength & Weakness of Call Center, Customer Premises Equipment (CPE). Supply Chain Management: E-logistics, Supply Chain Portal, Supply Chain Planning Tools (SCP Tools), Supply Chain Execution(SCE), SCEFramework, Internet's Effect on Supply Chain Power.

UNIT 4: E-Payment Mechanism: Payment through card system, E-Cheque, E-Cash, E-Payment, Threats& Protections. E-Marketing: Home - Shopping, E-Marketing, Tele-Marketing

UNIT 5: Electronic Data Interchange (EDI): Meaning, Benefits, Concepts, Application, EDI Model, Protocols (UN EDI, FACT/ GTDI), ANSIX-12, Data Encryption (DES/RSA) Risks of E-Commerce: Overview, Security for E-Commerce, Security Standards, Firewall, Cryptography, Key Management, Password Systems, Digital Certificates, Digital Signatures.

Text Book: 1. Electronic Commerce - Technologies & Applications, Bhaskar Bharat,

TMH Reference Books:

1. E-commerce, MM Oka, EPH
2. Frontiers of Electronics Commerce, Kalakotia, Whinston, Pearson Education
3. Electronic Commerce, Loshinpete, Murphy P. A., Jaico Publishing Housing
4. E-Commerce, Murthy, Himalaya Publishing.

UNIT-1

1. Electronic Commerce:

- Electronic commerce, commonly known as E-commerce is trading in products or services using computer networks, such as the Internet.
- Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems.
- Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle, although it may also use other technologies such as e-mail.

Definition of E-commerce:

Sharing business information, maintaining business relationships and conducting business transactions using computers connected to telecommunication network is called E-Commerce.

2. E-Commerce Categories:

1. Electronic Markets

Present a range of offerings available in a market segment so that the purchaser can compare the prices of the offerings and make a purchase decision.

Example: Airline Booking System

2. Electronic Data Interchange (EDI)

• It provides a standardized system

• Coding trade transactions

• Communicated from one computer to another without the need for printed orders and invoices & delays & errors in paper handling

• It is used by organizations that a make a large no. of regular transactions

Example: EDI is used in the large market chains for transactions with their suppliers

3. Internet Commerce

• It is use to advertise & make sales of wide range of goods & services.

• This application is for both business to business & business to consumer transactions.

Example: The purchase of goods that are then delivered by post or the booking of tickets that can be picked up by the clients when they arrive at the event.

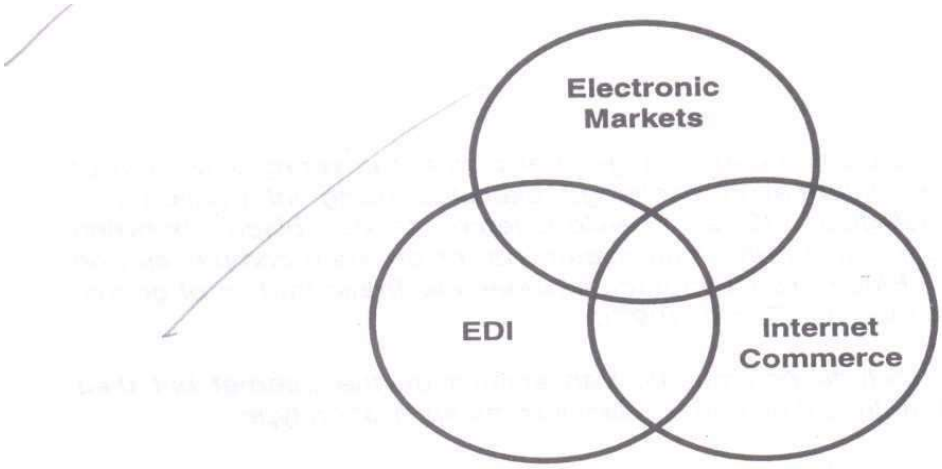


Fig. 1.1 The three categories of e-Commerce.

3. Advantages Of E-commerce:

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

4. Disadvantages Of E-commerce:

- Electronic data interchange using EDI is expensive for small businesses
- Security of internet is not very good - viruses, hacker attacks can paralise e-commerce
- Privacy of e-transactions is not guaranteed

- E-commerce de-personalises shopping

5. Threats of E-commerce:

- Hackers attempting to steal customer information or disrupt the site
- A server containing customer information is stolen.
- Imposters can mirror your ecommerce site to steal customer money
- Authorised administrators/users of an ecommerce website downloading hidden active content that attacks the ecommerce system.
- A disaffected employee disrupting the ecommerce system.
- It is also worth considering where potential threats to your ecommerce site might come from, as identifying potential threats will help you to protect your site. Consider:
- Who may want to access your ecommerce site to cause disruption or steal data; for example competitors, ex-employees, etc.
- What level of expertise a potential hacker may possess; if you are a small company that would not be likely to be considered a target for hackers then expensive, complex security may not be needed.

6. Features of E-Commerce:

- **Ubiquity**

  Internet/Web technology is The marketplace is extended beyond traditional available everywhere: at work, at home, and boundaries and is removed from a temporal and elsewhere via mobile devices, anytime. geographic location. ―Marketspace‖ is created; shopping can take place anywhere. Customer convenience is enhanced, and shopping costs are reduced.

- **Global reach**

  The technology reaches Commerce is enabled across cultural and across national boundaries, around the earth. national boundaries seamlessly and without modification. ―Marketspace‖ includes potentially billions of consumers and millions of businesses worldwide.

- **Universal standards**

  There is one set of There is one set of technical media standards technology standards, namely Internet across the globe.

- **Richness**

  Video, audio, and text messages Video, audio, and text marketing messages are are possible. integrated into a single marketing message and consuming experience.

- **Interactivity**

  The technology works Consumers are engaged in a dialog that through interaction with the user. dynamically adjusts the experience to the individual, and makes the consumer a co-participant in the process of delivering goods to the market.

- **Information density**

  The technology Information processing, storage, and reduces information costs and raises quality. communication costs drop dramatically, while currency, accuracy, and timeliness improve greatly. Information becomes plentiful, cheap, and accurate.

- **Personalization/Customization**

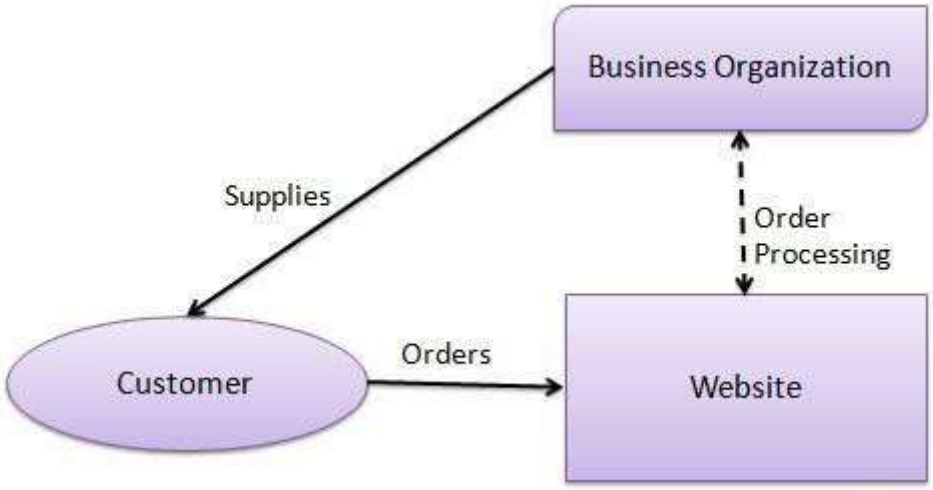
  The Personalization of marketing messages and technology allows personalized messages to customization of products and services are be delivered to individuals as well as groups. based on individual characteristics.

1.7 Business models of e-commerce:

There are mainly 4 types of business models based on transaction party.

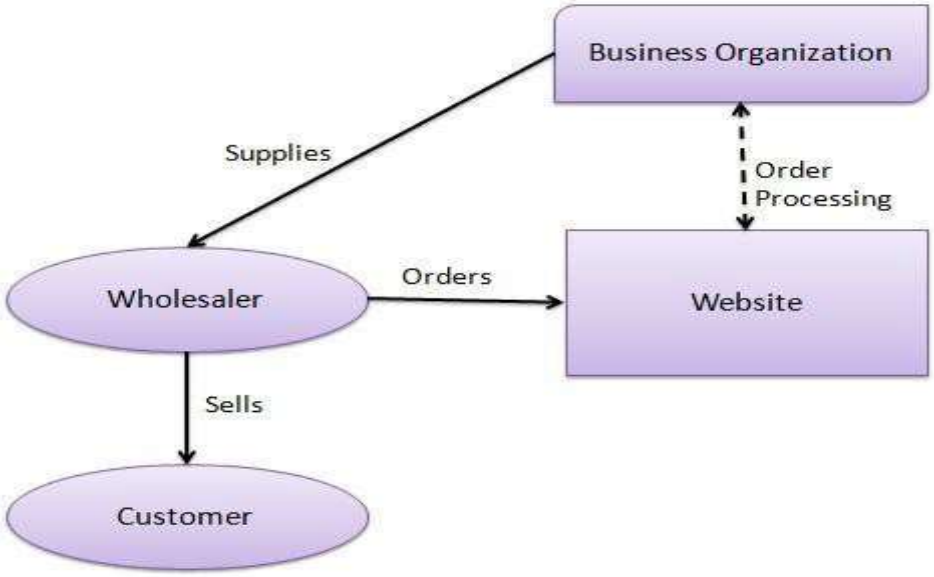
Business-to-Consumer (B2C)

In a Business-to-Consumer E-commerce environment, companies sell their online goods to consumers who are the end users of their products or services. Usually, B2C E-commerce web shops have an open access for any visitor, meaning that there is no need for a person to login in order to make any product related inquiry.



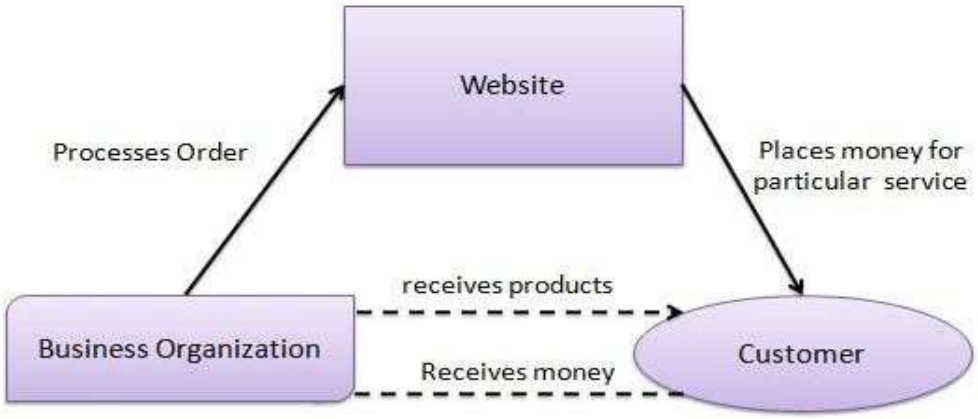
Business-to-Business (B2B)

In a Business-to-Business E-commerce environment, companies sell their online goods to other companies without being engaged in sales to consumers. In most B2B E-commerce environments entering the web shop will require a log in. B2B web shop usually contains customer-specific pricing, customer-specific assortments and customer-specific discounts.



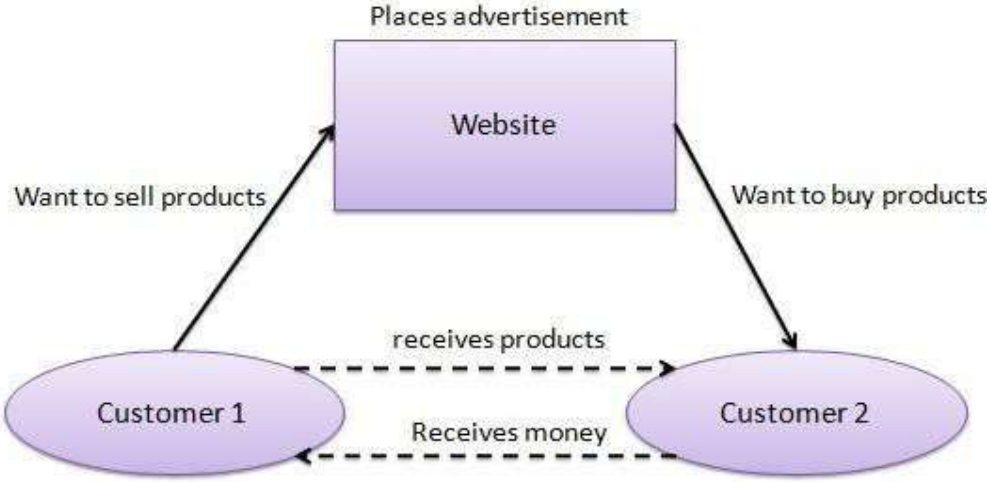
Consumer-to-Business (C2B)

In a Consumer-to-Business E-commerce environment, consumers usually post their products or services online on which companies can post their bids. A consumer reviews the bids and selects the company that meets his price expectations.



Consumer-to-Consumer (C2C)

In a Consumer-to-Consumer E-commerce environment consumers sell their online goods to other consumers. A well-known example is eBay.



1.8 E-Governance:

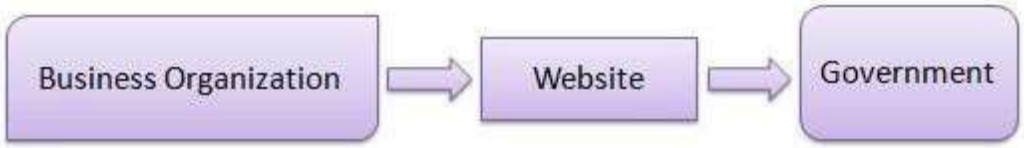
E-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework.

Through e-governance, government services will be made available to citizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in

governance concepts are government, citizens and businesses/interest groups. In e-governance there are no distinct boundaries.

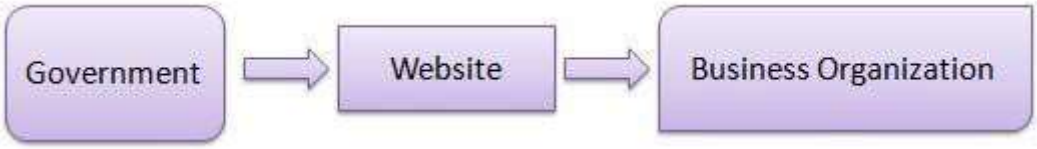
Business - to - Government (B2G)

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



Government - to - Business (G2B)

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



Government - to - Citizen (G2C)

Government uses G2C model website to approach citizen in general. Such websites support auctions of vehicles, machinery or any other material. Such website also provides services like registration for birth, marriage or death certificates. Main objectives of G2C website are to reduce average time for fulfilling people requests for various government services.

1.9 Different Types of Networking For E-Commerce:

Internet:

The Internet is a global network of computers that allows people to send email, view web sites, download files such as mp3 and images, chat, post messages on newsgroups and forums and much more.

The Internet was created by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1960's and was first known as the ARPANet. At this stage the Internet's first computers were at academic and government institutions and were mainly used for accessing files and to send emails. From 1983 onwards the Internet as we know it today started to form with the introduction of the communication protocol TCP/IP to ARPANet. Since 1983 the Internet has accommodated a lot of changes and continues to keep developing.

The last two decades has seen the Internet accommodate such things as network LANs and ATM and frame switched services. The Internet continues to evolve with it becoming available on mobile phones and pagers and possibly on televisions in the future.

Advantages of internet:

There many advantages to using the internet such as:

E-mail

Email is now an essential communication tool in business. It is also excellent for keeping in touch with family and friends. The advantage to email is that it is free (no charge per use) when compared to telephone, fax and postal services.

Information

There is a huge amount of information available on the internet for just about every subject known to man, ranging from government law and services, trade fairs and conferences, market information, new ideas and technical support.

Services

Many services are now provided on the internet such as online banking, job seeking and applications, and hotel reservations. Often these services are not available off-line or cost more.

Buy or sell products.

The internet is a very effective way to buy and sell products all over the world.

Communities communities of all types have sprung up on the internet. Its a great way to meet up with people of similar interest and discuss common issues.

A Leading-Edge Image

Presenting your company or organization as leading-edge shows your customers and prospective customers that you are financially strong, technologically savvy, and ready for the 21st century. And that you care enough about your customers to take advantage of new technologies for their benefit. And finally that you have the resources to support your clients in the most beneficial manner possible.

More and more advertisers on television, radio, magazines, and newspapers are including a Web address. Now is the time to avoid playing catch-up later.

Improved Customer Service

The companies are available to their customers 24 hours a day, 7 days a week. The Internet never sleeps. Whenever customer needs information about any company, products or services, they can access the company‘s Web Page.

Market Expansion

The Internet is a global system. Latest estimates are that there are about 40 million people with access to the Internet, and this number is growing every day. By simply posting a Web Page you are also addressing International markets.

Low Cost Marketing

Imagine developing a full color brochure without having to incur the costs of proofs, printers, wasted paper, long lead times between revisions, and more. Then imagine a full color product or services brochure that is interactive and which incorporates text, graphics, audio, and/or video. One that can be immediately updated without incurring the usual costs of product material updates.

Low Cost Selling

Without the cost of direct selling potential customers can get detailed information about your products or services at any time. And they can easily order your products over the Internet, or request additional information be sent to them via a request form on your Web page.

Lower Communication Costs

Your time, and your employees time, is valuable. Most businesses and organizations spend time answering the same questions over and over again. With a Web page you can make the answers

available to everyone immediately. You can also update your Wed page with new information quickly and easily.

Intranet:

- An intranet is a computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization. This term is used in contrast to extranet, a network between organizations, and instead refers to a network within an organization.
- The objective is to organize each individual's desktop with minimal cost, time and effort to be more productive, cost efficient, timely, and competitive.
- An intranet may host multiple private websites and constitute an important component and focal point of internal communication and collaboration.
- Any of the well known Internet protocols may be found in an intranet, such as HTTP (web services), SMTP (e-mail), and FTP (file transfer protocol). Internet technologies are often deployed to provide modern interfaces to legacy information systems hosting corporate data.

Uses of Intranet:

- Increasingly, intranets are being used to deliver tools, e.g. collaboration (to facilitate working in groups and teleconferencing) or sophisticated corporate directories, sales and customer relationship management tools, project management etc., to advance productivity.
- Intranets are also being used as corporate culture-change platforms. For example, large numbers of employees discussing key issues in an intranet forum application could lead to new ideas in management, productivity, quality, and other corporate issues.
- In large intranets, website traffic is often similar to public website traffic and can be better understood by using web metrics software to track overall activity. User surveys also improve intranet website effectiveness. Larger businesses allow users within their intranet to access public internet through firewall servers. They have the ability to screen messages coming and going keeping security intact.
- When part of an intranet is made accessible to customers and others outside the business, that part becomes part of an extranet. Businesses can send private messages through the public

network, using special encryption/decryption and other security safeguards to connect one part of their intranet to another.

- Intranet user-experience, editorial, and technology teams work together to produce in-house sites. Most commonly, intranets are managed by the communications, HR or CIO departments of large organizations, or some combination of these.
- Because of the scope and variety of content and the number of system interfaces, intranets of many organizations are much more complex than their respective public websites. Intranets and their use are growing rapidly.

Advantages:

- **Workforce productivity**: Intranets can help users to locate and view information faster and use applications relevant to their roles and responsibilities. With the help of a web browser interface, users can access data held in any database the organization wants to make available, anytime and — subject to security provisions — from anywhere within the company workstations, increasing employees' ability to perform their jobs faster, more accurately, and with confidence that they have the right information.
- **Time**: Intranets allow organizations to distribute information to employees on an *as-needed* basis; Employees may link to relevant information at their convenience, rather than being distracted indiscriminately by email.
- **Communication**: Intranets can serve as powerful tools for communication within an organization, vertically strategic initiatives that have a global reach throughout the organization. By providing this information on the intranet, staff have the opportunity to keep up-to-date with the strategic focus of the organization. Some examples of communication would be chat, email, and/or blogs. A great real world example of where an intranet helped a company communicate is when Nestle had a number of food processing plants in Scandinavia. Their central support system had to deal with a number of queries every day.
- **Web publishing**: allows cumbersome corporate knowledge to be maintained and easily accessed throughout the company using hypermedia and Web technologies. Examples include: employee manuals, benefits documents, company policies, business standards, news feeds, and even training, can be accessed using common Internet standards (Acrobat files,

Flash files, CGI applications). Because each business unit can update the online copy of a document, the most recent version is usually available to employees using the intranet.

- **Business operations and management**: Intranets are also being used as a platform for developing and deploying applications to support business operations and decisions across the internetworked enterprise.
- **Cost-effective**: Users can view information and data via web-browser rather than maintaining physical documents such as procedure manuals, internal phone list and requisition forms. This can potentially save the business money on printing, duplicating documents, and the environment as well as document maintenance overhead.
- **Enhance collaboration**: Information is easily accessible by all authorised users, which enables teamwork.
- **Cross-platform capability**: Standards-compliant web browsers are available for Windows, Mac, and UNIX.
- **Built for one audience**: Many companies dictate computer specifications which, in turn, may allow Intranet developers to write applications that only have to work on one browser (no cross-browser compatibility issues).
- **Promote common corporate culture**: Every user has the ability to view the same information within the Intranet.
- **Immediate updates**: When dealing with the public in any capacity, laws, specifications, and parameters can change. Intranets make it possible to provide your audience with "live" changes so they are kept up-to-date, which can limit a company's liability.
- **Supports a distributed computing architecture:** The intranet can also be linked to a company‘s management information system, for example a time keeping system.

1.10 Wireless Application Protocol:

- WAP is a technical standard for accessing information over a mobile wireless network.
- A WAP browser is a web browser for mobile devices such as mobile phones that uses the protocol.
- WAP is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and instant messaging.

The WAP layers are:

- Wireless Application Environment (WAE)
- Wireless Session Layer (WSL)
- Wireless Transport Layer Security(WTLS)
- Wireless Transport Layer (WTP)

Web security:

- It is a branch of Information Security that deals specifically with security of websites, web applications and web services.
- At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems. Typically web applications are developed using programming languages such as PHP, Java EE, Java, Python, Ruby, ASP.NET, C#, VB.NET or Classic ASP.

UNIT-2

1. Technological convergence:

- Technological convergence is the tendency that as technology changes, different technological systems sometimes evolve toward performing similar tasks.
- Digital convergence refers to the convergence of four industries into one conglomerate, ITTCE (Information Technologies, Telecommunication, Consumer Electronics, and Entertainment).Previously separate technologies such as voice data and productivity applications, and video can now share resources and interact with each other synergistically.
- Telecommunications convergence, network convergence or simply convergence are broad terms used to describe emerging telecommunications technologies, and network architecture used to migrate multiple communications services into a single network.
- Convergence in this instance is defined as the interlinking of computing and other information technologies, media content, and communication networks that has arisen as the result of the evolution and popularization of the Internet as well as the activities, products and services that have emerged in the digital media space.
- Convergent services, such as VoIP, IPTV, Mobile TV, Smart TV, and others, tend to replace the older technologies and thus can disrupt markets. IP-based convergence is inevitable and will result in new service and new demand in the market.

2. Technology Implications:

Convergent solutions include both fixed-line and mobile technologies. Recent examples of new, convergent services include:

- Using the Internet for voice telephony
- Video on demand
- Fixed-mobile convergence
- Mobile-to-mobile convergence

- Location-based services
- Integrated products and bundles

Convergent technologies can integrate the fixed-line with mobile to deliver convergent solutions. Convergent technologies include:

- IP Multimedia Subsystem
- Session Initiation Protocol
- IPTV
- Voice over IP
- Voice call continuity
- Digital video broadcasting - handheld

2.3 Collaborative Product Development:

- CPD is a business strategy, work process and collection of software applications that facilitates different organizations to work together on the development of a product. It is also known as collaborative product definition management (cPDM).
- Collaborative Product Development helps individual users and companies manage, share and view your CAD projects without the cost and complexity of purchasing an entire PDM or PLM solution. CPD comes in the form of a Software as a service delivery model, which allows for rapid iterations and little or no downloads and installs.
- Exactly what technology comes under this title does vary depending on whom one asks; however, it usually consists of the Product Lifecycle Management (PLM) areas of: Product Data Management (PDM); Product visualization; team collaboration and conferencing tools; and supplier sourcing software. It is generally accepted as not including CAD geometry tools, but does include data translation technology.

Technologies and methods used:

Clearly general collaborative software such as email and chat (instant messaging) is used within the CPD process. One important technology is application and desktop sharing, allowing one person to view what another person is doing on a remote machine. For CAD and product visualization applications an _appshare‘ product that supports OpenGL graphics is required. Another common application is Data sharing via Web based portals.

Specific to product data

With product data an important addition is the handling of high volumes of geometry and metadata. Exactly what techniques and technology is required depends on the level of collaboration being carried out and the commonality (or lack thereof) of the partner sites' systems.

Specific to PLM and CAx collaboration

Collaboration using PLM and CAx tools requires technology to support the needs of:

1. People: Personnel of different disciplines and skill levels;
2. Organizations: Organizations throughout an enterprise or extended enterprise with different rules, processes and objectives;
3. Data: Data from different sources in different formats.

Appropriate technologies are required to support collaboration across these boundaries.

- **People**

  Effective PLM collaboration will typically require the participation of people who do not have high level CAD skills. This requires improved user interfaces including tailorable user interfaces that can be tailored to the skill level and specialty of the user.

  Improved visualization capabilities, especially those that provide a meaningful view of complex information such as the results of a fluid flow analysis will leverage the value of all participants in the collaboration process. Effective collaboration requires that a participant be freed from the burden of knowing the intent history typically imbedded within and constricting the use of parametric models.

- **Organizations**

  Community collaboration requires that companies, suppliers, and customers share information in a secure environment, ensure compliance with enterprise and regulatory rules and enforce the process management rules of the community as well as the individual organizations.

- **Data**

  The most basic collaboration data need is the ability to operate in a MultiCAD environment. That is, however, only the beginning. Models from multiple CAD sources must be assembled into an active digital mockup allowing change and/or design in context.

2.4 Content Management System:

- A content management system (CMS) is a computer application that allows publishing, editing and modifying content, organizing, deleting as well as maintenance from a central interface. Such systems of content management provide procedures to manage workflow in a collaborative environment.
- CMSs are often used to run websites containing blogs, news, and shopping. Many corporate and marketing websites use CMSs. CMSs typically aim to avoid the need for hand coding, but may support it for specific elements or entire pages.

Main features of CMS:

- The function and use of content management systems is to store and organize files, and provide version-controlled access to their data. CMS features vary widely. Simple systems showcase a handful of features, while other releases, notably enterprise systems, offer more complex and powerful functions. Most CMS include Web-based publishing, format management, revision control (version control), indexing, search, and retrieval. The CMS increments the version number when new updates are added to an already-existing file. Some content management systems also support the separation of content and presentation.
- A CMS may serve as a central repository containing documents, movies, pictures, phone numbers, scientific data. CMSs can be used for storing, controlling, revising, semantically enriching and publishing documentation.

The content management system (CMS) has two elements:

- Content management application (CMA) is the front-end user interface that allows a user, even with limited expertise, to add, modify and remove content from a Web site without the intervention of a Webmaster.
- Content delivery application (CDA) compiles that information and updates the Web site.

2.5 Web Traffic:

Web traffic is the amount of data sent and received by visitors to a web site.
Web traffic is measured to see the popularity of web sites and individual pages or sections within a site. This can be done by viewing the traffic statistics found in the web server log file, an automatically generated list of all the pages served. A *hit* is generated when any file is served.

The following types of information are often collated when monitoring web traffic:

- The number of visitors.
- The average number of page views per visitor – a high number would indicate that the average visitors go deep inside the site, possibly because they like it or find it useful.
- Average visit duration – the total length of a user's visit. As a rule the more time they spend the more they're interested in your company and are more prone to contact.
- Average page duration – how long a page is viewed for. The more pages viewed, the better it is for your company.
- Domain classes – all levels of the IP Addressing information required to deliver Webpages and content.
- Busy times – the most popular viewing time of the site would show when would be the best time to do promotional campaigns and when would be the most ideal to perform maintenance
- Most requested pages – the most popular pages
- Most requested entry pages – the entry page is the first page viewed by a visitor and shows which are the pages most attracting visitors
- Most requested exit pages – the most requested exit pages could help find bad pages, broken links or the exit pages may have a popular external link

- Top paths – a path is the sequence of pages viewed by visitors from entry to exit, with the top paths identifying the way most customers go through the site
- Referrers; The host can track the (apparent) source of the links and determine which sites are generating the most traffic for a particular page.

UNIT-3

Content marketing:

- Content marketing is any marketing that involves the creation and sharing of media and publishing content in order to acquire and retain customers.
- It is a strategic marketing approach focused on creating and distributing valuable, relevant, and consistent content to attract and retain a clearly-defined audience — and, ultimately, to drive profitable customer action.
- Basically, content marketing is the art of communicating with your customers and prospects without selling.
- It is non-interruption marketing. Instead of pitching your products or services, you are delivering information that makes your buyer more intelligent.

2.6 Call centre:

- A call centre is a centralised office used for receiving or transmitting a large volume of requests by telephone.
- An inbound call centre is operated by a company to administer incoming product support or information inquiries from consumers.
- Outbound call centers are operated for telemarketing, solicitation of charitable or political donations, debt collection and market research.
- A contact centre is a location for centralised handling of individual communications, including letters, faxes, live support software, social media, instant message, and e-mail.
- A call centre has an open workspace for call centre agents, with work stations that include a computer for each agent, a telephone set/headset connected to a telecom switch, and one or more supervisor stations. It can be independently operated or networked with additional centres, often linked to a corporate computer network, including mainframes, microcomputers and LANs.
- The contact centre is a central point from which all customer contacts are managed. Through contact centres, valuable information about company are routed to appropriate

people, contacts to be tracked and data to be gathered. It is generally a part of company's customer relationship management.

7. Components of call centre:

There are 6 key components which should be integrated into the call centre operation:

- Location, building and facilities
- Customer
- Technology
- Process
- People
- Finance and business management

➢ **Location, building and facilities**

Where a centre is located is critical in terms of the cost of the building but more importantly the ability to recruit and retain employees to work in the centre. The ease and cost to get to a centre is important for those employed in the centre but also in the integration with the Head Office functions that the centre needs to work with. The facilities and working environment is more critical than for functional line departments because of the intensity with which the Agents have to sit at their desks and the need to manage resource patterns. Visiting a call centre and looking at how it might feel to work in it will be extremely telling as to how good the centres performance is, but also how the organisation view and treat their employees.

➢ **Customer**

Customers can be anyone, and the Agent needs to have the skills to be able to adapt their style and vocabulary to suit different customer types. The Agent talks to more customers in any one day that any other person in the organisation. If you want to know what is going on with customers, ask the Agents! With average call durations of less than 3 minutes, how do you form a relationship and build loyalty from a customer in that time. That is one of the biggest challenges that the Agents face, especially given many customers do not like the impersonal touch that call centres often provide.

➢ **Technology**

There are significant amounts of technology available and it is very easy to be bamboozled by it all! It very much depends on the size and nature of your business as to what you require. The basic equipment to handle calls is the Automated Call Distributor but these can range from basic to a Rolls Royce! Many centres do not fully utilise the technology that they have.

In addition there is usually a disjoint between what the technology can do and what it is actually used for.

- **Process**

Every centre has a multitude of processes, but the biggest challenge that it faces is to understand the end to end process from the customer perspective. The customer journey is what happens from the point in time when a customer decides to contact you through to the completion of that request or transaction. How long does this journey take and what does it feel like taking the steps along the way. How long is spent waiting? Does the agent have the customer details to hand? Can the agent answer the query first time? Does the fulfilment when expected? One very easy but critical way of looking at the customer journey is to mystery shop the centre and to see what it really feels like to be the customer. Put yourselves in the shoes of your key customer demographic type and call your own centre today.

- **People**

People are the most critical asset in a call centre as it is they who really deliver the business performance. Unfortunately the investment and perception of your staff may be rather poor. The people (Agents) often have to deal with difficult situations when things have gone wrong in your organisation and deal with a large volumes of calls that result, whilst not always having the necessary training or skills. However, the teams in Centres can be very resilient and are often very social, making the centre a great place to work. There are many different roles on offer and so they can a good environment to start and develop a career.

- **Finance and business management**

There will be more management information statistics in a call centre than in any other part of the organisation. The centre is measured from every different angle but unfortunately, this does not always give a complete picture!

One of the most challenging roles is the planning, measuring and reviewing of performance because so many centres are under pressure from calls and other expectations, that being able to step back and take an objective view maybe difficult. Most centres are run to very tight budgets so factors such as turnover of staff will have a huge impact.

2.8 Customer-Premises Equipment:

Customer-premises equipment or customer-provided equipment (CPE) is any terminal and associated equipment located at a subscriber's premises and connected with a carrier's telecommunication channel at the demarcation point . The demarc is a point established in a building or complex to separate customer equipment from the equipment located in either the distribution infrastructure or central office of the communications service provider.

CPE generally refers to devices such as telephones, routers, switches, residential gateways (RG), set-top boxes, fixed mobile convergence products, home networking adapters and Internet access gateways that enable consumers to access communications service providers' services and distribute them around their house via a local area network (LAN).

9. Supply Chain Management:

It is the process of planning, implementing, and controlling the operations of the supply chain with the purpose to satisfy customer requirements as efficiently as possible. Supply chain management spans all movement and storage of raw materials, work-in-process inventory, and finished goods from point-of-origin to point-of-consumption.

Supply chain management must address the following problems:

- Distribution Network Configuration: Number and location of suppliers, production facilities, distribution centers, warehouses and customers.
- Distribution Strategy: Centralized versus decentralized, direct shipment, cross docking, pull or push strategies, third party logistics.
- Information: Integrate systems and processes through the supply chain to share valuable information, including demand signals, forecasts, inventory and transportation.
- Inventory Management: Quantity and location of inventory including raw materials, work-in-process and finished goods.

10. Features Of Supply Chain Management:

In electronic commerce, supply chain management has the following features.

- An ability to source raw material or finished goods from anywhere in the world
- A centralized, global business and management strategy with flawless local execution

- On-line, real-time distributed information processing to the desktop, providing total supply chain information visibility
- The ability to manage information not only within a company but across industries and enterprises
- The seamless integration of all supply chain processes and measurements, including third-party suppliers, information systems, cost accounting standards, and measurement systems
- The development and implementation of accounting models such as activity based costing that link cost to performance are used as tools for cost reduction
- A reconfiguration of the supply chain organization into high-performance teams going from the shop floor to senior management.

2.11 Components Of Supply Chain Management:

The following are five basic components of SCM.

- **Plan:**

  This is the strategic portion of SCM. You need a strategy for managing all the resources that go toward meeting customer demand for your product or service. A big piece of planning is developing a set of metrics to monitor the supply chain so that it is efficient, costs less and delivers high quality and value to customers.

- **Source:**

  Choose the suppliers that will deliver the goods and services you need to create your product. Develop a set of pricing, delivery and payment processes with suppliers and create metrics for monitoring and improving the relationships. And put together processes for managing the inventory of goods and services you receive from suppliers, including receiving shipments, verifying them, transferring them to your manufacturing facilities and authorizing supplier payments.

- **Make:**

  This is the manufacturing step. Schedule the activities necessary for production, testing, packaging and preparation for delivery. As the most metric-intensive portion of the supply chain, measure quality levels, production output and worker productivity.

- **Deliver:**

  This is the part that many insiders refer to as logistics. Coordinate the receipt of orders from customers, develop a network of warehouses, pick carriers to get products to customers and set up an invoicing system to receive payments.

- **Return:**

  The problem part of the supply chain. Create a network for receiving defective and excess products back from customers and supporting customers who have problems with delivered products.

2.12 Measuring A Supply Chain's Performance:

The performance of a supply chain is evaluated by how it reduces cost or increases value. SCM performance monitoring is important; in many industries, the supply chain represents roughly 75 percent of the operating budget expense. Three common measures of performance are used when evaluating SCM performance:

- Efficiency focuses on minimizing cost by decreasing the inventory investment or value relative to the cost of goods sold. An efficient firm is therefore one with a higher inventory turnover or fewer weeks' worth of inventory on hand.
- Responsiveness focuses on reduction in both inventory costs and missed sales that comes with a faster, more flexible supply chain. A responsive firm is proficient in an uncertain market environment, because it can quickly adjust production to meet demand.
- Effectiveness of the supply chain relates to the degree to which the supply chain creates value for the customer. Effectiveness-focused supply chains are called ―value chains‖ because they focus more on creating customer value than reducing costs and improving productivity.

To examine the effect of the Internet and electronic commerce on the supply chain is to examine the impact the Internet has on the efficiency, responsiveness, effectiveness, and overall performance of the supply chain.

2.13 Advantages of Internet/E-Commerce Integrated Supply Chain:

The primary advantages of Internet utilization in supply chain management are speed, decreased cost, flexibility, and the potential to shorten the supply chain.

- **Speed:**

  A competitive advantage accrues to those firms that can quickly respond to changing market conditions. Because the Internet allows near instantaneous transfer of information between various links in the supply chain, it is ideally suited to help firms keep pace with their environments. Many businesses have placed a priority upon real-time information regarding the status of orders and production from other members of the supply chain.

- **Cost decrease:**

  Internet-based electronic procurement helps reduce costs by decreasing the use of paper and labor, reducing errors, providing better tracking of purchase orders and goods delivery, streamlining ordering processes, and cutting acquisition cycle times.

- **Flexibility:**

  The Internet allows for custom interfaces between a company and its different clients, helping to cost-effectively establish mass customization. A manufacturer can easily create a custom template or Web site for a fellow supply chain member with pre-negotiated prices for various products listed on the site, making re-ordering only a mouse click away. The information regarding this transaction can be sent via the Internet to the selling firm‘s production floor and the purchasing firm‘s purchasing and accounting departments. The accuracy and reliability of the information is greater than the traditional paper and pencil transaction, personnel time and expense is reduced, and the real-time dissemination of the relevant information to interested parties improves responsiveness. These advantages can benefit both firms involved in the transaction.

- **Shortening the supply chain:**

  Dell computers has become a classic example of the power the Internet can have on a supply chain. Dell helped create one of the first fully Internet-enabled supply chains and revolutionized the personal-computer industry by selling directly to businesses and consumers, rather than through retailers and middlemen. In mid-1996, Dell began allowing consumers to configure and order computers online. By 1998, the company recorded

roughly $1 billion in ―pure‖ Internet orders. By reducing sales costs and attracting customers who spend more per transaction, Dell estimates that it yields 30 percent greater profit margins on Internet sales compared to telephone sales.

2.14 Disadvantages of Internet/E-Commerce Integrated Supply Chain:

- **Increased interdependence:**

  Increased commoditization, increased competition, and shrinking profit margins are forcing companies to increase outsourcing and subcontracting to minimize cost. By focusing on its core competencies, a firm should be able to maximize its economies of scale and its competitiveness. However, such a strategy requires increased reliance and information sharing between members of the supply chain. Increased dependency on various members of the supply chain can have disastrous consequences if these supply chain members are unable to handle the functions assigned to them.

- **The costs of implementation:**

  Implementation of a fully-integrated Internet-based supply chain is expensive. This expense includes hardware cost, software cost, reorganization cost, and training costs. While the Internet promises many advantages once it is fully integrated into a supply chain, a significant up front investment is needed for full deployment.

- **Keeping up with the change in expectations:**

  Expectations have increased as Internet use has become part of daily life. When customers send orders electronically, they expect to get a quick confirmation and delivery or denial if the order can not be met. Increasingly, in this and other ways, customers are dictating terms and conditions to suppliers. The introduction of Internet-based supply chains make possible the change to a ―pull‖ manufacturing strategy replacing the traditional ―push‖ strategy that has been the standard in most industries.

UNIT-4

1. E-Payment System:

Electronic payment systems are central to on-line business process as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities.

Electronic payment systems and e-commerce are highly linked given that on-line consumers must pay for products and services. Clearly, payment is an integral part of the mercantile process and prompt payment is crucial. If the claims and debits of the various participants (consumers, companies and banks) are not balanced because of payment delay, then the entire business chain is disrupted. Hence an important aspect of e-commerce is prompt and secure payment, clearing, and settlement of credit or debit claims.

Electronic payment systems are becoming central to on-line business transactions nowadays as companies look for various methods to serve customers faster and more cost effectively. Electronic commerce brings a wide range of new worldwide business opportunities. There is no doubt that electronic payment systems are becoming more and more common and will play an important role in the business world. Electronic payment always involves a payer and a payee who exchange money for goods or services. At least one financial institution like a bank will act as the issuer (used by the payer) and the acquirer (used by the payee).

2. Types of Electronic Payment Systems:

Electronic payment systems are proliferating in banking, retail, health care, on-line markets, and even government—in fact, anywhere money needs to change hands.

- Organizations are motivated by the need to deliver products and services more cost effectively and to provide a higher quality of service to customers.
- The emerging electronic payment technology labeled electronic funds transfer (EFT).

- EFT is defined as ―any transfer of funds initiated through an electronic terminal telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution.

EFT can be segmented into three broad categories:

- **Banking and financial payments**
  - Large-scale or wholesale payments (e.g., bank-to-bank transfer)
  - Small-scale or retail payments (e.g., automated teller machines
  - Home banking (e.g., bill payment)
- **Retailing payments**
  - Credit Cards (e.g., VISA or MasterCard)
  - Private label credit/debit cards (e.g., J.C. Penney Card)
  - Charge Cards (e.g., American Express)
- **On-line electronic commerce payments**
  - **Token-based payment systems**
    - Electronic cash (e.g., DigiCash)
    - Electronic checks (e.g., NetCheque)
    - Smart cards or debit cards (e.g., Mondex Electronic Currency Card)
  - **Credit card-based payments systems**
    - Encrypted Credit Cards (e.g., World Wide Web form-based encryption)
    - Third-party authorization numbers (e.g., First Virtual)

3. E-Cash:

- There are many ways that exist for implementing an e-cash system, all must incorporate a few common features.
- Electronic Cash is based on cryptographic systems called ―digital signatures‖.
- This method involves a pair of numeric keys: one for locking (encoding) and the other for unlocking (decoding).

E-cash must have the following four properties.

- Monetary value
- Interoperability
- Retrievability
- Security

• Electronic cash is a general term that describes the attempts of several companies to create value storage and exchange system that operates online in much the same way that government-issued currency operates in the physical world.

• Concerns about electronic payment methods include:

– Privacy

– Security

– Independence

– Portability

Electronic Cash Storage:

• Two methods

– **On-line**

• Individual does not have possession personally of electronic cash

• Trusted third party, e.g. e-banking, bank holds customers‘ cash accounts

– **Off-line**

• Customer holds cash on smart card or electronic wallet

• Fraud and double spending require tamper-proof encryption

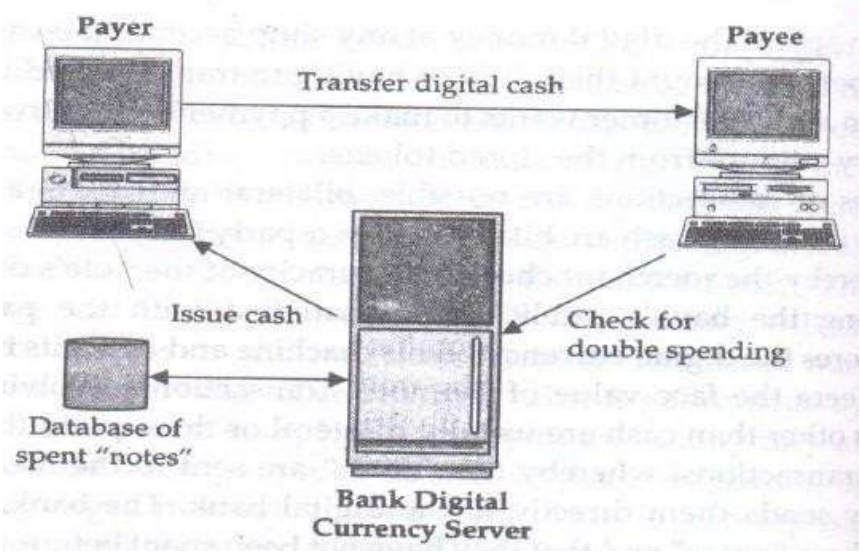
The purchase of e-cash from an on-line currency server (or bank) involves two steps:

- Establishment of an account
- Maintaining enough money in the account to bank the purchase.

- Once the tokens are purchased, the e-cash software on the customer‘s PC stores digital money undersigned by a bank.
- The users can spend the digital money at any shop accepting e-cash, without having to

open an account there or having to transmit credit card numbers.

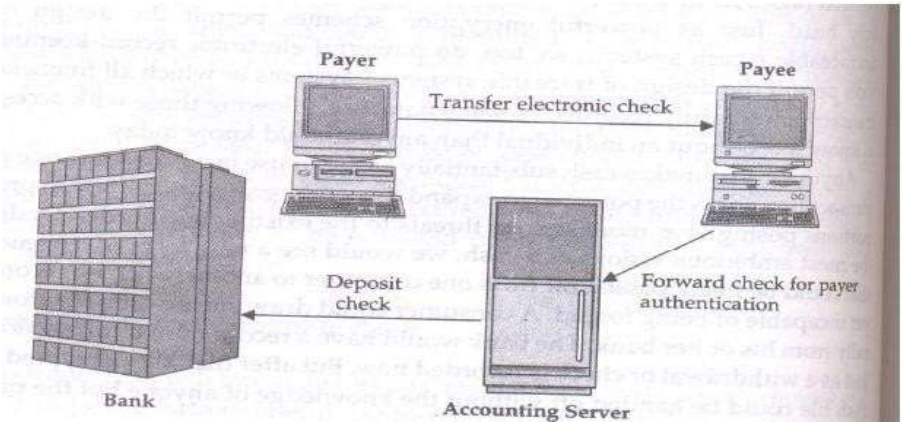
- As soon as the customer wants to make a payment, the software collects the necessary amount from the stored tokens



– Convenience

3.4 Electronic Checks:

- It is another form of electronic tokens.
- Buyers must register with third-party account server before they are able to write electronic checks.
- The account server acts as a billing service.



Advantages of Electronic Checks:

1. They work in the same way as traditional checks.
2. These are suited for clearing micropayments.
3. They create float & availability of float is an important for commerce.
4. Financial risk is assumed by the accounting server & may result in easier acceptance.

Smart Cards & Electronic Payment Systems:

- Smart cards have been in existence since the early 1980s and hold promise for secure transactions using existing infrastructure.
- Smart cards are credit and debit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic stripe.
- The smart card technology is widely used in countries such as France, Germany, Japan, and Singapore to pay for public phone calls, transportation, and shopper loyalty programs.

Types of Smart Cards:

- Relationship-Based Smart Credit Cards
- Electronic Purses also known as debit cards

- **Relationship-Based Smart Credit Cards:**
  - It is an enhancement of existing cards services &/ or the addition of new services that a financial institution delivers to its customers via a chip-based card or other device.
  - These services include access to multiple financial accounts, value-added marketing programs, or other information card holders may want to store on their card.
  - It includes access to multiple accounts, such as debit, credit, cash access, bill payment & multiple access options at multiple locations.
- **Electronic Purses:**

  To replace cash and place a financial instrument are racing to introduce electronic purses, wallet-sized smart cards embedded with programmable microchips that store sums of money for people to use instead of cash for everything.

The electronic purse works in the following manner:

- After purse is loaded with money at an ATM, it can be used to pay for candy in a vending machine with a card reader.
- It verifies card is authentic & it has enough money, the value is deducted from balance on the card & added to an e-cash & remaining balance is displayed by the vending machine.

Credit Card-Based Electronic Payment Systems:

Payment cards are all types of plastic cards that consumers use to make purchases:

– Credit cards

• Such as a Visa or a MasterCard, has a preset spending limit based on the user‘s credit limit.

– Debit cards

• Removes the amount of the charge from the cardholder‘s account and transfers it to the seller‘s bank.

– Charge cards

• Such as one from American Express, carries no preset spending limit.

Advantages:

– Payment cards provide fraud protection.

– They have worldwide acceptance.

– They are good for online transactions.

Disadvantages:

Payment card service companies charge merchants per-transaction fees and monthly processing fees.

5. Risks in Electronic Payment systems:

- Customer's risks
  - – Stolen credentials or password
  - – Dishonest merchant
  - – Disputes over transaction
  - – Inappropriate use of transaction details
- Merchant‘s risk
  - – Forged or copied instruments

– Disputed charges

– Insufficient funds in customer‘s account

– Unauthorized redistribution of purchased items

Electronic payments Issues:

- Secure transfer across internet
- High reliability: no single failure point
- Atomic transactions
- Anonymity of buyer
- Economic and computational efficiency: allow micropayments
- Flexibility: across different methods
- Scalability in number of servers and users

Security Requirements In Electronic Payment Systems:

- **Integrity and authorization**

  A payment system with integrity allows no money to be taken from a user without explicit authorization by that user. It may also disallow the receipt of payment without explicit consent, to prevent occurrences of things like unsolicited bribery. Authorization constitutes the most important relationship in a payment system. Payment can be authorized in three ways: via out-band authorization, passwords, and signature.

- **Out-band authorization**

  In this approach, the verifying party (typically a bank) notifies the authorizing party (the payer) of a transaction. The authorizing party is required to approve or deny the payment using a secure, out-band channel (such as via surface mail or the phone). This is the current approach for credit cards involving mail orders and telephone orders: Anyone who knows a user‘s credit card data can initiate transactions, and the legitimate user must check the statement and actively complain about unauthorized transactions. If the user does not complain within a certain time (usually 90 days), the transaction is considered ―approved‖ by default.

- **Password authorization**

  A transaction protected by a password requires that every message from the authorizing party include a cryptographic check value. The check value is computed using a secret

known only to the authorizing and verifying parties. This secret can be a personal identification number, a password, or any form of shared secret. In addition, shared secrets that are short - like a six-digit PIN - are inherently susceptible to various kinds of attacks. They cannot by themselves provide a high degree of security. They should only be used to control access to a physical token like a smart card (or a wallet) that performs the actual authorization using secure cryptographic mechanisms, such as digital signatures.

- **Signature authorization**

  In this type of transaction, the verifying party requires a digital signature of the authorizing party. Digital signatures provide non repudiation of origin.

- **Confidentiality**

  Some parties involved may wish confidentiality of transactions. Confidentiality in this context means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, and so on. Typically, the confidentiality requirement dictates that this information be restricted only to the participants involved. Where anonymity or un-traceability are desired, the requirement may be to limit this knowledge to certain subsets of the participants only, as described later.

- **Availability and reliability**

  All parties require the ability to make or receive payments whenever necessary. Payment transactions must be atomic: They occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any case) due to a network or system crash. Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable. Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronization protocols. These fault tolerance issues are not discussed here, because most payment systems do not address them explicitly.

E-Marketing:

- E-marketing is directly marketing a commercial message to a group of people using email. In its broadest sense, every email sent to a potential or current customer could be considered email marketing.
- It usually involves using email to send ads, request business, or solicit sales or donations,

and is meant to build loyalty, trust, or brand awareness.

- Email marketing can be done to either sold lists or a current customer database. Broadly, the term is usually used to refer to sending email messages with the purpose of enhancing the relationship of a merchant with its current or previous customers, to encourage customer loyalty and repeat business, acquiring new customers or convincing current customers to purchase something immediately, and adding advertisements to email messages sent by other companies to their customers.

Advantages:

- An exact return on investment can be tracked and has proven to be high when done properly. Email marketing is often reported as second only to search marketing as the most effective online marketing tactic.
- Email marketing is significantly cheaper and faster than traditional mail, mainly because of high cost and time required in a traditional mail campaign for producing the artwork, printing, addressing and mailing.
- Advertisers can reach substantial numbers of email subscribers who have opted in (i.e., consented) to receive email communications on subjects of interest to them.
- Almost half of American Internet users check or send email on a typical day with email blasts that are delivered between 1 am and 5 am local time outperforming those sent at other times in open and click rates.
- Email is popular with digital marketers, rising an estimated 15% in 2009 to £292 m in the UK.
- If compared to standard email, direct email marketing produces higher response rate and higher average order value for e-commerce businesses.

Disadvantages:

- A report issued by the email services company Return Path, as of mid-2008 email deliverability is still an issue for legitimate marketers. According to the report, legitimate email servers averaged a delivery rate of 56%; twenty percent of the messages were rejected, and eight percent were filtered.
- Companies considering the use of an email marketing program must make sure that their program does not violate spam laws such as the United States' Controlling the Assault of

Non-Solicited Pornography and Marketing Act (CAN-SPAM),the European Privacy and Electronic Communications Regulations 2003, or their Internet service provider's acceptable use policy.

Tele Marketing:

- Telemarketing is a method of direct marketing in which a salesperson solicits prospective customers to buy products or services, either over the phone or through a subsequent face to face or Web conferencing appointment scheduled during the call.
- Telemarketing can also include recorded sales pitches programmed to be played over the phone via automatic dialing.
- Telemarketing may be done from a company office, from a call center, or from home. It may involve a live operator voice broadcasting which is most frequently associated with political messages.
- An effective telemarketing process often involves two or more calls. The first call (or series of calls) determines the customer‘s needs. The final call (or series of calls) motivates the customer to make a purchase. Prospective customers are identified by various means, including past purchase history, previous requests for information, credit limit, competition entry forms, and application forms. Names may also be purchased from another company's consumer database or obtained from a telephone directory or another public list. The qualification process is intended to determine which customers are most likely to purchase the product or service.
- Charitable organizations, alumni associations, and political parties often use telemarketing to solicit donations. Marketing research companies use telemarketing techniques to survey the prospective or past customers of a client‘s business in order to assess market acceptance of or satisfaction with a particular product, service, brand, or company. Public opinion polls are conducted in a similar manner.
- Telemarketing techniques are also applied to other forms of electronic marketing using e-mail or fax messages, in which case they are frequently considered spam by receivers.

Disadvantages:

- Telemarketing has been negatively associated with various scams and frauds, such as pyramid schemes, and with deceptively overpriced products and services
- Telemarketing is often criticized as an unethical business practice due to the perception of high-pressure sales techniques during unsolicited calls.
- Telemarketers marketing telephone companies may participate in telephone slamming, the practice of switching a customer's telephone service without their knowledge or authorization.
- Telemarketing calls are often considered an annoyance, especially when they occur during the dinner hour, early in the morning, or late in the evening.

UNIT-5

Electronic Data Interchange(EDI):

- Electronic Data Interchange (EDI) - interposes communication of business information in standardized electronic form.
- Prior to EDI, business depended on postal and phone systems that restricted communication to those few hours of the workday that overlap between time zones.

Why EDI?

• Reduction in transaction costs

• Foster closer relationships between trading partners

EDI & Electronic Commerce

• Electronic commerce includes EDI & much more

• EDI forges boundary less relationships by improving interchange of information between trading partners, suppliers, & customers.

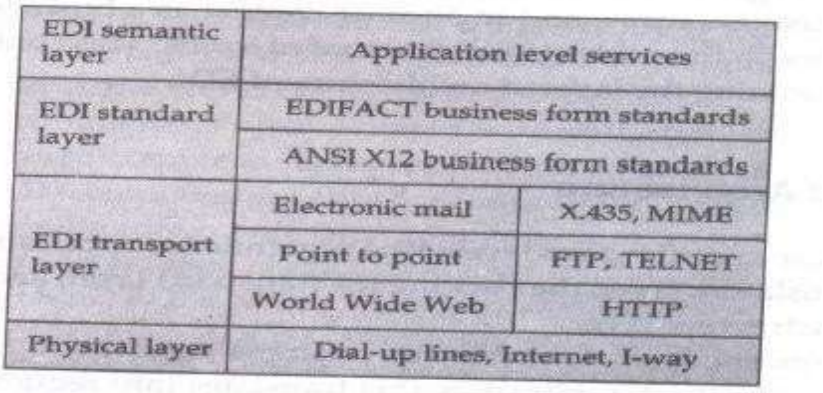
6. EDI layered architecture:

• Semantic (or application) layer

• Standards translation layer

• Packing (or transport) layer

• Physical network infrastructure layer



EDI semantic layer	Application level services	
EDI standard layer	EDIFACT business form standards	
	ANSI X12 business form standards	
EDI transport layer	Electronic mail	X.435, MIME
	Point to point	FTP, TELNET
	World Wide Web	HTTP
Physical layer	Dial-up lines, Internet, I-way	

EDI semantic layer:

• Describes the business application

- Procurement example

  – Requests for quotes

  - Price quotes
  - Purchase orders
  - Acknowledgments
  - Invoices
- Specific to company & software used

Standards translation:

• Specifies business form structure so that information can be exchanged

• Two competing standards

– American National Standards Institute(ANSI)X12

– EDIFACT developed by UN/ECE, Working Party for the Facilitation of International Trade Procedures

EDI transport layer

• How the business form is sent, e.g. post, UPS, fax

• Increasingly, e-mail is the carrier

• Differentiating EDI from e-mail

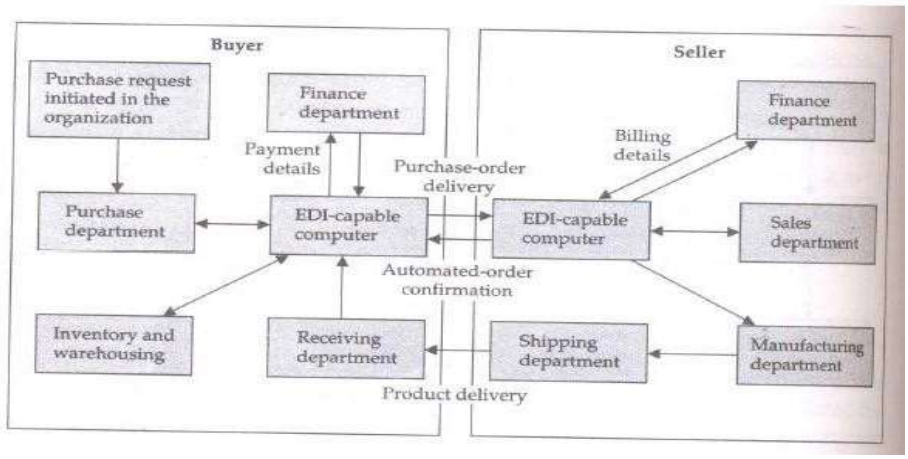
– Emphasis on automation

– EDI has certain legal status

Physical network infrastructure layer

• Dial-up lines, Internet, value-added network, etc.

Information flow with EDI:



1. Buyer sends purchase order to seller computer
2. Seller sends purchase order confirmation to buyer
3. Seller sends booking request to transport company
4. Transport company sends booking confirmation to seller
5. Seller sends advance ship notice to buyer
6. Transport company sends status to seller
7. Buyer sends Receipt advice to seller

8. Seller sends invoice to buyer
9. Buyer sends payment to seller

3.7 Applications of EDI:

1. Role of EDI in international trade:

- Reduced transaction expenditures
- Quicker movement of imported & exported goods
- Improved customer service through ―track & trace‖ programs
- Faster customs clearance & reduced opportunities for corruption, a huge problem in trade

2. Interbank Electronic Funds Transfer (EFT)

• EFTS is credit transfers between banks where funds flow directly from the payer‘s bank to the payee‘s bank.

• The two biggest funds transfer services in the United States are the Federal Reserve‘s system, Fed wire, & the Clearing House Interbank Payments System (CHIPS) of the New York clearing house

3. Health care EDI for insurance EDI

• Providing good & affordable health care is a universal problem

• EDI is becoming a permanent fixture in both insurance & health care industries as medical provider, patients, & payers

• Electronic claim processing is quick & reduces the administrative costs of health care.

• Using EDI software, service providers prepare the forms & submit claims via communication lines to the value-added network service provider

• The company then edits sorts & distributes forms to the payer. If necessary, the insurance company can electronically route transactions to a third-party for price evaluation

• Claims submission also receives reports regarding claim status & request for additional Information

3. Manufacturing & retail procurement using EDI

• These are heavy users of EDI

• In manufacturing, EDI is used to support just-in-time.

• In retailing, EDI is used to support quick response

8. EDI Protocols:

- ANSI X12
- EDIFACT

Comparison of EDIFACT & X.12 Standards:

- These are comprised of strings of data elements called segments.
- A transaction set is a set of segments ordered as specified by the standard.
- ANSI standards require each element to have a very specific name, such as order date or invoice date.
- EDIFACT segments, allow for multiuse elements, such as date.
- EDIFACT has fewer data elements & segments & only one beginning segment (header),but it has more composites.
- It is an ever-evolving platform.

Security Threats to E-commerce:

E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the commerce chain, the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.

Client threats

Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the widespread use of active content has changed this perception.

Active content: Active content refers to programs that are embedded transparently in web pages

and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. Active content is used in e-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VBScript.

Malicious codes: Computer viruses, worms and trojan horses are examples of malicious code. A trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A

worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.

Server-side masquerading*:* Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack.

Communication channel threats

The internet serves as the electronic chain linking a consumer (client) to an e-commerce resource. Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

Confidentiality threats: Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs onto a website – say www.anybiz.com – that contains a form with text boxes for name, address, and e-mail address. When one fills out those text boxes and clicks the submit button, the information is sent to the web-server for processing. One popular method of transmitting data to a web-server is to collect the text box responses and place them at the end of the target server‘s URL. The captured data and the HTTP request to send the data to the server is then sent. Now, suppose the user changes his mind, decides not to wait for a response from the anybiz.com server, and jumps to another website instead – say www.somecompany.com. The server somecompany.com may choose to collect web demographics and log the URL from which the user just came (www.anybiz.com). By doing this, somecompany.com has breached confidentiality by recording the secret information the user has just entered.

Integrity threats: An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing – pretending to be someone you are not or representing a website as an original when it really is a fake – is one means of creating havoc on websites. Using a security hole in a domain name server (DNS), perpetrators can

substitute the address of their website in place of the real one to spoof website visitors. Integrity threats can alter vital financial, medical, or military information. It can have very serious consequences for businesses and people.

Availability threats: The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely. For example, if the processing speed of a single ATM machine transaction slows from one or two seconds to 30 seconds, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitors‘ web or commerce sites.

Server threats

The server is the third link in the client-internet-server trio embodying the e-commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

Web-server threats: Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes – security weaknesses that provide openings through which evildoers can enter.

Commerce server threats: The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite, including an FTP server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.

Database threats: E-commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were disclosed or altered. Some databases store username/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.

Common gateway interface threats: A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs

are programs, they present a security threat if misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

Password hacking: The simplest attack against a password-based system is to guess passwords. Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

3.9 Security Requirements For E-Commerce:

Authentication:

This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it purports to.Without face-to-face contact, passing oneself off as someone else is not difficult on the internet.

In online commerce the best defence against being misled by an imposter is provided by unforgeable digital certificates from a trusted authority (such as VeriSign). Although anyone can generate digital certificates for themselves, a trusted authority demands real-world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and email client software.

Authentication can be provided in some situations by physical tokens (such as a drivers license), by a piece of information known only to the person involved (eg. a PIN), or by a physical property of a person (fingerprints or retina scans). Strong authentication requires at least two or more of these. A digital certificate provides strong authentication as it is a unique token and requires a password for its usage.

Privacy:

In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved via encryption. Sensitive data (such as credit card details, health records, sales figures etc.) are encrypted before being transmitted across the open internet – via email or the web. Data which has been protected with strong 128-bit encryption may be intercepted by hackers, but cannot be decrypted by them within a short

time. Again, digital certificates are used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

Authorization:

Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical world, authentication is usually achieved by forms requiring signatures, or locks where only authorized individuals hold the keys.

Authorization is tied with *authentication*. If a system can securely verify that a request for information (such as a web page) or a service (such as a purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed.

In the online world, authorization can be achieved by a manager sending a digitally signed email. Such an email, once checked and verified by the recipient, is a legally binding request for a service. Similarly, if a web-server has a restricted access area, the server can request a digital certificate from the user‘s browser to identify the user and then determine if they should be given access to the information according to the server‘s permission rules.

Integrity:

Integrity of information means ensuring that a communication received has not been altered or tampered with. Traditionally, this problem has been dealt with by having tight control over access to paper documents and requiring authorized officers to initial all changes made – a system with obvious drawbacks and limitations. If someone is receiving sensitive information online, he not only wants to ensure that it is coming from who he expects it to (authentication), but also that it hasn‘t been intercepted by a hacker while in transit and its contents altered. The speed and distances involved in online communications requires a very different approach to this problem from traditional methods.

One solution is afforded by using digital certificates to digitally ―sign‖ messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief

numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and compare it against the one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

Non-repudiation:

Non-repudiation is the ability to guarantee that once someone has requested a service or approved an action. Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Traditionally non-repudiation has been achieved by having parties sign contracts and then have the contracts notarized by trusted third parties. Sending documents involved the use of registered mail, and postmarks and signatures to date-stamp and record the process of transmission and acceptance. In the realm of e-commerce, non repudiation is achieved by using digital signatures. Digital signatures which have been issued by a trusted authority (such as VeriSign) cannot be forged and their validity can be checked with any major email or web browser software. A digital signature is only installed in the personal computer of its owner, who is usually required to provide a password to make use of the digital signature to encrypt or digitally sign their communications. If a company receives a purchase order via email which has been digitally signed, it has the same legal assurances as on receipt of a physical signed contract.

Security policy for E-commerce:

The security policy may cover issues like:

- What service types (e.g., web, FTP, SMTP) users may have access to?
- What classes of information exist within the organization and which should be encrypted before being transmitted?
- What client data does the organization hold. How sensitive is it? How is it to be protected?
- What class of employees may have remote access to the corporate network?
- Roles and responsibilities of managers and employees in implementing the security policy.
- How security breaches are to be responded to?

The security policy should also consider physical aspects of network security. For example,

- Who has access to the corporate server?
- Is it in a locked environment or kept in an open office?
- What is the procedure for determining who should be given access? The security policy regulates the activities of employees just as much as it defines how IT infrastructure will be configured. The policy should include details on how it is to be enforced
- How individual responsibilities are determined?

For it to be effective, the policy needs regular testing and review to judge the security measures. The review process needs to take into account any changes in technology or business practices which may have an influence upon security. Lastly, the policy itself needs to be regarded as a living document which will be updated at set intervals to reflect the evolving ways in which the business, customers and technology interact.

Security Standards:

There are various standards pertaining to the security aspects of enterprises. Some of them are

- ISO 17799 (Information technology – Code of practice for information security management).
- (ISO/IEC 2000).
- SSE-CMM (Systems security engineering – Capability maturity model).
- (SSE-CMM 2003).
- COBIT (Control objectives for information and related technology).
- (COBIT 2000).

ISO 17799 provides detailed guidelines on how a management framework for enterprise security should be implemented. It conceives ten security domains. Under each domain there are certain security objectives to be fulfilled. Each objective can be attained by a number of controls. The controls may prescribe management measures like guidelines and procedures, or some security infrastructure in the form of tools and techniques. It details various methods that can be followed by enterprises to meet security needs for e-commerce. It talks about the need for security policies, security infrastructure, and continuous testing in

the same manner as has been detailed above.

The main objective of the COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organizations. The SSE-CMM is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are in the Information Technology Security domain.

Firewall:

A firewall is a network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. Firewalls exist both as software to run on general purpose hardware and as a hardware appliance. Many hardware-based firewalls also offer other functionality to the internal network they protect, such as acting as a DHCP server for that network.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

Types of Firewall:

There are different types of firewalls depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

- Network layer Firewall
- Application layer firewall
- Proxy server
- Network address translation

- **Network layer Firewall:**

  Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply.

Network layer firewalls generally fall into two sub-categories,

- Stateful Firewalls
- Stateless Firewalls

Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the rule set for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

- **Application Layer Firewall:**

  Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

  On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

  Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket

filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.

Also, application firewalls further filter connections by examining the process ID of data packets against a ruleset for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided ruleset. Given the variety of software that exists, application firewalls only have more complex rulesets for the standard services, such as sharing services. These per process rulesets have limited efficacy in filtering every possible association that may occur with other processes.

- **Proxy server:**

A proxy server running either on dedicated hardware or as software on a general-purpose machine may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall. Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

- **Network Address Translation:**

  Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918.

  Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

Digital Signatures:

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, Brazil, and members of the European Union, electronic signatures have legal significance.

A digital signature scheme typically consists of three algorithms;

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.

- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Applications of digital signatures:

Authentication:

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity:

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation:

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Some digital signature algorithms:

- RSA-based signature schemes, such as RSA-PSS
- DSA and its elliptic curve variant ECDSA
- ElGamal signature scheme as the predecessor to DSA, and variants Schnorr signature and Pointcheval–Stern signature algorithm
- Rabin signature algorithm
- Pairing-based schemes such as BLS
- Undeniable signatures
- Aggregate signature - a signature scheme that supports aggregation: Given n signatures on n messages from n users, it is possible to aggregate all these signatures into a single signature whose size is constant in the number of users. This single signature will convince the verifier that the n users did indeed sign the n original messages.
- Signatures with efficient protocols - are signature schemes that facilitate efficient cryptographic protocols such as zero-knowledge proofs or secure computation.

Digital Certificate:

- It is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

- The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.
- The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the

sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

- The most widely used standard for digital certificates is X.509.

Contents Of a Typical Digital Certificate:

- Serial Number: Used to uniquely identify the certificate.
- Subject: The person, or entity identified.
- Signature Algorithm: The algorithm used to create the signature.
- Signature: The actual signature to verify that it came from the issuer.
- Issuer: The entity that verified the information and issued the certificate.
- Valid-From: The date the certificate is first valid from.
- Valid-To: The expiration date.
- Key-Usage: Purpose of the public key (e.g. encipherment, signature, certificate signing...).
- Public Key: The public key.
- Thumbprint Algorithm: The algorithm used to hash the public key certificate.
- Thumbprint (also known as fingerprint): The hash itself, used as an abbreviated form of the public key certificate