Table of Contents

Lesson 19

MAINTAINING STATE IN A STATELESS SYSTEM

You know that http is stateless. Another reason why we need to write scripts or develop our back end is that we want to maintain state. In other words, we want to link different clicks/steps involved in an e-commerce transaction. When we go to an ecommerce site, we are generally asked to take three different steps, that is, provide Registration information, and make selection of items (Add to Cart) and Confirm Order. The question is how do we create link or maintain state among these different steps. There are following options available for programmers in this regard:

A temporary file may be created on the server side and we code our scripts behind the steps/clicks - Register, Add to Cart and Confirm Order - in a way that the information of each step/click is stored in that temporary file using the same common ID. At the end our confirm order script puts this information in some database using insert query.

Another method is to use the client side or cookies for maintaining state. Information regarding Registration and Add to Cart can be stored in cookies and at Confirm Order cookies against these URLs would revert to the serve side and be stored in databases against a common ID.

We can also use hidden forms' fields. We keep data back and forth within forms to maintain state. Following is a piece of HTML code for a form (Add to cart) in which hidden fields are used. I have used pairs of input tags with type hidden and type checkboxes. (I can also use them in a For loop using Recordset object of ASP then it would be possible that these pairs of input tags are generated in a loop and information of records available in databases is directly picked up and printed for me). Because of type hidden the item name and item code/value for each item would be there in the form against each item but would remain hidden. When the user selects items (through check boxes) and presses Add to Cart his selected information would go to some script which would be coded such that it would open a new page with button Confirm Order. In this new form the item code or value of selected items would be present but would remain hidden. When a user presses the button Confirm Order the information of selected items is stored in the databases (through a script) against the item code present in the form, though hidden. We can say that state is maintained here between steps Add to Cart and Confirm Order in the sense that selections made in step Add to Cart were passed over or provided to the next step Confirm Order.

Example - Hidden Fields

```
<FORM NAME="Form1"> <INPUT TYPE= "HIDDEN" NAME= "Shirt1" VALUE="25"> <INPUT
TYPE= "CHECKBOX" NAME= "Check1">Blue Cotton Shirt <br> <INPUT TYPE= "HIDDEN"
NAME= "Shirt2" VALUE="26"> <INPUT TYPE= "CHECKBOX" NAME= "Check2" >Green Cotton
Shirt <br>
<INPUT TYPE= "HIDDEN" NAME= "Shirt3" VALUE="27"> <INPUT TYPE= "CHECKBOX"
NAME= "Check3">White Silk Shirt ….
<P>
<INPUT TYPE="submit" NAME="Go" VALUE="Register!"> <INPUT TYPE="RESET"
VALUE="Reset!"></FORM>
```

Another option is to keep everything in databases. Here, information of each step is recorded in appropriate tables of a database itself and linked up with the help of a commonID. It is relatively more costly and time consuming option.
We can use Servlets to write our scripts to speed up processing. It gets tricky, as one must have a solid knowledge of programming to implement these methods. Here, the idea is just to give you a broad concept/picture as to how the state is maintained.

Client server architecture

Note that we may have different tiers in client server architecture depending on where the processing of data takes place. In 1-tier architecture, the entire processing takes place at a single place/zone. For example,

in Fig. 1 below, the processing of data only takes place in the main frame and different machines are attached to it just as display terminals. Conversely, the entire processing may take place at individual terminals and a centralized machine called file server just stores the files having no role in the processing of data. Again, that would be an example of 1-tier architecture (Fig. 2). Example of 2-tier architecture is where processing of HTML code takes place on the client side and the web page request is processed on the server side (Fig. 3). In a 3-tier architecture, we can place our database management system or application software on a different processing zone or tier than the web server (Fig. 4). Similarly in a 4-tier architecture ,for example, we can place the payment processing system at the 4th tier. Thus, we can divide the client server architecture into n – tiers.

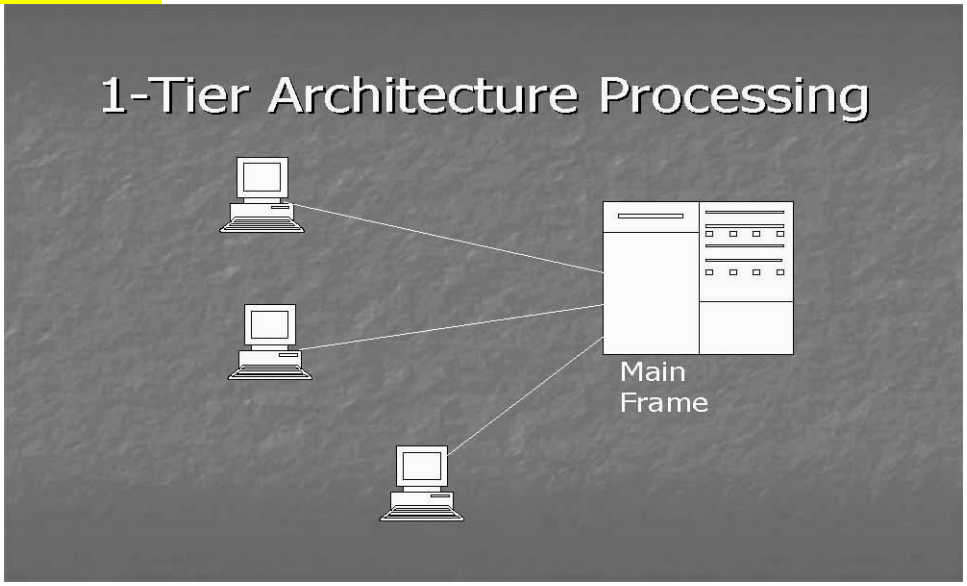

Fig. 1

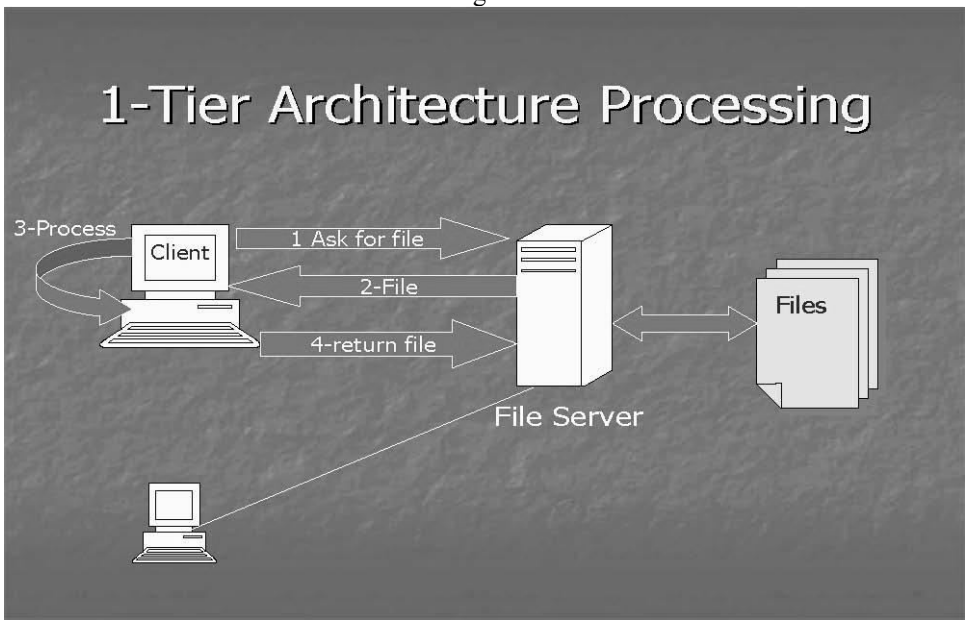

Fig. 2

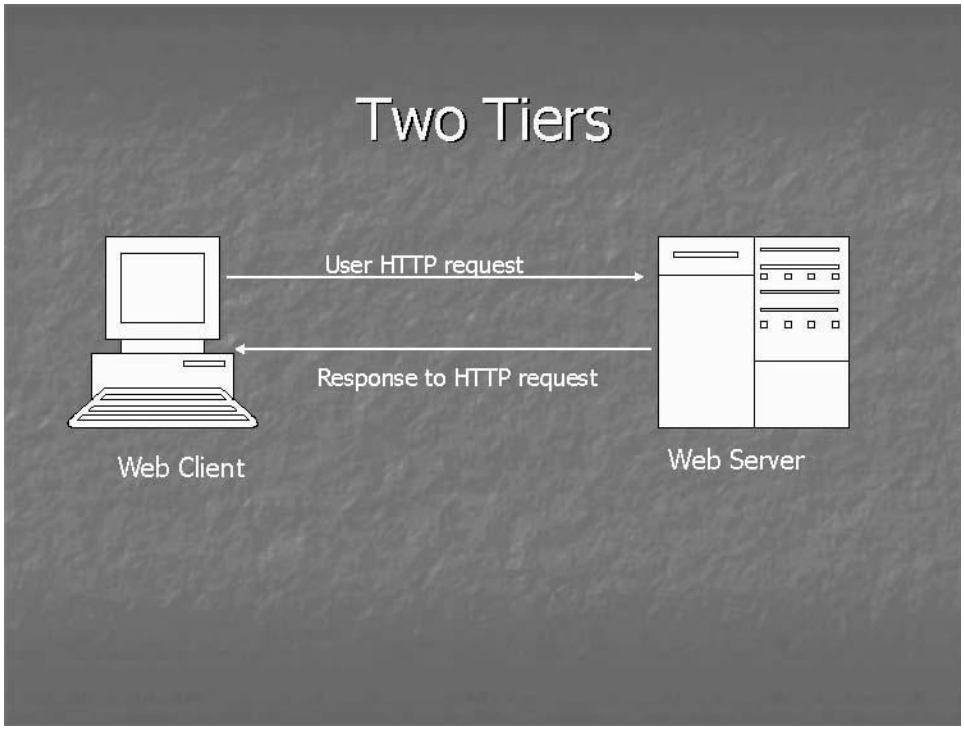

Fig. 3

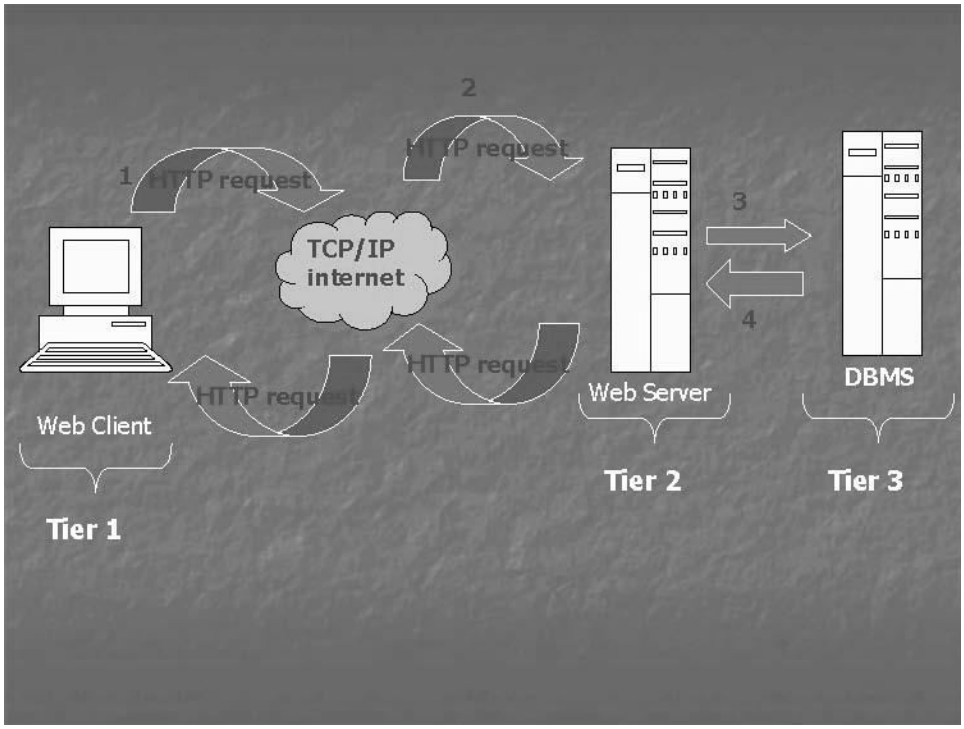

Fig. 4

Web server

You know that web server is a machine that serves up the web page requests of a client on the internet. It is a combination of hardware and software. Decision as regards the type of a web server is largely dependent on the volume and type of web activities. So, transaction processing sites generating dynamic pages with high traffic volumes would need web server software that is more efficient and can easily be upgraded.

Operating systems for web servers

A web server is a machine that serves client requests on the internet, combining hardware and software. The choice of server depends on the volume and type of web activities. Common operating systems include Microsoft Windows NT Server, Windows 2000 Advanced Server, Microsoft.NET Server, Linux, and Unix-based systems like Solaris.

Open source software, such as Apache HTTP server, MS Internet Information Server (IIS), and Sun ONE web server, is popular and secure. Web server

A computer must have an operating system to provide services to devices connected to a computer such as printers. Server operating systems are Microsoft Windows NT Server, Microsoft.NET Server, Linux or Unix based operating systems such as Solaris. Unix-based web servers are more popular and are considered to be more secure. Open source software, which is fast, efficient and easy to install. Open source software is developed by a community of programmers who make it available for download at no cost. Web Server Software Common examples of web server software are Apache HTTP server, MS Internet Information Server (IIS) and Sun ONE web server. Apache is open source code developed in 1994. Today, it dominates the web, because it is free and performs very efficiently. IIS comes with MS windows 2000 and NT operating systems. IIS's inclusion of ASP provides an environment in which HTML pages and scripts can be combined to produce dynamic web pages. Sun one (iPlanet or Netscape) web server is a joint product of AOL and Sun Microsystems. It can run on many operating systems including Solaris and Windows. Web Server Hardware Web Server computers have generally more memory. They have larger and faster hard disk drives and faster processors than the typical desktop PCs. Companies that sell web server hardware such as Dell, Hewlett Packard etc. all have configuration tools on their web sites that allow visitors to design their own web servers.

Performance of web server

Performance of web sever

- Performance of web servers is assessed based on throughput (number of requests handled) and response time (time taken to process a request).
- Throughput indicates the server's capacity, while response time measures its efficiency.

Performance of web servers can be evaluated mainly on the basis of two factors:

- Throughput indicates the number of requests that a particular server hardware and software can handle.
- Response time indicates how much time a web server requires to process one request.

Web server hardware architectures

. Some web sites are so large that we need more than one computer within each tier. For sites which have to deliver millions of individual pages and process thousand of customer and vendor transactions each day, site administrators must plan carefully how to configure their web server computers. They may adopt two different approaches in this regard. They can use centralized architecture approach where they can use few but very fast and large computers within each tier; or they may adopt decentralized approach using many less powerful computers and dividing workload among them. Web hosting choices ISPs also offer web hosting arrangements.

Shared hosting means that a client's web site is hosted on a server that simultaneously hosts other web sites and is operated by an ISP through its location.

In Dedicated hosting a web server is arranged by the ISP for a client but that client does not share it with other clients of the ISP. In both cases ISP owns the hardware but leases it to the client and is responsible for its maintenance. In Co-location hosting, the ISP offers on rent a physical space to client to install its own server hardware and software and maintain it by itself. Companies may opt to run a server in house which is called self hosting.

E-commerce software

Size and objectives of e-commerce sites vary thus variety of software and hardware products are developed which can be used to build those sites. Type of e-commerce software that an organization needs depends on several factors. Typically all e-commerce software must at least provide:

- A catalog display
- Shopping cart capabilities
- Transaction processing

Large or complex e-commerce sites also use software that adds other features and capabilities as follows:

- Middleware
- Application integration
- Web services

- Integration with ERP Software
- Supply chain management software
- Customer Relationship Management (CRM) Software
- Content Management Software
- Knowledge Management Software

Catalog display

A Static catalog is a simple list written in HTML. One has to edit the HTML code to change it. A dynamic catalog stores information about items in a database usually on a different computer accessible by the web server. It can provide photos, detailed description and search facility about the availability of items.

Shopping cart

In early days form based shopping cart was used wherein the user had to remember and type certain information. It is now replaced by electronic shopping cart/basket that keeps record of the items the customer has selected and allows customers to view the details of the items selected. The customer can add new items or remove items. To order an item, a customer simply clicks at that item option. All details of an item, including its price, product no. and order identifying information are stored automatically in the cart.

Transaction processing

It occurs when a customer clicks at checkout or confirm order button and is subjected to some payment processing mechanism. It represents the most complex part of online sale. Calculation of taxes, shipping costs etc. is important parts of this process. Some software enables a web server to obtain updated shipping rates by directly connecting to shipping companies' web sites.
Advanced functions of e-commerce software

Middleware

Large companies establish connections between their e-commerce software and their existing accounting system by using a type of software called Middleware which is a part of e-commerce software package.

Application integration

A program that performs a specific function such as creating invoices/bills or processing payment received from customers is called an application program. We know that Database Management Software stores information in a structured way. Experts should properly consider that their e-commerce software application programs must be compatible and fully integrated with the Database Management Software. For example if a company has existing inventory database then the experts should select that e-commerce application program that supports such a system.

Web Services

Web services are defined as a combination of software tools that allow application software in one organization communicate with other programs/applications over a network by using a specific set of standard protocols. For example a company that wants to gather all its financial management information in one spreadsheet can use web services to automatically get bank account details, information about loans, stock value etc. from different independent sources. Similarly, web services can be used to obtain price and delivery information about goods from different vendors/suppliers, review this information, place the order to the right vendor/supplier and track the order till shipment is received.

Lesson 20

INTEGRATION WITH ERP SYSTEMS

Enterprise Resource Planning

Enterprise Resource Planning (ERP) is a concept that integrates all aspects of a business e.g, accounting, logistics, manufacturing, marketing, planning, project management etc. at a single place. An ERP system such as SAP is expensive. E-commerce sites/software has to fully integrate with ERP software, wherever it is used.

Customer Relationship Management Software

Primary goal of customer relationship management is to understand each customer's needs and customize the product/service to meet those needs. CRM software gathers data from customer's activities on the web site of e-business. The software uses this data to help managers to conduct analytical study about their business/marketing.

Supply Chain Management (SCM) Software

Supply chain involves all activities associated with flow and transformation of goods from raw material stage to the finished stage and their supply to the end users. Supply chain management software helps companies to coordinate planning and operations with their partners in industry. SCM planning software helps companies develop demand forecasts using information from each player in supply chain. SCM execution software helps with tasks such as the management of warehouses and transportation facilities.

Content Management Software

Companies have found it important to use the web to share corporate information among their employees, customers, suppliers etc. Content Management Software helps companies control the large amounts of data, pictures/graphics and other files that play a crucial role in conducting business. It also offers different ways of accessing the corporate information which managers of a business might need for decision making.

Knowledge Management Software

Companies have started to find ways that help them manage the knowledge itself regardless of documentary representation of that knowledge. Software that has been developed to meet this goal is called Knowledge Management Software. It has features that allow it to read documents in electronic format, scanned paper documents, e-mail messages etc. so as to extract knowledge.

E-commerce Software

Following are the names of some well-known e-commerce software:

- Intershop Enfinity
- IBM's WebSphere Commerce Professional Edition
- Microsoft Commerce Server 2002

Agents

An agent is a software program that is capable of autonomous action in its environment in order to meet its objectives. Agents can be used for comparisons, filtering, web crawling, auctions etc. For example, there may be buyer agents and seller agents each with their goals and constraints. They can negotiate deals on behalf of the users. Agents can monitor health indicators and alert the individuals under given conditions.

Security issues over the internet

Security is the biggest factor slowing down the growth of e-commerce worldwide. For instance, when you enter your credit card no. in a text box, it is potentially exposed to millions of people on the internet and

can be misused. It is important to know following terms in connection with the security threats over the internet.

Back doors and Trojan horses

Back Doors are those hostile programs which, when run on a machine, install hidden services in order to give attackers remote access capabilities to a compromised machine. Trojan horses are those programs that appear harmless but actually have some malicious purpose. For example, HAPPY99.EXE is a Trojan horse that displays a firework and then sends copies of it to the e-mail addresses found on the system. The term Trojan Horse has been borrowed from history. In history it has been used to refer to a huge wooden horse where the whole Greek army was hidden during a war and the enemy was deceived because it could not figure out that.

Viruses and worms

Viruses and Worms are malicious programs that can travel between computers as attachments on email or independently over a network. These terms are sometimes used interchangeably; however, essentially they are different. Worms spread from computer to computer, but unlike viruses have the capability to travel without any help or human action. A worm can replicate itself which means that it can send copies of itself to everyone listed in the email address box on a system. Viruses, on the other hand, need to be activated through a human action. Another difference is that viruses modify existing programs on a computer unlike worms which can install back doors or drop viruses on the system they visit. A few years ago a worm called 'Love Bug' was triggered by a 23 years old student in Philippine. Its code was written in VBScript, and it traveled on the internet as an email attachment. It could send copies of itself upto 300 addresses found in the email address box. It could destroy files on the system as well as search for any passwords and forward a list of the same to the attacker. Within days it spread to 40 million computers in more than 20 countries causing a financial loss of about $ 9 billion.

Virus protection

- Install anti-virus software such as McAfee, Norton, Dr. Solomon, Symantec etc.
- Downloading of plug-ins from the internet be avoided (plug-ins are those programs that work with the browser to enhance its capabilities)
- Downloading of plug-ins should be done from the vendor's official website

- Newly obtained disks, programs or files should be scanned for viruses before use
- Installation of a firewall may also reduce the risk of virus attack

Hackers

Hackers or crackers are those individuals who write programs or manipulate technologies to gain unauthorized access to computers and networks

Active contents, active X control

Active content refers to programs.. embedded in web pages that can perform actions. Malicious active content, such as Applets, JavaScript, and Active X controls, can be used by hackers to install hidden services, collect sensitive information, or cause damage to the user's system.

Active content is a term generally ges to cause certain action. Malicious Active C d nos., user names, passwords etc. and any othe s, JavaScript and Active X Controls can be use t Applet is a compiled Java program that runs on made. Some malicious content can be sent by th cks a hacker can destroy the hard disk, disclos n. JavaScript programs can read list of URLs visited and seize information in the web forms. For example, if a user enters a credit card no. in the form, JavaScript code can send a copy of it to the hacker. Moreover, malicious content can be delivered through cookies using JavaScript that can reveal contents of files or destroy files. Active X Controls are those objects which contain programs placed on web pages to perform particular

tasks. They can originate form many languages, C, Visual Basic etc. When downloaded they can run on client machine like any other program. A hostile Active X Control can reformat a user's hard disk, send e-mails to all people listed in the mailbox or even shut down computers.

Out side attacks on a network

Eavesdropping/ sniffing/snooping

In this type of attack the hacker has the ability to monitor network traffic using some kind of network-monitoring software. For example, a hacker may install some backdoor or Trojan horse that can monitor the key strokes of a user while typing and send the typed information to the hacker.

Password attacks

Such attacks are basically a result of eavesdropping through which the hacker is able to know the account ID or password of a particular user. Then using it the hacker gains access to the network and gather information such as user names, passwords, computer names, resources etc. That can lead to modification, deletion or rerouting of network data.

IP address spoofing

You know that there are two IP addresses available on a data packet – IP addresses of the sender and the destination. The address of the destination only matters for routing. It is possible that a hacker (having special capabilities) seizes the control of a router, changes the IP address of the source/sender on data packets and thus forces the destination machine to send the information/web page to a different machine, that is, the machine of the hacker. This is called IP address spoofing.

Man in the middle attacks

In it the attacker is able to monitor, capture and control data between sending and receiving machines. He may apply IP address spoofing technique to divert the packets to its machine, then modify the packets and resend the misleading information to the actual client. Another form of man-in-the-middle attack is where the hacker is able to substitute the IP address of a genuine web site with the IP address of his own web site due to some security hole in the software that runs on a domain name server. A client would think that he is communicating or receiving the information form a genuine web site, though it would not be the case actually.

Denial of services (DOS) attacks

In this type of attack, the attacker gains access to the network and then send invalid data to network services or applications. These services or applications consequently become unable to perform their normal tasks or functions. Hence, sending a flood of data to a particular service or computer can cause it to overload or shutdown. This attack is specially used to take down websites on the internet, when repeated requests for web pages are deliberately initiated so as to choke down a web server. In early 2000 this attack was launched against some famous ecommerce web sites. Hackers arranged computers with special software initiating thousands of http requests per second for specific web sites causing the web servers to overload. Thus, these servers were made unable to fulfill the web page requests of the genuine users/clients. In distributed denial of service attack, the compromised system itself is used as a source for further attacks. The use of firewalls and a proper Intrusion Detection System (IDS) can minimize the risk of a DOS attack. It is also important to establish a security policy for an e-business organization outlining as to which assets have to be protected and how to be protected.

Lesson 21

FIREWALLS

A firewall is a combination of hardware and software that sits between the internet and internal network of an organization to protect the network from outside attack (Fig. 1). It can examine the data entering or leaving from the network and can filter the data according to certain rules, thus, protects the network from an attack. There are three main types of firewalls detailed as follow

---

Three types of firewalls are commonly used in network security to protect against unauthorized access and control traffic flow.

Packet filter firewalls filter packets based on IP addresses, port numbers, and protocols, providing basic security.

Circuit level firewalls monitor TCP/IP connections,

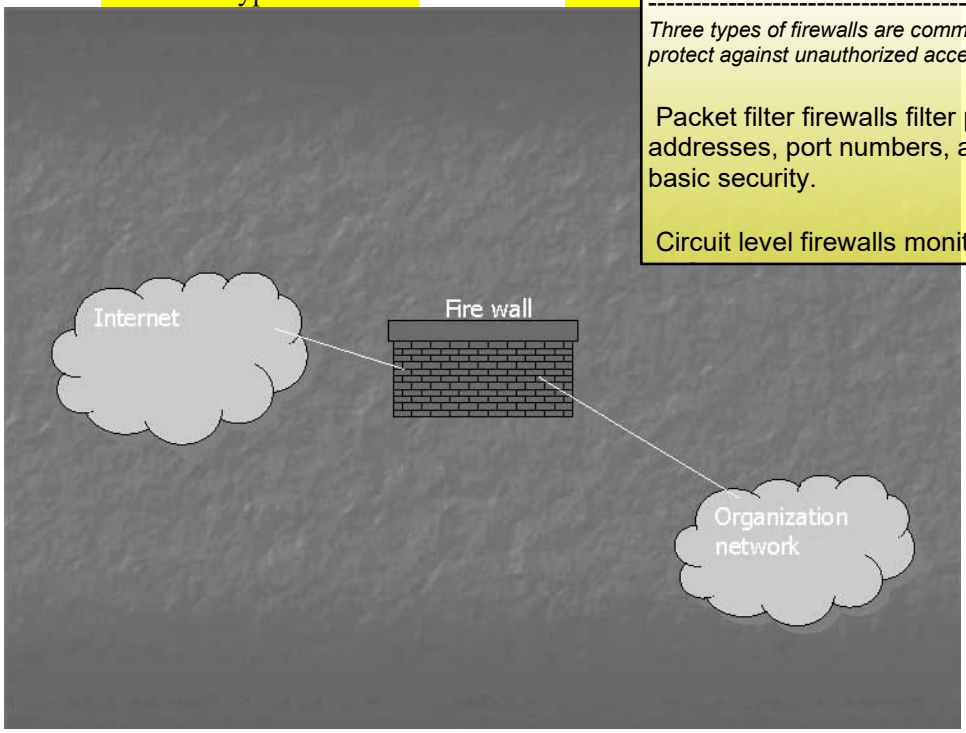

Fig. 1

Packet filter firewall

It uses a set of rules to determine whether outgoing or incoming data packets are allowed to pass through the firewall. For example, we can, as a rule, specify IP addresses of sending devices such that packets from these IP addresses are not allowed to enter the network. The Firewall would stop them from entering. A packet filter firewall is the simplest type of firewalls which operates at data link and network layers of the OSI model.

Circuit level firewall

ll. It also works on the basis of a set of rules for filtering packets but operates at the transport layer of the OSI Model so has greater functionality. As a rule, the higher the layer of OSI model where a firewall operates, the more sophisticated is the firewall. It can make packets sent from internal network to a destination outside the firewall appear as if they originated at the firewall. Thus information regarding hosts on the internal network remains secret. It can also determine whether TCP/IP connection between a host and a machine outside firewall has been properly established. Thus it can cut off any connection which has been hijacked by a hacker trying to pass through the firewall.

Application gateway firewall

rong user authentication to verify identity of a n layer protocols such us FTP. In contrast to s entering/leaving the network. It can block any yees of a company inside a firewall from ide. In other words, this type of firewall is used

---

It operates at the application layer. It filters traffic based on application-layer protocols like FTP, HTTP, or SMTP. It enforces user authentication and can restrict outgoing requests, such as blocking access to certain websites or preventing downloads of potentially harmful programs. Hybrid firewalls combine circuit level and application gateway features for enhanced security.

to control connections thus employees of a company can be restricted from connecting to certain web sites. We can combine circuit level capabilities with application gateway services to form Hybrid type of a firewall.

Proxy server

A proxy server sits between an internal trusted network and the untrusted network, that is, internet, **as you can see in Fig. 2 below.**

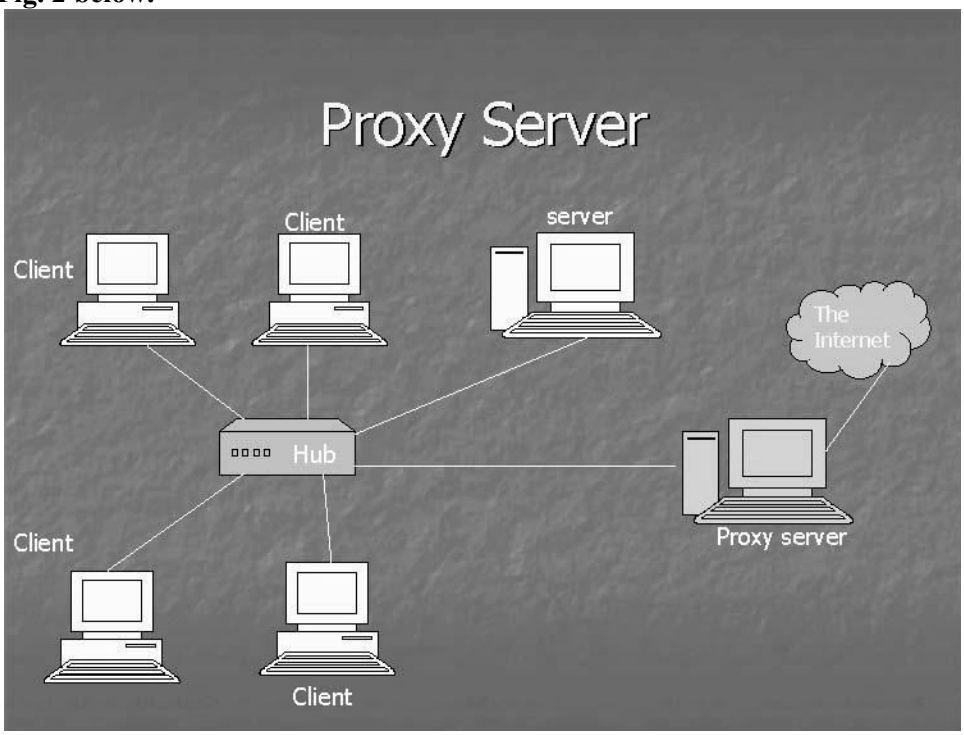

Fig. 2

Mainly, it can do three things:

- An http request from the browser goes to proxy server. It can affix its own IP address instead of IP address of the requesting machine; thus, it hides the information of the host. It downloads the requested page itself and afterwards supplies it to the user.
- It can also act as a firewall filtering requests for certain web pages.

- An important job it can do is to speed up the processing of http requests by caching web pages. Caching means that it can store the requested web pages in its memory (cache memory) for a certain period. The advantage of caching is that for subsequent web page requests the time of supply of the web pages is reduced. Instead of sending the request to actual web server, the proxy server can quickly supply the web page stored in its cache memory, thus, it saves the time of downloading the page.

Virtual private network (VPN)

Suppose that a client is sitting at a local branch network of a company and wants to become part of a bigger, head office network of that company located far away. One option for him is to set up a dial up connection, which means that he can be connected to a server machine lying in the head office network through a direct telephone line. That server machine may be called a **Remote Access Server (RAS)** and the client may be called a **Remote Access Client (RAC).** Remote access is a two way process so both RAS and RAC must be configured, first. Some windows operating systems provide the facility to configure the RAS and RAC. Basically, the client specifies the phone no. of RAS while configuring. After both RAS and RAC are configured, the client enters identification information (password etc.) and clicks at "Dial". Accordingly, phone no. of RAS is dialed and connection with RAS is setup. Once clients are connected to RAS, they can access the remote company network and its resources – servers, printers etc. A protocol,

Point to Point Protocol (PPP), is used to set up the dial up connection between RAC and RAS for exchange of data packets.

A VPN provides another option of remote access. It is defined as a secure, dedicated point to point connection over the internet.In VPN we use internet infrastructure for connection instead of a special telephone line. Both RAS (also called tunnel server) and RAC (also called tunnel client) are connected to the internet. Initially, both are configured for VPN. IP address of tunnel server must be specified during the configuration of tunnel client (instead of phone no.). The option of VPN is available if we explore the menu 'Internet Options'. We can enable VPN, thus. Similarly, tunnel server should also be configured so that a client's request for access can be authenticated. VPN connections or tunnels are managed by Point to Point Tunneling Protocol (PPTP) which due to encryption provides secure transport of private communications over the public internet. A VPN connection thus can be created between the branch office and the corporate head office.

VPN is a cost saving measure as compared to simple remote access using dial up connection. In VPN one makes a local call to the ISP and then using ISP's infrastructure, routers etc. one is connected to the internet. In other words a client can become part of the remote network through the internet. Note that a tunnel client just incurs the cost of a local call to the ISP and yet he can remain part of the remote corporate network for many hours. On the other hand, in case of dial up connection for remote access one has to pay the cost of a long distance call for as many no. of hours as one wants to be connected to the remote corporate network. This is going to be very expensive. VPN is the example of an extranet. You know that when two or more intranets are connected to each other they form an extranet. A manufacturing company thus can be connected to its suppliers of raw material and its distributors through VPN.

Security – the biggest challenge

There is a consensus that the issue of computer and data security is the biggest hurdle in the growth of e-commerce. Web servers also face this security threat. Programs that run on a server have the potential to damage databases, abnormally terminate server software or make changes in the information placed there. A number of international organizations have been formed to share information and combat security threats to computers and computer networks. The names of two such organizations are worth-mentioning:

- Computer Emergency Response Team (CERT)
- Systems Administrator, Audit, Network and Security Institute (SANS Institute)

The best response that the experts have come up with to tackle the security issue is in terms of cryptography.

Cryptography

Cryptography is the technique of converting a message into unintelligible or non-understandable form such that even if some unauthorized or unwanted person intercepts the message he/she would still not be able to make any sense out of it. Cryptography is thousands of years old.

Techniques used for cryptography Substitution In substitution we replace each letter in the message with another to make the message non-understandable. For example, each letter "a" in the message can be replaced with letter "d" and letter "b" with letter "e" and so on. Transposition It is based on scrambling the characters in a message. A transposition system may first write a message into a table row by row then the message can be read and rewritten column by column to make it scrambled **(see Fig. 3).**

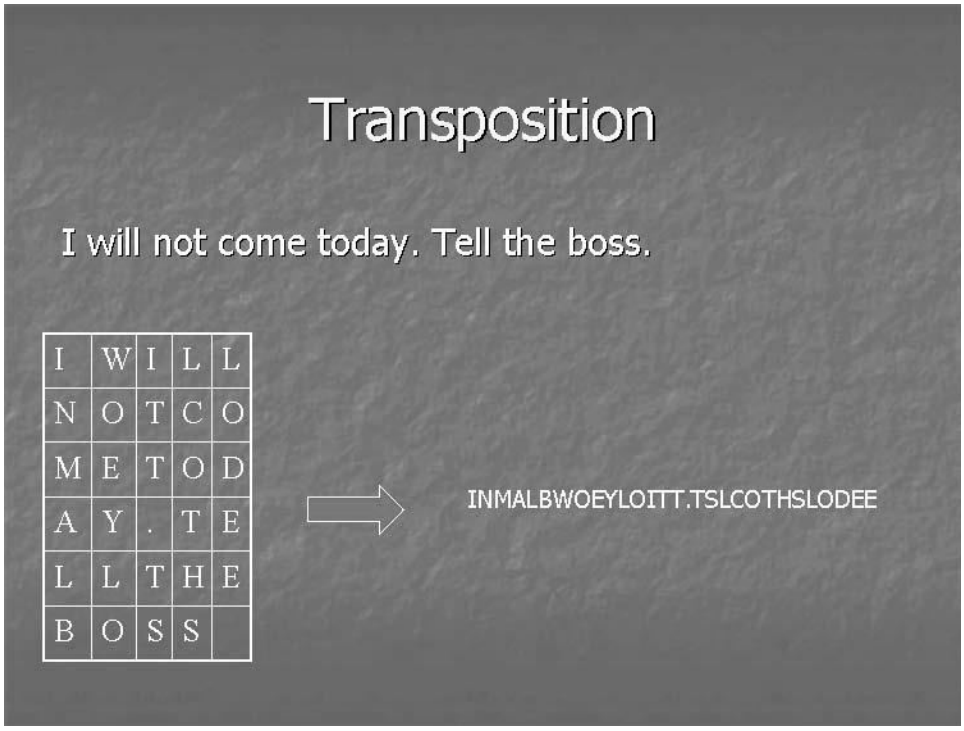

Fig. 3

Hist cally, cryptography has long been /. Julis Ceaser used a simple transposition cipher to scramble messages to give instructions to his commanders in the battlefield. Similarly,Hitler used Enigma encryption cipher to scramble messages sent by radio to German armies and u-boats during the Second World War. Cryptography has also been used for non-military purposes over the centuries. There are records of people using cryptography to protect religious secrets and to hide secrets of science and industry. In recent years, the use of cryptography in business and commerce appears to have surpassed its earlier use. It has made the rapid commercialization of internet possible. Without cryptography, it is doubtful that banks, businesses and individuals would feel safe doing business online.

Lesson 22

CRYPTOGRAPHY

Cryptography is a set of mathematical techniques used to ensure information confidentiality. Encryption involves scrambling a message with a key, while decryption involves unscrambling it using an appropriate key. Keys are randomly generated using cryptographic algorithms. PGP is a popular cryptographic system for public use.

Cryptography is a collection of mathematical techniques used to ensure information confidentiality. The process of scrambling a message with the help of a key is called encryption. The process of decrypting a message using an appropriate key is called decryption (see Fig. 1). The keys are usually randomly generated with the help of some cryptographic algorithm. Pretty Good Privacy (PGP) is the name of a popular cryptographic system which is available for general public use. There are two types of cryptography - Symmetric and Asymmetric cryptography.

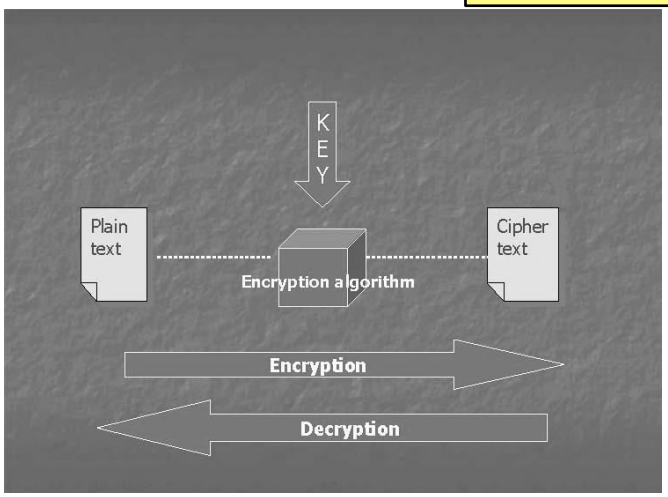

Fig. 1

Symmetric Cryptography

In symmetric cryptography same keys are used for encryption and decryption.

Asymmetric or Public Key Cryptography

In this type a pair of public and private keys is used for encryption and decryption (Fig. 2).

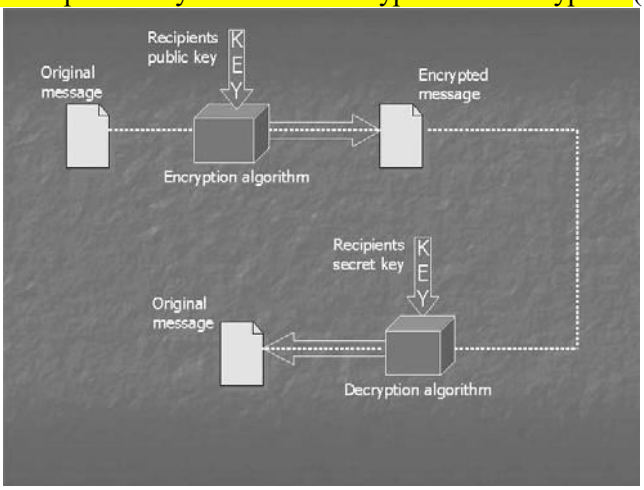

Fig. 2

Digital/electronic signature

An electronic signature means any letters, numbers, symbols, images, characters or any combination thereof in electronic form applied to an electronic document which can ensure authenticity, integrity and non-repudiation. It uses public key cryptography (Fig. 3). **Authenticity** means that the message is from a particular source/individual. Integrity means that the message has not been altered during transmission.

Non-repudiation means that the execution of the digital signatures cannot be denied by the one who is alleged to be the executor of those signatures.

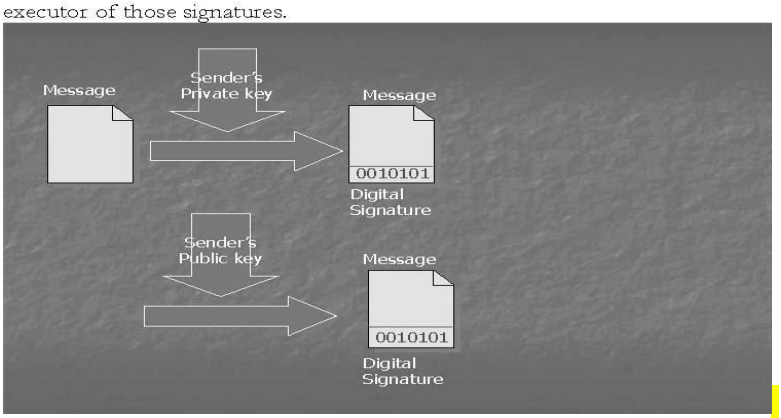

Fig. 3

Digital certificates

These are the certificates in electronic form which establish whether or not a public key belongs to the purported owner. A digital certificate at least comprises a public key, certification information (name, ID etc.) and electronic signatures of a certification aut hor ity. Digital certificates are prepared according to a generally accepted format called X.509 standard format.

Certification authority (CA)

A certification authority is defined to be a trusted public/private body that attests the association of a particular individual with his/her corresponding public key. A CA signs digital certificates with its private key. There are many CAs working in the field but the pioneering or the most reputed CA is Verisign which is based in America.

Certification authorities work in a hierarchical fashion. There is the CA at the top called root CA (the most reputed CA). It can issue certificates to CAs working below it and those CAs' can further issue certificates to CAs working under them. In this fashion a hierarchy of CAs is developed with each CA confirming the public key of the CA below it through a digital certificate. This concept is elaborated in Fig. 4 below.

Fig. 4

Assume that I want to send an encrypted or a confidential message to Mr. A. For that I need to know his public key. I can access a machine called key server and try to find his public key against his particulars (name, address, id etc). I may discover that a CA, CA1 below in hierarchy has issued a digital certificate to Mr. A against his particulars and has signed it with its private key. If that CA holds a reputation that I can trust it then I would rely upon that public key and use it for encryption. Otherwise, I should go up the hierarchy and see whether there is a certificate issued by CA2 certifying the public key of CA1. If that certificate is found then ideally I should go further up the hierarchy to check that the CA, above CA2 which

is root CA in this case has issued certificate to CA2 or not. In this manner I can check the certificates upto the root CA.

If all the certificates in the chain are available, then it should provide me the maximum trust that this key actually belongs to that particular user. However, if the chain is broken or any certificate is missing in between that might cause a dent in my trust on that public key. I would then be hesitant to use that public key appearing to be that of Mr. A. It is all a web or the model of trust. The greater is the reputation of a CA the more trust I shall have in the certificate issued by it authenticating the public key of a user. The CAs at the top level of hierarchy carry more trust. So, if Mr. A has a certificate directly from the root CA, his public key would be most trust worthy. In case he has a certificate directly from Verisign, the most reputed CA in the world then I should have maximum trust that this public key must be that of Mr. A whom I know. I should have trust that if Verisign has issued the certificate it would have done detailed investigation before issuing it to Mr. A. His name, address, identification would have been properly verified or confirmed before associating a public key with him through the certificate. If you are obtaining a certificate from a top level CA, which is more reputed, you have to pay more to that CA. So Mr. A has to pay relatively more to the root CA if he wants to obtain a certificate directly from the root CA. There are different levels of certificates attaching different levels of trust with them. We may have class, A, B or C type certificates. A Class A certificate would have more trust attached to it. Of course, one has to pay relatively more to get a class A certificate from a CA as compared to class B or C. However, in class A, a greater level of investigation would be involved before issuing a certificate to someone.

You may have noticed that the role of a Certification Authority is analogous or similar to a passport office. The issuance of passport by the passport office attaches credibility that this particular person is entitled to travel. However, the passport is not issued by the office until detailed enquiry/verification about the identity of the person is made. Once a person holds the passport, that confirms that this particular person whose, name, address etc. is appearing on the passport is entitled to travel. Similarly, if a digital certificate is issued by a reputed CA that would confirm to other people that this particular public key certified by the CA belongs to this individual only.

There is a reason why we use the concept of CAs. We use it for the verification of identify of a person. This is probably the best solution envisaged for such verification, though it may have certain loopholes in it. You can realize that the best thing is that Mr. A personally hands over his public key. On the other hand if I try to trace his public key against his particulars (name, address, and identification no.) on a key server there is a possibility that I end up discovering that there are three, four, five different public keys against the particulars of same Mr. A. Assume that all of them have been certified by different CAs. Now, I am confused that which of these is genuine so that I can use it. Indeed, only one of them is genuine and the rest are fraudulent keys registered by fraudulent people using particulars of Mr. A. In this situation I would use and rely upon that public key of Mr. A that has been certified by the most reputed CA among all the CAs. I would treat others as fraudulent. The objective of getting fraudulent keys is to intercept/receive the messages intended to be sent to a particular receiver. So, if someone intends to receive the messages delivered for Mr. A, he may register the key against his particulars and get a certificate in this behalf. Note that CAs are supposed to issue the certificate after proper enquiry, otherwise they may also be held liable under different laws.

Despite the loophole that fraudulent keys can be obtained in this set up, this system of certificates is believed to be the best for confirming authenticity of a person. Imagine that I want to send an encrypted message to someone in Canada from Pakistan. It would not be practical that first I contact him in Canada and in some manner obtain his public key and then send him the message using that. It would be more convenient, practical and time saving that I go to a key server, find his public key against his particulars and check whether it is certified by a reputed CA. In other words if the certificate of a well respected CA is there to authenticate his public key then I can use that public key. Behind this system of certificates and CAs, the idea is to make internet communication global in nature such that the authenticity of individuals is also ensured at the same time.

Lesson 23

HASH FUNCTION AND MESSAGE DIGEST

There are two terms that you should note here – hash function and message digest. Hash function is a one-way mathematical function applied to a message. Result of the hash function is unique to each message called Message Digest. A message digest is a single large number typically between 128 to 256 bits in length. Thus, we can have up to 2^{256} different messages each having a unique message digest associated with it. This gives rise to almost an incalculable figure. We can safely assume that each different message that can possibly be typed would have a unique message digest on applying a hash function. A hash function is said to be one way because we cannot go back to the original text on applying the hash function to a message digest. Basically, the concept of hash function and message digest is used to confirm the integrity of a message. Following is the example of a hash function that can be used in a code (no need to prepare it for exam)

```
"char XORhash( char *key, int len)
{
char hash;
int i;
for (hash=0, i=0; i<len; ++i) hash=hash^key[i];
return (hash%101);              /* 101 is prime */
      }"
```

Following example shows how a text message is encrypted and digitally signed using public key cryptography:

First of all, the sender types a text message "Together, we shall make Pakistan strong…". A hash function is applied on the message to get the message digest. Assume the message digest comes to be "1967…" in this case. The message is encrypted using public key of the receiver, thus it becomes scrambled or confidential. Then the sender adds his private key in the obtained message digest to create his digital signatures. This digitally singed message is received by the receiver, who applies the pubic key of the sender to decrypt the digital signature and reveal the message digest. Then the receiver uses his private key to unscramble the message itself, and applies the same hash function received from the sender to get a message digest. The receiver compares this message digest with the one sent by the sender through digital signature. If both are the same it ensures that the message has not been altered during its transmission. **Figures 1-4 given below explain this concept:**

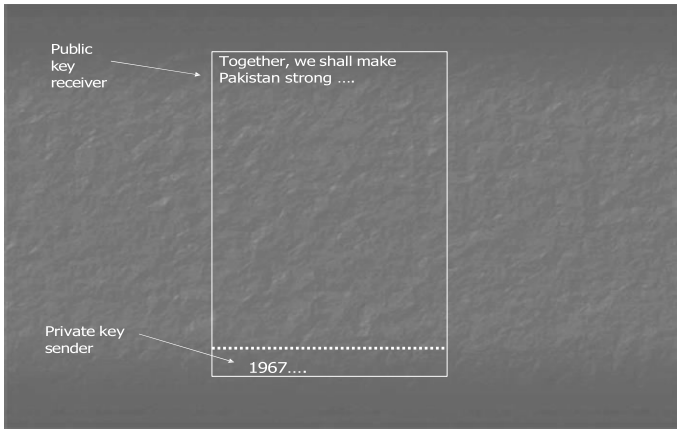

Fig. 1

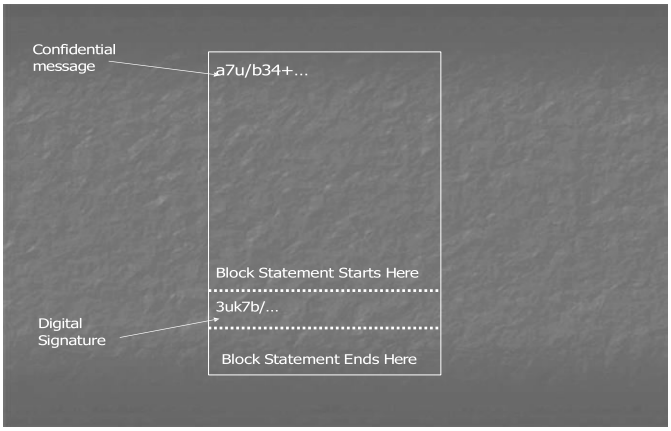

Fig.2

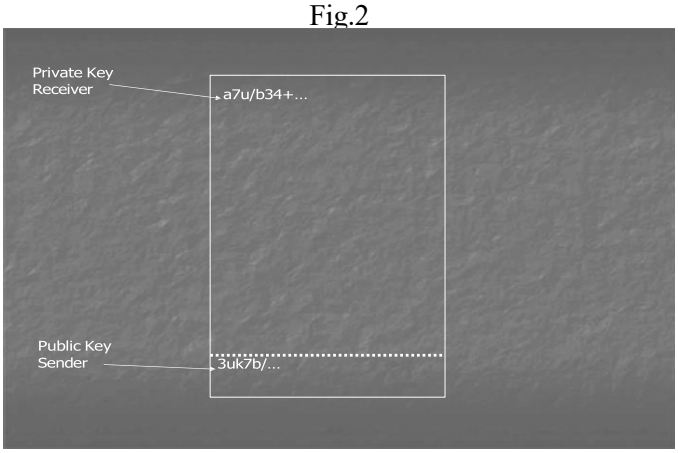

Fig. 3

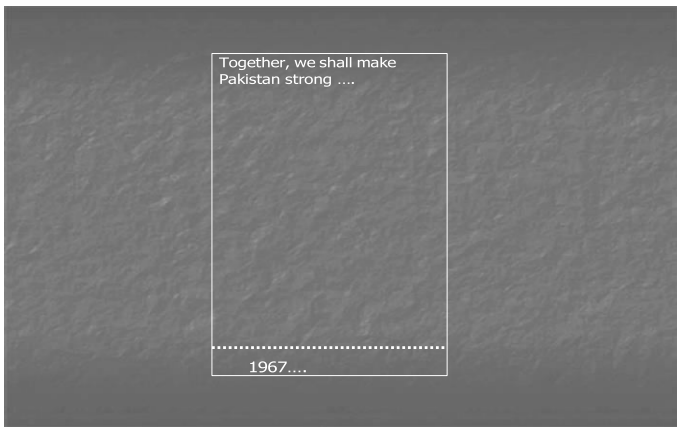

Fig. 4

Process of Sending Messages Using Public Key Cryptography

Fig. 5 below shows the working of the digital signature technology:

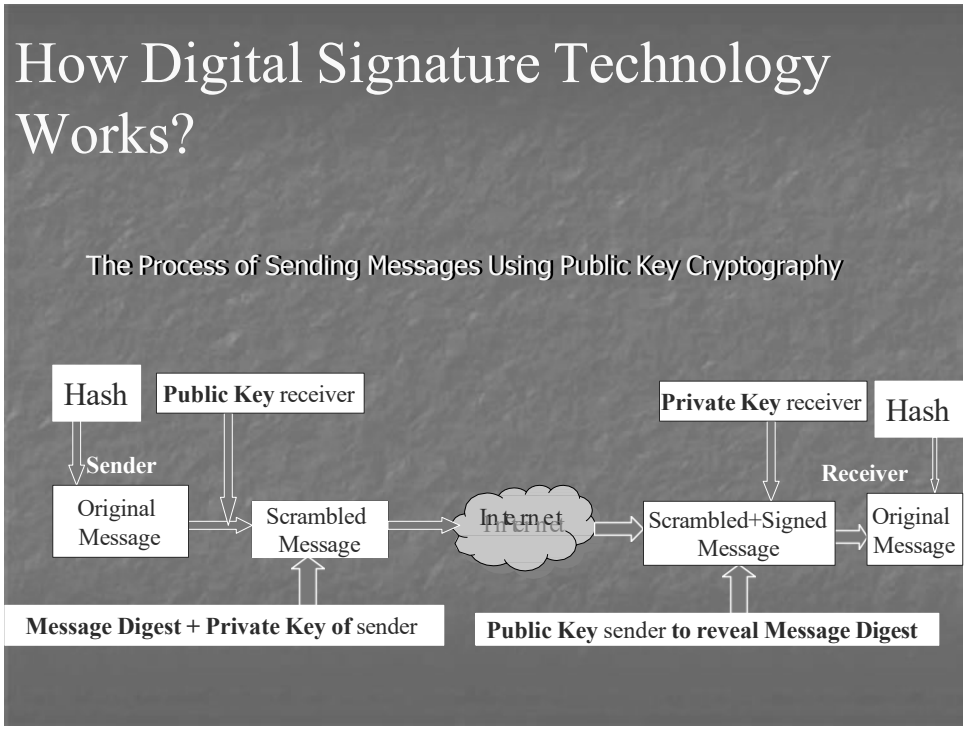

Fig. 5

Note that following steps are involved in the digital signature process:

1. Hash function is applied to the original message in order to find the message digest.
2. Public Key of the receiver is used to encrypt the message.
3. A digital signature is attached to the scrambled message by signing the message digest with Private Key of the sender.
4. The encrypted message, the digital signature and the hash function are sent to the receiver.
5. Public Key of the sender is used by the receiver to reveal the message digest and, thus, to confirm identity/authenticity of the sender. In this regard, the receiver finds the digital certificate certifying the public key of the sender and checks whether the digital signature can be decrypted with the public key on the certificate and whether or not this certificate had been issued to the sender by a trust-worthy certification authority.
6. Receiver uses his/her Private Key to decrypt the message. Private Key is a secret key only known to the user.
7. Receiver applies hash function to the received original message and computes the message digest. If this message digest matches with the one received from the sender, it confirms that the message has not been altered during transmission. This ensures integrity of the message.

Note that a
private keys. The advantage of using symmetric key is that since symmetric algorithms are faster as compared to asymmetric, therefore, the encryption of a message with the symmetric key takes place quickly. In order to send the symmetric key to the receiver, however, the asymmetric cryptography has to be used. PGP uses this system. See Fig. 6 below.

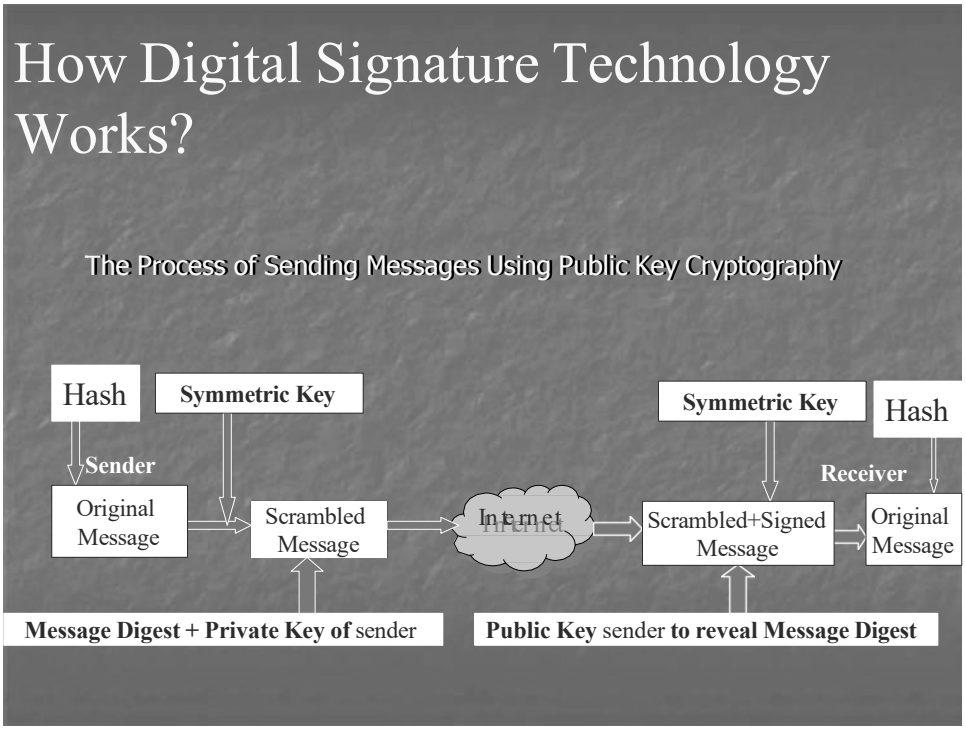

Fig. 6

Where only the authenticity is to be ensured and not the integrity, then a name or a piece of text can be chosen to create the digital signatures. In Fig. 7 below, the word "Imran" has been used to create a digital signature which can commonly be used for all different messages.

Note that a digital or electronic signature is believed to be more reliable as compared to paper signatures because it is not ordinarily possible to copy or forge an electronic/digital signature. But, that is very much possible in case of paper signatures.

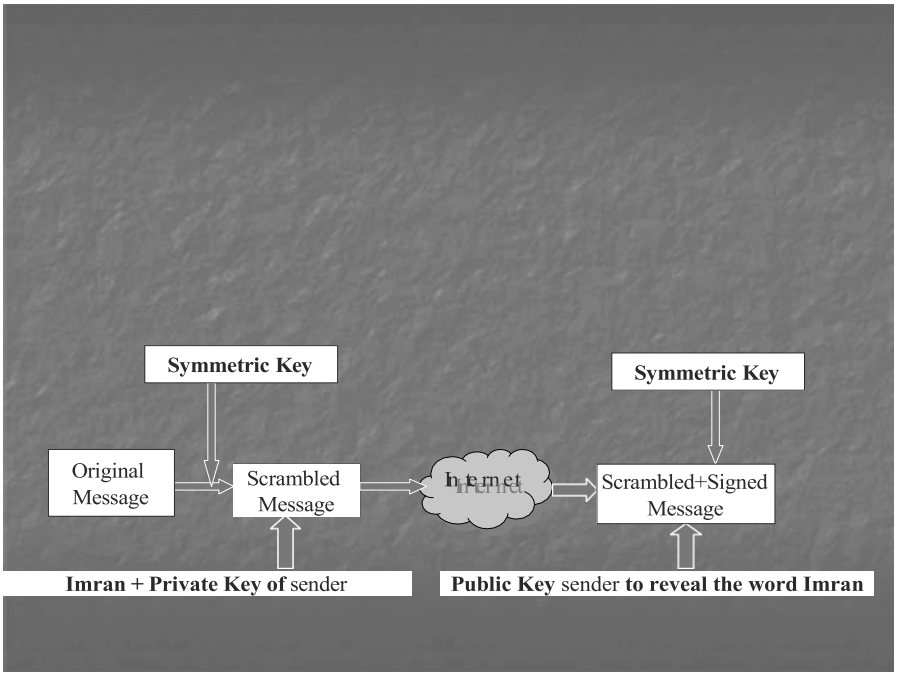

Fig. 7

Public Key Infrastructure (PKI)

A PKI is defines as a structured system that provides key management facilities, storage and management facilities of digital certificates and involves a certification authority. PKI has its application in online contracts, e-banking, electronic payment systems such as electronic checks, credit card based systems, electronic cash, micro payment systems etc.

Key Length

A s – 0's & 1's- inside a computer. If a key is 1 bit in length it means two possible keys, that is, 0 and 1. If a key is2 bits in length it means four possible key values, 00, 01, 10 and 11. A Key having 3 bits length means 8 possible values - 000,001,010,011,100,101,110,111. From this, one can derive a general formula, that is, Number of keys = 2(number f bits)

Lesson 24

SYMMETRIC KEY ALGORITHMS

Cryptographic algorithms are measured in terms of key length. Following is the list of some popular symmetric key algorithms:

- DES (Data Encryption Standard) – 56 bits
- IDEA (International Data Encryption Algorithm (IDEA) – 128 bits
- RC2 – (block cipher) 1-2048 bits
- RC (stream cipher) –1-2048 bits
- Rinjdael – 128-256 bits

Attacks on Symmetric Key Algorithms

- Following attacks have been reported on symmetric key algorithms:
- Key Search Attacks
- Cryptanalysis
- System-based Attacks

- Key Search (Brute Force) Attacks

In this type of attack an attempt is made by the attacker to decrypt the message with every possible key. Thus, the greater the key length, the more difficult it is to identify the key.

- Cryptanalysis

Encryption algorithms can be defeated by using a combination of sophisticated mathematics and computing power so that many encrypted messages can be deciphered without knowing the key. Such type of an attack is called cryptanalysis.

- System-Based Attacks

In it the attack is made on the cryptographic system that uses the cryptographic algorithm without actually attacking the algorithm itself.

Public Key Algorithms

Following is the list some popular public key algorithms:

- DSS – Digital Signature Standard based on DSA (Digital Standard Algorithm) – key length is between 512-1024 bits
- RSA
- Elliptic Curves

Attacks on Public Key Algorithms

Key Search Attacks

The public key and its corresponding private key are linked with each other with the help of a large composite number. These attacks attempt to derive the private key from its corresponding public key using that number. According to an estimate 1024 bit RSA public key may be factored due to fast computers by 2020. Note that both symmetric and asymmetric algorithms are based on different techniques. In case of

asymmetric algorithms the increase in key length does not much increase the difficulty level for the attacker as compared to symmetric algorithms. Thus, a 128-bit RC2 symmetric key may prove to be much stronger than a 1024 bit RSA asymmetric public key.

Analytical Attacks

Such attacks use some fundamental flaw in the mathematical problem on which the encryption system itself is based so as to break the encryption.

Quantum computing is the branch of computer science that deals with the development of cryptographic algorithms. It can also be used to find flaws in the cryptographic system/algorithms and to launch attacks.

Electronic Payment Systems

Most of the electronic payment systems on internet use cryptography in one way or the other to ensure confidentiality and security of the payment information. Some of the popular payment systems on internet include the credit-card based payment systems, electronic checks, electronic cash, micro-payment systems (milicent, payword etc.)

The Process of Using Credit Cards

It may be useful to see how payment is made through a credit card in the traditional sense. Fig. 1 below shows the steps to be followed in this regard:

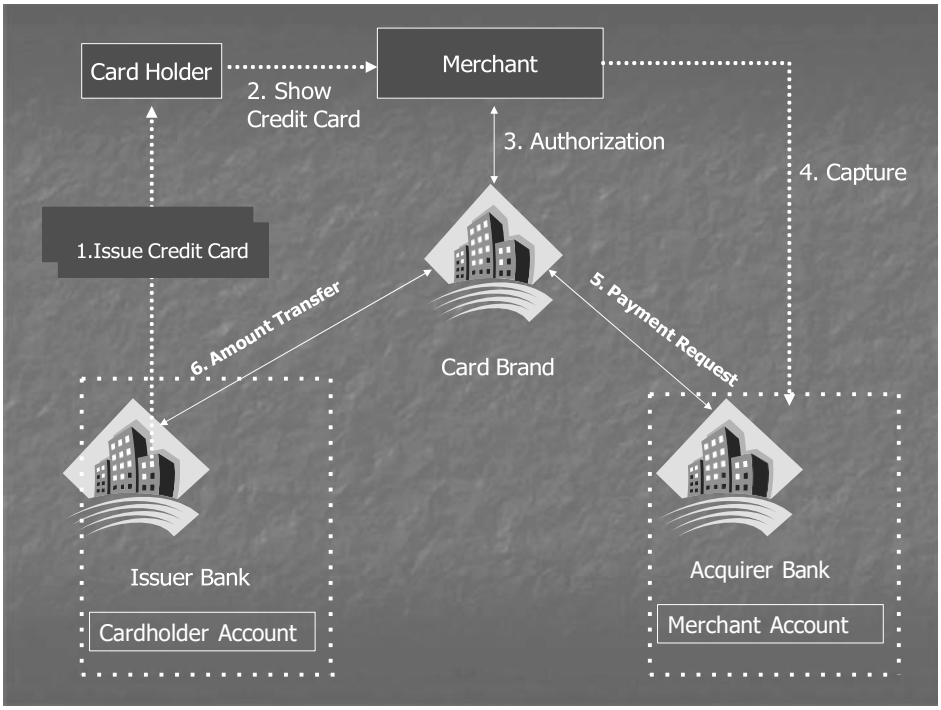

Fig. 1

1. A potential cardholder requests an issuing bank in which the cardholder may have an account, the issuance of a card brand (like Visa or MasterCard). The issuing bank approves (or denies) the application. If approved, a plastic card is physically delivered to the customer's address by mail. The card is activated as soon as the cardholder calls the bank for initiation and signs the back of the card.
2. The cardholder shows the card to a merchant whenever he or she needs to pay for a product or service.
3. The merchant then asks for approval from the brand company (Visa etc.) and the transaction is paid by credit. The merchant keeps a sales slip.

4. The merchant sends the slip to the acquirer bank and pays a fee for the service. This is called a capturing process.
5. The acquirer bank requests the brand to clear for the credit amount and gets paid.
6. Then the brand asks for clearance to the issuer bank. The amount is transferred from issuer to brand. The same amount is deducted from the cardholder's account in the issuing bank.

Note that in case of a credit card the issuer bank charges interest from the client at a specified rate on the amount lent. On the other hand, in case of a debit card no such interest is payable since the customer uses his/her own money in that case.

Virtual PIN Payment System

It is one of the earliest credit card-based systems launched for the internet in 1994 by a company; First Virtual Holdings, Inc. Virtual PIN system does not involve the use of encryption. Payment is made through the credit card in this system. The objective was to allow the selling of low-value information items without the use of any special client software or hardware.

Both merchants and buyers are required to register with First Virtual (FV). A buyer registering with FV forwards his or her credit card details and email address to FV and in exchange receives a pass phrase called, Virtual PIN. Buyer makes a telephone call to FV to provide his/her credit card number. FV establishes a link between the Virtual PIN and the credit card number without using the credit card number on the network. A Merchant goes through a similar registration process. He provides his bank details to FV and is given a merchant Virtual PIN. The merchant can now request to process payments from registered FV customers. The transfer takes place with the help of Automated Clearing House (ACH) service. Note that an ACH is a centralized system to which different banks are electronically connected forming a network for clearing payment requests. At the end the payment proceeds from the credit card issuer bank to the account of the merchant with acquirer bank (merchant's bank) through ACH, after FV deducts a per-transaction charge for its services.

Fig. 2 below shows the working of Virtual PIN payment system.

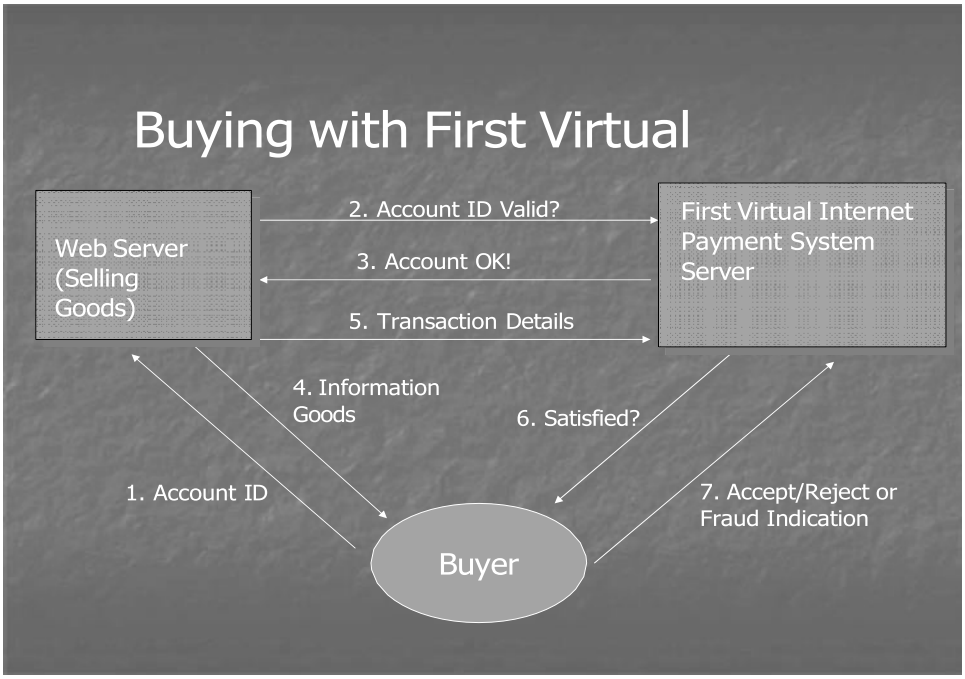

Fig. 2

A buyer browses the web server where FV registered merchant is selling goods. The buyer is asked to enter his/her Virtual PIN by the merchant site **(step 1).** Merchant queries the FV Internet Payment System Server (FVIPSS) to confirm Virtual PIN (**step 2).** If Virtual PIN is not blacklisted (**step 3)**, the merchant

may acknowledge this fact to the buyer by email and sends the goods, and also sends transaction details to FV **(steps 4 & 5)**. FVIPSS or simply FV server sends email to the buyer if the goods were satisfactory **(step 6).** There are three possible answers to that **(step 7)**. If the answer is "accept" then the payment proceeds, in case the answer is "reject" it means that either the goods have not been received or the buyer is not satisfied with the quality of goods. Then the payment is not made to the merchant. If the answer indicates "fraud" it means that the goods were never ordered. In such an eventuality the FVIPSS immediately blacklists Virtual PIN so that it cannot be used in the future.

Time period may be a few minutes to a few days for answering the email in step no. 6 above, otherwise FV shall proceed to arrange the payment. If a Virtual PIN has been stolen and the buyer does not indicate fraud within the time period for answering the said email the bogus transactions are possible before the Pin is finally blacklisted. A stolen credit card number can also be used to set up Virtual PIN associated with an email address controlled by the attacker to carry out bogus transactions.

Lesson 25

VIRTUAL PIN PAYMENT SYSTEM

A Virtual PIN can become compromised as a result of eavesdropping and bogus purchases are possible before it is blacklisted. Stolen credit card number can also be used to set up Virtual PIN associated with email addresses controlled by the attacker to carry out bogus transactions. After every 90 days buyer's credit card account is billed for the charges that have accumulated and the merchant's account is credited accordingly. FV does accounting for merchant and buyer; therefore, it takes a commission per transaction according to its policy.

A

Advantages of the Virtual PIN Payment System:

1. Simplicity: No special software is required at the front end, making it easy for users to make payments.
2. No encryption: The absence of encryption simplifies the payment process and eliminates the need for complex encryption mechanisms.
3. Suitable for low-cost information items: It is ideal for

tem, which means that no special
em is good for low-cost information items.
/music etc. where the cost of the items is not
ual financial loss to the merchant if there is a
ation items are made in case of a fraud. On the
ss if the purchase relates to the actual physical
is that pre-registration of the buyer and the merchant with FV is mandatory in this set up. Moreover, maintaining a bank account (in case of merchant) and having a credit card (in case of a buyer) is also essential part of this system. One can say that the merchant side is less secured in the transaction because the goods are delivered by the merchant before the payment is actually received. The popularity of this payment system declined after 1998 mainly because of the introduction and development of encryption based payment mechanisms.

Centralized Account Payment Model

This is a popular payment system on the internet. In this both the payer (buyer) and the payee (merchant) hold accounts at the same centralized on-line financial institution. Over 20 payment systems use this approach e.g., PayPal, E-gold, Billpoint, Cybergold, Yahoo! Pay Direct, Amazon.com Payments etc. This model is shown in Fig. 1 below:

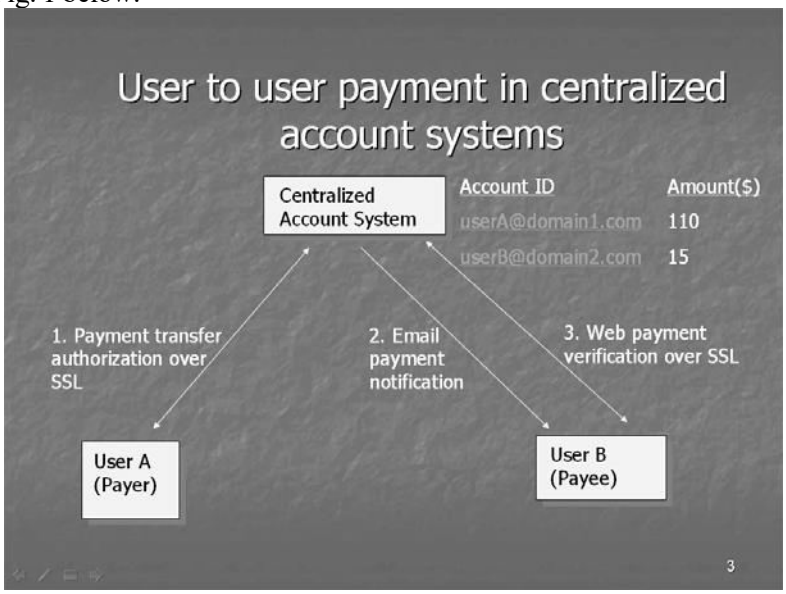

Fig. 1

On-line opening/funding of one's account is done in a centralized bank using credit/debit card or prepaid cards. To make payment an account holder is authenticated using an account identifier and a password, account identifier of the payee and the payment amountAll communication between the user and the bank is protected using **SSL (Secure Socket Layer)**, which is an encryption based protocol. The chosen account

identifier or the account ID is the one which is unique within the system against which the funds are lying in the online bank. Normally, the unique email addresses of the users are chosen as account identifiers. Payees are notified by email of the payment which they can confirm by viewing their account using SSL. A payee must open an account with the online centralized bank to receive the amount in case there is no such account already. In some payment systems which use this approach a question may be sent to the payee to verify his identity where the payer is not sure of that. For instance, Yahoo Paydirect allows a payer-specified question to be sent to the so called email of the payee. If the payer accepts the answer as proof of the correct identity of the payee the money is transferred otherwise the transaction is cancelled.

The centralized bank (depending upon its policy) charges a transaction fees either from the payer, or payee or both on funding an account or withdrawing funds from an account or receiving payments by the payee/merchant. This payment model requires that all participants must have their account with the same central payment system/bank. Note that the payee can eventually withdraw the money received in his account in the centralized bank through Automated Clearing House (ACH).

Electronic Checks

Financial Services Technology Consortium (FSTC) is a group of U.S banks, research agencies and government organizations formed in 1993. It has introduced the concept of electronic checks. An electronic check contains an instruction to the payer's bank to make a specified payment to a payee. Both, symmetric and asymmetric type of cryptography is used in this system. The payer and the payee are issued digital certificates in X. 509 standard format by their respective banks. These certificates are used to verify the digital signatures on the check. A bank may include account restrictions, maximum check value, or currencies allowed by the bank in the certificate

All individuals capable of issuing electronic checks will have an electronic check book device. An electronic check book device is a combination of secure hardware such as a smart card and appropriate software. A smart card is usually the size of a credit card having special software loaded on it. Information regarding secret/private key, certificate information and register of what checks have been signed/endorsed is normally stored in the smart card. Fig. 2 below shows the working of an electronic check in its typical format:

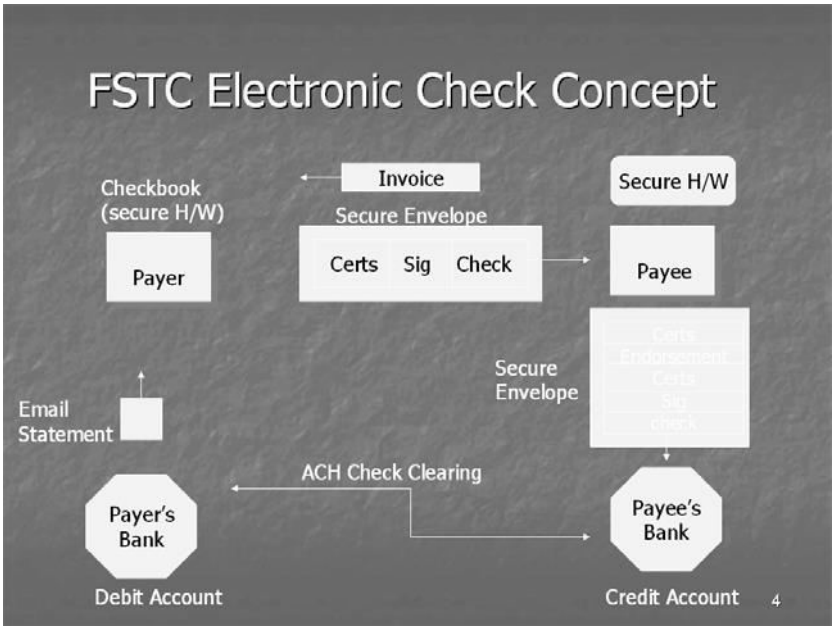

Fig. 2

A payer uses the electronic check book device in his computer system to generate a blank electronic check after filling the information regarding amount, date etc., and the electronic check is digitally signed by the payer through his private key. A certificate issued by the payer bank authenticating public key of the payer is also attached with the electronic check. This information is then sent to the payee in a secure envelope through email. A secure envelop is created when a user encrypts any information with a symmetric key, and

then that symmetric key itself is encrypted with the public key of the receiver. Accordingly, the payee, in this case, decrypts the secure envelop by first retrieving the symmetric key (by applying his private key), and then using that symmetric key to decrypt the information contained in the electronic check. The payee endorses (counter-signs) the check using some secure hardware device such as a smart card and forwards the check to the payee's bank in the form of a secure envelop. The bank clears the check with the help of traditional Automated Clearing House (ACH). Accordingly, the account of the payer is debited and the payee's account is credited. The banks send email statement to the respective parties.

Depending on the availability of processing infrastructure, there are four different scenarios for the processing of an electronic check. **These are shown below in figures 3-6. EFT stands for 'electronic funds transfer'.**

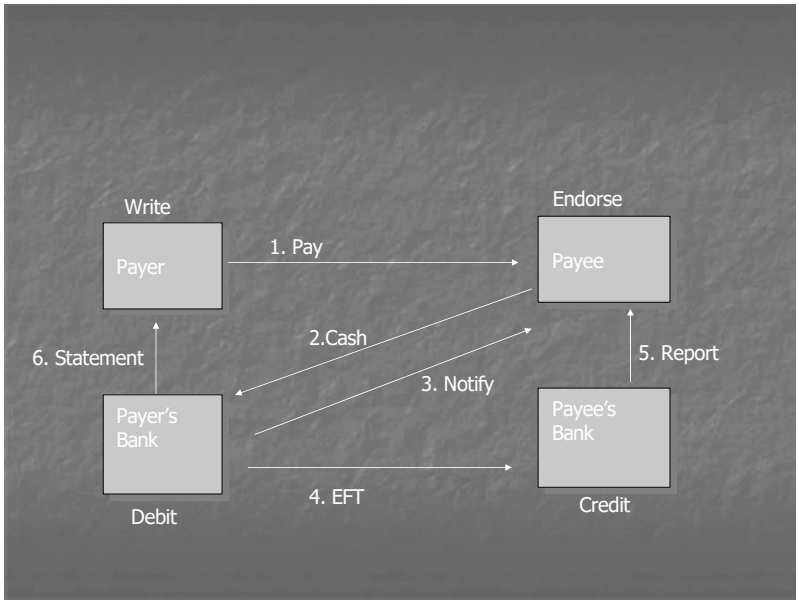

Fig. 3

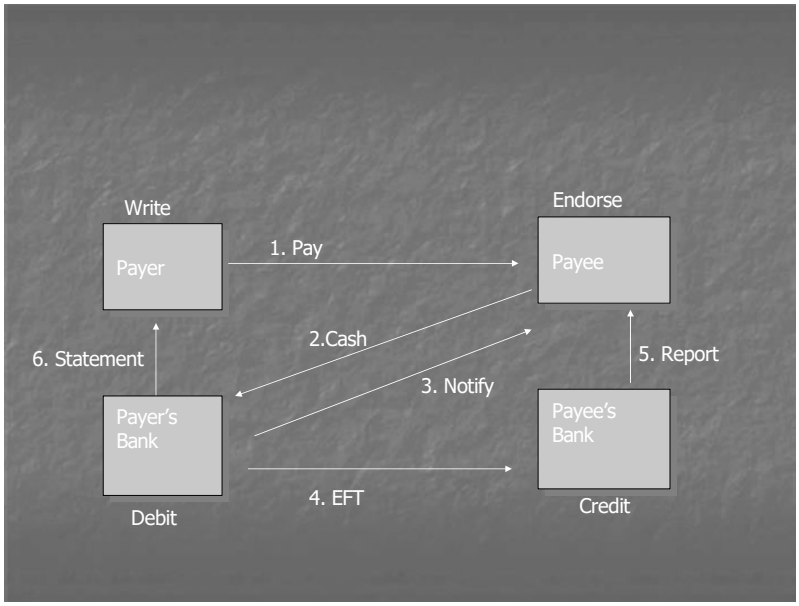

Fig. 4

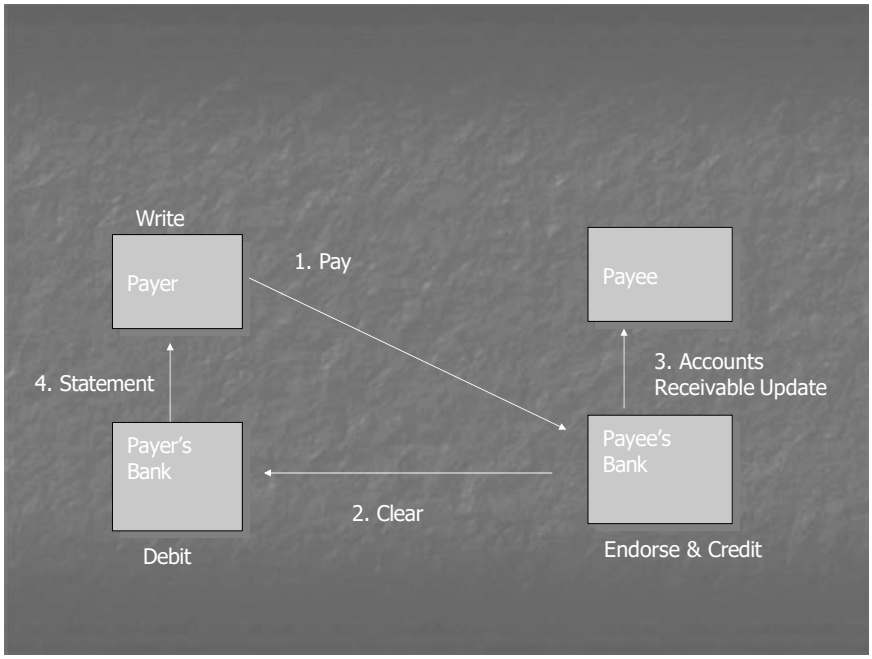

Fig. 5

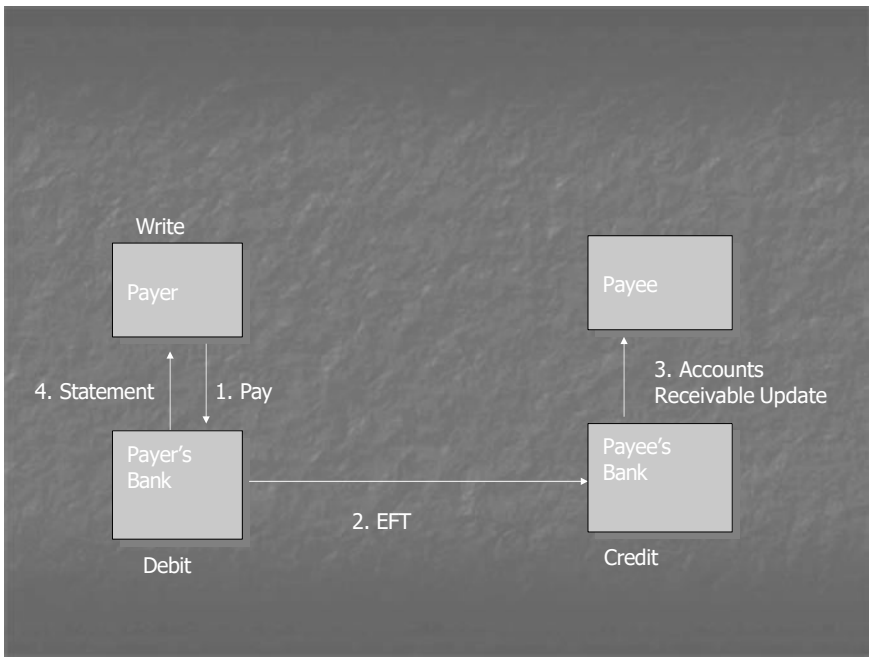

Fig. 6

Lesson 26

E-CASH PAYMENT SYSTEM

A company, DigiCash, has pioneered the use of electronic cash or e-cash. Anonymity of the buyer is the key feature of this system. There are three participants in it, namely, buyer, merchant and bank. Both, symmetric and asymmetric type of cryptography is used in this system.

Buyers and merchants, both, have accounts in the E-cash bank. Buyers withdraw coins against their account and store them in e-cash wallet software (Cyber wallet) on their computer. Cyber wallet stores and manages coins and records every transaction. Merchant forwards coins to e-cash bank which ensures that these have not already been spent and credits the account of the merchant.

E-cash Coins

The currency used in this payment system is called an e-cash coin or simply coin. A coin c elements or parts - serial #, key version and serial no. signed by the secret or private key of a certain denomination of the e-cash bank. In other words, a coin of one dollar would consist of the following:

Coin = Serial#, keyversion, $\{Serial\ \#\}SK_{\text{bank's \$1 key}}$

Each coin has a unique value, partly minted by the client and partly by the e-cash bank.

Minting of the coin

A long serial no. is randomly generated by the client's Cyber wallet in order to mint a coin. This serial no. is blinded, which means that it is multiplied with a blinding factor "r" and sent to the e-cash bank for signatures. Thus, the e-cash bank cannot see the serial no. it is signing. Key version (corresponding public k ey of the bank) is also part of the coin, and is sent usually at the time of account opening. A e-cash bank r ay have 1 dollar signature, 5 dollar signature or 10 dollar signature etc. If the client wants to mint a coin of 2 dollars then e-cash bank would use its private or secret key of 2 dollars to sign the serial no

How bank signs blindly?

. This blinding factor

It is used in the following mathematical expression which is sent to the bank for signatures.
Serial # . r^{e2} (mod m)
Public key of the bank consists of modulus 'm' and a no. 'e'. Bank signs with its secret key of 2 dollars (d2) such that:

(Serial #. $r^{e2})^{d2}$(mod m)=Serial#^{d2}.r^{e2d2}(mod m)
(Serial #. $r^{e2})^{d2}$(mod m)=Serial#^{d2}.r(mod m)

The product of e2 and d2 cancel out each other due the property of inverse relationship of keys. Bank cannot see serial # it is signing since it does not know 'r'. The expression "Serial#^{d2}.r(mod m)" is sent back by the bank to the client, who divides it with "r" to get the third part of a valid 2 dollar coin as follows:

Serail#^{d2}.r(mod m)/r=Serial#^{d2}(mod m)

Thus, minting of a 2 dollar coin is completed. In a similar fashion one can withdraw or mint coins of different denominations. E-cash bank signs the serial nos. and debits the account of the client. A client must maintain his account with the bank. So, if a client has $ 50 in his account with the e-cash bank and requests for the coins of a total value of $ 10, the amount left in his account after bank's signatures on the serial nos. would be $ 40.

Working of the E-cash model

Fig. 1 below shows the e-cash model:

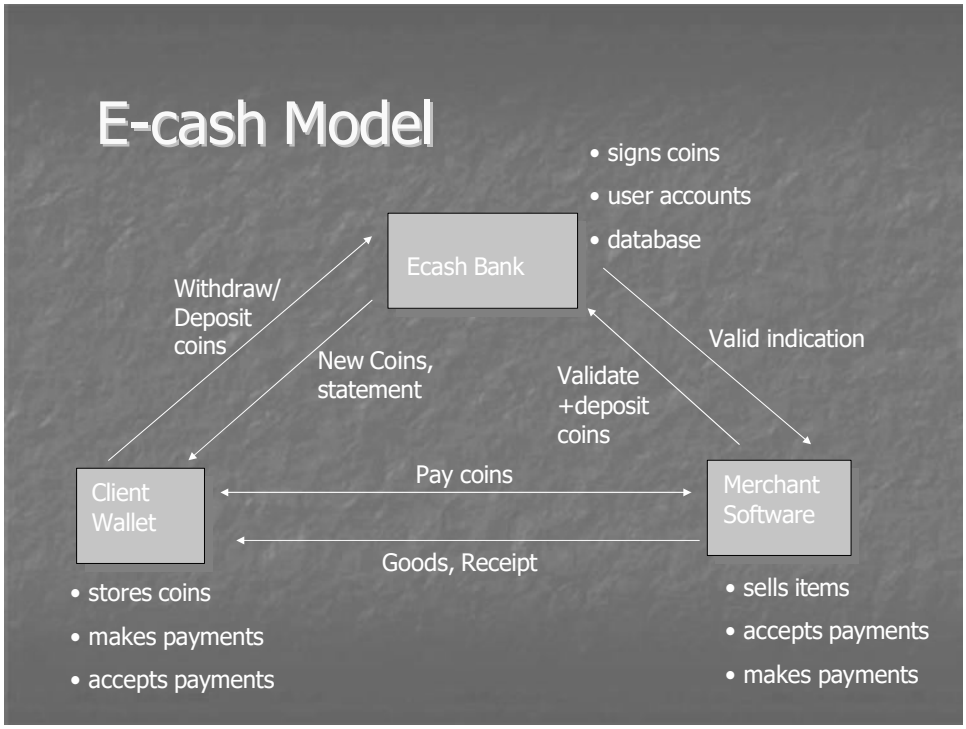

Fig. 1

Client wallet or cyber wallet can generate serial nos., store coins, make and accept payments. It can withdraw (get the coins minted) from the e-cash bank, and deposit coins at the payment stage to the bank. E-cash bank can issue new coins and send account statement to the client. On the merchant side, there is special merchant software. Thus, a merchant can sell items, accept payments from clients and also make payments. E-cash bank signs the serial nos., maintains accounts of the client and the merchant and also maintains a database in which the serial nos. of all such coins sent for payment are recorded. The client makes the payment to the merchant for the items bought. The payment is made through e-cash coins. Note that these coins are earlier got minted with the help of e-cash bank and remain stored in the cyber wallet. The coins are encrypted with the public key of the bank and are forwarded to the merchant for onwards deposit to the bank. The merchant cannot, therefore, view these coins. E-cash bank decrypts the coins using its corresponding private key and compares the serial nos. , thus revealed, with its database of spent coins to check the validity of the coins. If a revealed serial no. is not contained in the database, it proves that the coin is valid and unspent. The bank then sends the valid indication to the merchant and adds that particular serial no. in its database to prevent any chance of its being consumed in the future. The merchant then sends the goods and receipt of payment to the client.

Lesson 27

E-CASH PAYMENT SYSTEM

How anonymity is ensured in e-cash payment system?

Anonymity (یمانمگ) in e-cash payment systems ensures that the identity of the client/buyer is not disclosed. The system has two main stages: minting and deposit. Minting involves signing the serial number to provide a valid e-cash coin, while depositing coins for verification. The bank knows the serial number but has no clue about the specific client who sent them for payment purposes. This breaks the relationship between the client and the serial number at the minting and deposit stages to ensure anonymity.

The concept can be illustrated as follows:

Minting Stage:

A[illegible] client/buyer is not disclosed. Note that there are tw[illegible] and deposit stage. At minting stage the serial n[illegible]id e-cash coin. At this stage the bank knows as to[illegible]questing for the bank's signatures on the serial n[illegible]he blinding factor "r". On the other hand, the re[illegible] e-cash bank for checking validity). Now, bank k[illegible]nting stage) but has no clue about the specific c[illegible]ay have issued coins to many of its clients. It w[illegible]o amongst them has done the shopping and is making the payment now. Thus, by scheme, the relationship between the client and the serial no. is broken at the minting and deposit stage to ensure anonymity of the client. This concept may also be illustrated as follows:

Minting Stage

Serial number (unknown) Client (known)

Deposit Stage

Serial no. (known) Client (unknown)

Withdrawing Coins

Many coins of different denominations can be obtained in a single request to the bank.
The request is signed by the client with his private key and contains information about the serial nos. to be signed. The request is encrypted with a symmetric key and that symmetric key is encrypted with the public key of the bank, thus creating a secure envelope. The bank signs serial nos. in order to mint coins of requested denominations and forward them to the client/buyer.

E-cash Purchase

Having received an order the merchant sends a payment request to the client in the following format:
Payreq={currency,amount,timestamp,merchant_bank ID, merchant_accID, order description}

Cyber wallet automatically assembles the correct payment amount and pays.

Making the Payment

Coins used in the payment are encrypted with bank's public key, preventing the merchant to view them. Payment information is forwarded to the bank with encrypted coins during merchant's deposit. Only hash of the order description is included in payment information preventing the bank from knowing the order details.

Proving the Payment

Payer code is a secret generated by the client. A hash of it is included in the payment information so that client can later prove the payment if need be.

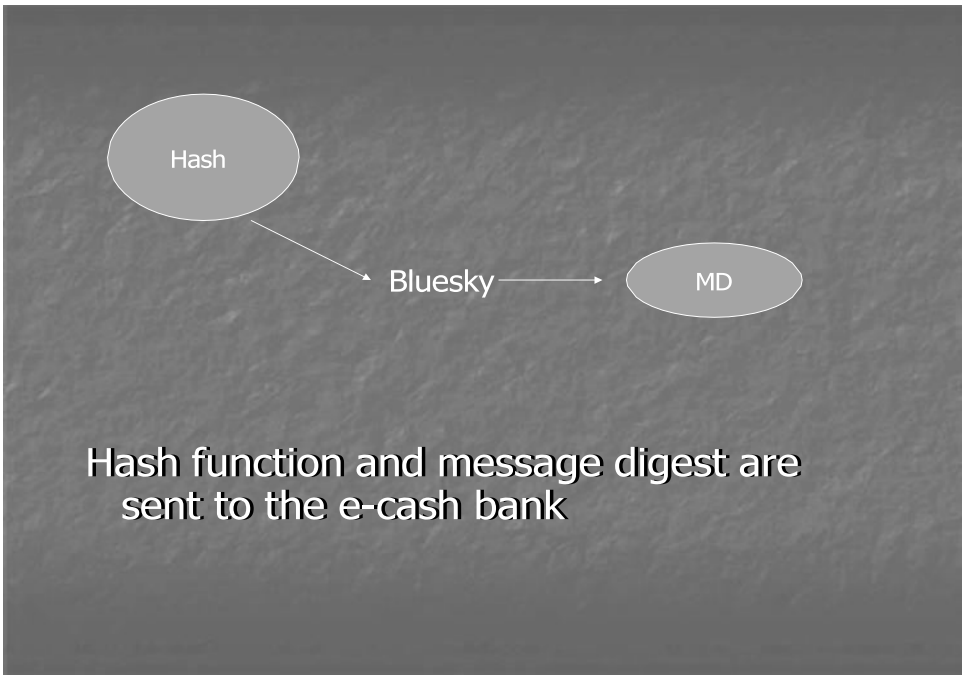

Fig. 1

For instance, the client may choose the word "Bluesky" as a code. By applying a hash function on this code, a message digest is obtained. Hash function and message digest are sent to the bank. In case a dispute arises and the payer has to prove that he had made the payment, he can forward the word/code "Bluesky" to the bank and request it to apply the hash function on it (which was earlier sent to the bank). If, on applying the hash function, the message digest comes to be the same as earlier available with the bank, it means that the person claiming to be the payer had succeeded in proving his payment, since only he was supposed to know the word "Bluesky".

Pa

Payment deposits are encrypted with a bank's public key and encrypted. E-cash banks check the validity of spent coins to prevent double spending. If valid, the bank credits the merchant's account. If the client sends valid coins worth $10, the merchant receives $100. The merchant can request the bank to transfer the amount to their acquirer bank via ACH, and the bank charges a commission for its services. E-cash banks play a backbone role in this system, charging a commission depending on their policy

A (anies the payment information. E-cash bank ma whether the coin is valid and whether it has alr erring to its database. If the coins are valid the ba sent valid coins worth $10 for payment to the me hen an amount of $ 10 would be added in his ac e-cash bank to transfer this amount in his ac ount with the acquirer bank. This can be done through ACH and the merchant can physically withdraw the money form the acquirer bank.

E-cash bank plays a backbone role in this set up and charges a specified commission for its services from the client and the merchant depending on its policy.

Lost Coins

In case network fails or computer crashes during payment transaction, coins might be lost. All signed blinded coins from last 16 withdrawals are sent by the bank to the client. Client uses the blinding factor known to its wallet to reveal the serial #. It then sends all serial nos. to the bank for its verification whether or not the coins have already been spent. After checking its database the bank credits the client's account with the value of unspent coins.

E-Cash & the Web

Fig. 2 below shows how e-cash payment system can be applied on the web:

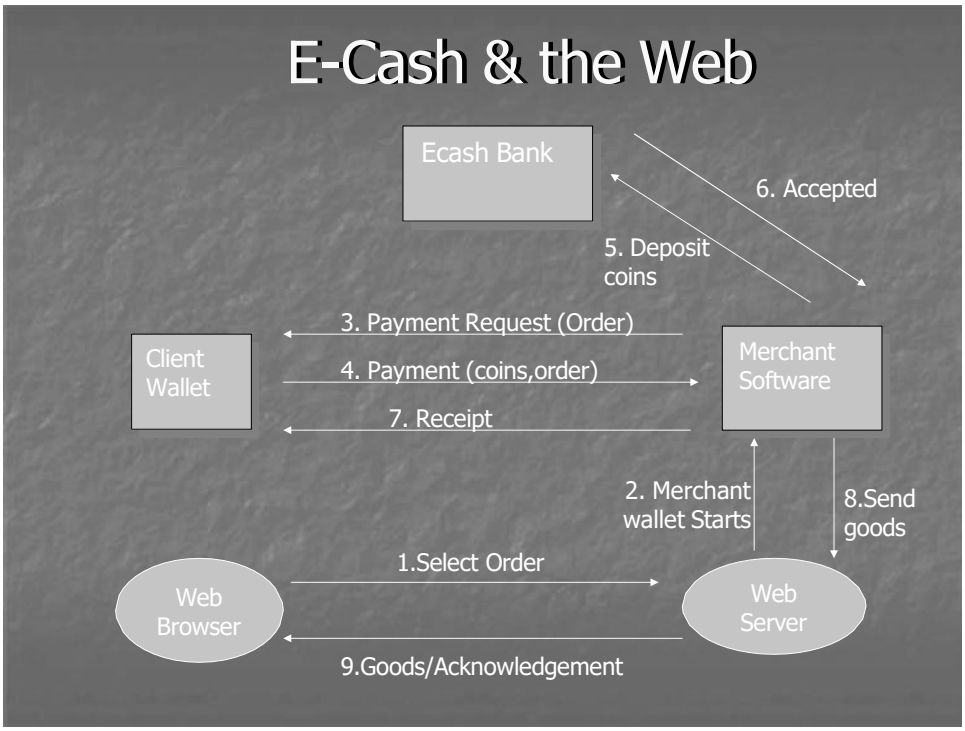

Fig. 2

[redacted]e. Web server software and merchant software are installed on the sever machine. A client selects an order and web server starts the merchant software/wallet **(steps 1 & 2**). Payment request is made by the merchant software and the client wallet pays through e-cash coins **(steps 3 & 4**). Merchant deposits the coins to e-cash bank for checking validity **(step 5)**. If the coins are valid an acceptance message is made to the merchant following which the receipt of payment is sent to the client by the merchant **(steps 6 & 7)**. Merchant software intimates the web server to send goods which acknowledges the fact to the web browser **(steps 8 & 9).**

Lesson 28

SECURE SOCKET LAYER (SSL)

s. SSL is built into many browsers. It operates at the TCP/IP layer of the OSI model, and uses a combination of symmetric and asymmetric cryptography. If there appears the word "https" in a URL, (e.g, https://www.microsoft.com) it indicates that the web server hosting this web site is SSL enabled. So, if a client machine is configured for SSL then any exchange of information between such a client and the web server would be in the encrypted form.
To configure a client machine for SSL following steps are required:

Internet Explorer:Tools menu->Internet options->Advanced tab-> Security (use SSL option can be checked)

SS

SSL handshake is a process that establishes secure communication between a client and a server during online transactions. They agree on encryption methods and authenticate each other. Once the handshake is complete, sensitive data like credit card information is encrypted and transmitted securely. However, a drawback is that merchants may store decrypted data, which can be a security risk.

SS ation methods. The combination of algorithms an to an SSL server, the SSL handshake begins, wh the strongest suite the two have in common. Th be used during the communication, selects cryptographic algorithms and authenticates the parties using digital certificates.
To start the SSL handshake process, a client sends a message to the server, the server responds and sends its digital certificate that authenticates its public key. The client (customer's browser) generates a secret symmetric key for the session. The client encrypts the secret key using the public key that it has just received and transmits it to the server. The server decrypts the message using its private key and now has the secret or symmetric key. Further communication between the customer's browser and the merchant's server can now be encrypted and decrypted using the secret session key.

SSL is commonly applied in online shopping as the customer puts in his/her credit/debit card information on the web form for payment purposes. If the web client and the server are SSL enabled, the SSL handshake would begin when the client enters the URL starting with "https". This handshake can be accomplished in seconds. The web form opens before the client. The client enters information in the text boxes of the form and on pressing 'submit' all such information is automatically encrypted with the agreed secret or session key. This secured/encrypted information travels across the internet and is retrieved by the server side where it is automatically decrypted with the help of same secret or session key. Even if someone intercepts the information, he cannot make any sense out of it because of encryption.

The greatest advantage of SSL is its simplicity. Since SSL is built into many browsers, no special encryption software is required either on the client or the server side. However, a drawback of SSL is that the merchant can store credit/debit card information after decryption that can be accessed by unauthorized parties from the merchant's database.

The process of SSL handshake is also explained in Fig. 1 below:

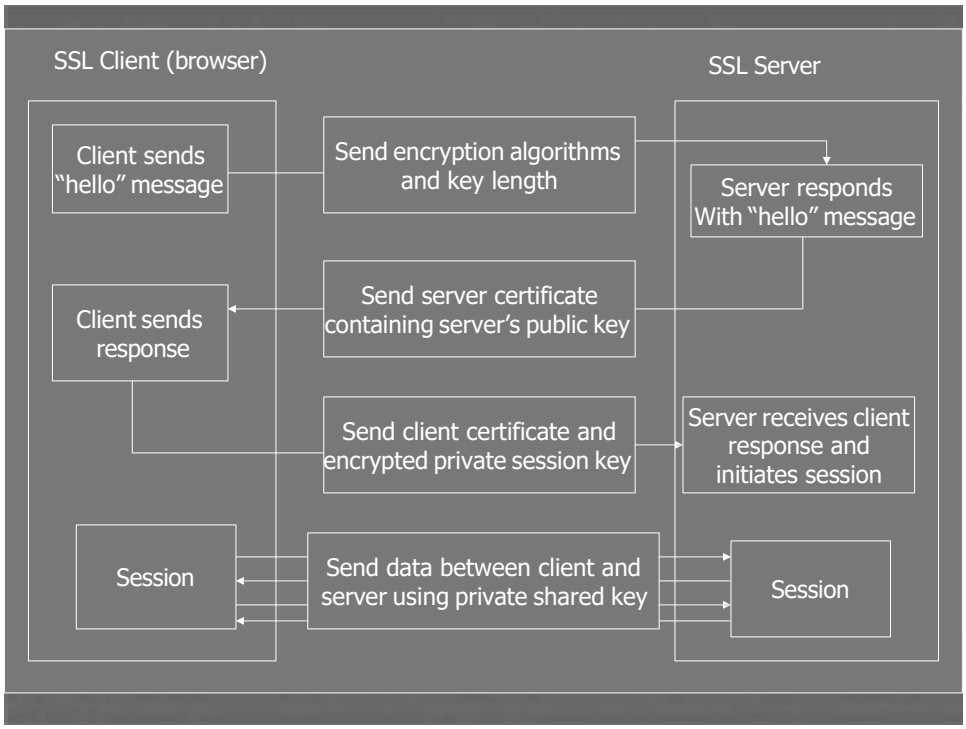

Fig. 1

Secure Electronic Transaction (SET)

The drawback in SSL that the credit card/debit card information remains with the merchant led to the development of a more sophisticated protocol called SET. It was developed in 1997 jointly by Visa, MasterCard, Netscape and Microsoft. There are four entities involved in a SET transaction – cardholder, merchant, and certification authority and payment gateway. The role of payment gateway is to connect entities on the internet with those which are not on the internet such as the electronic network of banks (see fig. 2 below). Payment gateway provides the security of data transmission to/from the acquirer bank. Merchants must have special SET software to process transactions. Customers must have digital wallet software that stores certificates and card information.

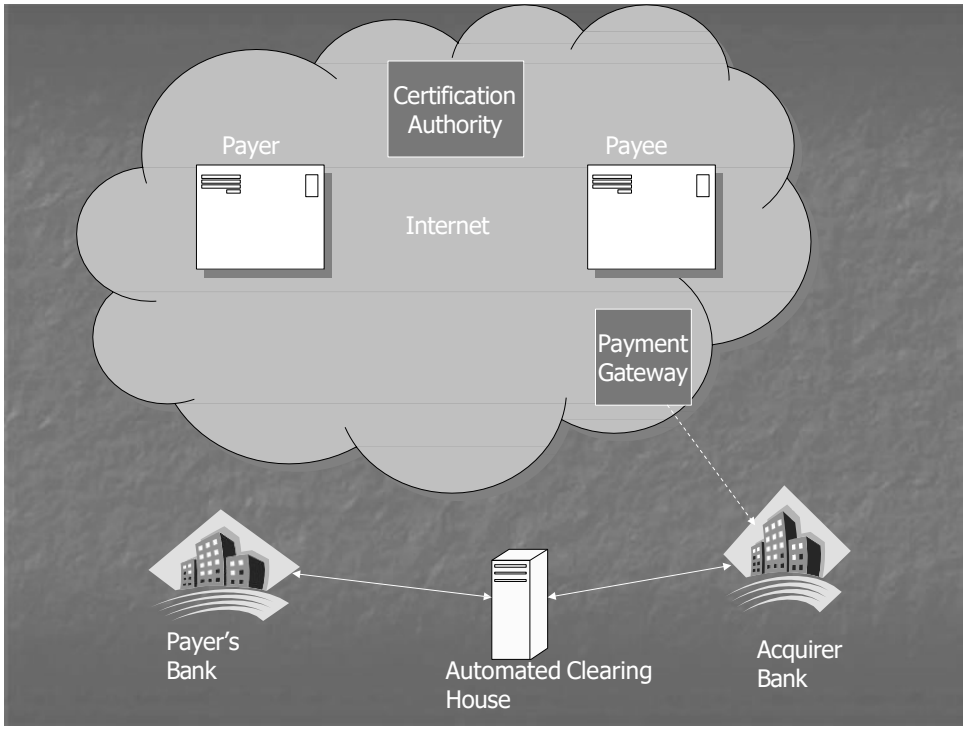

Fig. 2

D

In the SET (Secure Electronic Transaction) system, the dual signature scheme is used to protect privacy. It combines two message digests to create a new digest called the Dual Signature Message Digest (DSMD). This process helps hide the customer's credit card information from merchants and the order information from banks, ensuring privacy for both parties involved in the transaction.

In SET, the customer's order and account information are split. Message digests (MD1 and MD2) are

SI nts and hides order information from banks to **pr**

A digest is created by combining two message digests and creating a new digest called Dual **Si**. The following figure explains how the scheme of dual signatures is implemented in SET.

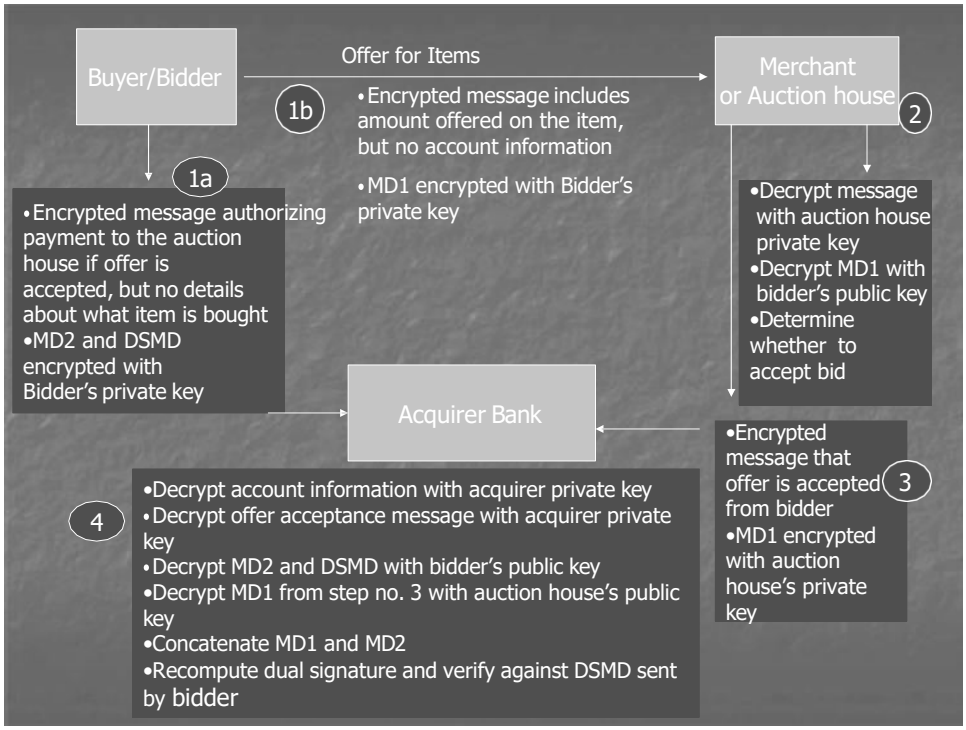

Fig. 3

SET software on the customer side splits the order information from the account information. MDI is the message digest obtained by applying hash function on the order information. MD2 is the message digest obtained by applying hash function on the account information. Both, MD1 and MD2 are concatenated and a third message digest, DSMD, is obtained by again applying the hash function on the concatenated message digests. The order information or the offer for items is forwarded to the merchant/auction house in an encrypted form along with its message digest (MD1) signed with the private key of the buyer/bidder **(step 1b)**. The merchant/auction house decrypts the order information/offer and verifies the signatures of the buyer/bidder through his/her digital certificate **(step 2)**. If the order/offer is acceptable to the merchant then the merchant signs the received MD1 with merchant's private key and sends it to the acquirer bank along with an encrypted letter of acceptance to the offer **(step3)**. On the other hand, the buyer sends the text based account information (credit card details) to the acquirer in an encrypted form. The buyer also sends MD2 (message digest related to account information) and DSMD to the acquirer bank signed with his/her private key **(step 1a)**. The acquirer bank decrypts this information. Mainly, the acquirer bank receives four pieces of information as follows **(step 4)**:

- MD1 from merchant/auction house related to order information
- Account information in encrypted form from the buyer
- MD2 related to account information from the buyer
- DSMD from the buyer

Acquirer bank concatenates MD1 and MD2 and applies the hash function to compute a message digest. Note that if this message digest is the same as the DSMD received by the acquirer, it ensures that a particular order information or offer is related to particular account information. At the same time, we have achieved our purpose that the order information should not reach the bank and the account information (credit card no. etc.) should not reach the merchant/auction house.

SETCo.

SETCo. is a company formed to lead the implementation and promotion of SET specifications It ensures that the vendors of SET software comply with the requirements laid down by its originators. A merchant holds certificate from card brand indicating that the merchant is authorized to accept credit card payment. The customer holds certificate from the card issuing bank. SETCo acts as a root certification authority in the certification hierarchy (see Fig. 4 below)

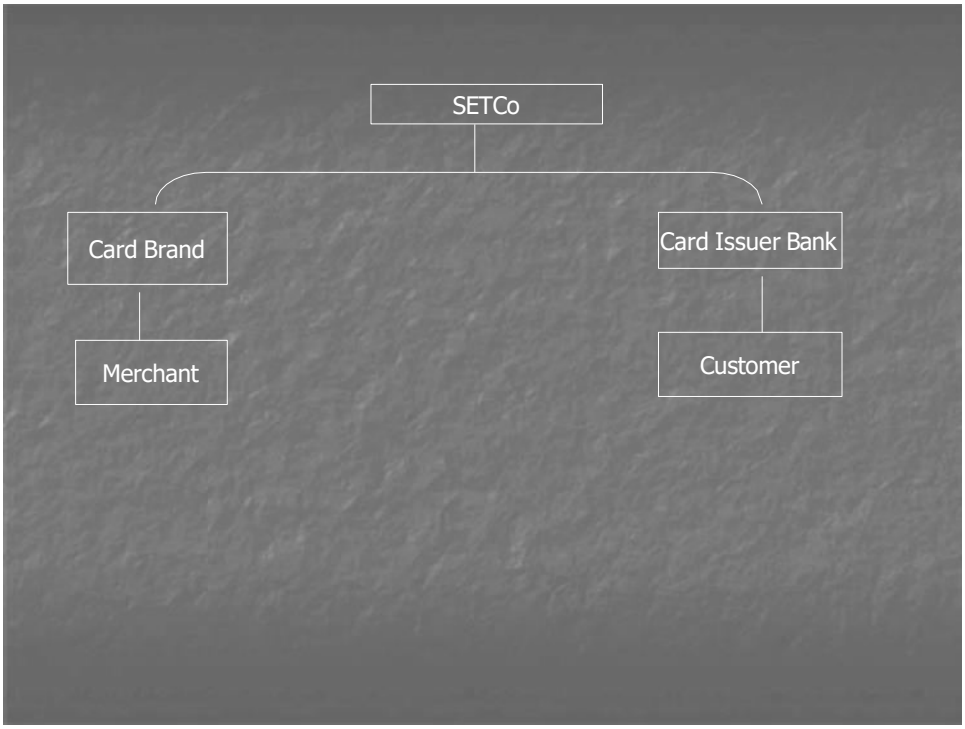

Fig. 4

SSL vs. SET

- SSL only handles secured transmission of credit card no. but SET is designed to handle the whole transaction in a secured manner using dual signatures.
- SSL is a general purpose protocol built into the browser, whereas SET requires software on, both, the client and the merchant side.
- SET uses a hierarchy of certificates for authentication.
- SET is complex and distribution of certificates is sometimes not stable.
- SET increases transaction cost.
- SET transactions are slower than SSL.
- SET uses a payment gateway for secured transmission of information.

E-Business

An e-business is defined as a company/entity that has an online presence. E-businesses that have the ability to sell, trade, barter or transact over the web can be considered as e-commerce businesses. An e-business model is defined by a company's policy, operations, technology and ideology.

Advantages of E-business

Some of the major advantages of an e-business as compared to a traditional business are as under:

- Personalized service
- High-quality customer service
- No inventory cost
- Worldwide reach of the business
- Electronic catalogues (convenient and quick transaction)
- Bulk transactions
- Improved supply chain management

Lesson 29

E-BUSINESS

Advantages of E-business

Some advantages of an e-business are given as under:

Personalized service

Product, place, price and promotion are generally recognized as the 4 P's of marketing in relation to traditional offline businesses. However, personalization is the 5th 'P' added to the other 4 P's when we talk about an e-business. In fact, the nature of internet technology is such that the information about the online customers including their buying behavior can be recorded in the databases. This information can be utilized by the e-commerce site to study the needs of a particular customer. Based upon that the site can do customization and provide a personalized service to the customer.

High-quality customer service

Customers can provide their feedback or register their complaints quite conveniently in case of online business as compared to offline business, and in light of that an e-business can improve its customer services.

No inventory cost

An e-business can have minimum overhead cost. You do not need to have any special physical place to start your business or hire any staff to operate the business as required in offline business. One can start an e-business as an intermediary or a middle man. In that case one does not require any warehouses for holding the inventory. An e-business can receive orders and get them fulfilled by procuring the ordered goods form open market without bearing the inventory cost.

Worldwide reach of your business

An online business has global reach. In a way people living anywhere in the world are potential customers of an e-business. Moreover, the e-commerce site is open 24 hours a day, so shopping can be done from there at any time.

Electronic catalogues

Electronic catalogues are used in case of an online shop. They have many advantages over paper catalogues. Therefore, online shopping can be done more quickly and in a more convenient environment.

Bulk transactions

One can do bulk transactions during one visit to an e-shop, since there is no limitation of collecting, packaging or carrying goods in contrast to shopping from a traditional offline shop.

Improved supply chain management

Typical members of a supply chain management are suppliers, manufacturers and end customers. If suppliers of raw material have online presence, the manufacturers can place emergency orders to them, which can be electronically/quickly processed on the supplier side. Thus, just in time delivery of raw material is possible without requiring the manufacturer to arrange for the accommodation to hold the inventory. Ultimately, the goods can be quickly delivered to the end customers due to the improved supply chain management.

Disadvantages of E-business

Some disadvantages of an e-business are given as under:

- **Less security**

The biggest obstacle in the growth of e-commerce is the issue of security. Internet is not a secured medium of communication. There are tools or options available to hackers whereby they can not only monitor but also control any data communicated over the internet. Particularly, people are not comfortable while providing their financial information (credit card no. etc.) online due to the fact that this information can be hacked and misused.

- **Less privacy**

The nature of internet technology is such that private information of the online customers can be easily collected and recorded on the server side. The buying pattern of a customer can be known to an e-shop with the help of certain sophisticated tools. You know that cookies can be used to track customers online. On one hand these technologies are useful for doing customization but on the other, they can be said to have caused the breach of informational privacy rights of a person.

- **No physical proximity with items purchased**

In certain cases the customers cannot decide about buying a thing before they can physically examine it. For example, a customer would ideally want to touch and feel the texture of a piece of cloth before buying. Similarly, a customer would actually want to smell a perfume before purchasing it. In the above or any similar case, people cannot expect to physically examine/test the thing while buying it online. Rather, they would prefer to buy such things from physical shops. An e-business has a limitation in this regard.

Online catalogues vs. Paper catalogues

Paper catalogs

Advantages

- Easy to create a catalog without high technology
- Reader is able to look at the catalog without computer system
- More portable than electronic catalog

Disadvantages

- Difficult to update changes in the product information
- Only limited number of products can be displayed

Online or electronic catalogs

Advantages

- Easy to update product information
- Able to integrate with the purchasing process
- Good search and comparison capabilities
- Able to provide timely, up-to-date product information
- Can provide broad range of product information
- Possibility of adding voice and motion pictures
- Cost savings
- Easy to customize

Disadvantages

- Difficult to develop catalogues
- Large fixed cost if used for small no. of products
- Need for customer skill to deal with computers and browsers

E-Business Models

Following are some popular online businesses that one currently finds on the web:

Storefront Model

It represents basic form of e-commerce where buyers and sellers interact directly. Merchants need to organize online catalog of products, take orders through their websites, accept payments in a secure environment and send items to the customers. They can also store and manage customer data in databases. A storefront model uses the shopping cart technology which allows customers to accumulate items they want to buy during shopping. This is quite popular in B2C transactions.

Auction Model

In this model there are auction sites to which the users can log-on and assume the role of a bidder or seller. As a seller, one has to specify the minimum price to sell one's item (called reserve price), the description of the item and the deadline to close the auction. At the end of the auction, the seller and the bidder are notified by the auction site and the payment mechanism and delivery mode is worked out. Auction sites charge commission on sales.

Online Banking

There is an online bank providing banking services to the customers through internet including services of electronic funds transfer.

Online Trading and Lending

Online trading is buying and selling of stocks/shares of listed companies using internet. Many brokerage houses have established an online presence. Online lending is providing loan through an internet transaction.

Online Recruiting

Employers can recruit and job searchers can search for jobs effectively through online recruiting web sites.

Online News Services

Many newspapers/magazines have online presence, providing 24-hour updates. Online publishing is attractive because printing and distribution costs are not involved in it.

Online Travel Services

One can make travel arrangements online without going to travel agent. It is convenient and less costly. There are online businesses which help customers find discount fares for airline tickets, hotel rooms and rental cars or assist in case of lost luggage.

Online Entertainment

Internet technology can quickly provide information with high quality multimedia. Therefore, such e-businesses have emerged which sell music albums, movie tickets, video films etc. The content can be easily downloaded by the customer in this case.

Online Automotive Sites and Energy Online

Certain web sites allow users to search and purchase new and used cars and their spare parts. Also, there are sites where buyers and sellers can buy, sell and distribute energy (oil, electricity etc.) on the web.

Selling Intellectual Property Online

Some e-businesses deal in the sale of intellectual property rights of companies such as patents, trade marks, trade names etc.

Online Art Dealers

Artwork can be bought from the web at a discount, e.g pictures, paintings, posters etc.

E- Learning

Universities and various training institutes are offering high-quality distance education over the web. E-books and other reading material can be easily downloaded to one's computer. Virtual University is an example of this type of business model.

Online Service Providers

These e-businesses help improve policies, procedures, customer service and general operations of other businesses. They can provide consultancy/professional services, for example, web site development services, online legal consultancy services etc.

Online Shopping Malls

Online shopping malls are those web sites which present customers with a wide selection of products and services at a single place. Thus, Instead of making several separate purchases, customers can use the mall's shopping cart technology to purchase items from many stores in a single transaction.

Portal Model

Portals are the web sites which provide chance to the visitors to find almost everything in one place. Horizontal portals provide information about a very broad range of topics. Search engine is the example of a horizontal portal. Vertical portals provide information pertaining to a single area of interest. Community Portals such as those related to medical or legal profession are the examples of a vertical portal. Online shopping is a popular addition to the some portals such as 'yahoo.com'. Portals allow users to browse independently owned storefronts unlike online shopping malls.

B

Brick-and-Mortar businesses are traditional businesses with physical stores, relying on face-to-face interactions.

Click-and-Mortar businesses are hybrid businesses with an online presence, allowing customers to shop online or visit a physical store for purchases

T es, respectively. Where a company is doing its b of lack of proper integration between the two d

Lesson 30

E-BUSINESS REVENUE MODELS

Experts have identified following revenue models on the web:

Web Catalogue Revenue Model

Though the goal of an e-business can be to reduce cost or improve customer service, however, the primary aim of most e-commerce sites is to generate revenue and earn profit. This is the most simple and common type of e-business model for generating revenue. This model would use electronic catalogue and shopping cart providing access to customers throughout the world. Businesses using this type of a model include online sellers of computers, electronic items, books, music, videos, toys, flowers, gifts, clothes etc. Payment received from customers is the source of earning revenue.

Digital Content Revenue Model

Web serves as a very efficient distribution mechanism of content. Therefore, one finds many e-businesses that offer different types of information services such as legal information, corporate information, government information, news and resources for academic libraries etc. These services can be customized by an e-business for different firm sizes depending upon their needs and usage pattern. Normally, a customer has to subscribe to such services by paying certain amount as subscription fee. This fee becomes the main source of generating revenue for the e-business. Instead of subscription fee, a credit card charge option can be made available for infrequent users. Online journals, newspapers, libraries fall under this category. Note that E-publishing eliminates high costs of paper printing and delivery of digital content is much quicker.

Advertising-Supported Revenue Model

In this model service/information is provided free of any charge to certain audience and the advertising revenue is sufficient to support the operation of the business and its cost. For example, Yahoo portal provides useful information and a search engine free of cost, but earns revenue through advertisements on its portal web site to bear the operational cost.

Advertising-Subscription Mixed Revenue Model

In this type, subscribers pay a fee and accept some level of advertising. Thus an e-business can earn its revenue from both the sources, that is, through subscription and advertisements. On web sites that use this model, normally, the subscribers are subjected to much less advertising than they are on advertising-supported sites. For instance, in case of certain online newspapers, a customer has to pay subscription fee for certain services/information whereas some services are free of charge as they are supported by advertising.

Fee-for-Transaction Revenue Model

There are businesses offering services for which they charge a fee based on the number or size of transactions they process. The business provides information to the customers which is required to complete a transaction and revenue is purely earned on that basis. For example, online travel agents receive a fee for facilitating a transaction that includes the making of travel arrangement for their clients, as well as, advising them about lodging, transportation etc. Stock brokerage firms also use this model as they charge their customers a commission for each transaction of stocks/shares executed through them.

Fee-for-Service Revenue Model

This model does not relate to services provided by agents or brokers to complete a transaction (the above case). Rather, the fee is charged on the basis of value of some service rendered. Professional services provided online by lawyers, doctors, accountants etc. relate to this type of revenue model. E-businesses that provide online entertainment and online games are also the examples of this type. In case of online games,

visitors pay to the business either by buying and installing game software on their computers or by paying a subscription fee for playing online for a limited time. This earns revenue for the business.

Internet Marketing

Internet has opened a new door of marketing opportunity to the marketers. Consequently, a new branch in the field of marketing has developed very rapidly in the past few years known as internet marketing or e-marketing. This topic can be covered under following main headings:

- Market Segmentation
- E-mail Marketing
- Banner Advertising
- Promotions
- Public Relations
- Partnering
- Customer Relationship Management
- Creating Brands on the Web
- Affiliate Programs
- Search Engines
- Global marketing

Market Segmentation

Businesses need to identify specific portions of their markets in order to target them with specific advertising messages. The practice called market segmentation divides the potential customers into segments or groups. Segments are defined in terms of demographic characteristics such as age, gender, marital status, income level and geographic location. For example, unmarried men between 19-25 years of age may be called one segment. Traditionally, marketers have used three types of variables to define three different market segmentations, namely, geographic segmentation, demographic segmentation and psychographic segmentation.

Geographic segmentation

In this type, c . For example, urban and rural customers can be the two segments on the basis of geography. Different marketing plan would be required for each segment.

Demographic segmentation

Here segmentation is done on the . Customers belonging to different age groups may have different product requirements. This type of market segmentation helps in identifying those requirements of different groups of customers.

Psychographic segmentation

Here . For example, a car manufacturing company may direct advertising for a sports car to customers who have a particular life style and like thrill in their lives.
Variables used in different segmentations can be combined. So, income level can be combined with location to create a particular segment.

Market Segmentation on the web

Note that the concept of market segmentation is equally applicable to e-businesses as it applies to physical businesses. Moreover, one can easily provide a particular sales environment in case of an e-business as compared to offline business. In a physical store, one cannot easily change the environment for different

customer segments. Therefore, display options, lighting, music, sales persons remain the same for all customers groups in a physical shop. However, web gives opportunity to present different store environment online to different customer segments. So, a web site may have a web page for children with the right kind of web design for children, and have a different web page designed exclusively for the old people. In other words, web can easily and usefully provide separate virtual spaces for different market segments. Some web retailers allow their customers to create their own product. For example there are computer companies online that allow their customers to choose component of a computer to configure their own computer according to their need. This is called one-to-one marketing.

- **Behavioral segmentation**

Creation of separate experiences for customers based on their behavior is called behavioral segmentation. Three identified behavioral modes of the customers on the web are:

– customers who just browse through the site with no intention of buying
Buyers – customers who are ready to buy right away
Shoppers – customers who are motivated to buy but want more information

An e-business site should devise right combination of marketing strategy to lure visitors in different behavioral modes to become its customers.

- **Choosing a Domain Name**

Choosing a suitable domain name is the first thing to be considered at the start of an online business. Due to the worldwide nature of the web, choose a domain name that people coming form different countries/cultures will be able to recognize, remember and type easily.

- **Marketing Research**

It consists of interviews, paper and phone surveys, questionnaires, findings based on previous investigations etc. to find strengths and weaknesses of your business and the business of your competitors. It also includes the analysis of opportunities and threats to your business. In case of e-businesses, marketers have a faster option to find/analyze information about the industry, customers or competitors, because the information is just a few clicks away. This kind of marketing research can be extremely beneficial for the success of an e-business.

- **Web design**

Basically, the only site. So, a good web design is another very important factor for the success of an e-business. Note that in online environment the competitors of an e-business are just a few clicks away, so if your web site design is not catchy or useful enough the visitors might not wait and immediately switch to a competitor's site. The cost of switching to competitors site is also very low in online environment. All this makes e-commerce very competitive. An internet marketer should particularly pay attention to the following considerations as regards web site design:

Easy site navigation – give a site map
Frequently asked questions (FAQs) section
Conveniently located contact information
Multimedia – use streaming video and audio – be aware the time each element takes to get loaded
Privacy policy – outline the policy about intended use of customers personal details
General outlook of the web site should be attractive making it sticky

Lesson 31

E-MAIL MARKETING

E-mail marketing campaigns are cheap and effective way to target potential customers. E-mails can instantaneously convey a marketing message to customers at distant areas. Personalized direct e-mails target customers with specific information – name, right product at the right time, special promotions etc. When your e-business is doing global marketing, e-mails can be first translated into proper languages as a personalization measure using specific translation software. Personalization technology (data mining) can also improve response rate tremendously. Where an e-business lacks resources for doing e-mail marketing on its own, it can outsource such campaign to outside firms. For instance, outsourcing services should be used when direct e-mailing becomes too difficult to manage and there is inadequate staff or technical support at the e-business level itself.

E-mails can be used to improve customer service by adding an e-mail link to your web site. Thus, you can receive your customers' complaints through e-mails. It should be ensured that your e-business is capable of handling expected volume of e-mails; otherwise it can bring poor reputation to your business when you receive complaints through emails but are unable to respond. Another advantage with emails is that they can be automatically sorted and sent to the relevant persons. E-mails can be used to inform customers about their order/shipment status etc. Internet mailing lists can also be conveniently used to send targeted personalized emails. You can also provide the "opt-in e-mail" option to your customers on your web site. If they opt for it, this means that they want to receive through email any product information, offers or promotions etc. in the future. Spamming is a term used to refer to mass e-mailing to customers who have not expressed any interest in a specific product or service. In different countries, spamming has been declared as an offence. E-mails can be combined with traditional direct marketing. Telemarketing (live interaction through telephone) and e-mails can be combined to reach prospective customers. Similarly, direct mailing and e-mails can also be combined.

Promotions

E-business promotions can attract visitors to your site and induce them to purchase. Promotional messages can be sent both online and offline. Some popular promotional methods are as under:

Frequent-flyer miles

The online business has a contract with an airline such that the customer of the business earns specific miles from the airline free of charge if he purchases from the online business items up to a certain value.

Point-based rewards

On the performance of a pre-specified action, customers can be entitled to point-based rewards – t-shirts, mugs etc. with the company's logo etc.

Discounts

Discount advertisements through magazines, newspapers, web sites etc. can attract new and repeat customers.

Free-trials

Customers can sign up for a free service. For example, they can be allowed to download software for certain days free of cost on trial basis before buying it.

Free shipping

Shipping cost may not be charged on the delivery of certain items as an incentive for the customers.

Coupons

Online coupons are placed on certain popular sites to attract customers for online shopping. They can use these coupons for shopping through specific web sites.

E-Business Advertising

Advertising is an attempt to disseminate information in order to effect a buyer-seller transaction. It is an impersonal and one-way mass communication paid for by the sponsors. Televisions, movies, newspapers and magazines are traditional ways for e-business advertising. On the other hand, Telemarketing and Direct marketing are attempts to personalize advertising in order to make it more effective. For e-business advertising it is important that your brand is unique and easy to remember. Publicizing URL on direct mails or business cards can increase brand awareness.

Banner Advertising

. These advertising messages are placed on popular web sites (host sites) which are frequently accessed and thus those who access a host site can look at the banner/advertising message and come to know about the brand/business which is advertising itself through the host site. The host site charges certain fee for providing space to the banner on its web site and thus generates income/revenue. This concept therefore is mutually beneficial for both the parties. Banners have different sizes and are placed on different positions on the web site. Banners can be simply for viewing as well as having link to the home page of the product or service. Business logo on a banner may increase brand recognition. Flashing, scrolling text, pop-up boxes and color changes grab viewer's attention. So, these techniques can effectively be used for creating a banner. As a marketer you should note how many ads the host site already carries. Also, note which position has a better chance of click through. There can be specific times for banner advertisement. Banner advertising space can be expensive for peak traffic times. Exchanging banners with another site is also an option. Some sites carry banner ads for free. For example, a business selling computers can host the banner of business selling computer books free of charge. These are related businesses which support each other so there can be an indirect benefit to the computer business for carrying the banner of computer books business in the sense that the latter is likely to spread more awareness about computers.

Advertising payment modes

Following payment modes can be accepted between the parties:

Monthly charges for online advertising
Cost per thousand (CPM) – fee for every thousand people viewing the banner
Pay-Per-Performance that includes:
Pay-per-click – fee according to no. of click to your site
Pay-per-lead – pay for every lead generated from the advertisement
Pay-per-sale – pay the host for every sale resulting form a click through
Exchanging advertising space on your site for advertising space on another's site

Note that the log file of the web server where the advertising web site is hosted contains a column in which the IP address of top-referring web site is recorded. Thus by studying the log file it can be found that how many visitors were diverted to the advertising site from the host web site (top-referring web site).

Web casting

Web casting is a term used to refer to internet-based broadcasting of audio and video content. It can provide two-way communication between the broadcaster and the listener or viewer. Marketers should consider some people may have slow internet access. Video conferencing is an example of web cast ing. For example, using this technique, doctors sitting in China, England and Pakistan etc. can, in real time, exchange and benefit from each other's ideas as if they are physically holding a meeting.

Interactive Advertising

It uses a combination of rich media (such as audio, video, animations) and traditional forms (such as print, TV or radio ads) in order to involve customers in advertising process to increase brand recognition. For

example, there is a famous business that uses this marketing technique. Its TV commercial induces/encourages viewers to access its website from where customers can select/download various action pictures and background music. Thus, by involving a customer in the advertising process itself, it attempts to increase its brand recognition for the customers.

E-business Public Relations

Public Relations (PR) keeps the customers and employees of a business current or updated as regards information about products, services and internal and external issues such as any promotional activities, new products, customer reactions etc. Following different modes can be used to disseminate information:

- Press releases
- Speeches
- Special events – seminars, video conferencing etc
- E-mails
- Chat sessions
- Bulletin board – people can post comments
- Presentations/exhibitions

P and other important news to the press or media via internet. There can be a press release section of your online business which can be accessed through a hyperlink. Moreover, video clips of news appearances, speeches, commercials can also prove to be an effective way of publicity.

Lesson 32

CUSTOMER RELATIONSHIP MANAGEMENT (CRM)

The sum of a company's customer service solutions constitutes its customer relationship management (CRM) system. Level of traffic at the online business site and the available resources would normally d provides fast and effective service to customers a CRM includes call handling, sales tracking and T s can be used to improve customer service, that is stem, call centers can be set up having customer s e-mails or online chatting. There are software t many number of internet users actually viewed a b cked on the advertisement. Log files consist of d each visitor's location, IP address, time of visit, f services of analyzing web log files. The results would show how effective your web site is and indicate the top-referring web sites. You know tha cookies allow e-commerce sites to record visitor behavior. They can be used to track customers online and do personalization. Many customers do not know that their information is being collected and used by the e-business site. Thus, informational privacy rights of customers can be breached in cases where cookies are used.

CRM is the collection of customer service solutions in a company. It provides fast and effective service, including call handling, sales tracking, and transaction support. Tools like log file analysis, cookies, and data mining improve customer service. CRM includes call centers with representatives accessible via phone, email, or chat. Feedback on ad views and clicks can be obtained. CRM aims to establish lasting customer relationships, build loyalty, and trust. Loyalty develops through five stages but can decline in the fifth stage, leading to relationship termination. Maintaining strong customer relationships is crucial for long-term success.

One major goal of CRM is to establish a long-lasting relationship between a company and its customers. Good customer services can help in building a sense of loyalty towards company and its products or services. Experts have pointed out five stages of loyalty as customer relationships develop over a period of time. One can find that the intensity of relationship increases as the customer moves through the first four stages. In the fifth stage a decline occurs and the relationship terminates.
See Fig. 1 below:

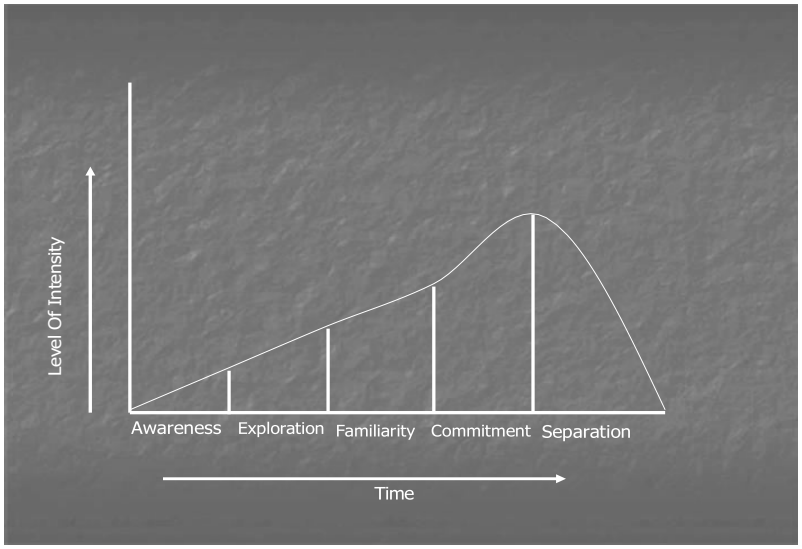

Fig. 1

Let us briefly examine these stages:

- **Awareness**

This is the first stage where customers recognize the name of the company or any of its products. However, they have never interacted with the company before . A company/business can achieve this level by properly advertising its brand.

- **Exploration**

At the exploration stage the potential customers know more about the company or its products . For instance, they may havevisited the web site of the company and have exchanged any information with it.

Familiarity

At this stage, customers have completed several business transactions with the company and know its policies regarding refund, privacy of information, discounts etc.

Commitment

Having completed a number of satisfactory transactions, some customers may have developed a strong sense of loyalty or preference for the products or brand of a company. They are said to be at the commitment stage in their relationship with a business. Such loyal customers often tell others about their satisfaction as regards products/services offered by the company. Sometimes, companies make concessions on price or other terms of business to bring customers into this stage.

Separation

After a period of time those conditions over which a valuable customer relationship is established might change. Customers might not be any longer satisfied with the product quality or customer service. On the other hand, a company may also find that a loyal customer is proving to be very expensive to maintain. Thus, the parties enter into the separation stage. Note that the objective of any marketing strategy is to bring the customers quickly to the committed stage and try to hold them there as long as possible.

Life Cycle Segmentation

These five stages are also called customer life cycle. Using them to create groups of customers is called customer life-cycle segmentation. Segment information is useful for companies to develop better relationship with the customers. Companies, thus, know about their customers and their level of relationship with the company, and can customize their product/service.

B

In B2B marketing, there is no direct contact with end users, unlike B2C. This limits the feedback and requires a different marketing approach, focusing on building strong client relationships and providing tailored solutions.

F egration between different steps in a customer tr , front-end and back-end operations should be fu

Key difference between B2C and B2B is that in case of B2B there is no direct contact with the end users, whereas this contact exists in B2C. Thus, an e-business can have direct response or feedback from its customers in B2C as compared to B2B. For example, an online business that deals in the supply of raw material to an online manufacturing business has a very limited chance of receiving direct feedback from end customers about its product/services due to lack of contact with them. That is one reason why a marketing plan is different in B2B from B2C.

Search Engines

A search engine is a program that scans web sites and forms a list of relevant sites based on keywords or other search-engines ranking criteria. It allows people to find information about their area of interest out of large amount of information available on the internet . Examples of famous e-businesses that provide search engine facilities are googl , altavista, yaho etc. As a marketer, after you have launched your e-commerce web site, you should look for the registration of the same with popular search engines so that your site appears on search engine results.

Lesson 33

META INFORMATION

Meta tags contain key information about a web page used by search engines to locate and rank websites. By submitting Meta information to search engines, websites can improve their visibility. Different search engines have their own ranking criteria, and sites with matching keywords and higher frequency in Meta information are ranked higher. Misusing competitors' Meta information to improve ranking is unethical and can be considered passing-off, an offense in many countries.

You know that a search engine to locate and rank the web site. You provide your Met prescribed registration fee and get your site registered with the sear information in its database. When a searcher types key words in the are matched with the Meta information recorded in the database of

Different search engines have different ranking criteria. Normally, those sites are ranked at the top by the search engine software where maximum keywords typed by the user match with the recorded Meta information of the site, as well as, such words appear in greater frequency in the Meta information. Some search engines search the entire internet each time. Many search engines rank the site by using a program called 'spider' which inspects the site before ranking. You know that one can view Meta information of one's competitor's web site. This information can be incorporated and misused by an e-business in its web site representing that to be its Meta information. Thus, such a business can improve its ranking on search engines by capitalizing upon the reputation of the business whose Meta information it actually is. In many countries, stealing and misusing Meta information in this manner to gain business/competitive advantage is considered as an offence known as the tort of passing-off.

Partnerships

Partnering means to form a strategic union with another company/business for mutual benefit or profit sharing. Partner businesses can provide complementary services and products to their customers and thus benefit each other. For example an e-business selling computer science books having a link to an e-business selling computers and vice versa can enter into a partnership for mutual advantage. Competitive advantage to both the businesses in this arrangement is that the customers are a link away from buying a complementary product/service. Thus, a person buying a computer from one site can be induced to buy computer science books from the partner's web site. Moreover, partners can exchange technical research or customer information. They can help each other in improving respective management or operations. Outsourcing a job to a partner can also be useful.

Affiliate Programs

An affiliate program is an agreement between two parties that one will pay the other a commission based on a specified customer action. It is not a strategic union as is partnership. Rather, it is for limited purpose and time. Banner advertising is the example of an affiliate program.

Branding

A . You can say that it is the trade name/symbol that reminds customers about the reputation of a company regarding its products or services.

Elements of Branding

Researchers have identified three elements of branding, that is,

- Differentiation
- Relevance
- Perceived Value

- **Product differentiation**

Product differentiation is the first condition to be met in order to create/establish a product/service brand. It means that a company must clearly distinguish its product from all others in the market in some significant way so that the product/service is different from that of its competitors. For example, you can

create/establish your brand on the basis that the soap manufactured by your business is unique in the market in the sense that it does not dissolve quickly in water.

Relevance

Relevance means to what degree is the product/service useful for potential customers. For example, you may have designed very distinguished jewelry but very few people use or purchase the same. In fact, it may prove to be too costly for most people to buy. Note that your product/service should be capable of easily relating itself to the people.

Perceived value

A product/service may be different and relevant (customers can see them using it), still they would not buy unless they find some perceived value in it. For example, a restaurant may be selling a unique dish that relates/associates itself to the taste of majority of people; still they may not be inclined to buy it because of certain negative associations, such as its high fat content.

Thus, to create or maintain a brand the above three elements have to be fulfilled.

Emotional branding vs. rational branding

Emotional Branding: Creating a brand image or connection with customers based on emotions and feelings. It is commonly used in traditional media where the audience is more passive.

Rational Branding: Focusing on logical and practical aspects of a brand to appeal to customers. It is often used in online marketing where customers have more control and can easily navigate away from emotional appeals.

Note that transferring existing brands to the web or using the web to maintain an existing brand is much easier and less expensive as compared to creating an entirely new brand on web. One common way of popularizing the brand of a business on the web is to provide its URL on product packaging, advertisements on TV or print media etc. One can also combine the URL with logo of a company on brochures, visiting cards etc. in order to popularize the brand.

Global Marketing

As a marketer, when you are , you have to keep certain considerations in mind. Your web design must provide content in various languages and provide prices in various currencies, so that people belonging to different countries/cultures can understand the information contained in your web site. A regular display of currency exchange rate information can be useful in this behalf. Today, tools exist that can translate emails and your web sites into different languages. Another important consideration should be as to whether the country where you are doing the business has the required infrastructure to support your e-business. For example, whether you have a proper distribution channel of your products in a country you are doing business in. Similarly, you should carefully choose a payment system for your e-business which is compatible with the environment of a country where you are doing business. For example, a payment mechanism using SET cannot be considered as compatible with business environment in most of the third world countries.

Lesson 34

DATA MINING

Data mining is the process of discovering patterns in large amounts of data, enabling businesses to identify customer behavior and target them with personalized messages. For example, a shopping store can use data mining techniques to identify demographic profiles and preferences for computer-related items. This information can be used by marketers to focus their marketing efforts on these individuals, saving time, energy, and mailing costs

Data Mining can be
where the data can be stored in databases, data warehouses, or
Data mining has a lot of business application in today's wo
customers and can effectively target them with personalize
Assume that there is a shopping store where the data
recorded/stored over a period of time. Using a data mining
pattern can be generated that can provide useful information
people having a certain demographic profile (age over 20 years and sex male) coming from a particular location have shown inclination to buy computer related items. It is an interesting clue for the marketers. In case there is a computer related item that is to be marketed in future, then marketing effort in this behalf should be focused on such persons instead of sending marketing messages at random. In other words, persons indicated by the pattern are the ones who are likely to respond to this kind of marketing initiative. Thus, if a company follows the pattern it can save time, energy and mailing cost.

Data warehouse

A data warehouse is a repository for long-term storage of data from multiple sources, organized so as to facilitate the management for decision making. Fig. 1 below shows how data collected at different sources is cleaned, transformed, integrated and loaded in a data warehouse from where it can be accessed by clients for data mining and pattern evaluation.

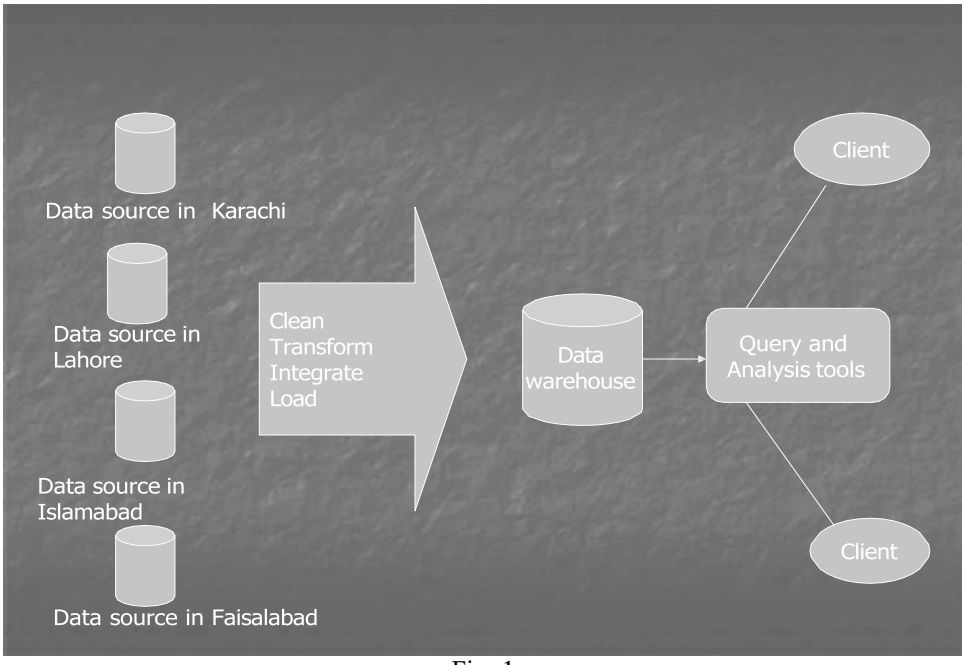

Fig. 1

Knowledge discovery

A knowledge discovery process includes data cleaning, data integration, data selection, data transformation, data mining, pattern evaluation and knowledge presentation.

Fig. 2 shows the knowledge discovery process:

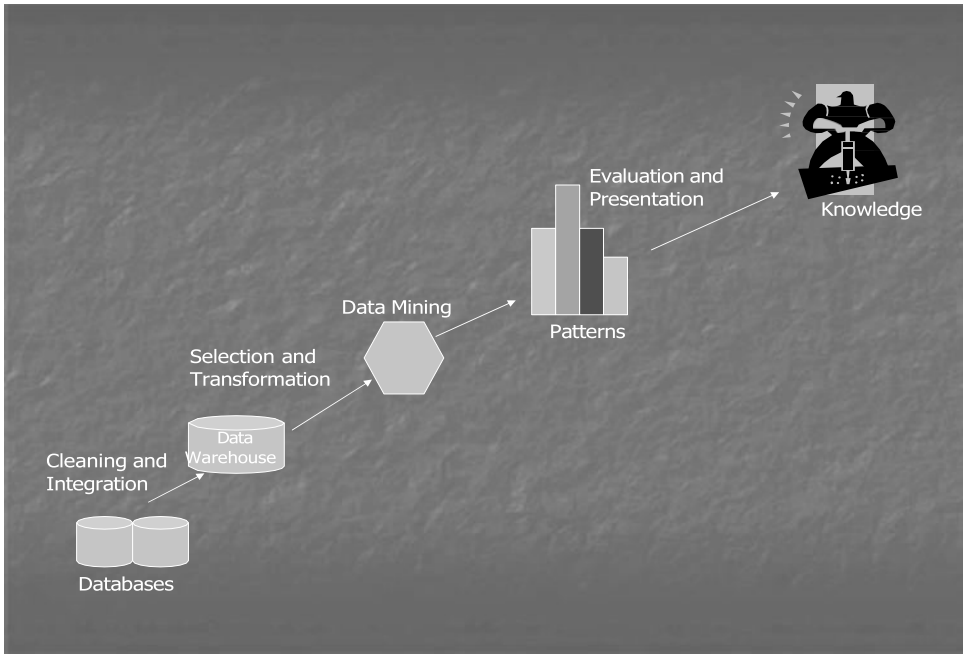

Fig. 2

Note that data mining is a step in the overall knowledge discovery process. Data must be cleaned, transformed, selected and integrated before data mining is performed. Data cleaning means that missing values should be provided in different fields/columns wherever needed and any impossible or erroneous values should be substituted by correct/reasonable ones. For example if the age of a person is typed as 1000 years in the column 'age' then an average age value can be put in its place. Where there are quite a few erroneous or missing values in a row, then that row can be discarded/deleted altogether. This process is called data selection. In data transformation, the data from all different sources is converted into the same format. For example, date typed under a column should be in the same format in the entire data collected through different sources. In data integration, data from all the sources is assembled or integrated into one and housed in the data warehouse. Now, this cleaned, transformed, selected and integrated data is fed to the data mining tool from a data warehouse for data mining purpose. The results/ patterns are evaluated by managers and useful knowledge is thus gained. Note that almost 80% of the total time used in a knowledge discovery process is spent on just making the data fit for mining, that is, data cleaning, data transformation, data selection etc.

Types of Data Mining

There are four main types of data mining as follows:

- Classification
- Association
- Characterization
- Clustering

Classification and association are predictive types of data mining while characterization and clustering represent the descriptive type.

Classification

It allows you to have a predictive model labeling different samples to different classes. The results of this type of mining/model are represented as (if-then) rules, decision trees, neural networks etc. Two important algorithms used for this type are ID3 Algorithm and Bayesian classification. Decision tree is a graphical representation of the if-then rules. Fig. 3 below shows the result of classification in the form of a decision tree. Initially, the whole data is divided into two sets – training data and test data.

In the example below, 'sex' is the target attribute/variable with males and females as the two classes. When no mining is done and values are picked at random, we find that males are 55% and females 45% in the training data. With a variation of 1 or 2 % the test data indicates a similar result. Classification algorithm may find the variable 'age' as the best predictor of males such that when the age is between 20 and 25 years the percentage of males rises to 60% in the training data and 59% in test data. Similarly, education and annual income can be discovered as other predictors for males, and so on. Thus, you can find a pattern that when age is between 20 and 25 years, and education is matric or below and annual income is less than one lac (assuming that the model ends at annual income), then there is a 65% probability (in the training data) and 64% probability (in the test data) that the sex of a person would be male. Similarly, a pattern for predicting females can also be obtained. Note that by using classification mining your probability of reaching males has increased from 55% (when no model is used) to 65% when the model is applied. Hence, if you want to launch/market a product for males and target them, you can use the model or pattern dug out through classification mining. Following this model there would be 65% chance that your message would reach the desired class of persons (males). You can send marketing messages to persons having the above profile to increase response rate. It would save time, energy and mailing cost.

In another example, three classes in a sales campaign may be 'good response', mild response' and 'no response' and different features of items such as 'price', 'brand', 'category' etc. can be found as predictors by the algorithm.

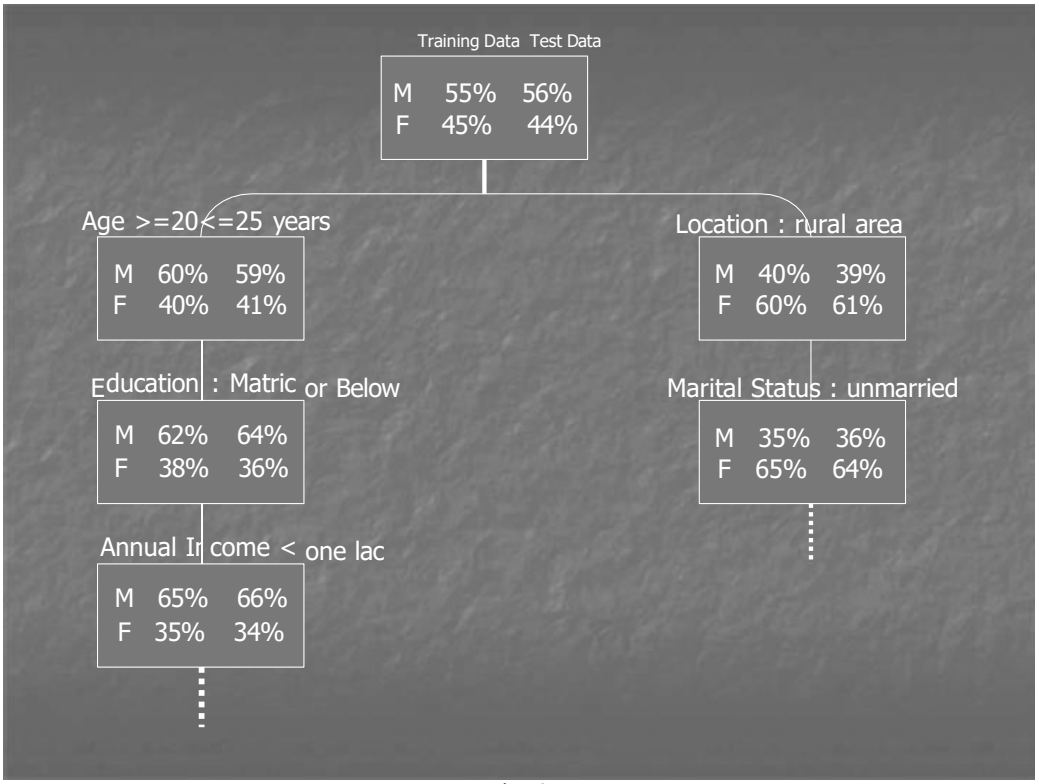

Fig. 3

Note that we split data into training and test data to judge the effectiveness of a rule, which means that a rule (for example, age>=20<=25 years) is picked up as such by the tool only if the test data also confirms the same rule with a variation upto 1or 2 % etc. The model is practically applied and the results are analyzed to calculate the efficiency of the tool/model.

Efficiency = actual/theoretical*100

In case after applying the model we actually reach 50% males whereas the predicted value was 66% (we take the figure in test data for calculation) then

Efficiency = 50/66*100= 75.75 %

The decision as to whether or not the same model should be used in the future would depend upon its efficiency. Normally, efficiency of a model close to 80% is considered as a good value.

Associ

Association analysis is a technique used for identifying common attribute-value conditions in data, such as market basket analysis. It helps identify strong bondages or affinity between items, such as strong purchases of one item. The Apriori algorithm is commonly used for association mining.

Associ ing attribute-value conditions that occur frequen rket basket analysis. For example, where we are by applying association mining we may discover that certain items have a strong bondage or affinity with each other such that when one item is purchased the other is purchased, too.Apriori algorithm is used for association mining.

Lesson 35

CONFIDENCE AND SUPPORT

There are two terms/measures used in association, that is, support and confidence. Confidence' is a measure of how often the relationship holds true e.g, what percentage of time did people who bought milk also bought eggs. Support means what is the percentage of two items occurring together overall. Mathematically, they can be expressed as follows if we take the example of eggs and milk:

Confidence = Transactions (eggs+milk)
Transactions (eggs or milk or both)

In case no. of transactions involving eggs and milk are 25 and those involving eggs or milk or both are 75 then confidence is 25/75*100=33.3%

Support = Transactions (eggs+milk)
Total no. of transactions

In case no. of transactions involving eggs and milk are 10 and total no. of transactions in a day are 50 then support is 10/50*100 = 20%

Suppose if confidence is 90% but the support is 5%., then we can gather from this that the two items have very strong affinity or relationship with each other such that when an item is sold the other is sold together, however, the chance of this pair being purchased out of the total no. of transactions is very slim, just 5%. One can adjust these measures to discover items having corresponding level of association and accordingly set marketing strategy. So, if I feed the data to the association mining tool and specify the percentage of confidence and support, it will list down the items that have association corresponding to these percentages. Results of association mining are shown with the help of double arrows as indicated below:

Bread ← ---→ Butter
Computer ←----→ Furniture
Clothes ← -- → Shoes

Using the result of association mining, a marketer can take a number of useful steps to set or modify marketing strategy. For example, items that have closeness/affinity with each other can be shelved together to improve customer service. Certain promotional schemes can be introduced in view of the association mining result etc.

Characterizatio

Characterization is a technique used to discover generalized concepts by examining data. It helps in understanding the overall behavior of the data by providing concise and generalized answers. For example, it can tell us how many students from a specific country are studying a particular field of education. By applying this technique, we can extract meaningful insights from the data.

It is discovering eralized levels for examining the general behavio nts of a university the students of different nationa sic history, physics etc. We can apply characteri swer in response to the question that how many students o a particular country are studying science or arts. See the following example:

Student name	Department	City of residence
Imran	History	Karachi
Alice	Physics	London
Ali	Literature	Lahore
Bob	Mathematics	Toronto
…		

In the above example, characterization tool can, for that matter, tell us that 02 Pakistani students are studying arts. Note that the concept of location and the field of education are generalized to Pakistan and arts, respectively.

The two algorithms used in characterization are Version Space Search and Attribute-Oriented Induction.

Clustering

Clustering is a technique that groups similar data objects together, while keeping dissimilar objects in separate clusters. It is useful for customer grouping, email categorization, and web usage analysis. The K-means algorithm is commonly used for clustering.

A cluster is a collection of objects which are similar to one another within the same cluster and are dissimilar to the objects in other clusters. For example, clustering can be used to group of customers, categories of emails in a mailing list, database, different categories of web usage from log files etc. It serves as a preprocessing step for other algorithms such as classification and characterization. K-means algorithm is normally used in clustering. In the example below you can see four clusters of customers based on their income level. K-means algorithm displays the result in the format as shown in Fig. 1 below:

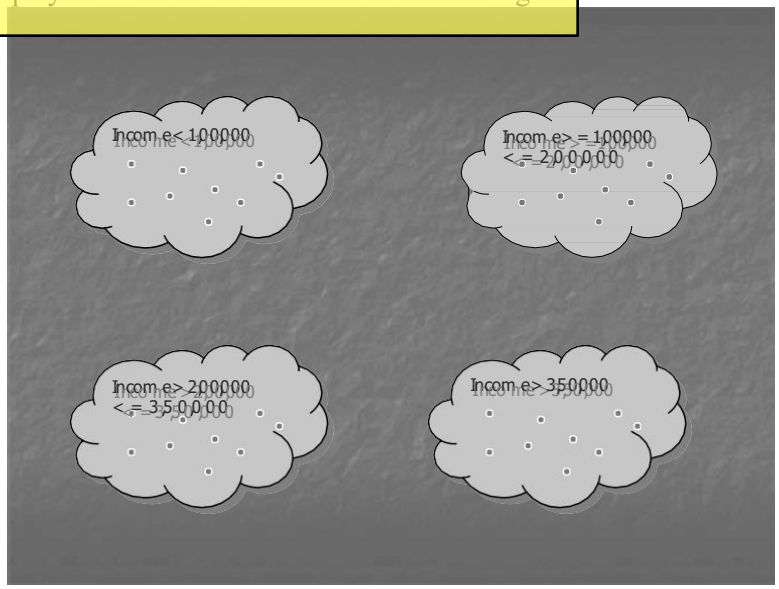

Fig. 1

Online Analytical Processing (OLAP)

OLAP makes use of background knowledge regarding the domain of the data being studied in order to allow the presentation of data at different levels of abstraction. It is different form data mining in the sense that it does not provide any patterns for making predictions; rather the information stored in databases can be presented/ viewed in a convenient format in case of OLAP at different levels that facilitates decision makers or managers. The result of OLAP is displayed in the form of a data cube **as shown in Fig. 2 below:**

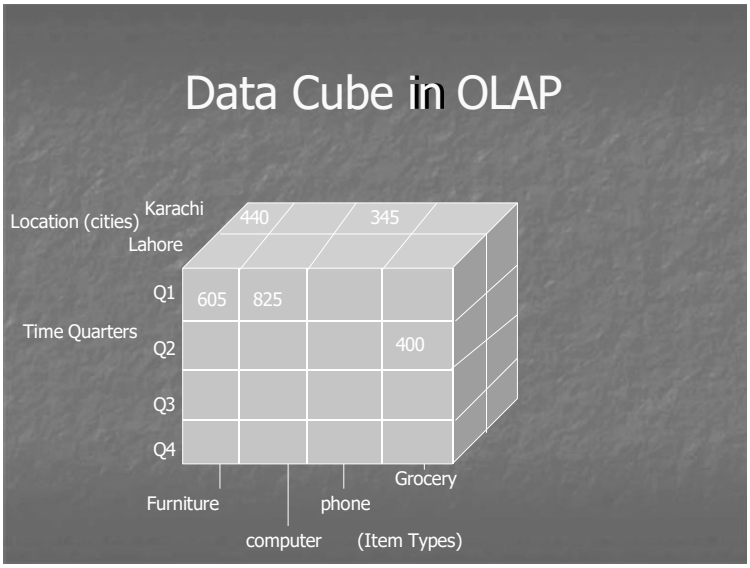

Fig. 2

Note that in the above diagram, time, item type and location are the three dimensions. OLAP data cube indicates the sale of 605 and 825 units of furniture and computers, respectively, in the first quarter of the year in Lahore, 440 units of furniture and 345 phone sets in Karachi in the first quarter, respectively, and 400 grocery items in Lahore during second quarter. Results can be displayed through data cube against more than three dimensions. For instance, variables, 'warehouse' and 'customer type' may also be added as dimensions to view the sale results. OLAP tool allows the use of different processes, namely, drill-down, roll-up, slice, dice etc. Using drill-down we can further dig the data to receive some specific information. For example using that I can find the sale of furniture in a specific month of the first quarter, say, February. Roll-up is the reverse of drill-down. In it we can sum-up or integrate the information in a particular dimension to show the result. For example the sale of furniture or computers in a particular year (rather than a specific quarter) can be viewed using roll-up. Similarly, through slice and dice information can be presented which is specific to certain dimensions of the data cube.

SAS (Enterprise Miner) and DB miner are the names of two commonly used tools for data mining and OLAP. Note that characterization can be used in respect of any data type whereas OLAP is generally used for numeric data alone.

Lesson 36

ELECTRONIC DATA INTERCHANGE (EDI)

EDI is used by organizations for transactions that occur on a regular basis according to a pre-determined format. It involves exchange of electronic business documents, i.e., purchase orders, invoices etc. EDI transactions are carried through special EDI software. This technology was popularly used before the introduction of e-commerce by different trading partners on private electronic networks. Key features of EDI include:

No paper work
No human intervention
Exchange of information takes place in seconds

EDI documents are formatted using published standards. Two popular EDI standards are - ANSI (American National Standards Institute) X12 standard and EDIFACT (United Nations Standard of Electronic Data Interchange for Administration, Commerce and Transport).

EDI Example

Assume E-Pens (a manufacturing company of pens and ballpoints) reviews sales and orders on monthly basis to make forecast of its sales for the coming month. Sales forecast is compared with the stocks of raw material and other components and a production plan is devised. This monthly plan needs to be flexible so that materials could be ordered at short notice if these are not available in the store. For instance, packaging material should only be ordered for just in time (JIT) delivery, so that E-Pens can cut down on its stock of packaging and reduce the inventory cost. On the other hand, packaging supplier also wants to improve its processing of orders, particularly urgent orders. Before using EDI technology, the order used to be generated in the following format:

From:
E-Pens

To: ABC & C0.

Order Ref:AC8484
Order Date:15.3.2006

Qty	Description	Product Code
1500	Superior –Red	PC-1075-R
1300	Superior – Silver	PC-1075-S

-End of Order-

After both E-Pens and its supplier start using EDI system, any amendment of the schedule on the production control system reviews the materials requirements and the order is automatically generated. In case the above paper order is to be generated using EDI software, the order data is coded and structured into a common and generally accepted format. The order would be written as follows in EDIFACT **(See Fig. 1 - not for exam):**

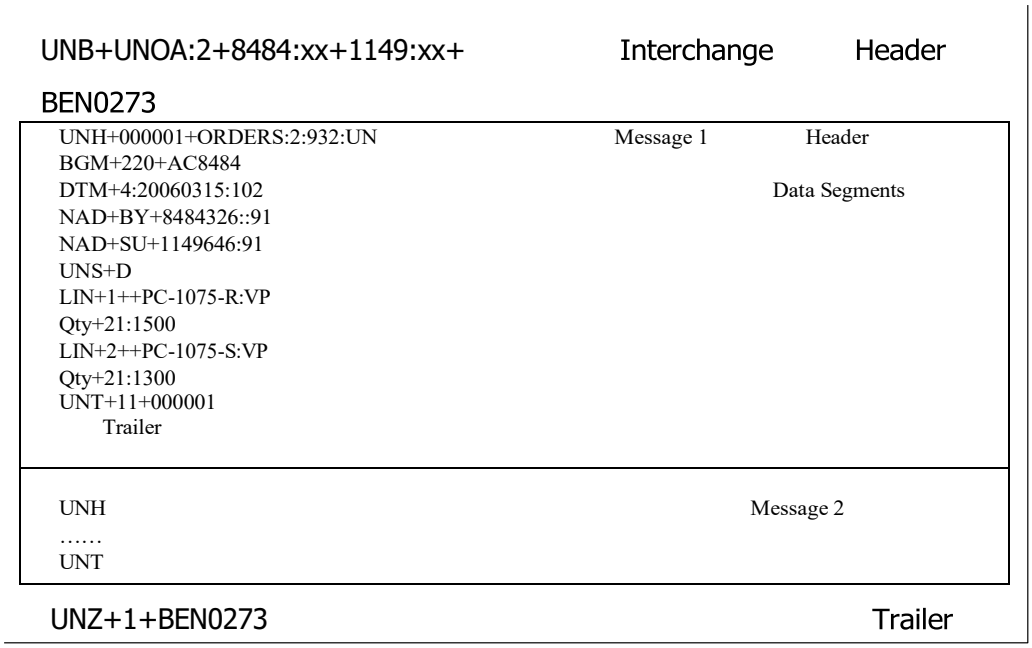

Fig. 1

In the above, 'UNB' refers to the start of interchange or envelop header, 'UNOA:2' to the United Nations Control Agency (level A) version 2, '8484' to sender code, '1149' to recipient code, 'BEN0273' to control reference, 'UNH' to message header, '000001' to message no., 'ORDERS' to the message type, '2:932' to version 2 and release 932, 'UN' to control agency. 'BGM' refers to beginning of message, '220' to message name code (i.e, order), 'AC8484' to order no., 'DTM' to date and time of message, '4' to a qualifier, '20060315' to date, '102' to format qualifier (century date), 'NAD' to name and address, 'BY' to buyer, 'SU' to supplier, '8484326' to buyer address code, '91' to code list agency, '1149646' to supplier address code. 'UNS' represents section control (that is, start of a section), 'D' is for section identification. 'LIN' indicates line item (e.g, line item number 1 and 2), 'PT-1075-R' and 'PT-1075-S' indicate item number, and 'VP' stand for item number type (that is, vendor part). 'QTY' represents quantity, '21' is quantity qualifier (indicating ordered quantity), '1500' and '1300' is the number of ordered quantity. 'UNT' is message trailer/end, '11' is control count (indicating no. of line segments in the message), '000001' is message no. 'UNZ' represents interchange trailer. Note that an interchange can have more than one message, as shown in Fig. 1 above.

Value Added Network (VAN)

Value added networks
valid trading partners using EDI. Each VAN has a centralized computer system that maintains two files for each user, that is,

Postbox: where outgoing messages are placed, and
Mailbox: where incoming messages can be picked up

VAN Example

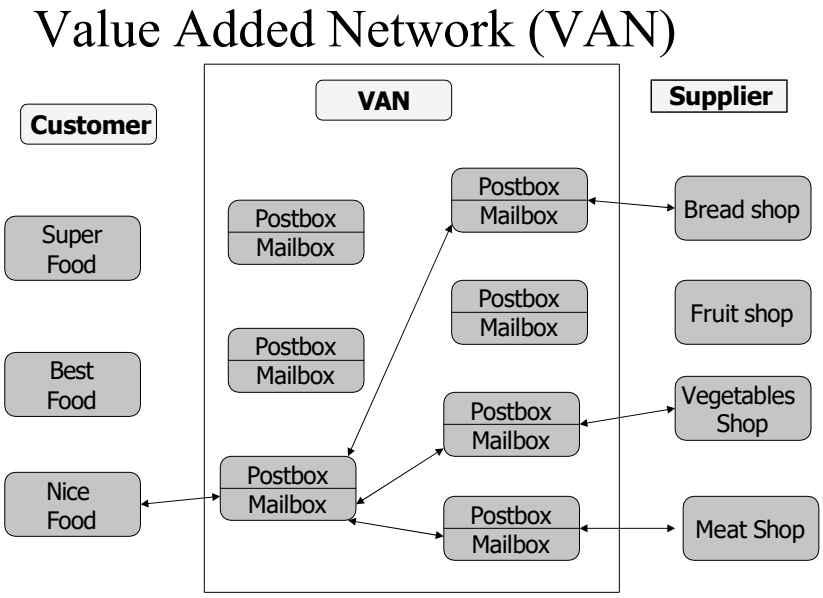

Fig. 2

Note that in Fig. 2 above, Nice Store needs to place orders for bread, meat and vegetables. It establishes a link to VAN through the dial up line, and sends EDI-based order messages for the three suppliers which are temporarily stored in its postbox. VAN computer system inspects postbox, unpacks interchanges (electronic envelopes), repackages them as new interchanges and moves them to the mailbox of the intended recipients. The three recipients check their mailboxes for new interchanges, pick them up and cause them to be transmitted to their respective processing systems. They can also send acknowledgment messages and cause them to be stored in their respective postboxes. VAN checks them and put them in the mailbox of Nice Food.

Advantages of VAN

---

1. Time Independence: Users can send and receive interchanges or messages at their convenience, without the need for simultaneous connectivity. This allows for flexibility in transaction timing.

2. Protocol Independence: VANs re-envelop interchanges with the appropriate transmission protocol when they are retrieved from the postbox. This ensures protocol compatibility between the sender and the recipient, even if their systems use different protocols

Two big advantages o l independence. Time independence means s can be carried out at the convenience of th users involved. Thus, they are not required to be conne cted with each other at the same time. Protoc l with the transmission protocol appropriate t by the VAN. Thus, a VAN can provide p ient, wherever that is missing.

Internet-Based EDI

Internet can support EDI in a variety of ways. Internet e-mail can be used as EDI message transport mechanism in place of having a VAN. An extranet can be created with the trading partner allowing a partner to enter information in the fields of web forms which correspond to the fields of EDI message. Also, web-based EDI hosting service can be utilized through web-based EDI software. However, a lot of work is still required to be done to make use of and popularize internet-based EDI.

Benefits of EDI

Some of the benefits of EDI are listed as under:

- Shortened ordering time

Since an order is generated automatically according to a pre-defined format, thus, the ordering time is very short.

- Cost cutting

An EDI transaction is more cost-effective in the sense that paper/stationary cost as well as cost of hiring staff to complete a transaction is eliminated in case of EDI. The only major cost is the expensive EDI software itself. However, once an EDI system is in place, it can save many expenses otherwise associated with a normal transaction.

- Elimination of errors

Messages are generated automatically, so the chances of any typing errors caused by human intervention are negligible.

- Fast response

An EDI message can be read and processed on the receiver side electronically with the help of EDI software. So, if the receiver is a supplier of raw material, it can quickly fulfill/implement the order as compared to a paper order.

- Accurate invoicing

Invoices or payment requests by the merchant/supplier can also be generated using EDI standard format, which are more accurate than paper invoices.

- EDI payment

EDI standard documents can be used to electronically provide financial information for payment purposes.

Enterprise Resource Planning (ERP)

ERP is an approach that attempts to integrate all departments and functions across a company onto a single computer system that can serve all those different departments' particular needs. For example, finance, manufacturing and the warehouse department of a company may have their own software to perform tasks specific to each one of them. However, each software can be linked together so that a customer service representative can see the credit rating of a customer from finance module, warehouse information from warehouse module, and shipment information from the shipment module. SAP is an example of ERP software. ERP is complex. It is not intended for public consumption as proper integration of ERP with e-commerce applications is still a major problem.

Electronic Banking

Electronic banking, , includes various banking activities conducted from home, business, or on the road, instead of at a physical bank location.

Advantages of e-banking

- Get current account balances at any time
- Obtain credit card statements
- Pay utility bills
- Download account information
- Transfer money between accounts

- Send e-mail to your bank
- Manage your own schedule
- Handle your finances from any location
- Apply for loans online

For banks, e-banking represents an inexpensive alternative to branch banking and a chance to enlist remote customers.

Lesson 37

PERSONAL FINANCE ONLINE

Personal finance allows the management of your financial matters in a customized manner. For example, tax calculations or financial budgeting can be done through personal finance software. Popular software packages for personal finance are Quicken, MS Money and Money 2003 etc. In personal finance online data is imported automatically into the register of transactions maintained by the software package as the account/transaction details are downloaded through the internet. This information can then systematically be used to calculate taxes or prepare a budget for certain activities.

Value Chain

EC includes so many activities that it is difficult to figure out where and how to use it in the business. One way to overcome this difficulty is to break business into many value adding activities. A strategic business unit is a combination of a particular product, distribution channel and customer type. In 1985 Michael Porter gave the idea of value chains in his famous book "Competitive advantage". A value chain is a way of organizing activities that each strategic business unit undertakes to design, produce, promote, market, deliver and support the products or services it sells.

Primary and Support activities

Porter identified that there are some primary activities as well as certain supporting activities in a strategic business unit. Following is the example of value chain for a strategic business unit **(see Fig. 1 below):**

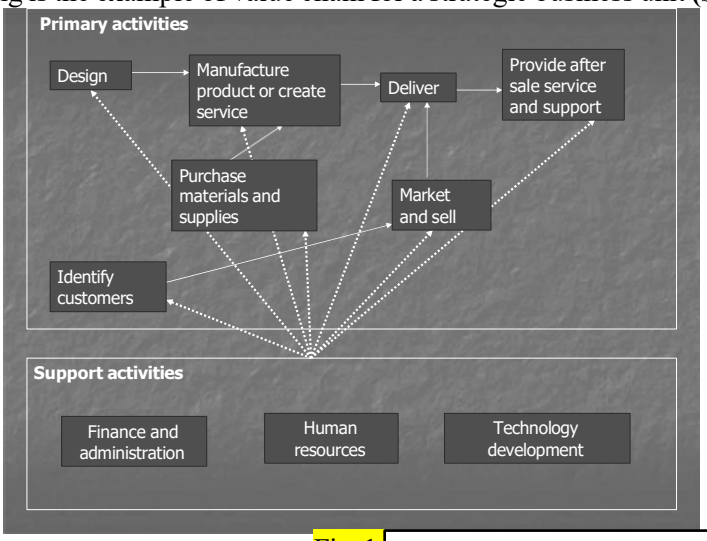

Fig. 1

****Primary activities include:****

- Identifying customers through market research and surveys
- Designing products from concept to manufacturing
- Purchasing materials and supplies, including vendor selection and quality monitoring

- 'Identify customers' refer to those activities which try to find new customers and ways to serve better to the existing ones, e.g, surveys and market research
- 'Design' activities take a product form concept stage. They include concept research, engineering, drawings preparation, testing, marketing
- 'Purchase materials and supplies' activities include procurement of material, vendor selection/qualification, negotiating supply contracts, monitoring supply schedules
- 'Manufacture product or create service' activities include transformation of material and labor into finished products, e.g, fabricating, assembling, packaging etc.
- 'Market and sell' activities give buyers a way to purchase and provide inducement for them to do so, e.g, advertising, promotions, managing salespersons, monitoring distribution channel, pricing etc.
- 'Deliver' activities relate to storage, distribution and shipment of final product, e.g, warehousing, selecting shippers, material handling, timely delivery to customers etc.
- 'Provide after sales service and support' refer to those activities that aim at promoting a continuing relationship with customers, e.g, installing, testing, repairing, maintaining a product, fulfilling warranties etc.

- Note that left to right flow does not mean a strict time sequence for these activities. For example, marketing activity can take place before purchasing materials.

- Importance of each primary activity depends on the product/service and the type of customers. For example, for certain type of businesses/products manufacturing activities are more critical and for others marketing activities may be more important.
- Support activities provide infrastructure for a business unit's primary activities as indicated in Fig. 1 above. Following are the support activities:
- 'Finance and administration' activities relate to accounting, paying bills, borrowing funds and complying with government regulations etc.
- 'Human resources' refer to the activities that coordinate management of employees, e.g, recruiting, hiring, compensation and benefits etc.
- 'Technology development' relates to activities which help improve product/service that a business is selling and also help improve processes in every primary activity, e.g, fields tests, maintenance of procedures, process improvement studies etc.

Industry value chains

It is useful to examine where a strategic business unit fits within its industry. Porter uses the term value system to describe larger stream of activities into which a business unit's value chain is embedded. Different strategic business units are associated, each having its value chain, to form industry value chain. By understanding how other business units in industry value chain conduct their activities, mangers can identify new opportunities for cost reduction and product improvement. **Fig. 2 below shows industry value chain of wooden furniture:**

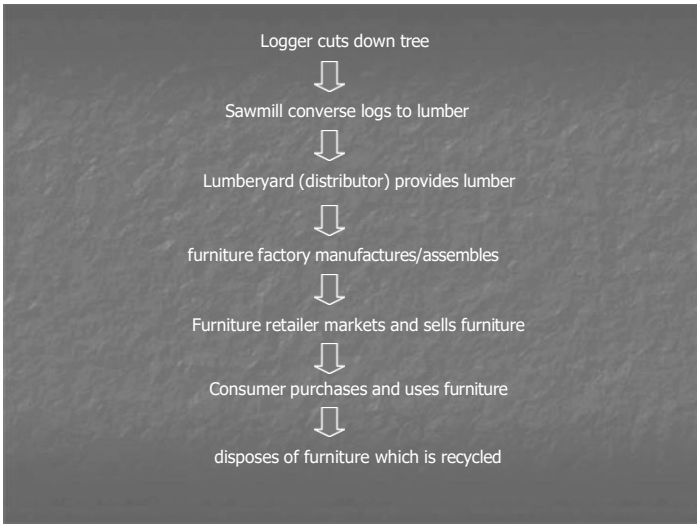

Fig. 2

Note that loggers grow and cut the trees to convert them into logs. Sawmill purchases logs and processes them in its processing unit to converts them to lumbers. The lumberyard business purchases lumbers form the sawmill business and sells them to furniture factory, which manufactures furniture using the lumbers. Furniture retailer buys the furniture from furniture factory and sells it to customers, who use it. After sometime the furniture is of no use and is disposed of by the customer. It can be then recycled. Note that each business unit has its own value chain. The analysis of industry value chain is useful for a sawmill business that is considering entering the tree harvesting/growing business or for furniture retailer who wants to be a partner with a transportation business. Industry value chain identifies opportunities up and down the product' s life cycle for increasing efficiency or the quality of product.

Examining value chains one finds that EC can help in four different ways as follows:

- It can reduce costs of a business;
- It can improve quality of products;

- It can help in reaching new customers or suppliers;
- It can create new ways of selling products.

For example, a software developer who releases annual updates of his software might consider eliminating software retailer from distribution channel for updates by offering to send updates through internet directly to his customers. In this way he can reduce the price of his product and increase sales revenue since revenue margin payable to the retailer can now be cut down from the price.

SWOT (strengths, weaknesses, opportunities and threats) analysis

In SWOT analysis, an analyst first looks into the business unit to identify its strengths and weaknesses then looks into the environment in which the business operates and identifies opportunities and threats presented by such environment.
While judging the strengths of a business, questions can be asked such as what does a business do well?. Does it have a sense of purpose and culture to support that purpose? While judging weaknesses of a business questions can be asked as to what does a company do poorly?. Has it any serious financial liabilities?. Has it got the required skilled manpower? In analyzing opportunities a company can try to find answers to questions, such as, what is the industry trend? Are there any new markets to enter/explore? Are there any new technologies to use?. In finding threats to a company's business it can ask questions as to what things the competitors of the business doing better? Are there any troublesome changes in company's business environment? Are there any new technologies or laws likely to be introduced that might cause problem to the company?

Example of Dell

Dell, a famous computer manufacturing brand, used SWOT analysis in mid 1990s to create a strong business strategy that made it a successful competitor in its industry value chain. It found that its strength was to sell directly to customers and design its computers to reduce manufacturing costs. It also found that it had no relation with local computer dealers. It faced threats from competitors which had much stronger brand names/quality at that time. Dell identified an opportunity by noting that its customers were becoming more knowledgeable about computers and could specify what they wanted to buy without Dell sales person helping them or answering their questions to develop configuration for them. Moreover, it decided to use internet as a potential marketing tool.

Dell took all four SWOT elements into consideration (see Fig. 3 below) and decided to offer customized computers. The computers could be built/configured according to the order or specifications of the customers who could place orders through phone and internet. Thus, it developed a strategy using its strengths effectively and avoiding reliance on dealer network. Note that brand and quality threats form competitors were reduced in this case by Dell's ability to deliver higher perceived quality of its product in the sense that each computer could be customized according to the needs/specifications of the customers.

Fig. 3

Lesson 38

SUPPLY CHAIN

Supply chain includes all the activities associated with the flow and transformation of goods from the raw materials stage all the way to the end user. Supply chain can be broken into three parts, that is, upstream activities, internal activities and downstream activities.

- Upstream activities relate to materials/services or the input from suppliers
- Internal activities relate to manufacturing and packaging of goods
- Downstream activities relate to distribution and sale of goods to distributors/customers

Fig. 1 below shows a simple example of supply chain of a milk processing unit. Note that milkmen supply milk to the processing facility. The processing business has ordered a corrugate paper company to supply boxes/paperboard for packaging. The paper company receives its raw material from a lumber company for manufacturing boxes. The lumber company also supplies paper to label printing business for making/printing paper labels. These are upstream activities. The boxes and labels should be available to the processing business at the packaging stage. The milk processing unit processes the milk, packages it in boxes and attaches labels to them. These are internal activities. The packaged milk is sent to distributors who distribute the same at different stores from where customers purchase. These are downstream activities.

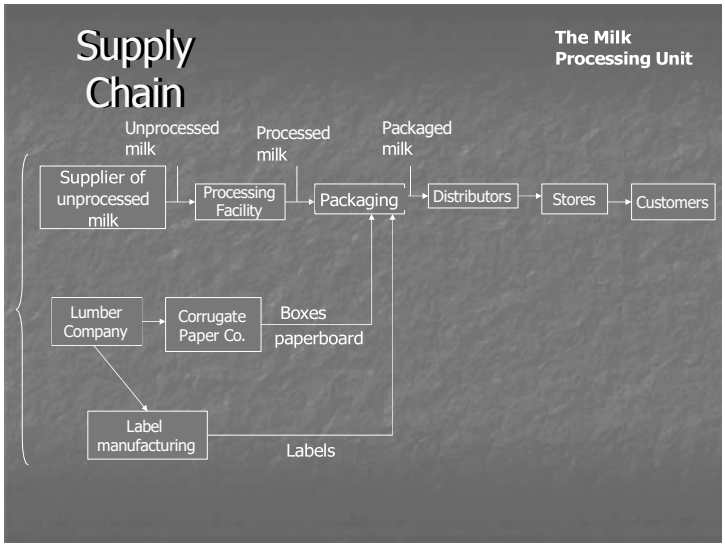

Fig. 1

Supply chain management

Engaging and negotiating with suppliers can be extremely beneficial. The process of taking active role in working with suppliers to improve products and processes is called supply chain management. Today, firms are reaching beyond limits of their own organizational structure. They are creating new network form of organization among the members of supply chain. Supply chain management is now used to add value in the form of benefits to the ultimate customer at the end of supply chain. It has become important for a business to work to establish long term relationship with at least small number of capable suppliers.

Internet technologies and supply chain

Internet is a very quick and effective tool of communication. On the other hand, communication is also a very critical element in supply chain management . Using internet technology:

- suppliers can share any information about changes in the customer demand;
- suppliers can haveimmediate notice of any changes in product design;
- drawings/specifications of a product can be quickly provided to the suppliers and vice versa;
- processing speed of a transaction can be increased;
- cost of handling a transaction can be reduced;

- chances of errors in entering transaction data are reduced;

Probably, the only disadvantage of using internet technology in a supply chain is that sometimes it may prove to be costly. However, in ultimate analysis, the advantages override the cost factor.

With the help of supply chain management software, one can not only manage the internal processes but also processes of other members of the supply chain. Therefore, it can be predicted that when and how much of certain product would need to be produced.

Examples of technology use in supply chain

A typical example of the use of technology in supply chain management is a company which is well-known worldwide as the largest producer of commercial aircrafts. It makes a big effort to keep its production on schedule. Most commercial airplanes require more than 1 million individual parts and assemblies and each airplane is configured according to specific needs of the purchasing airline. Timely availability of these parts must be ensured otherwise entire production schedule would be disturbed.

In 1997 the company had to stop its two assembly operations for several weeks due to errors in production and scheduling system causing it a huge financial loss. Thereafter, it decided to invest in information systems in every element of its supply chain. Involving its suppliers in the process, it began the use of EDI and internet technology, so that the suppliers could supply the right part or assembly at right time to prevent production delay. Now, the suppliers could get engineering specifications and drawings before the start of manufacturing using a secure internet connection, and plan their own business activities, accordingly. Also, members of the supply chain could have the knowledge of the completion of milestones and any changes in production schedule. In two years time, this approach resulted in reducing half the time needed to complete individual assembly processes. Thus, instead of waiting for 3 years the customer airlines could now have the ordered airplane ready for delivery in 10-12 months. Furthermore, the company launched a spare parts web site for ordering replacement parts. The site allowed customer airlines to register and order for replacement parts through browsers. Soon, the site was processing 5000 transactions per day at much lower cost as compared to orders cost through phone, mail, or fax. It also improved customer service in the sense that most parts could now be delivered the same day or the next day.

Another example is of a famous computer selling brand. It realized that by increasing the amount of information about its customers it was able to reduce amount of inventory it should hold. It decided to share this information with other members of the supply chain by allowing its top suppliers to have access to a secure web site which informed them about its latest sales forecasts, planned product changes or any warranty claims etc. It also provided information about its customers and their buying pattern. Thus, it helped suppliers to plan their own production in a much better way.

The above examples show how members of supply chain can work together to reduce inventory, increase quality of product, reduce production cost and increase process speed.

Supply chain and ultimate consumer orientation

Primary objective of supply chain is to help each company to meet needs of the consumer at the end of supply chain. This approach is called ultimate consumer orientation. In 1995, a company dealing in the business of production of tiers in America adopted a different approach by shifting its focus on tire dealers from ultimate customers. It created an extranet that allowed tire dealers to access tire specifications, inventory status and promotional information on the web. Thus, it gave opportunity to dealers to access product information directly and immediately. It also saved money since a web page is less expensive than answering thousands of phone calls daily by the company. This initiative provided a better service to dealers, so dealers using this extranet were not likely to recommend to customers a tire from the competing business.

Competitive Strategy

Ability of an organization to prosper arises from its competitive advantage over other organizations operating within its market sector. The strategy of a business to achieve this goal of competitive advantage is known as competitive strategy. Three basic strategies for competitive advantage are as under:

- Cost leadership
- Differentiation
- Focus

Cost leadership

It is the ability to sell the goods or provide the service at a price that is lower than that of competitors, and thus attract more customers.

Differentiation

Differentiation means that your product/service has certain quality that makes it more attractive than the one offered by your competitor, despite the price of your competitor's product/service is somewhat lower. For instance, you can beat your competitors for the reason that the air conditioner produced by your company is unique as it does not produce noise while in operation, whereas this feature is missing in the air conditioners produced by your competitors.

Focus

Focus strategy is defined as concentration on a single aspect of the market. That single aspect can be a particular market segment or market area or product type. For example, if my competitors are focusing on different market areas, I may, on the other hand, plan that I can be more profitable by concentrating on one particular area. It may be a particular province or a city etc. where I may have a better distribution channel.

Role of e-commerce in Competitive Strategy

By applying EC following major benefits can be derived:

- **Reduced administration/transaction cost**

Since things can be done electronically, so infrastructure or overhead cost (cost of building, staff, stationary etc) is reduced. Similarly, you can sell directly to your customers and it eliminates the cut/revenue payable to intermediaries or dealers. Thus, EC helps in achieving cost leadership.

- **Improved logistics supply chain**

Using EC one can have a quick response to the order placed. In other words, just in time delivery of the material is possible. It helps in reducing inventory and overall production cost and achieving cost leadership/differentiation.

- **Customization**

With the help of EC, customer data can be gathered and analyzing it customers can be served in a better manner according to their needs. One can, thus, implement differentiation and focus strategy.

- **Differentiate a product in terms of quality of service**

For example, online business of sale of music or books etc. In such cases delivery time and transaction cost is saved as customers can directly download the product from the web site, thus, it helps in achieving cost leadership and differentiation.

Lesson 39

PORTER'S MODEL OF COMPETITIVE RIVALRY

Porter's Model helps a firm to identify threats to its competitive position and to devise plans including the use of IT and e-commerce to protect or enhance that position. Porter identified five forces of competitive rivalry described as under:

- Threat of potential/new entrants to the sector
- Threat of substitute product or service in the existing trade
- Bargaining power of the buyers
- Bargaining power of the suppliers
- Competition between existing players

These five forces are also shown in Fig. 1 below:

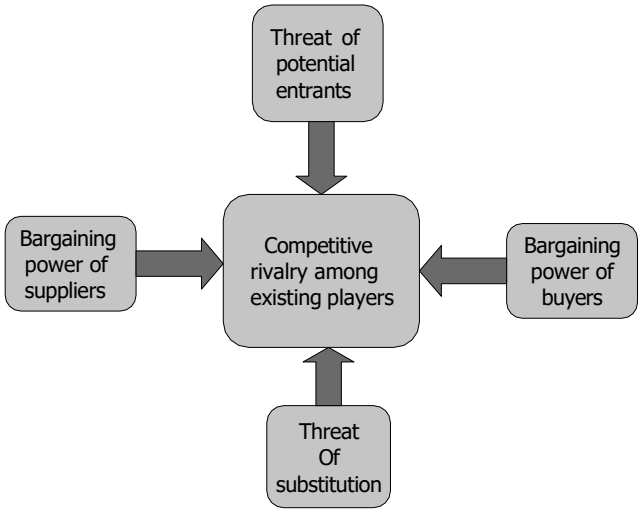

Fig. 1

Threat of new entrants

This threat relates to the ease with which a new company or a company in different product area can enter a given trade sector. Typically, barriers to entry are capital, knowledge or skill. IT/EC can be a barrier for new entrants, for instance, where competing businesses have heavily invested in EDI and are using the same, their investment would act as a barrier for new businesses to enter that trade sector. Conversely, advancements in technology have given rise to new ideas providing opportunity to new entrants without any need to build the IT infrastructure or make heavy investment to compete existing players. For example, to start online banking a company does not require heavy investment in constructing buildings (branch offices), hiring staff etc. as required in traditional banking. Rather, making use of internet technology coupled with a sound marketing plan, unique online banking services can be initiated.

Threat of substitution

This threat arises when a new product is available that provides the same function as existing product/service. For example, cotton fiber was, in the past, replaced by synthetic fiber, and glass bottles were substituted by plastic ones. This threat got materialized in case of music shops in physical world when due to the advent of e-commerce; music became available in downloadable format through the artist's

website. The site, in fact, had provided a substitute distribution channel. Another example is that of online banking which substituted traditional banking in physical world.

- **Bargaining power of buyers**

The cost of producing and distributing a product should be less than the price it can bring in the market in order to be profitable. Number of competitors and the supply of a product are the two major factors that determine bargaining power of the buyers. A buyer is in a strong position to bargain for low price if there are many competitors and/or the supply of the product in the market is in surplus. Note that with the help of e-commerce, low production cost, more inventory control and quick response time can be achieved. Besides, direct sale to the customers is also possible that cuts the cost of involving intermediaries. Therefore, a business using IT/EC can reduce the overall production cost and afford to keep the price of the product relatively low.

- **Bargaining power of suppliers**

Businesses try to find more favorable terms from their own suppliers. If supply of raw material is plentiful and/or there are many suppliers, the supply can be procured at a low price. Otherwise, position is more favorable to the supplier having more bargaining power. Ability to trade electronically is a factor in the quality of service and may be a requirement of the buying organization. Accordingly, bargaining power of a supplier is reduced if it is not electronically enabled.

- **Competition between existing players**

Competition among businesses is to get more buyers and trade at a price that produces an acceptable profit. If there are many players of the same size, capacity and strategy having little difference between their product/service, then there is fierce competition among them as regards the price of the product/service. Even a small change in the price of the product/service can be crucial for the business. Again, the use of EC can cause a significant difference by reducing administration/transaction cost, increasing efficiency of supply chain, improving product quality and customer service.
The five force analysis determines attractiveness of the industry whether to enter that industry as a business or not.

Strategic Planning Cycle

E-business competitive strategy is normally formed and implemented according to a planning cycle which is called strategic planning cycle.
There are four stages in this planning cycle as shown in Fig. 2 below:

Strategic Planning Cycle

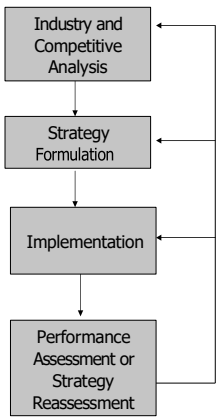

Fig. 2

- **Industry and competitive analysis**

It aims at identifying those factors on which the success of an EC project or business would depend. One way of doing that is to carry out SWOT analysis and study your business as well as the business of your competitors. Analysis of online competitor businesses is relatively easy since they are just a few clicks away on the web.

- **Strategy formulation**

Based upon this study of internal and external business environment and in light of a company's strengths and weaknesses, a competitive business strategy is formed. It may be a strategy of cost leadership, product differentiation or focus. One can also identify ways how information technology can be used to implement/enforce such strategy.

- **Implementation**

In the implementation stage, you build a plan to identify steps needed to put the strategy into action and practically take those steps. For example, where your strategy is to pursue differentiation in terms of quality of service by using/arranging a web-based call centre through which the customers can immediately register their complaints; then you will have to select appropriate individuals who are suitable for the job in the implementation stage. Creating a web team and defining the role/ responsibility of each member of the team is a critical component of implementation stage. For example, you define that this person would be the team leader; this would be in the technical staff (web master etc.) or the management staff. Note that involvement of key persons from marketing, accounting, finance, human resource, IT, customer relations etc. will be important in decision marking as to how a particular implementation plan can be executed. A strategic plan can be at times initially implemented in terms of a pilot project before launching it to a full scale. For example, an automobile manufacturer in America had implemented a plan/scheme which allowed the potential customers to have scheduled test drives before buying a particular car. Initially, this scheme was introduced to four American states but later it was implemented all over the country. Another point is to consider whether you should build your own infrastructure for execution or outsource the task of execution of a strategic plan. For example, where a strategic plan requires a particular web design, you can either mange your own team of web designers or outsource this task to an outside firm having expertise in this area.

- **Strategy assessment**

Results of implementation plan are monitored and assessed so that any corrective measures or expansion plan can take place. Basically, you want to assess whether your strategy has delivered what it was supposed to deliver; whether your strategy is still viable/workable in the ever changing environment. In strategy assessment phase, you can learn from your mistakes and do your future planning. In case your EC project has been a failure, you can identity the problems and try to remove them. Some of the corrective measures can be to property train your web team, establish or review your security or privacy policy, review or reassess your web design content, reconsider your marketing plan etc. For the strategy assessment, you can conduct surveys, collect information and receive feedback from different groups of people so that you have solid input from people coming from a variety of background. Sometimes, you have to entirety give up a particular strategy you followed and formulate a new strategy or set of strategies in light of the company's main objective or its mission.

Lesson 40

BARRIERS TO INTERNATIONAL E-COMMERCE

E-commerce is a combination of three different areas of study, namely, technology, business and law/policy. We have studied the technology and business side of e-commerce to a reasonably good extent. Now, we have to start the law and policy side of e – commerce. However, before we do that lets discuss some interesting issues related to the international aspect of e-commerce.

Barriers to International e-commerce

Barriers to international ecommerce include lack of trust, lack of infrastructure, language and culture.

Lack of Trust

It is very important for online businesses to establish trusting relationships with their customers like in the physical world where companies ensure that customers know who they are. However, it is difficult to build trust because a kind of anonymity exists for companies trying to establish web presence.

There was, once, a famous cartoon used to depict that on the internet nobody knows whether you are a dog. The issue of anonymity can be explained by the example that a visiting customer will not know in case of an online bank as to how large or well-established the bank is, simply by browsing through its web site. On the other hand, visitors would not become customers unless they trust the company behind the site.

Thus, a plan for establishing credibility of an online business is extremely crucial for its success. In this behalf, attention to the needs of the site visitors is very important while designing the web site, since it can be helpful in building trust with customers. For instance, there should be easy to find web pages that answer questions of the visitors. Note that companies with established brands can build trust for online business more quickly as compared to a new company/business without reputation, since a brand conveys expectations about how the online business would behave. For example, how the seller online business would react to a claim of refund by the customer.

Language

Only way to do business in other cultures is to be a part of such cultures. Language plays a very important role in this regard. In the first step you should provide local language versions of your web site. Software packages exist that can translate your web site content into different languages. Some sites translate all of their pages, but if the web site is very large then one can be selective in translation effort. Usually, home page, or pages related to marketing and product information or those related to any local interest/advertisement are given higher priority from translation point of view. Mainly two approaches are used for the translation of the content.

In the first approach, browser default language setting can be communicated to server when connection establishes between browser and server through 'http'. Server can thus detect default browser language setting and automatically redirect the browser to those set of pages in that language. Second approach is to include links to different language versions on the web site's home page. One can select any language by clicking the appropriate link. However, the link should show name of that language in that language so that the user can read/understand the information. It would be interesting to look at an estimate about the use of different languages over the internet **(see Fig. 1)**

Fig. 1

Culture

It should be useful to know about different cultural issues surrounding international e-commerce. Firstly, there is the issue of choice of name. For example, a famous car manufacturing company had chosen the name 'nova' for one of its car models, which could be understood by the people in Latin America in the sense that 'it will not go'. Similarly, a company selling baby foods in jars should not place the picture of a baby on the jar while doing business in certain parts of Africa, since in such parts it is customary (or part of the culture/tradition) to put on the jar the picture of contents contained in it.

Web designers must be careful about the choice of icons because they can have different meanings in different cultures. For instance, in U.S shopping cart is a good symbol for selecting and putting your items in a virtual place, whereas shopping basket is a more appropriate symbol or icon for the said purpose in Europe. Similarly, in India it would not be appropriate to use the image of a cow in a cartoon. In Muslim countries people can be offended by human pictures that violate the limit of Islamic parda. Use of colors in the web design can also be troublesome. For example, white color denotes purity in Europe and America but is associated with death and mourning in china and some Asian countries. Similarly, a web page divided into four segments can be unpleasant to a Japanese visitor because no. four is a symbol of death in that culture.

Some parts of the world have cultural environment that is not welcoming for ecommerce. For instance, in certain Islamic countries the exchange of information that conflicts with Islamic values is forbidden. Then, there are internet censorship activities of governments in certain parts of the world. For example, there are complex registration requirements/regulations in china imposed by the government which a business must comply with in order to engage in ecommerce.

The Chinese government conducts review of ISPs record. The ISPs have to maintain a record of their customers and retain copies of all their email messages etc. In China a number of internet cafés were closed down for violating the electronic record keeping procedures. Some countries do not have strict censorship requirement as above, but have strong cultural requirements. For example, in France an advertisement for a product or service must be in French, thus, an online business based in America wishing to ship products to its customers in France must provide French version of its pages if it intends to comply with French laws.

- **Infrastructure issues**

Internet infrastructure includes computers and software connected to internet and communication networks over which data packets can travel. In many parts of the world, telecommunication industry is either owned by the government or is strictly regulated by the government. This government control or regulations have retarded growth of infrastructure to a limit that sometimes it cannot fully support internet data traffic. For example, there is the huge issue of low bandwidth (slow data communication) in most third world countries.

In Europe, cost for internet connection is considered quite high, discouraging people to spend more time on surfing the web while shopping. Moreover, international transactions mostly require physical handling of goods by several freight carriers and shipping companies. This storage and handling normally requires monitoring by government custom officers, which is not done in domestic transactions. A coordinated effort is, therefore, required between customs brokers, freight agencies and government officials in such cases due to complex government regulations.

According to an estimate, almost half of all businesses on the web turn down international orders because of the lack of proper infrastructure to handle such transactions, thus losing millions of dollars.

Electronic Transactions Ordinance, 2002 (ETO)

ETO is the law introduced in 2002 which extends to the whole of Pakistan. It basically provides legal recognition to documents in electronic form and to electronic signatures. To understand this law, it would be useful to revise the concept related to the working of digital signature technology (refer to Lecture no. 23). We shall look at salient provisions/features of this law as it directly deals with e-commerce in Pakistan. Section 2 of the ETO defines different terms used in it. For convenience these terms have been reproduced here (you do not need to memorize these for exam).

- "**'Certificate'** means a certificate issued by a Certification Service Provider for the purpose of confirming the authenticity or integrity or both, of the information contained therein, of an electronic document or of an electronic signature in respect of which it is issued".

- "**'Cryptography services'** means services in relation to the transformation of contents of an electronic document from its original form to one that cannot be understood or decoded by any unauthorized person".

- "**'Accredited Certification Service Provider'** means a Certification Service Provider accredited under this Ordinance to issue certificates for the use of its cryptography services".

- "**'Certification Practice Statement'**, means the statement prepared by a certification service provider specifying the practices it employs in relation to the issuance of certificates and matters connected therewith".

- "**'Originator'**, means a person by whom, or on whose behalf, electronic document purports to have been generated or sent prior to receipt or storage, if any, but does not include an intermediary".

- "**'Addressee'** means the person intended by the originator to receive the electronic communication but does not include an intermediary".

- "**'information system'** means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information".

- "**'Electronic Signature'** means any letters, numbers, symbols, images, characters or any combination thereof in electronic form, applied to, incorporated in or associated with an electronic document, with the intention of authenticating or approving the same, in order to establish authenticity or integrity, or both".

- "'**Authenticity'** means, in relation to an electronic document or electronic signature, the identification of and attribution to a particular person or information system".

- "'**Integrity'** means, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time".

'Appropriate authority' means the relevant entity responsible for making decisions:

- For Federal Legislative List matters: Federal Legislature or Federal Government.
- For Concurrent Legislative List matters with a Federal law: Federal Legislature or Federal Government.
- For other Concurrent Legislative List matters:

- [illegible] l Legislative List of the Constitution of the Islamic Republic of Pakistan, 1973, the Fede ral Legislature or Federal Government;

- In relation to items contained in the Concurrent Legislative List of the Constitution of the Islamic Republic of Pakistan, 1973, for which a Federal law is in force, the Federal Legislature or Federal Government, and, in all other cases, respective Provincial Legislature or Provincial Government;

- In relation to the functions of the Federal Government or respective Provincial Governments being discharged by a statutory body, that statutory body ; and

- In relation to matters in respect whereof the Supreme Court or the High Courts are empowered to make rules for the regulation of their proceedings, the Supreme Court or High Court, as the case may be".

Section 3 of the ETO provides:

"No document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in electronic form and has not been attested by any witness".

Section 4 of the ETO provides:

"The requirement under any law for any document, record, information, communication or transaction to be in written form shall be deemed satisfied where the document, record, information, communication or transaction is in electronic form, if the same is accessible so as to be usable for subsequent reference".

Note that by virtue of Sections 3 and 4 above, the requirement of law for a document to be in writing shall be deemed satisfied if that document is in electronic form. Consequently, if a law requires that one must send a legal notice before filing a case against a government organization and that legal notice is sent in electronic form (e-mail attachment); it would be said that the requirement of law has been fulfilled in terms of sections 3 and 4 above.

Lesson 41

ELECTRONIC TRANSACTIONS ORDINANCE, 2002 (ETO) (CONTINUED….)

Generally speaking the term 'Appropriate authority' includes the five legislative assemblies (national assembly and four provincial assemblies), the federal government and four provincial governments, the Supreme court of Pakistan and four High courts, and any statutory body working in relation to the functions of federal or provincial governments. A statutory body is a body/organization established under some statute/law. For example, the Lahore Development Authority (LDA) is a statutory body established under the Lahore Development Act, 1975 (a provincial statute).

The Constitution of Islamic Republic of Pakistan, 1973 is the supreme law of the country, which means that every other law in Pakistan has to confirm to the terms of the constitution. It contains two legislative lists at its end, that is, the Federal legislative list and Concurrent legislative list. The federal legislative list sets out those items/subjects on which only the federal legislature can make laws such as the subject related to defense of Pakistan and armed forces etc. On the other hand, matters contained in concurrent legislative list are those on which both the federal and provincial legislature can enact/make laws, such as the subject related to marriage and divorce etc.

Section 6 of the ETO lays down the conditions for validly retaining a document in electronic form as follows:

> "6. The requirement under any law that certain document, record, information, communication or transaction be retained shall be deemed satisfied by retaining it in electronic form if :
>
> - The contents of the document, record, information, communication or transaction remain accessible so as to be usable for subsequent reference;
> - The contents and form of the document, record, information, communication or transaction are as originally generated, sent or received, or can be demonstrated to represent accurately the contents and form in which it was originally generated, sent or received; and
> - such document, record, information, communication or transaction, if any, as enables the identification of the origin and destination of document, record, information, communication or transaction and the date and time when it was generated, sent or received, is retained."

Note that basically the conditions for validly retaining a document in electronic form are that such document must be accessible for subsequent reference, it should reliably be comparable with its original form and its origin and destination is identifiable as also the date and time of its generation.

Section 7 of the ETO provides legal recognition to electronic signatures and advanced electronic signatures in following terms:

> - "7. The requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures or advanced electronic signatures are applied."

Note that a presumption of truth is attached to advanced electronic signatures, which means that a court should assume that an advanced electronic signature was validly executed, and the burden to prove otherwise would be on the party that denies its execution. The difference between an electronic signature and advanced electronic signature does not seem to be clear in ETO. It appears that an advanced electronic signature involves an accredited certification service provider, whereas an electronic signature can be executed without its help to prove authenticity and/or integrity.

Legal documents are ordinarily required to be written/typed on printed papers which one has to purchase for certain value under the law, that is, Stamp Act, 1899. Similarly, the Qanoon-e-Shahadat Order, 1984 (the

main law of evidence in Pakistan) also generally requires each executed document to be witnessed by at least two male witnesses. Copies of certain documents can be notarized also, which would mean that a copy can be signed/stamped by a duly appointed person called notary public confirming that the copy relates to a particular original document.

By virtue of **Sections 10 and 11 of the ETO**, the stamp duty and the requirement of attestation/notarization has been waived for a period of two years or till such time the provincial governments devise appropriate measures. For convenience the two sections are reproduced as under:

- "10. Notwithstanding anything contained in the Stamp Act, 1899 (II of 1899), for a period of two years from the date of commencement of this Ordinance or till the time the Provincial Governments devise and implement appropriate measures for payment and recovery of stamp duty through electronic means, whichever is later, stamp duty shall not be payable in respect of any instrument executed in electronic form."

- "11. Notwithstanding anything contained in any law for the time being in force, no electronic document shall require attestation and notarization for a period of two years from the date of commencement of this Ordinance or till the time the appropriate authority devise and implement measures for attestation and notarization of electronic documents, whichever is later."

Section 13 of the ETO talks about as to who would be deemed/supposed to have sent an electronic communication. It is given as follows:

- "13. (1) Unless otherwise agreed as between an originator and the addressee, an electronic communication shall be deemed to be that of the originator if it was sent:
  - By the originator himself;
  - By a person who had the authority to act for and on behalf of the originator in respect of that electronic communication; or
  - By an automated information system programmed by, or on behalf of the originator.

- Unless otherwise agreed as between the originator and the addressee, the addressee is to regard an electronic communication as being that of the originator, and is entitled to act on that assumption if:
  - The addressee has no reason to suspect the authenticity of the electronic communication; or
  - There do not exist any circumstances where the addressee knows, or ought to have known by exercising reasonable care, that the electronic communication was not authentic."

Note that an electronic communication would be deemed to be sent by an originator, if the originator himself, or his attorney/representative or his automated information system sends the same. The addressee is entitled to treat it as the communication of the originator if there exist no reason for a suspicion.

Lesson 42

ELECTRONIC TRANSACTIONS ORDINANCE, 2002 (ETO) (CONTINUED….)

An originator can attach a condition with the electronic communication that it would be deemed to be sent only if the addressee acknowledges its receipt. An originator can also specify the mode in which the acknowledgment would be acceptable. Then only such mode can be used for sending the acknowledgment.

Section 14 is the relevant provision in this behalf:

- "14. Unless otherwise agreed where the originator has stated that the electronic communication is conditional on receipt of acknowledgment, the electronic communication is treated as though it has never been sent, until the acknowledgment is received.

- Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by:

    - any communication, automated or otherwise, by the addressee ; or
    - any conduct of the addressee, sufficient to indicate to the originator that the electronic communication is received."

Section 15 of the ETO provides guideline as regards the place and time of dispatch and receipt of an electronic communication in the following terms:

- "15. Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic communication occurs when it enters an information system outside the control of the originator.

- Unless otherwise agreed between the originator and the addressee, or unless proved otherwise, the time of receipt of an electronic communication is determined as follows:

    - If the addressee has designated an information system for the purpose of receiving the electronic communication, receipt occurs:
    - At the time when the electronic communication enters the designated information system; or
    - If the electronic communication is sent to an information system of the addressee that is not the designated information system, at the time when the electronic communication is retrieved by the addressee;

    - If the addressee has not designated an information system, receipt occurs when the electronic communication enters an information system of the addressee.

- Sub-section (2) applies notwithstanding that the place where the information system is located may be different from the place where the electronic communication is deemed to be received under subsection (4).

- Unless otherwise agreed between the originator and the addressee, an electronic communication is deemed to be dispatched at the place where originator ordinarily resides or has his place of business, and is deemed to be received at the place where the addressee ordinarily resides or has his place of business.

- For the purpose of this section:

- If the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;
- If the originator or the addressee does not have a place of business, reference is to be made to the usual place of residence ; and
- "Usual place of residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted."

Note that sub-sections 1-3 of the above section deal with the time of dispatch and receipt of an electronic communication. In general terms, an electronic communication is deemed to have been sent by an originator at the time it enters the information system beyond the control of the originator. On the other hand, it is deemed to be received by the addressee at the time it enters his information system or his designated/specified information system. Note that the determination of time of dispatch and receipt of the electronic communication is crucial with regard to the calculation of limitation period in which a legal action has to be taken by a party.

Remember that under the law a legal action is ordinarily initiated within a specified time period, beyond which such an action is not maintainable. This is called the law of limitation. Main idea behind the law of limitation is that a party should be vigilant/alert in bringing its claim in a court of law. Sub-section 4 provides the guideline as to how the place of dispatch and receipt of an electronic communication can be determined. Basically, it describes the place of dispatch and receipt of an electronic communication to be where the originator or the addressee ordinarily reside or have their respective businesses.

Note that the determination of place of dispatch and receipt of electronic communication is important to fix the territorial jurisdiction. Territorial jurisdiction refers to the legal competence or right of a court of a particular area/territory to entertain and decide a case.

Section 16 states that no one shall have a legal right to insist upon an appropriate authority to create, issue, accept or retain a document in electronic form. However, where an appropriate authority under a law issues, creates, retains, accepts or provides any mechanism for payment/transaction, it, on its own, can decide that a document would be in electronic form for the above purposes. Also, it would be entitled to specify the manner/format for any such documents, procedures, the type of electronic signatures etc. This provision is reproduced here for a reference:

- "16. Nothing contained hereinbefore shall confer a right upon any person that any appropriate authority should accept issue, create, retain, preserve any document in electronic form or effect monetary transaction in electronic form.

- Any appropriate authority pursuant to any law or procedure:

  - Accepts the filing of documents, or requires that documents be created or retained;
  - Issues any permit, certificate, license or approval; or
  - Provides for the method and manner of payment, procurement or transaction

May notwithstanding anything contained to the contrary in such law or procedure:

  - Accept the filing of such documents, or creation or retention of such documents in the form of electronic documents;
  - Issue such permits, certificate, licence or approval in the form of electronic document; or
  - Make such payment, procurement or transaction in electronic form.

- In any case where an appropriate authority decides to perform any of the functions in clause (1) (i), (ii) and (iii) of sub-section (2) may specify:

  - The manner and format in which such electronic documents shall be filed, created, retained or issued;

- When such electronic document has to be signed, the type of electronic signature, advanced electronic signature or a security procedure required;
- The manner and format in which such signature shall be affixed to the electronic document, and the identity of or criteria that shall be met by any certification service provider used by the person filing the document;
- Control process and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic documents, procurement, transactions or payments; and
- any other required attributes for electronic documents or payments that are currently specified for corresponding paper documents."

Note that the above provision provides the legal basis for e-government.

Under Section 17 a certification service provider, which is not accredited, can still be engaged in providing certification services. Note that a certification service provider is the same as a certification authority you are familiar with. Section 18 provides that the Federal Government shall establish a Certification Council, which is a high level body comprising five members. The qualifications of the members of the Council are mentioned in Section 19. The Council shall have its own fund under Section 20. The functions of the Certification Council are described in Section 21. Mainly, the council would grant, renew, suspend, revoke any accreditation certificates to the certification service providers, and would monitor compliance of certification service providers with the provisions of the ordinance. It would also be responsible for setting up and maintaining a repository/database where information about accreditation certificates and digital certificates issued to the subscribers would be placed and accessible by public at large. For quick reference the relevant provisions are quoted below:

- "17. Nothing in this Ordinance shall impede or in any way restrict the rights of any certificate service provider to engage in the business of providing certification services without being accredited.
- No person shall hold himself out as an accredited certification service provider unless he holds a valid accreditation certificate issued under section 24 by the Certification Council."
- **"18**. Within sixty days of the promulgation of this Ordinance, the Federal Government shall, by notification in the official Gazette, constitute a Certification Council to be known as Electronic Certification Accreditation Council.
- The Certification Council shall be a body corporate with perpetual succession and a common seal, and shall by the said name sue or be sued.
- The Certification Council shall comprise of five members, with four members from the private sector. One of the Members shall be designated as the chairman."

"19. of the five members of the Certification Council:

- One shall be telecommunications engineer with at least seven years work experience, of which at least one year is in the field of cryptography services;
- Two shall be professional or academics with at least seven years work experience in the field of information technology;
- One shall have an administrative background with at least seven years experience in a private or public organization; and

- One member shall be an advocate with at least seven years experience and adequate knowledge of laws relating to information technology and telecommunications."

"20. the funds of the Certification Council shall comprise of:

- Grants from the Federal Government;
- Fee for grant and renewal of accreditation certificate; and
- Fee, not exceeding ten Rupees, for every certificate deposited in the repository; fines."
- **"21.** The Certification Council shall perform such functions as are specified in this Ordinance or may be prescribed.
- Without prejudice to the generality of the foregoing subsection, the Certification Council shall:
    - Grant and renew accreditation certificates to certification service providers, their cryptography services and security procedures;
    - Monitor and ensure compliance by accredited certification service providers with the terms of their accreditation and revoke or suspend accreditation in the manner and on the grounds as may be specified in regulations;
    - Monitor compliance of accredited certification service providers with the provisions of this Ordinance;
    - Establish and manage the repository;
    - Carry out research and studies in relation to cryptography services and to obtain public opinion in connection therewith;
    - Recognize or accredit foreign certification service providers;
    - Encourage uniformity of standards and practices;
    - Give advice to any person in relation to any matter covered under this Ordinance;
    - Make recommendations to an appropriate authority in relation to the matters covered under this Ordinance."

For the creation/management of information repository, there is **Section 23 in the ETO** as follows:

- "23. The Certification Council shall establish and manage a repository for all accreditation certificates, certificates issued by accredited certification service providers and for such other information as may be specified in regulations made by the Certification Council.
- The Certification Council shall take appropriate measures to ensure the security of all information contained in the repository.
- All information contained in the repository shall be open to public inspection.
- Notice of suspension or revocation of any accreditation or of certificate issued by an accredited certification service provider, shall be posted in the repository within the prescribed time."

Lesson 43

ELECTRONIC TRANSACTIONS ORDINANCE, 2002 (ETO) (CONTINUED….)

Section 24 of the ETO provides that Certification Council shall make regulations specifying the criteria/procedure for the grant of accreditation certificates to the certification service providers. The provision is reproduced as follows:

- "24. The Certification Council may grant accreditation to certification service provider, its cryptography services, electronic signature or advanced electronic signature and security procedures who comply with the criteria for accreditation specified in the regulations.
- The terms and conditions of the accreditation, including those relating to duration of the accreditation, renewal, suspension or revocation, shall be specified in regulations.
- The fee for grant and renewal of the accreditation shall be as prescribed.
- The form and manner of proceedings for the consideration of application for grant, renewal, suspension or revocation of accreditation shall be specified in the regulations provided that, the regulations shall provide for a transparent procedure with due regard to the right of hearing."

Note that a certification service provider shall have proper right of hearing before a decision on its application for the grant of accreditation certificate is made. This is based on the fundamental principle of law that no body should be condemned unheard (also called the principle of natural justice).

Under Section 25, each certification service provider shall prepare a Certification Practice Statement (CPS) as prescribed by the regulations of the Certification Council. CPS would be a policy document of the certification service provider, which would be filed along with the application for grant of accreditation certificate.

A copy of the certification practice statement shall be maintained at the office of the Certification Council and shall be open to public inspection. Subject to any regulations made by the Council, a CPS would normally include information for persons adversely affected by a wrong/false certificate, the extent of liability, policy about suspension or revocation of certificates etc**. For details you can see section 25 below** (no need to memorize any such section, just try to build a general sense):

- "25. Each certification service provider, desirous of being accredited, shall prepare and have at all times accessible a certification practice statement in such form and with such details, particulars and contents as may be specified in regulations made by the Certification Council.
- Without prejudice to the generality of the foregoing, the regulations may provide for:
  - Prompt information to persons likely to be adversely affected by any event relating to the information system of the certification service provider or inaccuracy, invalidity or misrepresentation contained in a certificate;
  - Identification of subscribers;
  - Suspension or revocation of certificates;
  - Accuracy of information contained in a valid accreditation certificate;
  - Foresee ability of reliance on valid accreditation certificates; and
  - Deposit of certificates or notification of any suspension or revocation of any accreditation certificate or any other fact or circumstance affecting the certificate, in the repository.

- The certificate practice statement shall be submitted to Certification Council for approval along with the application for accreditation.

- Any subsequent change in the approved certification practice statement shall be initiated and processed in such manner as may be specified in regulations made by the Certification Council, and upon approval by the Certification Council, shall be incorporated in the certification practice statement.

- A copy of the certification practice statement shall be maintained at the office of the Certification Council and shall be open to public inspection.

- Subject to such limitations as may be specified in the regulations made under sub-section (1), a certification service provider shall, during the period of validity of an accreditation certificate published for reliance by any person, be deemed to warranting to such person that:

    - the certification service provider has complied with the requirements of this Ordinance, rules and regulations made under this ordinance ; and

    - the information contained in the certificate is accurate.

- The Certification Council may suspend or revoke the accreditation of a certification service provider for failure to comply with the provisions of this section:

Provided that, an order for suspension or revocation of accreditation shall be made in the manner specified in regulations made under sub-section (1) after providing reasonable right of hearing."

All applications and matters before the Certification Council should be decided as quickly as possible through a speaking order (order containing reasons). The Council may appoint such officers, employees and advisers as it considers necessary, and can also establish regional or local offices for due performance of its functions.

Section 31 of the ETO specifies that it does not apply to five different types of documents, namely, a negotiable instrument, a power of attorney, a trust, a will, a contract of sale or conveyance of immoveable property. Accordingly, such documents are still required to be in paper form.

A negotiable instrument includes a promissory note, a bill of exchange and a check. A promissory note is an unconditional promise or undertaking to pay a specified amount to a specified person. A bill of exchange is an order by a person (person 'A') to another person (person 'B') to make certain payment to a third person (person 'C') on behalf of 'A'. A check is a type of bill of exchange where the bank is asked by a person (drawer of the check) to make specific payment to the person in whose favor the check is written. A power of attorney is the document through which some authority is given by a person to another to do certain acts or things on behalf of the person who executes the power of attorney. A document of trust or trust deed is prepared to create a trust. A trust can own property in its name.

The property of the trust is used for the benefit of specified persons named in the trust deed called beneficiaries of the trust. The person who establishes the trust is called author of the trust. The persons who mange the affairs of the trust are called trustees. A will is a document through which someone can name the person(s) who would be entitled to own his property after his death. A document through which the ownership in a property is legally transferred to someone is called a conveyance deed (such as a sale deed).

A contract of sale of immoveable property (land etc.) and/or a conveyance deed in this behalf are still required to be in paper form. Note that the Federal Government, however, has been given the power to make whole or any part of the ETO applicable to all or any of the above documents through a notification in the official gazette.

For reference, section 31 is given as under:

- "31. Subject to sub-section
- Nothing in this Ordinance shall apply to:
  - a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881 (XXVI of 1881);
  - a power-of-attorney under the Powers of Attorney Act, 1881 (VII of 1882);
  - a trust as defined in the Trust Act 1882 (II of 1882), but excluding constructive, implied and resulting trusts;
  - a will or any form of testamentary disposition under any law for the time being in force; and
  - a contract for sale or conveyance of immovable property or any interest in such property.
- The Federal Government after consultation with the provinces may, by notification in the official Gazette and subject to such conditions and limitations as may be specified therein, declare that the whole or part of this Ordinance shall apply to the whole or part of one or more instruments specified in clauses (a) to (e) of sub-Section (1)."

Section 32 of the ETO says that courts in Pakistan shall have jurisdiction or authority to decide any matter that relates to persons or information systems or events in Pakistan and covered by the terms of the Ordinance. Assume that someone from England accesses an information system in Pakistan and deletes or modifies the data of a person contained therein without any authority, then this act may be treated as an offence under the ETO and Pakistani courts would have jurisdiction to try such a matter. Note that ETO would have an overriding or dominating effect as opposed to a law which is inconsistent with its terms.
Sections 32 and 33 are reproduced as under in this behalf:

- "32. The provisions of this Ordinance shall apply notwithstanding the matters being the subject hereof occurring outside Pakistan, in so far as they are directly or indirectly connected to, or have an effect on or bearing in relation to persons, information systems or events within the territorial jurisdiction of Pakistan."
- "33. The provisions of this Ordinance shall apply notwithstanding anything to the contrary contained in any other law for the time being in force."

Sections 34 to 37 of the ETO deal with offences. Four different types of offences are mentioned in ETO. Where a subscriber obtains a certificate from the certification service provider providing false information, deliberately, he is guilty of an offence. Any directors or other officers of a certification service provider commit an offence in case they issue a certificate knowing that it is false or they do not cancel a certificate after they have come to know that the information it contains is wrong/false.

A person who accesses or attempts to access an information system with or without the intention to acquire information contained therein is also guilty of an offence under the ETO in case he does so without any authority.

A person would also be said to have committed an offence where he, without any authority, deletes, removes, or alters any information contained in any information system, or he hinders or attempts to hinder access to an information system without any authority to do so. Note that each of the above offences prescribes imprisonment or fine or both. The aforesaid provisions are reproduced below in case you want to look into details: (for exam you are not supposed to memorize these sections)

- "34. any subscriber who:
  - Provides information to a certification service provider knowing such information to be false or not believing it to be correct to the best of his knowledge and belief;
  - Fails to bring promptly to the knowledge of the certification service provider any change in circumstances as a consequence whereof any information contained in a certificate accepted by the subscriber or authorized by him for publication or reliance by any person, ceases to be accurate or becomes misleading, or
  - Knowingly causes or allows a certificate or his electronic signatures to be used in any fraudulent or unlawful manner, shall be guilty of an offence under this Ordinance.
- The offence under sub-section (1) shall be punishable with imprisonment either description of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both."
- "**35.** Every director, secretary and other responsible officer, by whatever designation called, connected with the management of the affairs of a certification service provider, which:
  - Issues, publishes or acknowledges a certificate containing false or misleading information;
  - Fails to revoke or suspend a certificate after acquiring knowledge that any information contained therein has become false or misleading;
  - Fails to revoke or suspend a certificate in circumstances where it ought reasonably to have been known that any information contained in the certificate is false or misleading;
  - Issues a certificate as accredited certification service provider while its accreditation is suspended or revoked; shall be guilty of any offence under this Ordinance.
- The offence under sub-section (l) shall be punishable with imprisonment either description of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both.
- The certification service provider or its employees specified in sub-section (1) shall also be liable, upon conviction, to pay compensation for any foreseeable damage suffered by any person or subscriber as a direct consequence of any of the events specified in clauses (a) to (d) of sub-section (1).
- The compensation mentioned in sub-section (3) shall be recoverable as arrears of land revenue."
- "**36.** Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorized to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both."
- **"37**. Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorized to do any of the foregoing, shall be guilty of an offence under this Ordinance.

- Any person who does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorized to do any of the foregoing, shall be guilty of an offence under this Ordinance.

- The offences under sub-section (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees, or with both."

Lesson 44

GLOBAL LEGAL ISSUES OF E-COM

The ETO establishes jurisdiction with session courts in Pakistan. The court hierarchy involves civil and criminal courts, with appeals moving through district, session, high, and Supreme Courts. Global e-commerce legal issues include jurisdiction, online contracts, copyright, domain disputes, defamation, privacy, internet taxation, and cybercrimes. The ETO has some shortcomings, such as unclear electronic signature distinctions and missing international aspects of e-commerce.

The jurisdiction to try offences under the ETO is vested with the sess
out of place to mention here about the hierarchy of courts in Pakista
divided into two classes on the basis of nature of wrong, namely, civil
with the private rights of the parties, whereas the object of criminal l
wrongs such as breach of contract are deemed to violate only the right
general. On the other hand, a criminal wrong (crime) is an act deemed
general such as theft or murder etc. and the state itself is a party in such matters.

At the bottom of hierarchy, the court having jurisdiction to try civil wrongs is the civil court and the one having jurisdiction to try crimes is the court of magistrate. Appeal against the decision of a civil court or magistrate, in many cases, can be filed in the District court (in civil matters) and in the Session court (in criminal matters), respectively. Further, an appeal can be filed in the High court, in most cases, against the decision of the district/session court.

Likewise, the decision of the High court can be challenged in most cases before the Supreme Court of Pakistan, which is the apex court (the court at the top of the hierarchy). It may be noted that High Court in certain matters has an extraordinary jurisdiction to entertain cases under Article 199 of the Constitution of Pakistan, which is called the writ jurisdiction of the High Court. For instance, where a government body has breached any law, a writ can directly be filed in the High court against such a body.

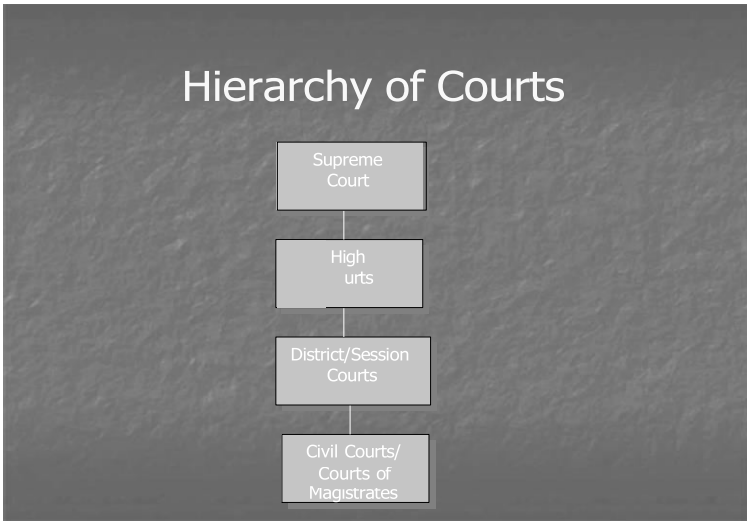

Fig. 1

Most of the countries have, by now, made laws providing recognition to electronic documents and electronic signatures. They have basically followed a model law on e-commerce proposed by a U.N. body called UNCITRAL (United Nations Commission on International Trade Law) in 1996. On analysis, it appears that ETO has certain deficiencies. For instance, difference between an electronic signature and an advanced electronic signature is not clear. Sections dealing with the offences of violation of informational privacy and damage to information/informational systems are too broadly worded, which may lead to confusion. International aspects of e-commerce such as recognition of the foreign certificates and electronic signatures etc. are missing. Difference in the role of accredited certification service providers and non-accredited ones has not been logically defined in the ETO. Above all, the rules (to be made by the Federal Government) and regulations (to be made by the Certification Council) under the ETO are not in place after so many years have elapsed since its enforcement.

Let us now examine some major global legal issues of e-commerce. They are listed as follows:

- Territorial jurisdiction
- Online contracts
- Copyright in cyberspace
- Domain name and trademark conflicts
- Online defamation
- Online privacy
- Issues of taxation on internet
- Cyber crimes

- **Territorial Jurisdiction**

There are different forms of jurisdiction. Territorial jurisdiction refers to the competence of a court to decide a case on the basis of certain geographical area/territory. So, if a dispute arises in Karachi, the courts in Karachi would only have territorial jurisdiction, and the case cannot be filed in Islamabad or Lahore. Ordinarily, territorial jurisdiction lies where the defendant resides or carries on business or the cause of action has wholly or partly arisen or the immoveable property is situated (in case the matter relates to land etc.).

Note that the person who files a lawsuit is called plaintiff and the person against whom it is filed is called defendant. Thus, if a contract is signed at Lahore under which Mr. Ali has to deliver certain goods to Mr. Imran at Karachi and Mr. Ali resides at Rawalpindi, then Mr. Imran can file a suit against Mr. Ali for his failure to deliver the goods. This suit can be filed at any of the three places, that is, Lahore, Karachi or Rawalpindi.

Note that there is no question of any conflict of laws in this scenario since laws all over Pakistan are almost the same. However, things get complicated when we talk of a legal dispute in cyberspace because of the nature of the internet which transcends any geographical boundaries. Here, different countries, having different set of laws, may come into picture having certain linkage with the internet transaction. The issue of territorial jurisdiction becomes complicated when we try to find that the court of which country has the lawful jurisdiction to decide the internet dispute.

For example, an Australian firm having web site in English doing ecommerce does not indicate to its customers that it is an Australian firm. The web server hosting its site may be located in Canada, and people maintaining this site may be the residents of England. Assume a Pakistani buys certain goods from this Australian firm and is, later, unhappy with the goods received. He might want to file a lawsuit against the Australian firm. The border/boundary based system of jurisdiction in the physical world does not help this Pakistani in determining where to file the case. He may consider filing the case in any of the countries which have linkage or connection with the transaction, namely, Australia, England, Canada or Pakistan. Another example is of a defamatory message sent from England defaming a Canadian. The web site may be hosted in Sweden, and the ISP providing services may be located in Brazil. Again, four different countries having different set of laws are emerging in this transaction, that is, England, Canada, Sweden and Brazil.

In all such matters the plaintiff has an option to choose the country/forum for filing his case. Obviously, the plaintiff would choose the forum whose laws are more favorable to him as compared to the defendant. The relative ease with which the plaintiff in cyberspace can drag the defendant to the forum of the plaintiff's choice is called forum shopping. So, if the law of evidence in Singapore suits the plaintiff and he can also establish cause of action or linkage of the internet transaction with Singapore, then the case may be legitimately filed there. One of the key tests that the courts have prescribed to determine territorial jurisdiction in cyberspace is to examine the level of interactivity, commercial nature and effects of the exchange of information.

Online contracts

In the physical world three elements must be satisfied in order to make a valid contract, namely, offer, acceptance and consideration. The same three elements must also be present in case of a valid online contract. An offer is a commitment with certain terms made to another party such as willingness to buy or sell certain product.

A contract is formed when a party accepts the offer of another party for consideration. Consideration is the agreed exchange of something valuable for both the parties such as money, property or services. For example, Mr. 'A' offers to buy a basket of apples for Rs. 200, which is accepted by Mr. 'B' and thus a lawful contract comes into existence between them. Here, consideration for Mr. 'A' is the basket of apples he is getting, and for Mr. 'B', Rs. 200 in exchange of his apples. In most cases when you click 'I accept' or 'I agree' button on a web page, it indicates your acceptance to the terms of a certain offer, and this can give rise to a lawfully binding contract (also known as a click wrap agreement).

It is not necessary to have a written contract. The contract can be made orally or by conduct or through correspondence. So, offers and acceptances can occur in the cyberspace when parties exchange email messages, engage in EDI, fill out web forms or download a web page. An offer can be revoked as long as no payment, delivery of service or other consideration has been accepted. Note where a seller advertises goods for sale on a web site, it is not making an offer but is inviting offers from potential buyers.

Normally, by looking at a web ad, the buyer can send an order, which in fact is an offer the seller can accept, to form a contract. If the seller cannot supply the ordered items it has an option to reject the offer or make a counter offer. Then the buyer has the option to accept or reject the counter offer

(See Fig. 2 below to understand the concept).

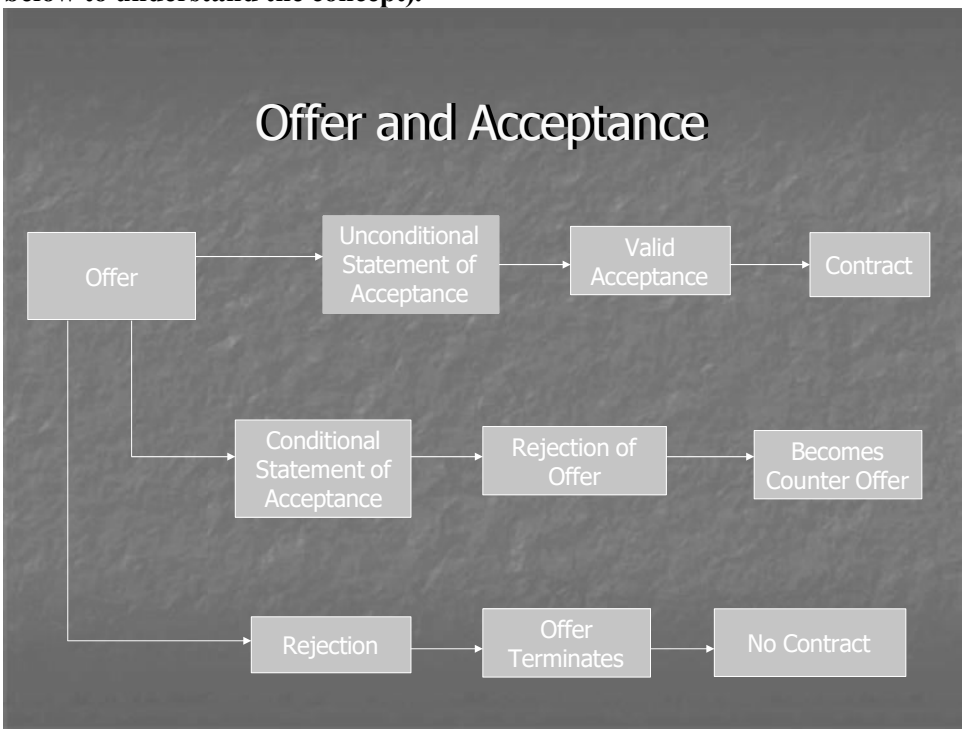

Fig. 2

In online environment acceptances may be issued by an imposter/cheater that does not have authority to bind the online business. To overcome this problem companies and individuals can use digital signatures to establish identity in online transactions.

It is particularly desirable that where a contract is of significant amount, parties should require each other to use digital signatures to establish identity and to confirm that person making an acceptance has the authority to bind the company. Where due to the failure of a company to protect the passwords stored with it, an imposter is able to enter company's system and accept an offer; a court might find such negligent

company to be responsible for the breach of a contract. In such circumstances the company may be directed to fulfill the terms of the contract or pay compensation to the aggrieved party.

Copyright in cyberspace

Copyright is a huge area of concern in cyberspace due to the nature of internet technology. A copyright is an exclusive right granted by law to the author or creator of a literary or artistic work to reproduce, print, publish or make copies of such work. Creations or works that can be copyrighted include books, music, artwork, audio and video recordings, computer software, architectural drawings, product packaging etc.

Note that there is no copyright in ideas. Only, a particular form or expression of the idea can be copyrighted. If an idea cannot be separated from its expression, the work cannot be copyrighted. Thus, in most cases, mathematical calculations cannot be copyrighted. Most web pages are likely to be protected by copyright because words, graphics and html tags are arranged in such a manner that it may give rise to an original work. Naturally, it causes a problem. Each time an http request is made by a client, a copy of the html document can be made on the client machine. Similarly, where ISPs are engaged in caching, an extra copy of the web page is made/stored in cache memory on the system of the ISP. Some people had argued that copyright law could not be enforced on the internet in the above circumstances.

There is a concept of 'fair use' or 'fair dealing' in copyright law that provides legitimate exceptions to copyright violation. Generally, fair use of a copyrighted work includes copying it for use in criticism, comment, news reporting, teaching, scholarship or research. Experts draw support from this concept of 'fair use' to deal with the problem of copyright over the internet. It is also argued that in cases where the author of a work has himself provided a hyperlink leading to his work, he should be regarded as giving the implied authority or license to download or make copies of his work. In such an eventuality, the issue of copyright should not arise according to an opinion.

Generally, the protection under 'fair use' may be sought on the following basis:

Nature of use:- the work has been used for educational and/or non-profit purposes only;
Nature of work:- if the copied work contains factual information then it may be more effectively covered under the fair use clause as opposed to some creative work;
Extent of the work copied:- if the amount of work copied is insignificantly small then the courts might take a view favorable to the accused;
Effect on the market value of the work:- A person alleged with the copyright violation may escape any liability arguing that the work has not been circulated to many people and there has not been any negative impact on the value of actual work due to the circulation.

When you make fair use of a copyrighted work you should provide citation to the original work to avoid any charge of plagiarism. The charge of plagiarism can be leveled against a person who tries to copy the expression of the original author presenting it be his expression in order to obtain credit for the academic work. Academic institutions can take serious action against students/persons who are found guilty of plagiarism.

It may be interesting to refer to the famous 'Napster case', here. The company, Napster, had a web site. It used to provide software and a network to millions of people using which they could exchange music files on internet that they had copied and compressed into MP3 format. Many music recording companies sued Napster for facilitating violations of their copyright. Napster argued that it only provided the way or machinery but was not directly involved in copyright violation. Disagreeing with that the courts in America found that Napster was guilty of vicarious or contributory copyright infringement, as it was capable of supervising infringing activity and was obtaining a financial benefit for such an activity. Eventually, the court ordered that Napster site should be shut down. Napster agreed to pay 26 million dollars in damages for copyright infringement to a group of music companies and agreed to pay copyright holders for the music that would be downloaded in future.

World Intellectual Property Organization (WIPO) is a U.N. sponsored body. In 1996 it proposed two international treaties on copyright which were signed by many countries of the world. Those who signed these treaties agreed to adopt or amend laws in their respective countries to ensure protection to copyrighted work of the author of a signatory country in view of the new infrastructure or technological developments in respect of digital information exchange.

Lesson 45

GLOBAL LEGAL ISSUES OF E-COMMERCE

Patent infringement

A patent is an exclusive right granted by law to make, use and sell an invention. In order to be patentable, the invention must be unique, genuine, and useful according to the prevalent technological standards. Patenting software programs is not considered a popular option these days. Firms, which had developed software programs for web sites, have experienced that obtaining a software patent is expensive and quite time consuming. Therefore, copyright registration of software programs is considered a more feasible option. It may, however, be interesting to talk about 'business process patents' which have value for e-commerce companies. These patents are granted on 'methods of doing business', and protect a specific set of procedures for doing a certain business activity. For instance, a famous online business has conceived a unique 1-click purchasing method. Another e-business has a peculiar price tendering system ('name your own price' system). Similarly, an online business uses a specific approach of aggregating information from different web sites. The aforesaid businesses have found their respective business process patents to be quite useful. However, in the opinion of some experts the grant of such business process patents can cause unfair monopoly of the recipients. The courts have yet to decide complicated issues involving business process patents.

Trade mark and domain name conflicts

A trade mark is that sign/symbol that associates the manufacturer or service provider with the manufactured goods or services, respectively. For instance, where the letter 'u' is written in a particular style (say in a circle) on the product packaging, it can be termed as a trade mark. A trade name is that name or brand under which a business carries on its business activity to become recognizable. Often, a trade name can be used as a part of the trade mark. A domain name is the user friendly name used to access a web site, such as 'vu.edu'. Domain names are unique and global in nature which means that there cannot be two similar domain names. On the other hand, trade marks/trade names can be multiple and localized. Thus, same trade mark/trade name can be used in relation to the same product/service in different countries or geographical areas. Similarly, same trade mark/trade name can be used in relation to different products/services within the same geographical area. Based upon this distinction between trade marks/trade names and the domain names, the experts have identified four areas of conflict as follows:

Cyber squatting

The act of intentionally registering domain names containing trademarks/trade names of prominent companies to later blackmail or demand ransom from those companies is called cyber squatting. It is regarded as an offence in most countries. Assume there is a firm 'Glory Enterprise' and it wants to have its web site. It also wants to have the word 'glory' as a part of its domain name because for years it has been recognized in the physical world through this word. However, at the time of registration of its domain name it finds that a person Mr. 'A' who has nothing to do with the business of the firm or the word 'glory' has already registered a domain name containing this word as a part of it. Since there cannot be two similar domain names, the firm is forced to request Mr. 'A' to transfer that domain name to it. In response, if Mr. 'A' blackmails or claims ransom from the said firm, he would be said to have committed cyber squatting.

Concurrent use

This problem arises when two organizations have apparently legitimate claim to use the same domain name but cannot do so due to the uniqueness of domain names. Suppose, there is a company manufacturing electronic goods and another company selling French fries. Under the traditional trade mark law both these companies can have the same trade mark/trade name such as 'frys'. The problem arises when both apply for the registration of a domain name containing the word 'frys'. Here, both are

legitimate claimants of this domain name but due to the element of uniqueness of domain names only one of them can be assigned the desired domain name.

Parasites

Parasite domain names are variants on famous domain names, and are confusingly similar to them to gain business advantage. For instance, a software company may intentionally register a domain name as 'macrosoft.com' (a variant of domain name of the famous company 'Microsoft') to take advantage of the reputation of 'Microsoft'. The idea is that someone intending to reach the web site of 'Microsoft' may mistype or misspell and reach the web site of 'Microsoft', instead. xyz.com vs. xyz.org

This problem arises due to the fact that second level domain names can be assigned to multiple top-level domains. For example, 'whitehouse.org' and 'whitehouse.com' are two valid domain names. The former may take you to the web site containing information about the residence of the American President, whereas the later may have been deliberately registered with the same second level domain but a different top-level domain to gain business advantage. Thus, it is quite possible that a person wishing to know about the residence of the American President reaches an irrelevant or pornographic web site after typing the word 'Whitehouse' on a search engine.

International Corporation for Assigned Names and Numbers (ICAAN), which supervises the task of registration of domain names worldwide, has developed and implemented a policy known as Uniform Dispute Resolution Policy (UDRP) for deciding domain name disputes. It enables trademark holders to claim/retrieve domain names by invoking mandatory arbitration proceedings at different arbitration forums or service providers. Arbitration is a legal concept in which parties, through an agreement, appoint/nominate a person or a panel to act as a judge in the matter instead of referring the dispute to the ordinary court of law. The decision of the arbitrator is regarded as final and binding on the parties. World Intellectual Property Organization (WIPO) based in Switzerland is one such arbitration service provider nominated under the UDRP.

Online Defamation

A defamatory statement is a false statement that injures the reputation of on another person or company. If a statement injures the reputation of a product or service instead of a person, it is called product disparagement. Suppose, someone circulates a news item in the media about the reputation of a doctor, alleging him to be professionally incompetent and negligent. This doctor may then file a lawsuit against that person claiming that his reputation has been injured due to such an act. Often, in cases of defamation the plea taken by the defendant is that his statement is not false. Rather, it is a 'fair comment'. In case defamation is done using the internet, it is termed as online defamation. In countries abroad, the courts are replete with cases of online defamation, mainly, because the person causing defamation can expect to remain anonymous due to the nature of internet technology.

It is difficult to draw a clear line between justifiable criticism and defamation. So, commercial web sites should avoid making negative or critical statements about other persons or products. Similarly, web site designers should avoid any defamation liability when indulged in the alteration or modification of a picture or image of a person. They should not depict such person in derogatory or negative sense. Moreover, any online statement about the competitors must be carefully reviewed before posting it on the web, lest it contains any element of defamation.

Closely connected with online defamation is the issue of liability of the internet service providers (ISPs). ISPs provide the channel for communication. An ISP may be accused of aiding in the commission of online defamation where it provides hosting service to a web site containing defamatory material. Courts have prescribed a test in determining ISP's liability in such a case. Accordingly, where the ISP has editing control; it can review any defamatory material and take it down from the web site; it should be treated as a publisher. In such a case the ISP can be held liable for online defamation. Conversely, where the ISP has no editing control over the offensive material posted on a web site; it would be merely acting as a distributor. In such a case, the ISP can escape liability for online defamation.

Online Privacy

Issue of online privacy is constantly evolving as internet grows as a tool of communication and commerce. Due to the nature of internet technology, it is possible for web sites to collect information about page viewing habits of visitors, product selection and demographic information (age, sex etc.) about the customers. This may threaten informational privacy rights of such visitors/customers. Cultural difference in different countries is the reason why there are different levels of expectations about privacy in different parts of the world. Many countries have, today, privacy laws such as Canada, European Union (EU) etc. Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA) is the federal law in Canada in this regard. In 1998, the EU adopted a directive on the protection of personal data, which gave the form of law to different constitutional guarantees/rights about privacy existing in most European countries. This is applicable to all internet activities. The directive also prevents businesses from exporting personal data outside EU unless this data is protected in the exporting country according to the provisions of the directive. In the Unites States of America, the government has avoided to introduce any firm privacy regulations. Companies in the U.S.A. are entitled to make policies or devise mechanism to regulate privacy issues themselves. The companies have adopted two different approaches in this regard, that is, opt-out approach and opt-in approach. In more common opt-out approach, the company collecting information assumes that the customer does not object to a specific use of information unless the customer specifically denies the permission. Thus, the company may use the collected information for its own purpose, as well as, sell or rent it out to other firms or persons.

In less common opt-in approach, the company collecting information assumes that it cannot use the information for any other purpose except the one for which it is collected. Accordingly, it cannot sell, market, or rent out this information to other firms/persons unless the customer specifically chooses to allow such a use. Experts have highlighted four guiding principles to form the basis of any privacy legislation. These are as follows:

- collected data may be used for improved customer service;
- sharing of personal data with outside firms/persons should not be allowed unless the customer consents to that;
- customers should have the right to receive information about what type of data has been collected from them and in what manner has it been used;
- customers should have the right to ask for the deletion of any of their data collected by the company.

Internet Taxation

Companies doing business on the web are subject to same taxes as any other business. However, traditional businesses operating at one location are subject to only one set of tax laws, but due to the international scope of ecommerce, e-businesses might have to comply with multiple tax laws enforced in different countries. An online business is subject to various taxes which include income tax, transaction taxes and property tax. Income tax is levied by the national or state or local government (where the business is located) on the net income generated by business activities. Transaction taxes include sales tax and custom duties which are levied on the products or services a business sells. Sales tax is levied on goods sold to customers. Traditionally, businesses have to file sales tax return with a competent authority and remit sales tax which they have collected from their customers on the sale of products or services. Custom duties are taxes levied or imposed by countries on the import of goods into the country. Property taxes are imposed by a government (including a local government) on personal property and real estate used in the business. Among these, income tax and sales tax are more important.

Note that a government acquires the power to tax a business when that business establishes a connection with the area controlled by such government. Thus, connection between a tax payer and a government is called nexus. It is necessary to understand ‘nexus’ in order to determine where a particular tax has to be paid by an online business. E-businesses doing business in more than one

country have to deal with the issue of nexus to know the governments/countries entitled to levy/receive taxes from them. Generally, the principle is that if a company undertakes sufficient business activities in a particular country it establishes nexus with that country and becomes liable for filing returns in that country and it must comply with its tax laws. Therefore, an e-business may be required to separately file tax returns and pay taxes in different countries. A web site maintained by a company in the United States must pay income tax to the American government on income generated inside and/or outside of the U.S.A. However, to avoid the issue of double taxation, the U.S. tax law allows credit/refund for taxes paid (if any) to the foreign countries in relation to foreign earnings. It is important for an online seller to know where the customer is located and what the law of sales tax is in that country or jurisdiction to determine whether or not a particular item is subject to sales tax.

Cyber Crimes

The use of internet technology has given rise to crimes which could not be conceived of a few years ago. Such crimes more suitably called cyber crimes include online fraud, online hate (spreading hatred against a community through internet), cyber-stalking (sending threatening messages using internet), online terrorism, distribution of pornography, using a computer for launching attacks on other computers etc. Today, many countries of the world are busy in either drafting new laws to deal with the issue of cyber crimes or making suitable amendments in existing criminal code. Again, the issue of territorial jurisdiction is critical in this behalf. For instance, where a Pakistani resident commits a cyber crime against a Canadian resident, the question arises whether or not the Canadian court can take an action against this Pakistani, particularly, where the act of Pakistani is not considered criminal under the Pakistani law.