ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

Certificate in e-Commerce

CEC-04

E-payment System and M-commerce

Block – 01

Electronic Payment Systems

Unit-1 Payment Processing Network And Payment Gateway

Unit-2 Electronic Payment Modes/Systems

Expert Committee

Dr. P.C Samantaray
Former Principal
Institute of corporative Management
Bhubaneswar –**Member**

Dr . K.C Padhy
Ex. DGM, State Bank of India & Former Principal
SBI Staff Training Institute
Sambalpur – **Member**

Dr. S.N. Mishra
Dept. of Tourism & Hospitality Management
BJB (Autonomous) College,
Bhubaneswar, – **Member**

Dr. Mihir Ranjan Nayak
Director, Planning
KIIT University - **Member**

Prof (Dr.) Susanta K. Moharana
Former Principal
Regional College of Management &
Consultant,
School of Business & Management
Sambalpur, Odisha - **Convener**

Course Writer

Dr. Suresh Chandra Das
Reader in Commerce
U.N Autonomous College
Adaspur, Cuttack

Course Editor

Dr. S.K Moharana
Consultant (Academic)
Odisha State Open University,
Sambalpur

Material Production

Dr. Jayanta Kar Sharma
Registrar
Odisha State Open University, Sambalpur

Printed by : Sri Mandir Publication, Sahid Nagar, Bhubaneswar

Unit-1 Payment Processing Network And Payment Gateway

Learning Objectives

After reading this chapter, students should be able to:

- Understand the meaning of electronic payment systems
- Discuss the payment processing network and its mechanism
- Understand the SET Protocol
- Enumerate the Benefits of Payment Gateways

Structure

1.1 OVERVIEW

E-payment system is a way of making transactions or paying for goods and services through an electronic medium without the use of check or cash. It's also called an electronic payment system or online payment system. The electronic payment system has grown increasingly over the last decades due to the widely spread of internet-based banking and shopping. As the world advance more on technology development, a lot of electronic payment systems and payment processing devices have been developed to increase, improve and provide secure e-payment transactions while decreasing the percentage of check and cash transaction. E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labor cost. Being customer friendly and

less time consuming than manual processing, it helps business organization to expand its market reach / expansion.

1.2 THE PAYMENT PROCESSING NETWORK

Purchasing online may seem to be quick and easy, but most consumers give little thought to the process that appears to work instantaneously. For it to work correctly, merchants must connect to a network of banks, processor and other players. The players of the payment processing network are:

1. Merchant: Merchant is a business that sells services or merchandise and accepts credit cards as payment, and the Acquirer is the bank through which the Merchant has its merchant account. For the Cardholder to do business with the Merchant, the Issuer and Acquirer must belong to the same Interchange Association, such as Visa or MasterCard.

2. Cardholder: The individual consumer owning the card and responsible for paying the card account. The Cardholder uses the card to pay for goods and services, and pays cash to the Issuer upon receipt of the card account statement.

3. Acquirer: The bank through which the Merchant has its merchant account. Upon settlement of a transaction, the Acquirer deposits funds in the Merchant's bank account. The Acquirer's revenue comes from the difference between the merchant discount and an interchange discount paid to the Issuer. The Acquirer is at risk if the Merchant defaults on refunds or chargebacks. Most major banks act in an Acquirer role.

4. Issuer: The bank that issues the credit card to the Cardholder, pays the Acquirer for the discounted amount of any transactions on the card, and collects payment from the Cardholder. The Issuer's revenue comes from the interchange discount plus any fees and interest paid by the Cardholder. The Issuer is at risk if the Cardholder fails to pay their balance.

5. Interchange Association: The association of banks that allows any Merchant customer of a member-acquiring bank to accept a credit card from any Cardholder customer of a member-issuing bank. Visa and MasterCard are the dominant

interchange associations worldwide. The interchange associations provide brand support as well as facilities for performing the actual transaction interchange.

6. Processor: A third party company, also known as a processing network that accepts electronic credit card transactions from Merchants and processes them for an Acquirer. The processor handles notifying the Acquirer of the transactions (so that funds can be deposited in the Merchant's account) as well as transmitting the transactions to the Interchange Association. An Acquirer is typically associated with just one Processor, and pays that Processor for its services. Each Processor has a different protocol for receiving transaction information from Merchants. Third party Processors are primarily used in the United States, where the multitude of smaller banks allows them to offer economies of scale. Outside the United States, each country typically has a very small number of banks, so each bank handles its own transaction processing.

7. Gateway: A third party company that accepts electronic payment transactions over the Internet and sends them directly to the Processor for processing. There are two types of gateway companies, companies that develop their own software such as TPI Software's Payment Server, CyberSource and Authorizer.net and companies like CardService International that use a third party company's software from someone like ClearCommerce and Paylinx to process the transactions. These companies are known as Commerce Service Providers or CSPs.

8.Application Developers: The individual responsible for integrating payments into business applications, whether custom systems or vertical- market products, many have found the transaction processing protocols complicated and fast-changing, as well as inconsistent among different processing networks. This drove demand for transaction-processing modules or components that could be easily integrated into applications without having to worry about these complexities.

1.3 HOW PAYMENT PROCESSING WORKS

This diagram illustrates how real-time, electronic credit card processing works.

Step-1: Purchaser places order.

Step-2: Merchant securely transfers order information to CyberSource over the Internet. CyberSource receives order information and performs requested services.

Step-3: CyberSource formats the transaction detail appropriately and securely routes the transaction authorization request through its payment gateway to the processor.

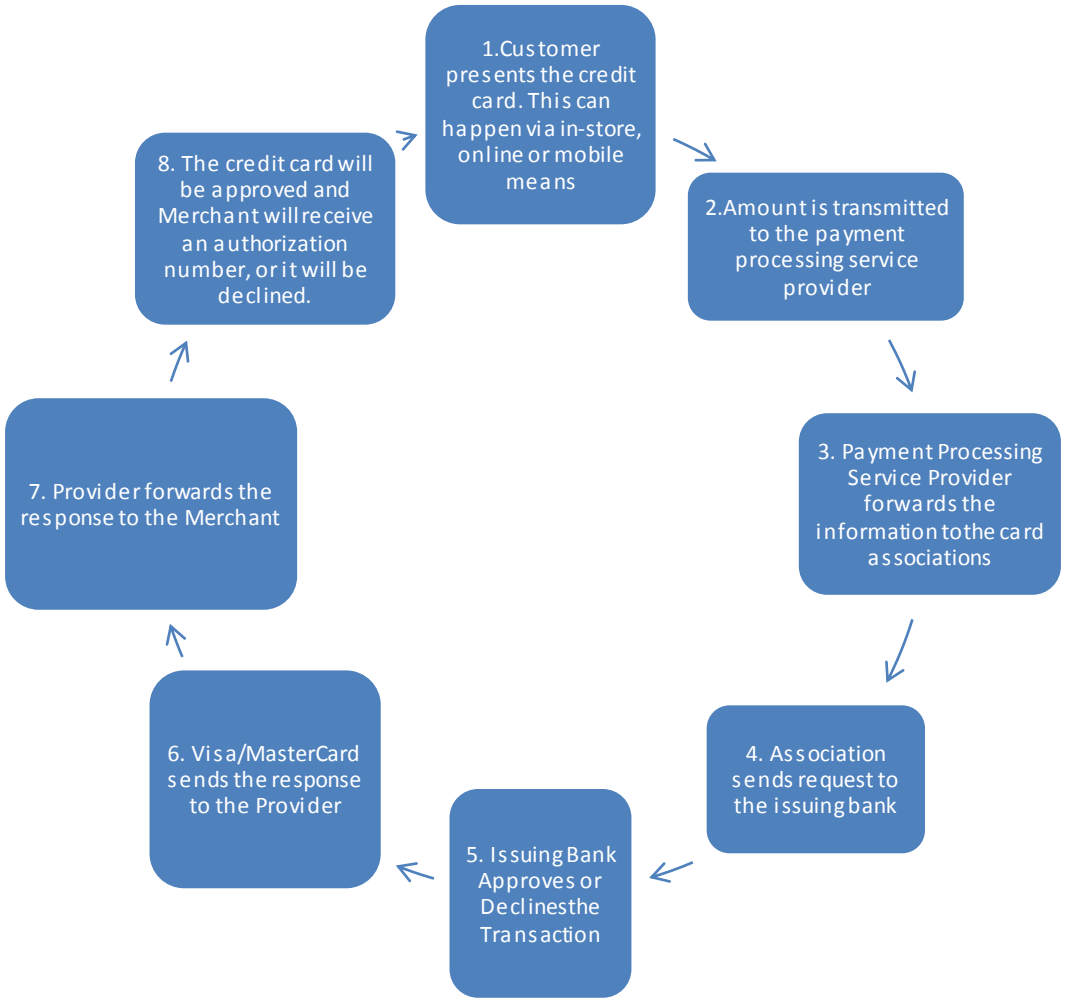
Step-4: The transaction is then routed to the issuing bank (purchaser's bank) to request transaction authorization.

Step-5: The transaction is authorized or declined by the issuing bank or card

Step-6: CyberSource returns the message to the merchant.

Step-7: Issuing bank approves transfer of money to acquiring bank.

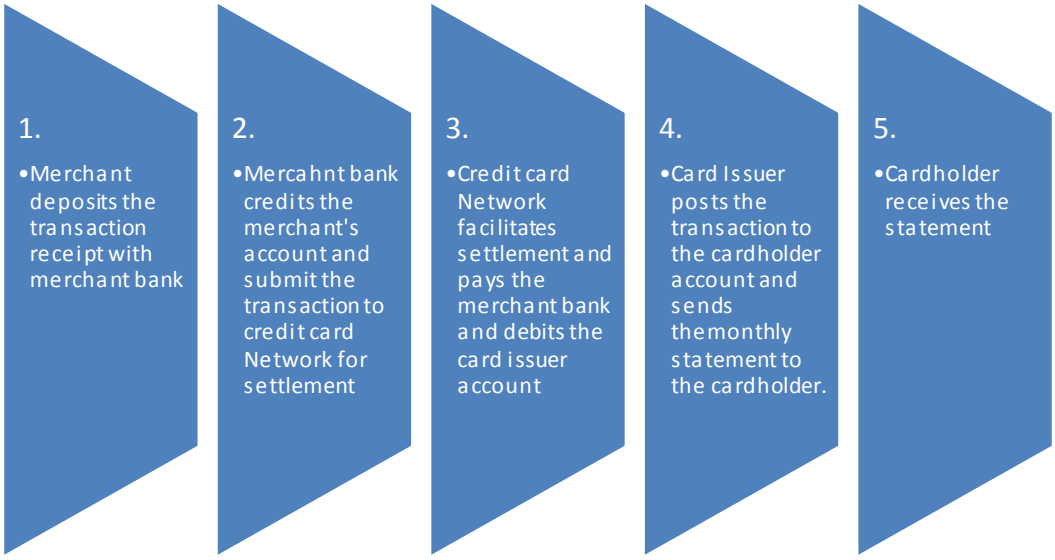
Step-8: The acquiring bank credits the merchant's account.



1.4 PAYMENT PROCESSING SETTLEMENT

By accepting credit cards at store, customers become an integral part of the payment processing system, which is why it is important that customers develop a clear picture of the card transaction process: what it is, how it works and who participates in it. This basic knowledge will help clients understand the major payment processing components and how they affect the way clients do business.

Credit card payments are not completed until the transaction information is submitted to the processing bank. Typically transactions are submitted electronically and all point-of-sale (POS) and virtual payment processing systems are programmed to automatically do that at pre-defined intervals, usually at the end of the business day. Exceptions are made for merchants who cannot connect to the processor at the time of the transaction, for example taxis and limousine services, street fairs, etc. In such cases, merchants can submit their transactions on paper.



1.5 SECURITY PROTOCOLS FOR WEB COMMERCE

Security in E- commerce is very important part since communication can be easily intercepted, messages can be inserted, and the absolute identity of involved parties may be uncertain. There is a lack of a consistent and coherent set of protocols to

cover the needs of merchants and consumers. However, one should minimize the effects of security failures on cyberspace for reliable electronic commerce systems. Security tries to accomplish the following tasks:

(i) Authentication which identifies buyer and also makes sure that person is who he/she claims to be. Used methods are i.e. digital signature, finger prints, password or smartcards etc.

(ii) Data integrity which means, that there must be a way to verify that data is not changed during the transactions.

(iii) Confidentially must be preserved, so information concerning the tarns action are need to know basis.

(iv) Non repudiation, which means that person who did the payments is not able afterwards deny doing so.

Among other considerations, it needs to consider the following important issues:

(i) ***Electronic Identification Strategy:*** It requires cryptographic security techniques to ensure transaction authentication and choose between secret key cryptography (SKC) MACing (Message Authentication Code) or public key cryptography (PKC) digital signatures.

(ii) Level of Security: The determination of a security level will have impact on the type of electronic identification means given to clients. The choice is between logical securities in software-based authentication or physical security if a security device is introduced into the picture.

(iii) Client Authentication Strategy: With the PKC digital signatures, this issue is rooted in the PKI security model, and the role of certification authorities (CA). Where with SKC, the foremost options are the manual delivery of cryptographic keys or implied security model suggests the client enrolment.

(iv) Confidentiality Requirements: Even if the critical aspect of E-commerce security is transaction authentication, confidentiality requirements are a significant design issue. This confidentiality requirements issue is independent from the selection of a security model. Obviously, when the confidentiality mechanisms are considered, the selection of SKC or PKC does matter.

1.5.1 E-COMMERCE SECURITY PROTOCOLS

While purchasing a product online, the potential purchaser fills in the payment (credit card) information, and sends that information to the merchant over the internet. At the merchant's site

(A) Secure Sockets Layer (SSL)

In 1994, Netscape developed its first standard of Secure Socket Layer (SSL) to implement secure environment to exchange the information over the Internet and made it public for implementation in fall 1994. SSL is a security protocol protects communications between any SSL -enabled client and server software running on a network that uses TCP/IP, Gopher, FTP, Telnet etc.

SSL approach is to add a layer on top of the existing network transport protocol and beneath the application. This approach applied by adding an intermediate step, requiring negotiation of secure transmission options, to the establishment of a network connection. Data flowing between the client and the server on that connection is encrypted before transmission and decrypted before it can be used by the receiving system.

During SSL connection establishment only the server is authenticated using a digital certificate (authentication of the customers usually occurs through customer name and password after the SSL connection has been established). SSL also offers the option for client authentication based on digital certificates.

Advantages of SSL

(i) Transparency- since SSL provides security at the session layer, its presence is completely invisible either to the merchants' Web shop software or the customer. This is especially important for merchants because there's no cost for integrating SSL with their existing systems, other than the cost of installing the certificate.

(ii) Ease of use for customers-SSL is already built into commonly used Web browsers and there is no need to install any additional software.

(iii) Low complexity - the system is not complex, resulting in minimal impact on transaction speed.

Disadvantage of SSL

SSL has some serious problems when it comes to meet the security challenges of today financial sector.

(i) The merchant cannot reliably identify the cardholder. SSL does provide the possibility of client authentication with the use of client certificates; such certificates are not obligatory and are rarely used. Furthermore, even if the client possesses a certificate, it is not necessarily linked with his credit card.

(ii) SSL only protects the communication link between the customer and the merchant. The merchant is allowed to see the payment information. SSL can neither guarantee that the merchant will not misuse this information, nor can it protect it against intrusions whilst it is stored at the merchant's server.

(iii) Without a third-party server, SSL cannot provide assurance of non-repudiation.

(iv) SSL indiscriminately encrypts all communication data using the same key strength, which is unnecessary because not all data need the same level of protection. For example, a credit card number needs stronger encryption than an order item list. Using the same key strength for both creates unnecessary computational overhead.

(B) Secure Electronic Transactions (SET)

It is a standardized industry wide protocol specification designated to secure payment transactions and authenticate the parties involved in the transaction in any type of networks including Internet. VISA and MasterCard developed the SET standard with collaboration from leading software companies such as Microsoft, Netscape, RSA, VeriSign, and other. SET was created to provide the trust needed for consumers. The protocol uses cryptography and digital certificates to provide confidentiality of the information, ensure payment integrity, and authenticate merchants, banks, and cardholders during SET transaction.

SET Specifications

- SET uses RSA Data security public key cryptography in order to encrypt and decrypt transaction packets along with the use of digital certificates and digital signature for authentication of all parties to the transaction and validation that information has not been tampered with.
- SET makes online transactions even safer by using digital certificates to verify that consumers and merchants are both authorized to use and accept Visa cards. It's the electronic equivalent of a consumer looking for a Visa decal in a merchant's store window, and a merchant checking the consumer's signature on the back of a Visa card. Merchants worldwide are currently adopting SET.
- SET incorporates the use of public key cryptography to protect the privacy of personal and financial information. As a result, with SET, consumers' payment card information is protected all the way to the financial institution. The merchant cannot read this information in the payment transaction.
- With SET, cardholders can validate that the Internet merchant is legitimate through the merchant's digital certificate. SET software automatically checks that merchant has a valid certificate representing their relationship with their financial institution. This provides consumers with the confidence that their payments will be handled with the same Visa promise that they trust today.

Advantages of SET Protocol

(i) Confidentiality, authentication and data integrity was verified by a large collection of security proofs based on formal methods.

(ii) In the standard variant of the protocol, SET prevents merchants from seeing the customer payment information, since this information is encrypted using the payment gateway's public key.

(iii) To ensure merchant privacy, SET prevents the payment gateway from seeing the order information.

Disadvantages of SET

(i) The customer must install additional software, which can handle SET transactions.

(ii) The customer must have a valid digital certificate.

(iii) Implementing SET is more costly than SSL for merchants as well.

(iv) Adapting their systems to work with SET is more complicated than adapting them to work with SSL

(v) Business banks must hire companies to manage their payment gateways, or install payment gateways by themselves.

(vi) Despite being designed with security in mind, SET also has some security issues. In a variant of the SET protocol, the merchant is allowed to see the customer payment information, just as with SSL.

(vii) SET employs complex cryptographic mechanisms that may have an impact on the transaction speed.

1.6 PAYMENT GATEWAY

A payment gateway is an ecommerce service that processes credit card payments for online and traditional brick and mortar stores. Payment gateways facilitate these transactions by transferring key information between payment portals such as web-enabled mobile devices/websites and the front end processor/bank. Payment gateways fulfill a vital role in the ecommerce transaction process, authorizing the payment between merchant and customer. Popular payment gateways include PayPal/Braintree, Stripe, and Square. A **payment processor** analyzes and transmits transaction data. **Payment gateways** authorize the transfer of funds between buyers and sellers.

1.6.1 How payment gateways work

Payment Gateways are software and servers that transmit Transaction information to Acquiring Banks and responses from Issuing Banks (such as whether a transaction is approved or declined). Essentially, Payment Gateways facilitate communication within banks. Security is an integral component of all payment gateways, as sensitive data such as Credit Card Numbers need to be protected from any fraudulent parties. The card associations have created a set of rules and security standards which must be followed by anyone with access to card information including gateways. This set of

rules and security standards is called the Payment Card Industry Data Security Standard (PCI-DSS or PCI).

Submitting an order is usually completed using HTTPS protocol, which securely communicates personal information through the parties involved in the Transaction. Many Payment Providers, such as 2Checkout, enable Merchants with added options when a cardholder purchases a service or product. Aside from providing the ability for real-time transactions, these providers can help to translate currencies between two parties in different countries, as well as bridge language and payment methods. Payment gateways usually charge those who use them a per transaction fee.

Payment Gateway is the service that automates the payment transaction between the shopper and merchant. It is usually a third-party service that is actually a system of computer processes that process, verify, and accept or decline credit card transactions on behalf of the merchant through secure Internet connections. The payment gateway is the infrastructure that allows a merchant to accept credit card and other forms of electronic payment. When referring to payment gateways used for Internet transactions, it may also be called an IP payment gateway.

When a customer places an order from an online store, the payment gateway performs several tasks to finalize the transaction:

(i) Encryption: The web browser encrypts the data to be sent between it and the vendor's web server. The gateway then sends the transaction data to the payment processor utilized by the vendor's acquiring bank.

(ii) Authorization Request: The payment processor sends the transaction data to a card association. The credit card's issuing bank views the authorization request and "approves" or "denies."

(iii) Filling the Order: The processor then forwards an authorization pertaining to the merchant and consumer to the payment gateway. Once the gateway obtains this response, it transmits it to the website/interface to process the payment. Here, it is interpreted and an appropriate response is generated. This seemingly complicated and

lengthy process typically takes only a few seconds at most. At this point, the merchant fills the order.

1.6.2 Clearing Transactions

The steps outlined above are repeated in an effort to "clear" the authorization via a consummation of the transaction. However, the clearing is only triggered once the merchant has actually completed the transaction (shipping the order). The issuing bank changes the "auth-hold" to a debit, allowing a "settlement" with the vendor's acquiring bank. The processor is then relied upon to settle all of the vendor's approved authorizations with the acquiring bank at the end of the day.

1.6.3 Other Payment Gateway Functions

Payment gateways also screen orders with a myriad of helpful tools. This screening process filters out as much fraud as possible. Examples of gateway fraud detection tools include:

- Delivery address verification
- AVS checks
- Computer finger printing technology,
- Velocity pattern analysis
- Identity morphing detection
- Geolocation

Payment gateways even calculate tax amounts to authorize requests transmitted to the processor.

1.6.4 Different Types of Payment Gateways in E-Commerce

The different types of payment gateways are:

Type 1 - Hosted Payment Gateways

Hosted payment gateways will take a customer off from site's checkout page. Once customer clicks on pay now button at website, customer will be redirected to payment

service provider (psp) page. Here customer needs to fill his/her payment details. Once the customer has paid, he/she will be redirected back to website to finish the checkout process. Another option is using an iframe. Payment service provider (PSP) creates a form (iframe) that the merchant store inserts to their website. By this merchants securely accept credit and debit card without capturing or storing card information on their website. Payment information is collected by using an inline frame (iframe). The form is hosted by the PSP, so when customers fill up the form, the PSP receives the data. For recurring payments, profile is created for customer with information of recurrence count , frequency, amount etc. Payment gateway will deduct recurring payments with the help of created profile and then sends payment notification to website. Refund and Cancellation of Payment need to be handled at Payment gateway's site.

Type 2 - Pro / Self Hosted Payment Gateways

For these types of gateways, it is needed to ask the payment details from customers, at website. After asking the details, merchant needs to send the collected data to the Payment Gateway's url. Some gateways need the data in specific format while some need any hash key or specific security/secret key. In case of recurring the next payments is deducted by payment gateway itself and send notification for the same. Refund and cancellation process need to be initiated from Payment Gateway's website.

Type 3 - API / Non Hosted Payment Gateways - Payments at Merchant's site

Some merchants wants full control on their checkout process and don't want to direct customers from their checkout page. It allows customers to enter their credit or debit card information directly on checkout page and process payments using their API's or using some HTTPS queries. This type of gateways mostly supports recurring as well as fixed payments.

Based on entered details system will internally create a payment calls to the payment gateway. These call could be of creating customer profile (for recurring only) at

gateway for automatic future payments OR only for one-time payment. After creating call, payment gateway sends the notification in response to these calls. System needs to handle it and intimate the customer for successful payment or the error (if there is any).

Some payment gateway also provide facility for Payment inquiry, Payment cancellation (cancels the future payment), Refund etc.

Type 4 - Local bank integration

These payment gateways are also considered as hosted payment gateways which work in straightforward manner. Customer will be redirect to Payment Gateway's website and there he/she need to fill the payment details and contact details. After making payment customer will be redirected back to website and notification data is also sent with redirection. These types of payment gateways didn't support recurring payment, refund and cancellation. Merchants need to do them manually.

Type 5 - Direct Payment Gateway

Some of the payment processor doesn't support Instant payment notification. They create profile and deduct the required amount from the customer's credit card on scheduled basis but does not inform the system (who requested for the amount). They just inform that whether credit card is approved or not. So in this case, system needs to make an inquiry on regular interval to the payment processor that whether the required payment is received or not and accordingly provide further service.

.

Type 6 - Platform Based Payment Gateway Solutions

These types of payment gateways provides platform to sell digital and physical goods directly from their server. Merchants need to create products or subscription in provided platform and customers are redirected via check out button to this platform. Customers are more likely to complete a purchase in their preferred language, and currency.

A payment gateway authorizes payments for retailers in all business categorizations. They ensure that sensitive information, such as credit card numbers, entered into a virtual terminal or on an E-commerce website, are passed securely from the customer to the merchant and from the merchant to the payment processor through the use of encryption.

Traditionally, merchant account providers (payment processors) and payment gateways have operated separately, but in recent years, many processors have come to offer all-in-one solutions—merchant processing services and gateway services.

1.6.5 Benefits of a Payment Gateway

The trend toward merchant account providers teaming up with payment gateway services and offering complete merchant account and payment processing packages has grown because of the many benefits for merchants, including but not limited to:

(i) Secure transactions. Payment gateways utilize industry-standard encryption and effectively protect sensitive data, protecting both merchant and consumers from fraud.

(ii) Expanded customer base. Payment gateways enable shoppers from around the world to have access to store and can expand customer base exponentially.

(iii) Bundled with shopping cart. Payment gateways often bundle shopping cart software with their programs. The software allows customer to select products with the click of a mouse, add them to his or her shopping cart, and complete the purchase at checkout.

(iv) Faster transaction processing. A payment gateway is much faster than manual processing, and customers can make a purchase without the inconvenience of long waits or lines.

(v) Added convenience. Having a payment gateway means store is open 24/7, and customers can shop at any hour of the day or night from the comfort of their own homes.

1.6.6 **Payment Gateways in India**

Professionals associated with the E-commerce industry admit the fact that Payment Gateway is one the most crucial factors of their business. After all, gateway application service providers enable safe, secure and speedy online payments. Some of the Payment Gateways in India are:

(a) ***Payzippy:*** PayZippy is Flipkart's very own Payment Gateway Service for Indian merchants. The company is treated as a separate entity headed by Flipkart Group. Their impressive clientele list, besides Flipkart, includes online players like Bluestone, Babyoye, Makemytrip, Lenskart, Caratlane, and Zansaar. They offer quick and convenient service that is PCI DSS certified. With zero setup fees and annual maintenance cost (for now), Payzippy has been zooming ahead since its launch last year. With a brand like Flipkart backing it, this gateway has managed to create a lot of buzz in a short span of time.

(b) ***PayU India*****:** Owned by Naspers, PayU is a global company with its presence in countries like Hungary, Poland, Russia, South Africa and India among others. With an impressive 12% conversion rate coupled with noteworthy customer service, PayU has roped in biggies like Jabong and Snapdeal. The service provider offers four pricing packages, Risk Management System, Multi Currency Gateway, Mobile optimised payment page, IVR Payment, Store Card Feature and Payment Analytics. Zepo, one of India's top platforms for start-ups has only good things to say about PayU. Therefore, it doesn't come as a surprise that they also offer a free PayU gateway to people who sign up with them.

(c) ***CC Avenue*****:** CCAvenue undoubtedly is one of the biggest payment solution providers in India as nearly 85% of Indian e-commerce merchants avail their services. The key features includes 100+ payment options, Multiple Currency Processing, Retry Option, Customization, Audit & Analytics and large window for on boarders. If you already have a website, you can also integrate CCAvenue shopping cart for free.

(d) ***Citrus Pay*:** Citrus is one of the top 3 payment gateway companies in India and the feat is worthy to be applauded, since it is only a 3 year old venture. Started by Satyen Kothari and Jitendra Gupta, their aim was to simplify online payment and make it quick & effective while following all safety protocols. Right from Emirates, Etihad, Airtel, Bagskart, Meru, Zivame, Esselworld, Kaya, PVR Cinemas, Healthkart, they all use Citrus Pay. They offer 3 packages, monthly charges for which are Rs. 7000 for Easy Starter, Rs. 10000 for Level Up, and Rs. 15000 for Power Packed.

(e) ***Direcpay*:** An arm of Times of Money (Times Group), Direcpay seems to be a safe option. Their security system is PCI-DSS certified and Norton Secure. They also offer easy integration, registration and flexible payment process besides providing EMI options. It takes about 5 days to activate your account after the documents are verified by concerned authorities.

1.7 Let's sum-up

A payment gateway authorizes payments for retailers in all business categorizations. They ensure that sensitive information, such as credit card numbers, entered into a virtual terminal or on an E-commerce website, are passed securely from the customer to the merchant and from the merchant to the payment processor through the use of encryption. Traditionally, merchant account providers (payment processors) and payment gateways have operated separately, but in recent years, many processors have come to offer all-in-one solutions—merchant processing services and gateway services. A processor is a system that connects the cardholder's bank with the merchant's bank, and the card brands (e.g. Visa, Mastercard, Discover, etc.), and makes sure that all of the money ends up in the proper place. In other words, the processors take the money from the cardholder's bank account and deliver it to the merchant's bank account.

1.8 Key terms

- Secure Socket Layer (SSL) Protocol

- Payment Gateway
- Secure Electronic Transaction (SET) Protocol
- Authorization
- Acquiring Bank
- Merchant

1.9 Self-Assessment Questions

(I) Write down all the participants involved in the processing of payments made on internet.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

(ii) Write short notes on different types of Payment Gateways .

_____

_____

_____

_____

(iii) What is Payment Gateway? What is its role in electronic payment services?

1.10 Further Readings

2. Adesh K Pandey, Concepts of E-Commerce, Katson Books, New Delhi
3. Rabindra Goel, E-commerce, New Age International Publishers, New Delhi

1.11 Model Questions

(i). Explain the working of payment processing in brief.

(ii) What is SET protocol? Enumerate the main features of SET protocol.

Unit-2 Electronic Payment Modes/Systems

Learning Objectives

After reading this chapter, students should be able to:

- Understand the different types of electronic payment systems
- Discuss the meaning of credit cards and problems associated with credit cards
- Understand the different types of smart cards
- Enumerate the use of electronic wallet

Structure

1.7 TYPES OF ELECTRONIC PAYMENT SYSTEM

There are several payment methods supporting electronic payments over the internet:

(i) Electronic payment cards (credit, debit, charge)
(ii) Virtual credit cards
(iii) E-wallets (or e-purses)
(iv) Smart cards
(v) Electronic cash (several variations)
(vi) Wireless payments
(vii) Stored-value card payments
(viii) Loyalty cards
(ix) Person-to-person payment methods
(x) Payments made electronically at kiosks

1.8 CREDIT CARDS

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.

(a) The card holder – Customer
(b) The merchant - seller of product who can accept credit card payments.
(c) The card issuer bank - card holder's bank
(d) The acquirer bank - the merchant's bank
(e) The card brand - for example , visa or mastercard.

1.2.1 Credit card payment process

The following steps will elaborate the payment process through credit card

Step 1: Bank issues and activates a credit card to customer on his/her request.

Step 2: Customer presents credit card information to merchant site or to merchant from whom he/she want to purchase a product/service.

Step 3: Merchant validates customer's identity by asking for approval from card brand company.

Step 4: Card brand company authenticates the credit card and paid the transaction by credit. Merchant keeps the sales slip.

Step 5: Merchant submits the sales slip to acquirer banks and gets the service chargers paid to him/her.

Step 6: Acquirer bank requests the card brand company to clear the credit amount and gets the payment.

Step 7: Now card brand company asks to clear amount from the issuer bank and amount gets transferred to card brand company.

1.9 DEBIT CARDS

Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account

immediately and there should be sufficient balance in bank account for the transaction to get completed. Whereas in case of credit card there is no such compulsion.
Debit cards free customer to carry cash, cheques and even merchants accepts debit card more readily. Having restriction on amount being in bank account also helps customer to keep a check on his/her spending.

Differences between Credit card and debit card

While all three are plastic forms of currency, there are quite a few differences between credit cards and debit cards. Given below are the major differences between the two:

Debit cards can be used anywhere, but require access to real-time funds. If user is looking for a card that can be used for transactions as well as to withdraw cash, then a debit card is the one for him. Debit cards can be used at ATM machines to withdraw funds that are already available to you. In other words, once the withdrawal is complete, the money will be debited from savings/current account in real time. The same goes for purchases made using your debit card at restaurants, malls, cinemas, etc.

If user does not have sufficient funds in his account at the time of making a purchase using his debit card, the transaction would go through if his card is linked to an overdraft account (which would permit him to withdraw a set sum that is over and above the amount he actually has in his bank account). If user has not linked his card, the transaction would not go through and the card will be declined.

Some debit cards could also entitle you to cash back, or a return of a portion of the amount user spends on his card. This facility depends on the type of debit card he possesses and on other factors such as the type of transaction and the place the transaction is being made.

Credit cards can be used anywhere and function like mini-loans. A credit card is, for all intents and purposes, a loan that the bank provides to the user at the time of

making a purchase. Credit cards are not directly linked to savings or current account, meaning there is no real-time deduction of money every time user makes a purchase using his credit card. User will have to make a monthly payment at the end of his credit card billing cycle, where he will be required to make a payment towards his outstanding amount.

User can choose to either pay off the whole amount or pay only a fraction of the cost, known as the minimum amount due. The balance amount, if any, attracts interest, which will accrue until the entire amount has been paid off.

Applying for a credit card affects your credit score, which is the basis of user's creditworthiness. Financial institutions look at credit score before approving a loan or a credit card, as the score is used to judge whether or not user will be able to repay the loan or outstanding amount on his credit card. Credit cards also come with more additional benefits in the form of extended warranties or special offers, such as cash back, frequent flyer miles, etc.

1.10 SMART CARDS

Smart card is again similar to credit card and debit card in appearance but it has a small microprocessor chip embedded in it. It has the capacity to store customer work related/personal information. Smart card is also used to store money which is reduced as per usage. Smart card can be accessed only using a PIN of customer. Smart cards are secure as they stores information in encrypted format and are less expensive/provide faster processing.Mondex and Visa Cash cards are examples of smart cards.

A smart card resembles a credit card in size and shape, but inside it is completely different. First of all, it *has* an inside -- a normal credit card is a simple piece of plastic. The inside of a smart card usually contains an **embedded microprocessor**. The microprocessor is under a gold contact pad on one side of the card. Think of the microprocessor as *replacing* the usual magnetic stripe on a credit card or debit card.

Smart cards are much more popular in Europe than in the United States. In Europe, the health insurance and banking industries use smart cards extensively. *Every* German citizen has a smart card for health insurance. Even though smart cards have been around in their modern form for at least a decade, they are just Magnetic stripe technology remains in wide use in the United States. However, the data on the stripe can easily be read, written, deleted or changed with off-the-shelf equipment. Therefore, the stripe is really not the best place to store sensitive information. To protect the consumer, businesses in the U.S. have invested in extensive online mainframe-based computer networks for verification and processing. In Europe, such an infrastructure did not develop -- instead, the card carries the intelligence.

The microprocessor on the smart card is there for **security**. The host computer and card reader actually "talk" to the microprocessor. The microprocessor enforces access to the data on the card. If the host computer read and wrote the smart card's random access memory (RAM), it would be no different than a diskette.
Smarts cards may have up to 8 kilobytes of RAM, 346 kilobytes of ROM, 256 kilobytes of programmable ROM, and a 16-bit microprocessor. The smart card uses a serial interface and receives its power from external sources like a card reader. The processor uses a limited instruction set for applications such as cryptography.

Smart cards can be used with a smart-card reader attachment to a personal computer to authenticate a user. Web browsers also can use smart card technology to supplement Secure Sockets Layer (SSL) for improved security of Internet transactions.

1.4.1 Advantages of Using Smart Cards

The advantages of smart card are:

(i) More Secure

This simple technology has revolutionized the payment card industry and increased the level of card security. These cards use encryption and authentication technology

which is more secure than previous methods associated with payment cards. The microprocessor chip embedded at the heart of the smart card requires contact to the card reader and certain areas of the chip can be programmed for specific industries.

(ii) Safe to Transport

Another advantage to having a smart card is their use in the banking industry (and many other sectors). These cards give the holder freedom to carry large sums of money around without feeling anxious about having the money stolen. In this regard, they are also safe because the cards can be easily replaced, and the person would have to know the pin number to access its stored value. This takes care of the problem with cash; once it is stolen it is nearly impossible to trace and recover it.

(iii) Double as an ID Card

A third advantage of using a smart card is that they can provide complete identification in certain industries. There are numerous benefits of using smart cards for identification. A driver's license that has been created using smart card technology can give the police the ability to quickly identify someone whose been stopped for speeding or reckless driving. These cards can be used by health professionals to identify someone who is brought in by an ambulance but unconscious or unable to speak.

(iv) Prevents Fraud

Other benefits of using smart cards for identification can be used by governments to prevent benefits and social welfare fraud to ensure the right person is receiving the welfare benefit. Some countries are using the smart cards to identify temporary workers who have been given work permits. This has the potential to reduce immigration fraud. Smart cards are just as easy to use as a credit or debit card, but considerable more secure. They are lightweight and easy to carry. This makes it easy to have one card to pay for parking, access to the office, and for buying lunch at the office cafeteria.

1.4.2 Types of Smart Cards

The term "smart card" is loosely used to describe any card that is capable of relating information to a particular application such as magnetic stripe cards, optical cards,

memory cards, and microprocessor cards. It is correct, however, to refer to memory and microprocessor cards as smart cards.

- **Magnetic stripe cards.** A magnetic stripe card has a strip of magnetic tape material attached to its surface. This is the standard technology used for bank cards and can only store data which cannot be updated.
- **Optical cards.** Optical cards use some form of laser to read and write to the card.
- **Memory cards.** Memory cards can store a variety of data, including financial, personal, and specialized information, but cannot process information.
- **Microprocessor cards.** Smart cards with microprocessors look like standard plastic cards, but are equipped with an embedded Integrated Circuit (IC) chip. They can store information, carry out local processing on the data stored, and perform complex calculations. These cards take the form of either "contact" cards (which require a card reader) or "contactless" cards (which use radio frequency signals to operate).

1.4.3 The Microprocessor Smart Card

The microprocessor smart card is defined as an IC chip contact card with a microprocessor and memory. The size of a credit card, this smart card contains a dime-sized microchip that can process and store thousands of bits of electronic data. Unlike passive devices (such as a memory card or magnetic stripe card) that can only store information, the microprocessor smart card is active and able to process data in reaction to a given situation.

This capability to record and modify information in its own non-volatile, physically protected memory makes the smart card a powerful and practical tool - smart cards are small and portable, they can interact with computers and other automated systems, and the data they carry can be updated instantaneously.

1.4.4 Current Applications of Smart Card

A smart card, as mentioned above, is a portable computational device with data

storage ability. As such, they can be a very reliable form of personal identification and a tamper-proof, secure information repository. The main possible applications of smart cards are the following:

(i) Payphones: Outside of the United States there is a widespread use of payphones equipped with card readers rather than p; or in addition to p; coin recognition and storage. The main advantages are that the phone company does not have to collect coins, and the users do not have to have coins or remember long access numbers and PIN codes. Smart cards have the further advantage over magnetic stripe cards of being reloadable, and allowing advanced features like phone banking, automatic memory dialing and on-line services.

(ii) Mobile Communications: Smart cards are used as identification device for GSM digital mobile phones. The card stores all the necessary information in order to properly identify and bill the user, so that any user can use any phone terminal.

(iii) Banking & Retail: Smart banking cards can be used as credit, direct debit or stored value cards, offering a counterfeit- and tamper-proof device. The intelligent microchip on the card and the card readers use mutual authentication procedures that protect users, merchants and banks from fraudulent use. Other services enabled by smart cards are advanced loyalty programs and electronic coupons.

(iv) Electronic Purse: A smart card can be used to store a monetary value for small purchases. Card readers retrieve the amount currently stored, and subtract the amount for the goods or services being purchased. Groceries, transportation tickets, parking, cafeterias, taxis and all types of vending machines are only some of the purchases that often do not reach amounts to justify the hassle of using a credit card (a cash card reader does not require a permanent phone connection with a host computer). Radio-read smart cards will allow the free flow of people through transportation systems, avoiding the need of ticketing machines or validation gates.

(v) Health Care: Smart cards allow the information for a patient's history to be reliably and safely stored. Health care professionals can instantaneously access such information when needed, and update the content. Instant patient verification allows immediate insurance processing and refund. Doctors and nurses themselves can carry smart card-based IDs that allow secure, multi-level access to private information.

(vi) ID Verification and Access Control: The computational power of smart cards allows running mutual authentication and public-key encryption software in order to reliably identify the bearer of the card. For higher security needs, a smart card is a tamper-proof device to store such information as a user's picture or fingerprints. Smart cards can be used also for network access: in addition or in alternative to user IDs and passwords, a networked computer equipped with a smart card reader can reliably identify the user.

1.11 ELECTRONIC CHECK PAYMENT

Essentially, an eCheck or electronic check is a form of online payment where money is electronically withdrawn from the payer's checking account, transferred over the ACH network, and deposited into the payee's checking account. With an ACH merchant account, a business can withdraw payments for a good or service directly from their customer's bank account. **The payment must be authorized by the customer**, either by signed contract, acceptance of a website's "Terms and Conditions" or a recorded voice conversation.

How Does Electronic Check Processing Work?

Electronic check processing is somewhat similar to paper check processing, only faster. Instead of a customer manually filling out a paper check and sending it to the business they need to pay, today's technology allows the process to happen electronically, saving both time as well as paper waste.

Four main steps to processing an electronic check:

1. **Request Authorization:** The business needs to gain authorization from the customer to make the transaction. This can be done via an online payment form, signed order form, or phone conversation.
2. **Payment Set Up:** After authorization is complete, the business inputs the payment information into the online payment processing software. If it is a recurring payment, this information also includes the details of the recurring schedule.
3. **Finalize and Submit:** Once payment information is properly entered into the software, the business clicks "Save" or "Submit" and starts the ACH transaction process.
4. **Payment Confirmation and Funds Deposited:** The payment is automatically withdrawn from the customer's bank account, the online software sends a payment receipt to the customer, and the payment itself is deposited into the business's bank account. Funds are typically deposited into the merchant's bank account three to five business days after the ACH transaction is initiated.

The Electronic Check (also known as the 'eCheck' or 'e-check'):

- Leverages the check payments system, a core competency of the banking industry.
- Fits within current business practices, eliminating the need for expensive process re-engineering.
- Works like a paper check does but in pure electronic form, with fewer manual steps.
- Is designed to meet the needs of businesses and consumers in the 21st century, using state of the art security techniques.
- Can be used by all bank customers who have checking accounts, including small and mid-size businesses which currently have little access to electronic payment systems.
- Enhances existing bank accounts with new e-commerce features.

Features of echecks

- contain the same information as paper checks contain
- are based on the same rich legal framework as paper checks
- can be linked with unlimited information and exchanged directly between parties
- can be used in any and all remote transactions where paper checks are used today
- enhance the functions and features provided by bank checking accounts
- expand on the usefulness of paper checks by providing value-added information

1.12 ELECTRONIC WALLETS

A To combat theft, simplify your finances, avoid being the "check-writing guy" in line at the store and maybe even ward off trips to the chiropractor, perhaps it's time for a wallet upgrade. For that, a customer might consider the digital wallet. In general, though, a **digital wallet** (also sometimes called an **e-wallet**) is a transformation in the way customers pay for things. Many digital wallet services work through apps on smartphone. At the supermarket, for instance, customer might simply tap his/her phone to a compatible check-out register to pay instantly.

No matter what form it takes, a digital wallet is based on encryption software that substitutes for old, analog wallet during monetary transactions. Customers benefit from the protection and convenience. Merchants benefit because they're more protected against fraud and they sell more products, faster. A smartphone digital wallet will help customers pay for stuff, but it will also store concert tickets, bus and subway passes and gift cards. Retailers will reward your loyalty by offering instant freebies, discounts and coupons. A digital wallet could alter the way customer organizes his finances and his life in general.

1.12.1 Advantages of the Digital Wallet

The advantages of digital wallet are:

(i) **Lower Costs:** Employing the use of digital wallets removes the need for intermediaries, in a variety of forms. Purchases in-store may no longer require a cashier because the purchasing process becomes as simple as a tap or scan of a mobile device. Applications like Square can replace expensive POS (point of sale) systems that will reduce transaction costs for the business.

(ii) **Competitive Advantage:** Digital wallet applications provide a more convenient transaction processing method for customers, giving businesses that employ this technology a competitive edge in the market. It redefines the user experience of paying and incorporates a novelty aspect to each purchase.

(iii) **Modern:** Traditional cash-only businesses, such as craft fairs and flea markets, can now accept debit and credit cards. This opens up an entirely new aspect to payment methods in large markets, introducing many business opportunities and greater potential revenue.

(iv) **Convenience**: Users are able to get through a purchase in mere seconds with a simple tap or scan of their mobile device. The experience of purchasing items becomes quicker and easier - leading to a greater sense of satisfaction. Furthermore, with faster transactions, checkout lines within stores become much shorter.

1.13 ELECTRONIC TOKEN-BASED PAYMENT SYSTEM

The digital token based payment system is a new form of electronic payment system which is based on electronic tokens rather than e-cheque or e-cash. The electronic tokens are generated by the bank or some financial institutions. Hence we can say that the electronic tokens are equivalent to the cash which are to be made by the bank.

1.7.1 Categories of Electronic Tokens

***(a) Cash or Real Time*:-** In this mode of electronic tokens transactions takes place via the exchange of electronic currency (e-cash).

(b) Debit or Prepaid:- In this electronic payment system the prepaid facilities are provided. It means that for transactions of information user pay in advance. This technology is used in smart card, electronic purses etc.

(c) Credit or Postpaid;- These types of electronic token based on the identity of customers which issue a card, their authentication and verification by a third party. In this system the server authenticate the customers and then verify their identity through the bank. After all these processing the transaction take place. Example is E-Cheques.

The Digital Token based system has following issues for which they are established:-

1. Nature of transaction for which instrument is designed: - In this category, the design issues of token take place. It may be designed to handle micro payments. It may be designed for conventional products. Some tokens are designed specifically and other generally. The design issue involve involvement of parties, purchase interaction and average amount.

2. Means of Settlement:- The Digital Tokens are used when their format must be in cash, credit, electronic bill payments etc. Most transaction settlement methods use credit cards while other used proxies for values.

3. Approach to Security, Anonymity and Authentication:- Since the electronic token are vary from system to system when the business transaction take place. So it is necessary to secure it by intruders and hackers. For this purpose various security features are provided with electronic tokens such as the method of encryption. The encryption method use the digital signatures of the customers for verification and authentication.

4. Risk Factors: - The electronic tokens may be worthless and if the customer have currency on token than nobody will accept it, If the transaction has long time between delivery of products and payments to merchants then merchant exposes to the risk. so it is important to analysis risk factor in electronic payment system.

1.14 ELECTRONIC PAYMENT SECURITY

Security is an essential part of any transaction that takes place over the internet. Customer will loose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions −

Confidential − Information should not be accessible to unauthorized person. It should not be intercepted during transmission.

Integrity − Information should not be altered during its transmission over the network.

Availability − Information should be available wherever and whenever requirement within time limit specified.

Authenticity − There should be a mechanism to authenticate user before giving him/her access to required information.

Non-Repudiabiity − It is protection against denial of order or denial of payment. Once a sender sends a message, the sender should not able to deny sending the message. Similarly the recipient of message should not be able to deny receipt.

Encryption − Information should be encrypted and decrypted only by authorized user.

Auditability − Data should be recorded in such a way that it can be audited for integrity requirements.

Measures to ensure Security

Major security measures are following −

Encryption − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypt the data using a secret code and specified receiver only can decrypt the data using the same or different secret code.

Digital Signature − Digital signature ensures the authenticity of the information. A digital signature is a e-signature authentic authenticated through encryption and password.

Security Certificates − Security certificate is unique digital id used to verify identity of an individual website or user.

1.15 LET'S SUM-UP

The emergence of e-commerce has created new financial needs that in many cases cannot be effectively fulfilled by the traditional payment systems. The advent of the Electronic commerce has prompted the invention of several payment tools to facilitate the completion of business transactions over the Internet. There are different methods to pay electronically. Recognizing this, virtually all interested parties are exploring various types of electronic payment system and issues surrounding electronic payment system and digital currency. Broadly electronic payment systems can be classified into four categories: Online Credit Card Payment System, Online Electronic Cash System, Electronic Cheque System and Smart Cards based Electronic Payment System. Each payment system has its advantages and disadvantages for the customers and merchants. These payment systems have numbers of requirements: e.g. security, acceptability, convenience, cost, anonymity, control, and traceability. Therefore, instead of focusing on the technological specifications of various electronic payment systems, the researcher has distinguished electronic payment systems based on what is being transmitted over the network; and analyzed the difference of each electronic payment system by evaluating their requirements, characteristics and assessed the applicability of each system. To sustain in the competition more banks are following e-commerce and especially using e-payment mechanism. Though Indian economy is basically cash driven, still India is not far behind in adopting E-payment services in retail and banking sector.

1.16 KEY TERMS

- **Credit Card**: Credit card is small plastic card with a unique number attached with an account.
- **Debit Card**: Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number.

- **Smart Card**: A smart card resembles a credit card in size and shape, but inside it is completely different. A smart card usually contains an **embedded microprocessor**.
- **Digital Wallet**: Sometimes called an **e-wallet** is a transformation in the way customers pay for things.
- **Electronic Token**: Electronic tokens are generated by the bank or some financial institutions. Hence we can say that the electronic tokens are equivalent to the cash which are to be made by the bank.

1.17 SELF-ASSESSMENT QUESTIONS

(II) Write down the meaning of smart cards and elaborate the different types of smart card.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

(ii) Write short notes on Electronic Wallets.

_____

_____

(iii) Write short note of debit card.

1.18 FURTHER READINGS

4. Adesh K Pandey, Concepts of E-Commerce, Katson Books, New Delhi
5. Rabindra Goel, E-commerce, New Age International Publishers, New Delhi

1.13 MODEL QUESTIONS

(i) What is a credit card? How is the credit card transactions carried out? Explain.

(ii) How electronic checks are advantageous over the traditional checks?

UNIT-1

RECORDS MAINTENANCE/MANAGEMENT

1. **Define filing and explain its importance.**

Filing means keeping documents in a safe place and being able to find them easily and quickly. Documents that are cared for will not easily tear, get lost or dirty. A filing system is the central record-keeping system for an organisation. It helps to be organised, systematic, efficient and transparent. It also helps all people who should be able to access information to do so easily. Filing is important as:

1. It helps in increasing efficiency of office because filing helps in providing records in required time to make quick decisions
2. Filing helps in protection of important documents from fire, dust, insects, theft and mishandling.
3. Previous records are base of past records and they are used as a immediate reference.
4. It helps in documentation of proof and legal evidence in the time of disputes
5. It helps in formulation of future planning
6. It helps in providing legal proofs to fulfill legal formalities
7. It helps in handling customers and correspondence carefully to maintain the goodwill of the office
8. It helps in taking feedback.

2. **Discuss the pros and cons of centralized filing.**

Centralised filing denotes a system of filing where files relating to different departments are preserved at a central place of the organisation. The location of filing equipment and personnel in a single section is called centralised filing.

The following are the broad advantages of centralised filing:

a) It ensures uniformity and standardisation of filing system as the filing operation of various departments is done at one place.

b) Centralised filing avoids unnecessary duplication of filing equipments.

c) It ensures better supervision and here better work is performed by-a group of specialists under the control of a supervisor.

d) As all the records are kept at one place, it facilitates easy location of records.

e) Centralised filing avoids botheration of departments for record keeping.

f) Cross referencing of letters becomes possible in centralized filing system.

There are also certain disadvantages with centralized filing which are briefly explained below.

Disadvantages or Limitations of centralized filing

1. Records may become more vulnerable since they are stored in one central location.

2. It may cause great delay in bringing records if most office staff required several documents at a time.

3. The risk of loss due to fire, theft and the like is more since all the documents are stored in only one place.

4. The filing department may enforce rules and procedure rigidly regarding receiving and returning the files. This may affect the smooth functioning of functional department operations.

5. More human resources and time are spent on the locating and returning the files at precious time.

6. Sometimes, the same documents or records are required by more than one department. It creates strained relationship among staff.

7. It is very difficult to maintain secret and confidential documents.

8. If specialized staffs are not appointed in the filing department, there may be a large number of misfiling.

9. The filing department may become a storage place of unwanted and unnecessary documents.

10. If some papers or pages are missed, it is very difficult to find such papers and no possibility of fixing responsibility on any body.

11. The centralized filing is not suitable if the organization has its functional department in different geographical areas.

UNIT-2

OFFICE CORRESPONDENCE AND MAIL SERVICE

1. **Write short notes on Inward Mail System.**

Office correspondence means communication in writing on subject of mutual interest either within the organization or outside the organization and it takes the form of a letter, a circular, and a notice. The written communication sent through the post office or the messenger is called, "dak" or mail. When the 'dak' is received by an office from different sources it is called as incoming mail. Handling of such incoming mail has given a paramount importance because improper handling of data create various problems. Hence the mail should be handled with speed and accuracy.

Efficient handling of mail requires establishment of a definite procedure which are termed as steps of handling of mail. These steps are :

1. Receiving the mail.
2. Sorting the mail.
3. Opening the mail.
4. Scrutiny of the contents.
5. Date stamping.
6. Recording the mail.
7. Distribution of mail.
8. Follow up action.

Receiving the Mail: Generally mails are received once or twice a day delivered by the postman. When the volume of correspondence is large, a post box or post bag is hired in the post office and an office peon is required to collect the mail form the post office. Sometimes letters are received through the messengers of other offices.

Sorting the Mail: Sorting of letters means grouping of letters on definite order. The letters are grouped either on the basis of their nature or destination or contents. Sorting of letters may be done before opening of letters or after opening of letters. When it is undertaken before opening, private and confidential letters are separated from the ordinary letters.

Opening the Mail: In small organization letters are opened by the officer or head clerk. When the volume of letters are large, these are opened by mail-opener. In a large organization mails are handled by a mailing department and a clerk is engaged in opening of letters. Till the date of receipt of letter is recorded, the envelopes detached from the letters should be kept. When the letters are marked private, these are opened by the concerned person.

Scrutiny of Contents: After the letters are opened, the contents are removed from the envelopes and are scrutinised. The purpose of scrutiny is to ascertain the department to which the letter relate. Any enclosures of the contents should be properly verified and noted.

Stamping the Mail: After proper scrutiny, the date stamping of letter is done. Sometimes the date and time of receipt is stamped on the letter. For stamping of letters, a stamp is prepared which contains the serial number, the date of receipt and time of receipt if necessary. A reference stamp is attached if the letters relate to number of departments.

Recording the Mall: After the stamping work, letters received are recorded in inward mail register or letters received book. Before recording of letters in the register, the contents are scrutinized properly so as to ensure the department to which it belongs. The inward mail register contains serial number, date of receipt, senders name and address, nature of contents, subject of the letter in brief, remarks and initials of the officer with date.

Distribution of the Mail: This is the last step in the inward mailing routine. In this stage letters are handed over to the concerned department. The letters are distributed through messengers or sometimes with the help of mechanical devices like conveyor-belt or pneumatic tube.

Follow up Action: Follow up action is very important because it is concerned with keeping track of mail. This stage makes on enquiry whether the letter is replied or not.

2. **Briefly describe the content of a business letter.**

A **business letter** is more formal than a personal letter. It should have a margin of at least one inch on all four edges. It is always written on 8½"x11" (or metric equivalent) unlined stationery. There are **six** parts to a business letter.

1. The Heading. This contains the return address (usually two or three lines) with the date on the last line. Sometimes it may be necessary to include a line after the address and before the date for a phone number, fax number, E-mail address, or something similar. Often a line is skipped between the address and date. That should always be done if the heading is next to the left margin. It is not necessary to type the return address if one is using stationery with the return address already imprinted. Always include the date.

2. The Inside Address. This is the address one is sending his letter to. Make it as complete as possible. Include titles and names if he knows them. This is always on the left margin. If an 8½" x 11" paper is folded in thirds to fit in a standard 9" business envelope, the inside address can appear through the window in the envelope. An inside address also helps the recipient route the letter properly and can help should

the envelope be damaged and the address become unreadable. Skip a line after the heading before the inside address. Skip another line after the inside address before the greeting.

3. The Greeting. Also called the salutation. The greeting in a business letter is always formal. It normally begins with the word "Dear" and always includes the person's last name. It normally has a title. Use a first name only if the title is unclear--for example, the office manager is writing to someone named "Leslie," but do not know whether the person is male or female. The greeting in a business letter always ends in a colon.

4. The Body. The body is written as text. A business letter is never hand written. Depending on the letter style one chooses, paragraphs may be indented. Regardless of format, skip a line between paragraphs. Skip a line between the greeting and the body. Skip a line between the body and the close.

5. The Complimentary Close. This short, polite closing ends with a comma. It is either at the left margin or its left edge is in the center, depending on the Business Letter Style that one uses. It begins at the same column the heading does. The block style is becoming more widely used because there is no indenting to bother with in the whole letter.

6. The Signature Line. Skip two lines and type out the name to be signed. This customarily includes a middle initial, but does not have to. Women may indicate how they wish to be addressed by placing **Miss, Mrs., Ms.** or similar title in parentheses before their name. The signature line may include a second line for a title, if appropriate. The term "By direction" in the second line means that a superior is authorizing the signer. The signature should start directly above the first letter of the signature line in the space between the close and the signature line. One should use blue or black ink.