Unit-III

E-Payment System:

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

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

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

3.2 Types of Electronic Payment Systems:

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

- Organizations are motivated by the need to deliver products and services more cost effectively and to provide a higher quality of service to customers.
- The emerging electronic payment technology labeled electronic funds transfer (EFT).
- EFT is defined as ―any transfer of funds initiated through an electronic terminal telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution.

EFT can be segmented into three broad categories:

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

❖ **Credit card-based payments systems**

- Encrypted Credit Cards (e.g., World Wide Web form-based encryption)
- Third-party authorization numbers (e.g., First Virtual)

3.3 E-Cash:

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

E-cash must have the following four properties.

- Monetary value
- Interoperability
- Retrievability
- Security

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

• Concerns about electronic payment methods include:

– Privacy

– Security

– Independence

– Portability

Electronic Cash Storage:

• Two methods

– **On-line**

• Individual does not have possession personally of electronic cash

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

– **Off-line**

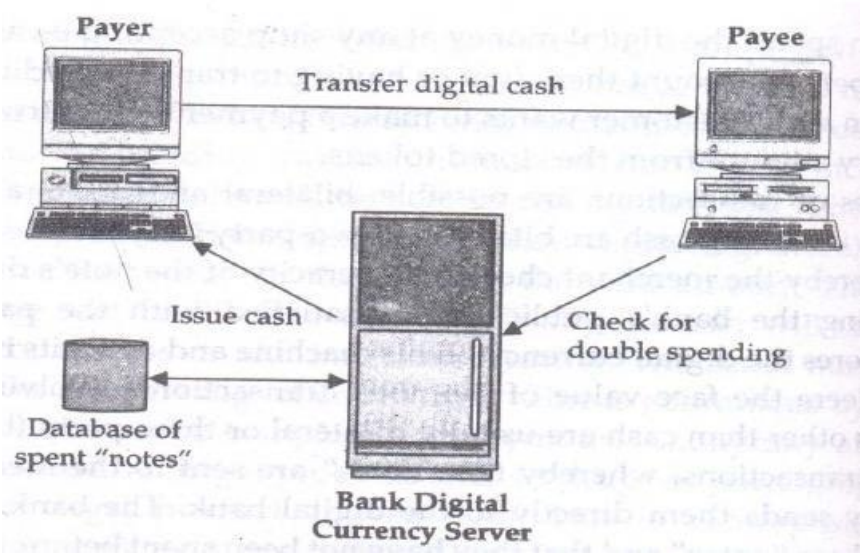
• Customer holds cash on smart card or electronic wallet

• Fraud and double spending require tamper-proof encryption

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

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

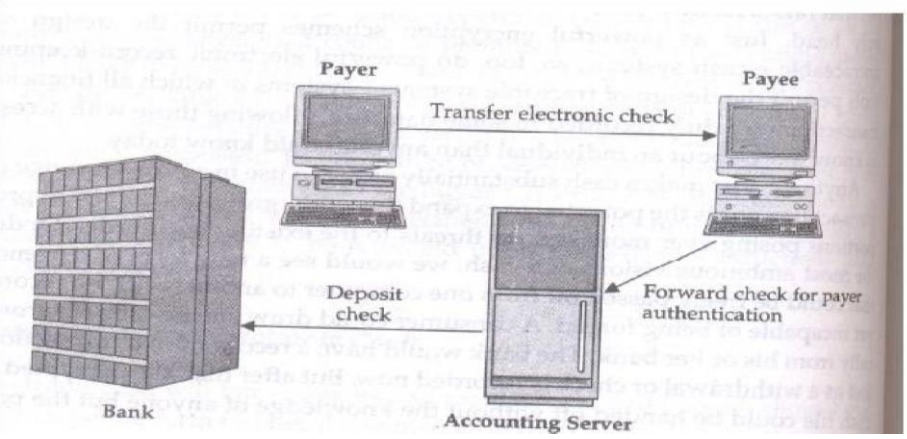
- Once the tokens are purchased, the e-cash software on the customer‘s PC stores digital money undersigned by a bank.
- The users can spend the digital money at any shop accepting e-cash, without having to open an account there or having to transmit credit card numbers.
- As soon as the customer wants to make a payment, the software collects the necessary amount from the stored tokens



– Convenience

3.4 Electronic Checks:

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



Advantages of Electronic Checks:

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

3.5 Smart Cards & Electronic Payment Systems:

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

Types of Smart Cards:

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

➢ **Relationship-Based Smart Credit Cards:**

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

➢ **Electronic Purses:**

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

The electronic purse works in the following manner:

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

Credit Card-Based Electronic Payment Systems:

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

– Credit cards

- Such as a Visa or a MasterCard, has a preset spending limit based on the user‘s credit limit. – Debit cards
- Removes the amount of the charge from the cardholder‘s account and transfers it to the seller‘s bank. – Charge cards
- Such as one from American Express, carries no preset spending limit. **Advantages:**

– Payment cards provide fraud protection.

– They have worldwide acceptance.

– They are good for online transactions.

Disadvantages:

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

3.6 Risks in Electronic Payment systems:

- Customer's risks
  - – Stolen credentials or password
  - – Dishonest merchant
  - – Disputes over transaction
  - – Inappropriate use of transaction details
- Merchant‘s risk
  - – Forged or copied instruments
  - – Disputed charges
  - – Insufficient funds in customer‘s account – Unauthorized redistribution of purchased items

3.7 Electronic payments Issues:

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

Security Requirements In Electronic Payment Systems:

- **Integrity and authorization**

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

- **Out-band authorization**

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

- **Password authorization**

  Atransaction protected by a password requires that every message from the authorizing party include a cryptographic check value. The check value is computed using a secret known only to the authorizing and verifying parties. This secret can be a personal identification number, a password, or any form of shared secret. In addition, shared secrets that are short - like a six-digit PIN - are inherently susceptible to various kinds of attacks. They cannot by themselves provide a high degree of security. They should only

be used to control access to a physical token like a smart card (or a wallet) that performs the actual authorization using secure cryptographic mechanisms, such as digital signatures.

- **Signature authorization**

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

- **Confidentiality**

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

- **Availability and reliability**

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

3.8 Electronic Data Interchange(EDI):

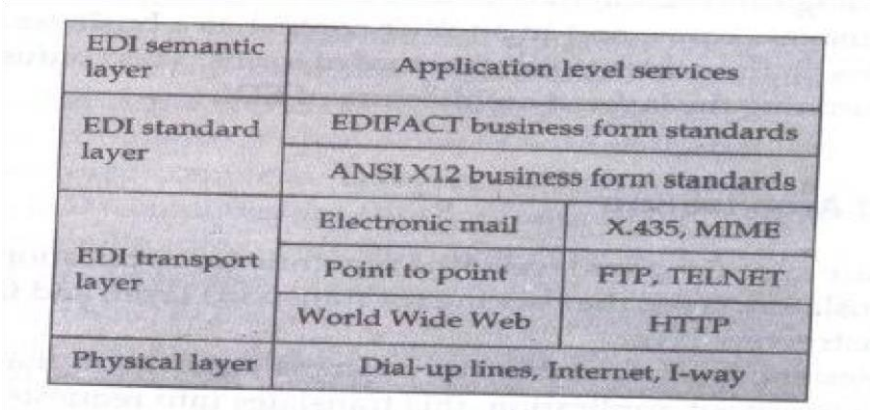
- Electronic Data Interchange (EDI) - interposes communication of business information in standardized electronic form.
- Prior to EDI, business depended on postal and phone systems that restricted communication to those few hours of the workday that overlap between time zones.

Why EDI?

- Reduction in transaction costs
- Foster closer relationships between trading partners **EDI & Electronic Commerce**
- Electronic commerce includes EDI & much more
- EDI forges boundary less relationships by improving interchange of information between trading partners, suppliers, & customers.

3.9 EDI layered architecture:

- Semantic (or application) layer
- Standards translation layer
- Packing (or transport) layer
- Physical network infrastructure layer



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

EDI semantic layer:

- Describes the business application
- Procurement example
  – Requests for quotes
  – Price quotes
  – Purchase orders
  – Acknowledgments
  – Invoices
- Specific to company & software used

Standards translation:

- Specifies business form structure so that information can be exchanged
- Two competing standards
  – American National Standards Institute(ANSI)X12

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

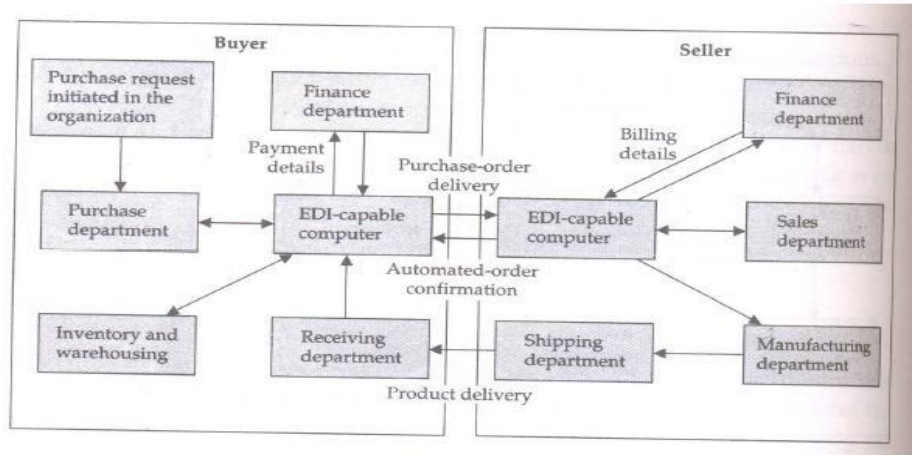
EDI transport layer

- How the business form is sent, e.g. post, UPS, fax
- Increasingly, e-mail is the carrier
- Differentiating EDI from e-mail
  – Emphasis on automation
  – EDI has certain legal status

Physical network infrastructure layer

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

Information flow with EDI:



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

3.10 Applications of EDI:

1. Role of EDI in international trade: Reduced transaction expenditures

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

2. Interbank Electronic Funds Transfer (EFT)

- EFTS is credit transfers between banks where funds flow directly from the payer‘s bank to the payee‘s bank.
- The two biggest funds transfer services in the United States are the Federal Reserve‘s system, Fed wire, & the Clearing House Interbank Payments System (CHIPS) of the New York clearing house

3. Health care EDI for insurance EDI

- Providing good & affordable health care is a universal problem
- EDI is becoming a permanent fixture in both insurance & health care industries as medical provider, patients, & payers
- Electronic claim processing is quick & reduces the administrative costs of health care.
- Using EDI software, service providers prepare the forms & submit claims via communication lines to the value-added network service provider
- The company then edits sorts & distributes forms to the payer. If necessary, the insurance company can electronically route transactions to a third-party for price evaluation
- Claims submission also receives reports regarding claim status & request for additional Information

4. Manufacturing & retail procurement using EDI

- These are heavy users of EDI
- In manufacturing, EDI is used to support just-in-time.
- In retailing, EDI is used to support quick response

3.11 EDI Protocols:

- ANSI X12
- EDIFACT

Comparison of EDIFACT & X.12 Standards:

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

3.12 E-Marketing:

- E-marketing is directly marketing a commercial message to a group of people using email. In its broadest sense, every email sent to a potential or current customer could be considered email marketing.
- It usually involves using email to send ads, request business, or solicit sales or donations, and is meant to build loyalty, trust, or brand awareness.
- Email marketing can be done to either sold lists or a current customer database. Broadly, the term is usually used to refer to sending email messages with the purpose of enhancing the relationship of a merchant with its current or previous customers, to encourage customer loyalty and repeat business, acquiring new customers or convincing current customers to purchase something immediately, and adding advertisements to email messages sent by other companies to their customers.

Advantages:

- An exact return on investment can be tracked and has proven to be high when done
- properly. Email marketing is often reported as second only to search marketing as the most effective online marketing tactic.
-

- Email marketing is significantly cheaper and faster than traditional mail, mainly because of high cost and time required in a traditional mail campaign for producing the artwork, printing, addressing and mailing.

Advertisers can reach substantial numbers of email subscribers who have opted in (i.e., consented) to receive email communications on subjects of interest to them.

Almost half of American Internet users check or send email on a typical day with email blasts that are delivered between 1 am and 5 am local time outperforming those sent at other times in open and click rates.

- Email is popular with digital marketers, rising an estimated 15% in 2009 to £292 m in the UK.

- If compared to standard email, direct email marketing produces higher response rate and higher average order value for e-commerce businesses.

Disadvantages:

- A report issued by the email services company Return Path, as of mid-2008 email deliverability is still an issue for legitimate marketers. According to the report, legitimate email servers averaged a delivery rate of 56%; twenty percent of the messages were rejected, and eight percent were filtered.

- Companies considering the use of an email marketing program must make sure that their program does not violate spam laws such as the United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),the European Privacy and Electronic Communications Regulations 2003, or their Internet service provider's acceptable use policy.

3.13 Tele Marketing:

- Telemarketing is a method of direct marketing in which a salesperson solicits prospective customers to buy products or services, either over the phone or through a subsequent face to face or Web conferencing appointment scheduled during the call.
- Telemarketing can also include recorded sales pitches programmed to be played over the phone via automatic dialing.
- Telemarketing may be done from a company office, from a call center, or from home. It may involve a live operator voice broadcasting which is most frequently associated with political messages.

- An effective telemarketing process often involves two or more calls. The first call (or series of calls) determines the customer‘s needs. The final call (or series of calls) motivates the customer to make a purchase. Prospective customers are identified by various means, including past purchase history, previous requests for information, credit limit, competition entry forms, and application forms. Names may also be purchased from another company's consumer database or obtained from a telephone directory or another public list. The qualification process is intended to determine which customers are most likely to purchase the product or service.

- Charitable organizations, alumni associations, and political parties often use telemarketing to solicit donations. Marketing research companies use telemarketing techniques to survey the prospective or past customers of a client‘s business in order to assess market acceptance of or satisfaction with a particular product, service, brand, or company. Public opinion polls are conducted in a similar manner.

- Telemarketing techniques are also applied to other forms of electronic marketing using email or fax messages, in which case they are frequently considered spam by receivers.

Disadvantages:

- Telemarketing has been negatively associated with various scams and frauds, such as pyramid schemes, and with deceptively overpriced products and services
- Telemarketing is often criticized as an unethical business practice due to the perception of high-pressure sales techniques during unsolicited calls.

- Telemarketers marketing telephone companies may participate in telephone slamming, the practice of switching a customer's telephone service without their knowledge or authorization.

- Telemarketing calls are often considered an annoyance, especially when they occur during the dinner hour, early in the morning, or late in the evening.

3.14 Security Threats to E-commerce:

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

Client threats

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

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

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

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

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

Communication channel threats

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

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

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

Integrity threats can alter vital financial, medical, or military information. It can have very serious consequences for businesses and people.

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

Server threats

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

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

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

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

Common gateway interface threats: A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs are programs, they present a security threat if misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious

CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

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

3.15 Security Requirements For E-Commerce:

Authentication:

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

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

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

Privacy:

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

HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

Authorization:

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

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

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

Integrity:

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

One solution is afforded by using digital certificates to digitally ―sign‖ messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and compare it against the

one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

Non-repudiation:

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

3.16 Security policy for E-commerce:

The security policy may cover issues like:

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

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

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

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

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

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

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

The main objective of the COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and

professional organizations. The SSE-CMM is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are in the Information Technology Security domain.

3.17 Firewall:

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

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

Types of Firewall:

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

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

➢ **Network layer Firewall:**

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

Network layer firewalls generally fall into two sub-categories,

- Stateful Firewalls
- Stateless Firewalls

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

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

- **Application Layer Firewall:**

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

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

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for

processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.

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

- **Proxy server:**

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

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

- **Network Address Translation:**

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

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

3.18 Digital Signatures:

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

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

A digital signature scheme typically consists of three algorithms;

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Applications of digital signatures:

Authentication:

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

Integrity:

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

Non-repudiation:

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

Some digital signature algorithms:

RSA-based signature schemes, such as RSA-PSS

DSA and its elliptic curve variant ECDSA

ElGamal signature scheme as the predecessor to DSA, and variants Schnorr signature and Pointcheval–Stern signature algorithm

- Rabin signature algorithm
- Pairing-based schemes such as BLS
- Undeniable signatures

Aggregate signature - a signature scheme that supports aggregation: Given n signatures
- on n messages from n users, it is possible to aggregate all these signatures into a single
- signature whose size is constant in the number of users. This single signature will
- convince the verifier that the n users did indeed sign the n original messages.
-

• Signatures with efficient protocols - are signature schemes that facilitate efficient cryptographic protocols such as zero-knowledge proofs or secure computation.

3.19 Digital Certificate:

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

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

- The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. • The most widely used standard for digital certificates is X.509.

Contents Of a Typical Digital Certificate:

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

Payment in E-Commerce

Types of payment in e-commerce

Payment is a main part of commercial transaction against the goods supplied. In E-commerce four types of payment are made. They are as under -

1) Credit card payments
2) Electronic cheque payments
3) Payment for services such as internet, these payments is micro or small payment.
4) Electronic-cash payments
5) Digital cash (e-cash)
6) Online stored value system
7) Smart Cards

8) B2B payment system

Credit card payment - Online credit card is much similar to actual card being used no card impression is taken and no signature is available. For credit card payment there is a participation of four members. They are as follows:

- Customer and credit card of him
- Merchant who accept the credit card (such as VISA, MASTER CARD etc)
- issuing Bank of the credit card which collects payment from customers.

•In this process the bank or the financial institution sets up an account with a merchant and authenticates the card information which is send electronically by merchant and sanctions sales depending on the credit card status of the customer. Bank then accepts the credit cards. Credit cards may be of different credit card companies. Merchant gets the payment from the bank with guarantee. Bank issuing credit card returns financial information.

When customer wants to purchase he or she adds the item to the merchant's shopping cart When the customer wants for the payment a secure tunnel through the internet is created using SSL (Secure Socket Layer). Using encryption SSL secures the session during which the credit card information will be sent to the merchant and protects the information. Once the consumer credit card information is received the merchant software contacts a clearing house which authenticates credit card and verifies account balances. Clearing house contacts the issuing bank to verify the account information. Once verified the issuing bank credits the account of the merchant's bank. The debit to the consumer account is transmitted to the consumer [21].

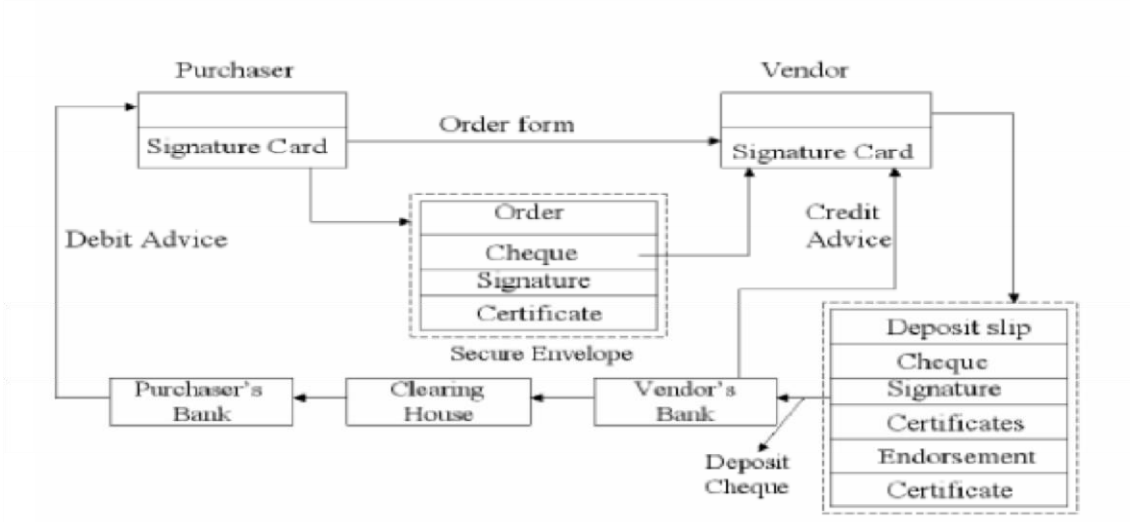
Electronic Cheque Payment

A special hardware is required in order to sign the cheques which are used to do transactions which are attached to PC.A special hardware is used to do encryption of the signature. Public keys of the business partners are authenticated by certifying agencies.

Steps in transaction

1. Purchaser sends Purchase order and payment advice with his private key. He encrypts his Public key certificate using vendor's public key and sends it to vendor.
2. Vendor converts the message in the readable format using his private key checks certificate and cheque and then attaches deposit slip encrypts with

Figure 1.8: Electronic Cheque Payment



Payments of Small Amounts on Internet

bank's public key and sends it to bank.. Then he also sends public key certificate after encryption

3. After checking the signatures and credits, bank clears cheque. Credit advice is given to vendor and combined debit advice is sent to purchaser from time to time. Payment for services such as internet, these payments is micro or small payment.

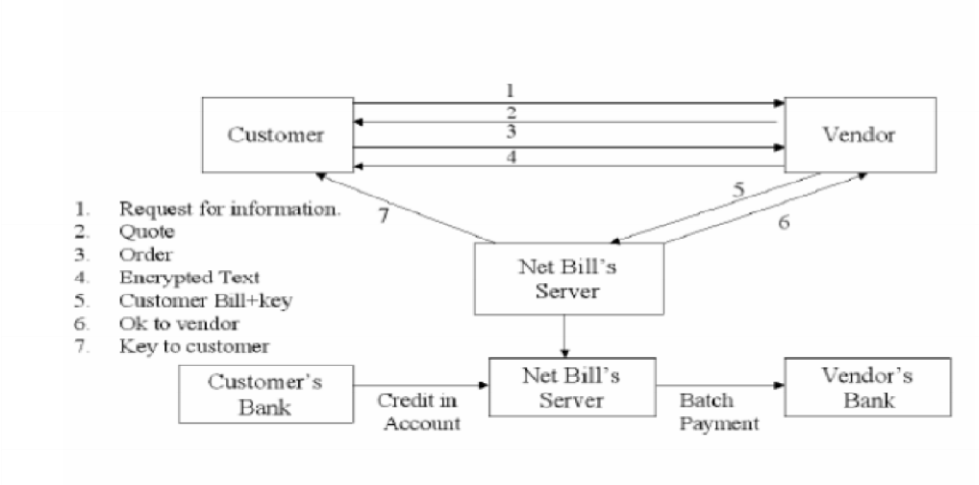
NETBILL'S PROPRIETARY SYSTEM

- Only after customer is charge, information delivered
- After information is delivered, vendor guaranteed payment
- Net bill is the intermediary

MAJOR STEPS

- When customer asks for information, vendor sends encrypted information to the customer but without encryption to customer.
- Along with the information obtained, Payment order is sent to vendor
- Copy of purchase order and key for decryption is sent by Vendor to NET BILL.
- Credit of the customer is checked by NET BILL. If it is ok it sends key to customer.
- Vendor account is credited and customer account is debited and a key is send to the customer to debit customer account.
- Customer decrypts information

Figure 1.9: Paying for Small Internet Transactions



Electronic Cash (Digital Cash)

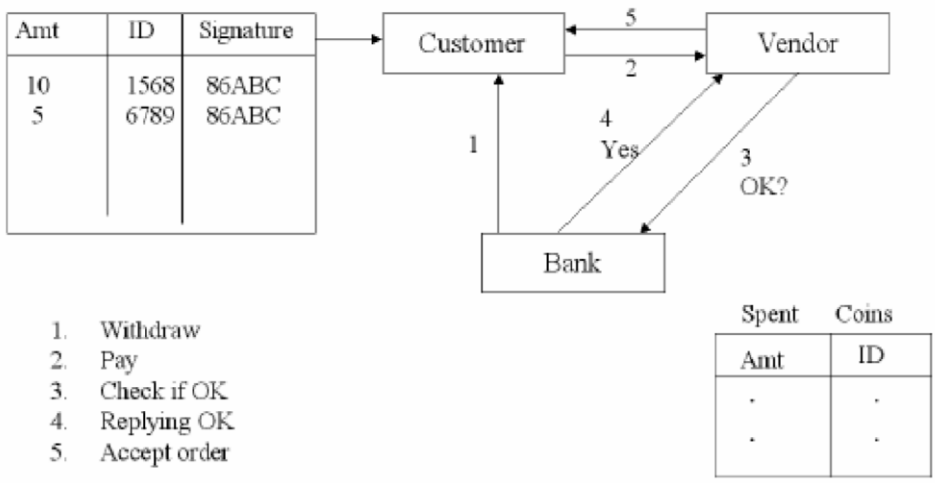
- For small payment Cash payment is done
- Cash preserves secrecy
- Cash should not be traceable
- It is cheaper than credit card transaction
- DES is normally used for these transactions as it is cheap and amount involved is small

Traceable cash payments

STEPS

1. Customer withdraws coins in various denominations signed by bank Structure of the file is as follows- serial no, denomination, signature of bank A copy of issued coins is stored by bank.
2. Using signed coins customer pays to vendor.
3. Bank checks for whether it is current or spent
4. If it is current, it authorizes dispatch of goods and credits vendor account with electronic coins

Figure 1.10: Electronic cash



Digital cash was one of the first forms of alternative payment systems developed for e-commerce. The early generations of digital cash were quite complex and required the generation of entire new payment industry standards & practices. First generation digital cash worked as follows - To use e-cash customer had to first establish an account at bank that was using e-cash system. Once the account was established the customer then downloads digital wallet software on his computer. Then the customer could request a transfer of digital cash. Once the digital wallet had cash the consumer could spend that cash at merchants who were willing to accept it. The software would deduct the cash from the digital wallet and transfer to the merchants. The merchant could then transfer the cash back to the bank to confirm that it has not been double spent. The bank would then cancel the e-coins and credit the merchant's account at the bank. These early concepts were not market successes proving too complicated for both consumers and merchant. One variation on the digital cash concept is gifi cash which is a form of e-cash that is earned as a "points". Two of the best providers of gifi cash are Beenz.com (which issued points as a reward for purchase) and Flooz.com (which could be purchased as a form of gift certificate) both ceased operations in August 2001.Mypoints.com which issues points that can be redeemed for merchandise or gift certificates (but not cash) at partners sites in exchange for viewing ads or trying special offers is still in business as of August 2001. However mypoints.com can be considered a gift cash provider although the primary focus of its efforts is developing loyalty programs for clients rather than providing an online currency

[21]. The way of handling digital cash and its details are given in table no. 1.8[20] **Table No. 1.6 Types of Digital Cash and their Year Founded /description**

System	Year Founded /description
First Virtual	1994 – 1st secured stored value system based on credit card pre use deposits and pin numbers. Ceased operations in 1998.
Digital Cash (e–cash)	1996 Encryption based stored value system requiring digital wallet on hard drive to store e-coins. Ceased operations in 1998 returned as ecash
Millicent	1996 Digital equipment Corporation's entry into micro payment e-cash. Now a Compaq platform product with multiple options.
Peer to peer payment Systems	
Paypal	1999 free P2P micropayment system
Yahoo Paydirect	1999 . Free Yahoo P2P payment service
Money Zap	1999 Western Union fee-based money transfer system

Online Stored value system: Makes customer pay instantly to merchants and other individuals based on value stored in an online account. Some stored value systems require the user to download a digital wallet (for example Monetta's debit service and eCharge's prepaid service) where as others require to simply sign up and transfer money from their existing credit card accounts into an online stored value account. Online stored value systems rely on the value stored in a consumer's bank checking or credit card account. For example Ecount offers a prepaid debit account. To use Ecount a consumer first establishes an account with Ecount funded by a credit or debit card. Account information is transferred via the web using SSL. Once Ecount has verified the account and its balance with the consumer's card issuing bank. Consumers can shop on the web where Mastercard is accepted and email payments to individuals. Ecount debits the consumers account and transfers the funds to the merchant or individuals. At the end of the month the consumer's card issuing bank sends a statement showing the debit to Ecount. Rocketcash is another company that offers online stored value system in this case aimed at teenagers **[20]**. Table no. 5 gives detail online stored value system and use of cards.

Table 1.7: Online Stored Value System

System	Year Founded /Description
Ecount	1998 Prepaid debit account
Monetta Prepaid	2000 Prepaid virtual card that allows consumers to make online payments without using a credit card or bank account digital wallet.
Monetta Debit	2000 Account that allows users to pay fro m existing checking savings online of credit accounts Digital Wallet
eCharge	1997 Prepaid account with digital wallet.
Millicent	1998 Prepaid cards purchased at convenience stores (Japan only)
Smart Cards	
Mondex	1994 smart card stored value system in which value is stored on a chip on a card.
American Express Blue	1999 bined credit and smart card

Smart Cards as Stored Value System - are another kind of stored value system based on credit cards that have embedded chips that store personal information. Where as credit cards store a single charge account number in the magnetic strip on the back smart cards can hold 100 times more data including multiple credit card numbers and information regarding health insurance transportation personal identification bank accounts and loyalty programs such as frequent flyer accounts. This capacity makes them an attractive alternative to carrying dozen or so credit and ID card in a physical wallet. Smart cards can also require a password unlike credit cards adding another layer of security. There are two types of smart cards – contact & contactless depending on the technology embedded. In order for contact cards to be read they must be physically placed into a card reader while contact less cards have an antenna built in that enables transmission of data without direct contact. A stored value smart card such as retail gift card purchased in a certain dollar value is an example of contact card because it must be swiped through a smart card reader in order for payment to be processed. A highway toll payment system such as EZPass is an example of a contactless smart card because the EZPass device in the card is read by a remote sensor with the appropriate toll automatically deduced from the card at the end of the trip. The Mondex card is one of the original smart cards invented in 1990 by Natwest bank in England [21]. **B2B Payment Systems -** Most of the payment are

done physically by checks because of the complexity of the B2B business. There are two main types of B2B payment systems that have risen to the challenge. They are – 1) Systems that replace traditional banks 2) existing banking systems extending to the B2B marketplace. No system on the market today yet provides all of the features listed. Actrade is an example of an online B2B payment system that replaces the functionality provided traditionally by banks. Actrade serves as an international marketplace intermediary in the payment process by paying foreign sellers immediately and allowing domestic buyers a variable time a variable time period for repayment.