Electronic Payment System:

- An e-commerce payment system facilitates the acceptance of electronic payment for online transactions.
- Also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.
- Electronic payment is an integral part of electronic commerce.
- Broadly defined electronic payment is a financial exchange that takes place online between buyers and sellers
- Three factors are stimulating interest among financial institutions in electronic payments
  a. Decreasing technology cost
  b. Reduced operational and processing cost
  c. Increasing online commerce.

Overview of the Electronic Payment Technology

- Electronic payment first emerged with the development of wire transfers services such as western Union.
- There was no any banking environment and it was indeed a telegraph company
- Authentication was provided by only signature at the other end of the transmission that verified that the intended party had indeed received the funds.
- During 1960s and 1970s private networking technology has enabled the development of alternative electronic funds transfer(EFT) systems.
- EFT have shortened the time of payment instruction transfer between banks however it have not change the fundamental structure of the payment system.
- Recent innovations in electronic commerce aim to affect the way consumers deal with payments and appear to be in the direction of real time electronic transmission ,clearing and settlement system.
- Recently several innovations helped to simplify consumer payments .these includes
  - ❖ Innovations affecting consumers :credit card and debit cards ,automated teller machines(ATMS) and electronic banking
  - ❖ Innovations enabling online commerce: digital cash, electronic checks, smart cards (also called electronic purses) and encrypted credit cards
  - ❖ Innovations affecting companies: the payment mechanisms that banks provide to corporate customers such as interbank transfers through automated clearing house

The online shopping Experience:

- Consumers browses for items using web browsers ,views an online catalog on web pages etc
- Consumers selects items to be purchased on the basis of prices, brand value, quality and other variables.
- The merchants presents the consumer with an order form containing the list of items, their prices and total prices which includes shipping ,handling and taxes.
- The consumer selects the means of payment.
- The consumers sends the merchant a completed order and a means of payment,
- The merchant request payment authorization from the consumer's bank
- The merchants sends the customer a confirmation of the order shipment and payment
- The merchant ships the goods or performs the requested services as per the order.
- The merchant requests payment from the consumer's financial institutions.

Limitations of traditional payment instruments:
- Lack of security
- Handling micropayments
- Inconvenience
- Incompatibility
- Delay due to verification and authorization
- Risk of loss or theft
- Processing cost for micropayments too high
- Less convenient
- Cash payment necessitates meeting between buyer and seller
- Security risk
- Not everyone accepts credit cards
- Some buyers do not have credit cards

Hence to better suit the needs of electronic commerce several companies are developing entirely new forms of financial instruments such as digital cash, electronic money and electronic checks.

Requirements for e-payments:
- **Atomicity**
  - Money is not lost or created during a transfer
- **Good atomicity**
  - Money and good are exchanged atomically
- **Non-repudiation**
  - No party can deny its role in the transaction
  - Digital signatures

Electronic or Digital Cash:

- Digital cash is a system of purchasing cash credits in relatively small amounts, storing the credits in your computer, and then spending them when making electronic purchases over the Internet Most merchants accepting digital cash so far, however, use it as an alternative to other forms of payment for somewhat higher price purchases. There are several commercial approaches to digital cash on the Web. Among these are eCash from DigiCash and Cybercash.
- Electronic or digital cash combines computerized convenience with security and privacy that improve on paper cash.
- Digital cash attempts to replace paper cash as the principal payment vehicle in online system.
- Although the 3 decades of development of electronic payment system ,cash is still the dominant form of payment because of lack of customer trust in banking system, inefficient clearing and settlement of noncash transaction and negative real interest rates on bank deposits.
- In comparision to cash , debit and credit cards have a number of limitations like they are only identification cards owned by the issuer and restricted to one user and also their usages requires an account relationship and authorization system
- So it is need to create a form of digital cash that has some of the properties of cash.

E-cash Concept

1. Consumer buys e-cash from Bank
2. Bank sends e-cash bits to consumer (after   charging that amount plus fee)
3. Consumer sends e-cash to merchant
4. Merchant checks with Bank that e-cash   is valid (check for forgery or fraud)
5. Bank verifies that e-cash is valid
6. Parties complete transaction: e.g., merchant   present e-cash to issuing back for deposit   once goods or services are delivered.

Properties of Electronic   Cash:

Digital cash must have the following four properties

- ➢ **Monetary value:** digital cash must have a monetary value , it must be backed by cash , bank authorized credit or a bank certified cashiers check.
- ➢ **Interoperability :** Digital cash must be interoperable or exchangeable as payment for other digital cash, paper cash ,goods or services
- ➢ **Retrievability:** it must be storable and retrievable .Remote storage and retrieval would allow user to exchange digital cash from home or office or while travelling. The cash could be stored in a remote computers memory in smart cards or on any special purpose devices

> ➤ **Security :** it should not be easy to copy or tamper with while it is being exchanged.

Digital Cash on Action:
- Digital cash is based on the cryptographic called a digital signature.
- This method involves a pair of numeric keys that work in tandem: one for locking or encryption and the other for unlocking or decryption.
- Message Encoded with one numeric key can only be decoded with other numeric key.
- The encryption is kept private and the decryption key is made public.
- By supplying all customers with its public key a bank enables customers to decode any message or currency encoded with the bank's private key.
- Before digital cash can be used to buy products or services it must be procured from a currency server

Purchasing Digital Cash from currency servers:

The purchase of digital cash from an online currency server or bank involves two steps the establishment of an account and the maintenance of sufficient money in the account to back any purchases .some customers might prefer to purchase digital cash with paper currency either to maintain anonymity or because they don't have bank accounts. Currently the most digital cash system require that customers have an account with a central online bank. To support global access digital cash must be available in multiple currencies backed by multiple banks.

Electronic checks (e-cheques):
- Electronic checks are designed to accommodate the many individuals and entities that might prefer to pay on credit or through some mechanism other than a cash.
- Electronic checks are modeled on paper checks except that they are initiated electronically , use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account.
- The security/ authentication aspects of digital checks are supported via digital signatures using public key cryptography.
- Ideally electronic check will facilitate new online services by: allowing new payment flows (the payee can verify funds availability at the payer's bank , enhancing security at each step of the transaction through automatic validation of the Electronic signature by each party (payee and banks) and facilitating payment integration with widely used EDI based electronic ordering and billing processes.

- Electronic checks are delivered either by direct transmission using telephone lines, or by public networks such as the internet.
- Electronic check payments (deposits) are gathered by banks and cleared through existing banking channels such as automated clearing houses.
- This integration of the existing banking infrastructure with public networks provides an implementation and acceptance path for banking, industry and consumers to build on existing check processing facilities.
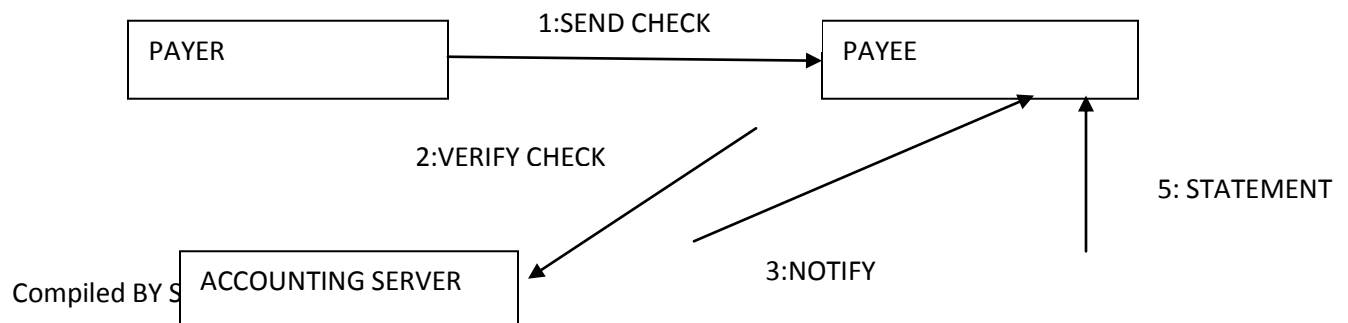
Benefits of Electronic Checks:
 Electronic checks have the following advantages:
- It works in the same way as traditional checks thus simplifying customer education.
- It retain the basic characteristics and flexibility of paper checks while enhancing the functionality
- It can be easily understood and readily adopted.
- It is well suited for clearing micropayments
- It can also be validated automatically
- Electronic checks create float and the availability of float is an important requirement for commerce.

Electronic Check in Action:
The electronic check process works in the following ways:
- Electronic check users must register with a third party account server before they are able to write electronic checks.
- The account server also acts as a billing service
- The registration procedure can vary depending on the particular account server and may require a credit card or a bank account to back the checks.
- Once registered a consumer can then contact a seller for goods and services.
- Using email or other transport methods the buyer sends an electronic check to the seller for a certain amount of money.
- When deposited the check authorizes the transfer of account balances from the account against which the check was drawn to the account to which the check was deposited.
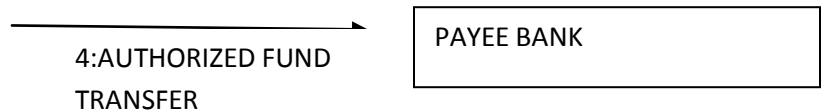

PAYER — 1:SEND CHECK → PAYEE

2:VERIFY CHECK

5: STATEMENT

ACCOUNTING SERVER

3:NOTIFY

PAYEE BANK

4:AUTHORIZED FUND
TRANSFER

FIG: CHECK ENCASHMENT PROCESS

Online Credit Card Based Systems:

- Used for the majority of Internet purchases
- Has a preset spending limit
- Currently most convenient method
- Most expensive e-payment mechanism
- Credit card payment negotiation involves two steps
  - ➢ The merchant presents the customer with product / service price,order confirmation and status , delivery notifications and payment options accepted by the merchant and
  - ➢ the buyer presents the merchant with payment choice and associated information in a secure manner.
- There is no standard way of sending secure payment instructions over the web
- Currently , consumers can shop ,look at content and read products descriptions in the web environment but have to go off line in order to use their credit cards to actually make their purchases.
- Different vendors for credit cards are working to make their customer assure about the security of their services.
- The different payment schemes require customers to set up special accounts and / or buy or download and install special software for their personal computer.
- Safe credit card based commerce will not be possible until security standards are in place.
- Security standards ensure the negotiation of payment schemes and protocol and safe transport of payment instructions

FIGURE 7-13 *Processing a payment card order*
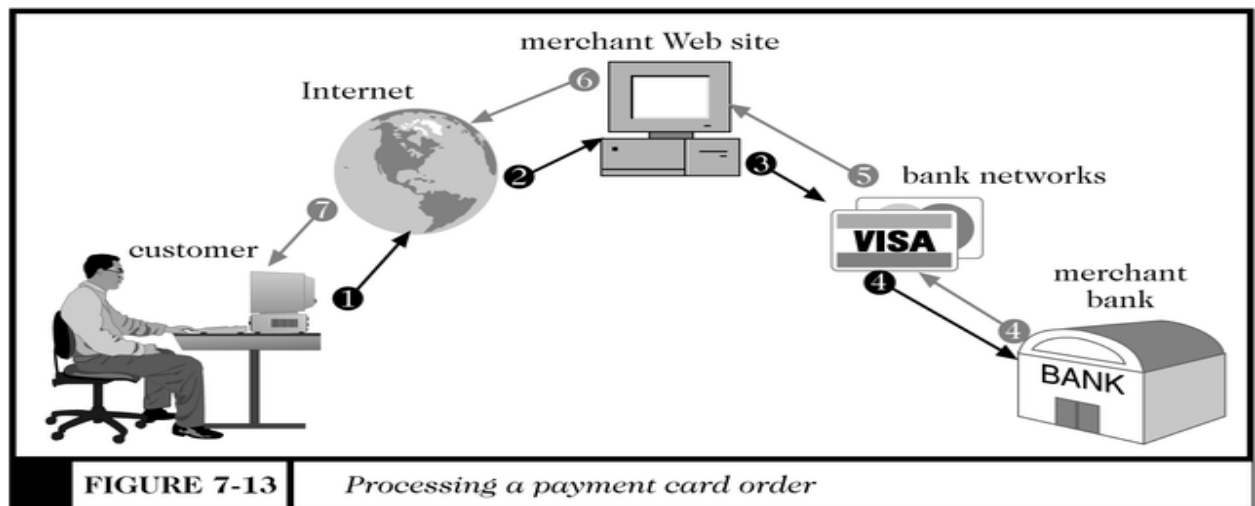
Types of credit card Payments:

Credit card based payments can be divided into three categories

- **Payments using plain credit card details:**
    - ➢ The easiest method of credit card payment is the exchange of unencrypted credit cards over a public network such as telephone lines or the internet.
    - ➢ The low level of security inherent in the design of the internet makes this method problematic
    - ➢ Authentication is also a significant problem and the vendor is usually responsible for ensuring that the person using the credit card is its owner

- **Payment using encrypted credit card details:**
    - ➢ Encryption is initiated when credit card information is entered into a browser or other electronic commerce device and sent securely over the network from buyer to seller as an encrypted message.
    - ➢ There are still certain factors to consider before sending them out such as the cost of a credit card transaction itself which might prohibit low value payments   (micropayments)
    - ➢ The process of making payment using encrypted credit card details are as follows

1. A customer presents his or her credit card information along with an authentic signature or other necessary information securely to the merchant
2. The merchant validates the customer's identity as the owner of the credit card account
3. The merchant relays the credit card charge information and digital signature to his or her bank or online credit card processor.
4. The bank or processing party relays the information to the customer's bank for authorization approval.
5. The customers bank returns the credit card data , charge authentication and authorization to the merchant.

- **Payments using third party verification:**
  - One solution to security and verification problems is the introduction of a third party to collect and approve from one client to another.
  - Information seller and buyers only need an internet mailbox and a First virtual account .
  - First virtual (FV) makes servers available to sellers lacking the computer capacity or warehouse internet servers to handle their sales directly.
  - The following seven step process captures the essence of FV system.
    1. The consumer acquires an account number by filling out a registration form which gives FV a customer profile that is backed by a traditional financial instruments such as credit card
    2. To purchase an article , product or other information online , the consumer request the item from the merchant by quoting her FV account number. the purchase can take place in one of two ways : the consumer can automatically authorize the "merchant" via browser settings to access her FV account and bill her or she can type in the account information.
    3. The merchant contacts the first virtual payment server with the customers account number.
    4. The first virtual payment server verifies the customer's account number for the vendor and checks for sufficient funds
    5. The first virtual payment server sends an electronic message to the buyer . This message could be an automatic WWW form or a simple email. The buyer responds to the form or email in one of three ways: yes ,I agree to pay; No I will not pay or Fraud , I never asked for this.

6. If the First virtual payment server gets a Yes from the customer the merchant is informed and the customer is allowed to download the material immediately.
7. First Virtual will not debit the buyer's account until it receives confirmation of purchase completion. Buyers who receive information or a product and decline to pay may have their accounts suspended.

Secure Electronic Transactions (SET):

- Secure electronic transactions is a protocol for encrypted credit card payment transfers.
- SET is based on public key encryption and authentication technology .
- The objective of payment security are to provide authentication of cardholders, merchants and acquirers ; provide confidentiality of payment data ; preserve the integrity of payment data and define the algorithms and protocols necessary for these security services.
- The major **objective of SET** are defined below
  1. **Confidentiality of information:** provides confidentiality by the use of message encryption
  2. **Integrity of information:** SET ensures that message content is not altered during the transmission between originator and recipient. Information integrity is ensured by the use of digital signature.
  3. **Consumer account authentication:** merchants need to verify that a consumer is a legitimate user of valid account number . digital signatures and a digital certificates ensure consumer account authentication by providing a mechanism that links a consumer to a specific account number.
  4. **Merchant authentication :** the SET specifications provide a way for consumer that a merchant has a relationship with a financial institution that allows that merchant to accept bank card payments,. It is ensured by the use of digital signatures and merchant certificates.
  5. **Interoperability:** the SET specifications must be applicable on a variety of hardware and software platforms and must not prefer one over another.

Smart cards:

- Plastic card containing an embedded microchip
- Smart cards also called stored value cards use magnetic stripe technology or integrated circuit chip to store customer specific information , including electronic money.
- The cards can be used to purchase goods or service , store information , control access to accounts and perform many other functions.

- Smart cards offer clear benefits to both merchants and consumers, they reduce cash handling expenses and losses caused by fraud, enhance consumer convenience and safety.

Smart card Applications:
- Ticketless travel
- Authentication, ID
- Medical records
- E-cash
- Store loyalty programs
- Personal profiles
- Government
    - Licenses
- Mall parking

Digital/Electronic wallets:

Software that resides on a buyer's computer and holds digital cash, and a digital certificate with a digital signature, as well as billing, shipping, and payment information for online transactions. Also called electronic wallet.

Consumer ,legal and business issues:
The key consumer issues associated with payment system include:
- **Consumer** protection from fraud arising from efficiency in record keeping
- Transaction privacy and safety
- Competitive pricing of payments services to ensure equal access to all consumers
- Right to choice of institutions and payment methods

Record keeping and Proof of Payments:
- **All** electronic payment systems need to be able to keep automatic records.
- An automatic record is an after the fact transcription of what happened , created .

Managing Information Privacy:
- The electronic payment system must ensure and maintain privacy.
- Privacy must be maintained against intruders on the network and against unauthorized insiders.
- The user must be assured that they cannot be easily duped or falsely implicated in a fraudulent transactions.
- This protection must be apply throughout the whole process by which a good is purchased and delivered.

Risk and Threat on electronic payment system:

One important challenge of e-commerce is risk management. The working of the payment systems incurs three major risks; mistake, privacy problems and credit risk.

Risks from Mistake and Disputes

Consumer Protection

Virtually all electronic payment systems require some ability to keep automatic records. Once information has been electronically caught , it is easy and not expensive to keep.

The intangible nature of electronic transactions and resolution of the disputes relying alone on records, a general law of payment dynamics and banking technology might be : No data should be discarded. Features of these automatic records are :

1. Permanent storage
2. Accessibility and traceability
3. A payment system database and
4. Data transfer to payment maker, bank or monetary authorities.

The need of keeping of records for the purposes of risk management conflicts with the transaction anonymity(secrecy) of cash. An unknown payment system without automatic record keeping facility will be difficult for bankers and government to accept. However, customers might feel that all this record keeping is an invasion of privacy.

Managing Information Privacy

The electronic payment system must provide and maintain privacy. Every time one purchases goods using a credit card, subscribes to a magazine or accesses a server that information goes into a database somewhere. This violates one the unspoken laws of doing business; that the privacy of customers should be protected as possible.

All details of a consumer's payments can be easily be aggregated : Where, when and sometimes what the customer buys is stored. This data collection tells much about the person and as such can conflict with the individual's privacy.

Privacy must be maintained against eavesdroppers on the network and against unauthorized insiders. The users must be given assurance that they cannot be easily duped or falsely implicated in a fraudulent transaction. This protection has to be applied on the whole transaction protocol.

Managing Credit Risk

Credit risk is an important concern in systems of net settlement because a bank's inability to settle its net position could give rise to a chain reaction of failures of the banks. The digital

Compiled BY Sudip Raj Khadka

central bank must prepare policies to handle this possibility. Various alternatives exist, each with advantages and disadvantages.

A digital central bank guarantee on settlement issues eradicates the insolvency test from the system because banks will more easily assume credit risks from other banks,

Designing E-Payment System:

It includes several factors:

• **Privacy**. A user expects to trust in a secure system; just as a telephone is a safe

• **Security.** A secure system verifies the identity of two-party transactions through "user authentication" & reserves flexibility to restrict information/services through access control

• **Intuitive interfaces**. The payment interface must be as easy to use as a telephone.

• **Database integration.** With home banking, for ex, a customer wants to play with all his accounts.

• **Brokers.** A "network banker"-someone to broker goods & services, settle conflicts, & financial transactions electronically-must be in place

• **Pricing.** One fundamental issue is how to price payment system services. For e.g., from cash to bank payments, from paper-based to e-cash. The problem is potential waste of resources.

• **Standards**. Without standards, the welding of different payment users into different networks & different systems is impossible.