CHAPTER 5

Electronic Payment System

After setting up a web site, e-commerce business firm must address another important component of an e-commerce infrastructure: enabling customers to easily pay for products and services online. As far as payments are concerned, trust and acceptance pay a great role in e-commerce. Traditionally a customer sees a product, examine it, and purchase it by paying cash, cheque or credit card. But in e-commerce, the customer does not see the product directly and payments are made electronically.

However, traditional payment systems have proven to be unsuitable for e-commerce since it involves the costs and complexity of transactions over the Internet. Conventional ways of paying for goods and services do not work suitably over the Internet. Existing payment systems for the real world, such as credit cards are widely accepted as means of payment on the Internet. However their use creates many difficulties among users because of the risk involved.

The existing payment systems are also not ideal for merchants, because of the high transaction costs, fraudulent activity and the multiple parties involved in payment processing. Because of these problems, customers are not showing much interest in e-commerce activities that involve paying over the Internet. This situation in turn affects merchants who are losing potential customers. Hence, there is a need for well-performing and user-friendly payment systems that would satisfy both merchants and customers. Demand is therefore high for a simple Internet payment method approach that provides easier Internet connectivity between buyers, sellers, and the financial networks that move money between them. EPS enable a customer to make payment for the goods or service purchased on line.

Electronic Payment is defined as a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument such as encrypted credit card numbers, electronic cheques or digital cash that is backed by a bank or an intermediary, or by a legal tender.

The Internet Payment Processing System

We have to examine the main participants in an e-commerce payment processing system in order to understand the need for Internet payment services. The participants in an online electronic payment transaction include the following:

1. ***The customer:*** Customer in the e-commerce may be an individual or organisation who buy products or services on line and hold a payment card such as a credit card or debit card from an issuer.

2. ***The issuer:*** The issuer means a financial institution, such as a bank, that provides the customer with a payment card. The issuer is responsible for the cardholder's debt payment.

3. ***The merchant:*** The person or organization that sells goods or services to the cardholder via a Web site is the merchant. The merchant that accepts payment cards must have an Internet Merchant Account with an acquirer.

4. ***The acquirer:*** Acquirer is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. The acquirer provides authorization to the merchant within customer's credit limit. The acquirer also provides electronic transfer of payments to the merchant's account, and is then reimbursed by the issuer via the transfer of electronic funds over a payment network.

4. ***The payment gateway:*** This function operated by a third-party provider, processes merchant payments by providing an interface between the merchant and the acquirer's financial processing system. A payment gateway is an e-commerce application service provider service that authorizes payments for e-businesses, online Shopping, etc.

Payment gateway protects credit cards details by encrypting sensitive information, such as credit card numbers, to ensure that information passes securely between the customer and the merchant and also between merchant and payment processor.

5. ***The processor:*** The processor is a large data centre that processes credit card transactions and settles funds to merchants, connected to the merchant on behalf of an acquirer via a payment gateway.

Basic Steps of an Online Payment

The basic steps of an online payment transaction include the following:

Step 1: The customer places an order online by selecting items from the merchant's website and sending the merchant a list.

Step 2: The buyer submits a payment request through his cell phone, computer or mobile payment processor.

Step 3: The service provider routes the data via a secure connection to the buyer's bank or Credit Card Company.

Step 4: The buyer's bank either approves or declines the transaction based on the buyer's available funds or credit. If approved, the transaction is routed back to the payment provider to be processed.

Step 5: The payment provider stores the transaction and send a record to both the seller and buyer.

Step 6: The goods or services are sent to the buyer and the buyer's bank sends the funds to the seller.

Digital Payment Requirements

Irrespective of the type of payment mechanism, digital payment methods should have some characteristics to meet its basic requirements. The important basic requirements are the following.

1. ***Acceptability:*** This refers to whether the payment method is supported globally. It should be available and accessible to all type of buyers and sellers. It should be honoured and accepted by all banks and financial institutions. For instance, cash is accepted widely and thus has high level of applicability. Applicability of a payment system may vary from country to country. Debit cards and credit cards have high acceptability, while cheques are not common method for purchase.

2. ***Affordability:*** The costs of implementing and using the system must be affordable for consumers and merchants. Both buyers and sellers may not be willing to pay significantly high extra cost to participate in Internet e-commerce transactions. For example, consumers are not willing to pay for a digital certificate in order to conduct e-commerce transactions although it is required in some e-payment scheme such a SET. Merchants will also not wish to invest significantly in engineering e-payment infrastructure.

3. ***Anonymity:*** Anonymity is the desire to protect one's privacy, identity and personal information. For some transactions, identities of the parties in the transactions could be protected by anonymity. Anonymity suggests that it is not possible to discover someone's identity or to monitor an individual's spending patterns.

4. ***Convertibility:*** Naturally users will select payment mechanisms as financial instruments according to their needs. It is important that funds represented by one mechanism be easily convertible into funds represented by others. It should be exchangeable with all forms of money whether it is digital or traditional.

5. ***Efficiency:*** There are lots of discussions on the ability of payment systems to accept "micropayments". Small payments are amounts less than a Rs.50 or 100; micropayments are less than ten rupees. Systems should be able to receive small payments without performance degradation and posing high costs of transactions. The costs per transaction should be reasonable for processing small amounts.

6. ***Flexibility:*** The system must allow e-commerce consumers to order products or services from any location, and not just from one PC. Alternative forms of payment are needed in online payment environment. The payment infrastructure should support several payment methods including instruments similar to credit cards, cheques and even anonymous electronic cash. These instruments should be integrated into a common framework.

7. ***Interoperability:*** A payment system is interoperable if it is not dependent on one organization, but is open and allows as many as necessary interested parties to join. The system must be interoperable between different computing platforms, web browsers and server software packages in order to enable its use by the widest possible range of e-commerce consumers and merchants.

This can be achieved by means of open standards for the technology that is used. It is natural, though, that companies that implement new technologies treat them as knowhow, because of the added value they create by investing in the technologies; therefore it is not always sensible to demand interoperability.

8. Reliability: The system must be reliable since it is used for the transmission and manipulation of sensitive information. Naturally, users would like to see that system is reliable, because the smooth running of an enterprise will depend on the availability of the reliable payment infrastructure,

9. Security: The payment method is secured, in particular whether it is easy to perpetrate different kinds of fraud such as forged payment. For electronic cash systems the issue of security has a special angle of counterfeiting, which means that no one should be able to produce electronic tokens on their own. Another angle is double spending; design should ensure that electronic tokens couldn't be spent twice.

10. Scalability: As the commercial use of the Internet grows, the demands for efficient payment infrastructure will also increase. The payment infrastructure as a whole should be scalable which means it should be able to handle the addition of users and merchants, so that systems will perform normally without affecting performance. Least scalable systems are those that require from users and vendors purchase and installation of additional hardware; this often hampers development of electronic cash systems.

11. Traceability: Anonymity relates to the characteristic of traceability. Traceability shows how easy it is to trace money flows, sources of funds or link spent funds to a customer via payment activities. There are lots of films where police is able to find someone who is using credit cards in any place in India and even worldwide. This suggests that credit cards are traceable.

12. Trust: Trust is essential to conduct e-commerce. Trust in this context refers to the degree of confidence that money and personal information will be safe and that parties involved will not act against user's interest. People trust payment system only if it is conducted in a proper way and that money will not be stolen or misused. On the other hand, even if we use an imperfect system we believe that vendors, banks and credit cards companies will not use the information against us. Another aspect of trust is that other parties should have trust in the payment systems we want use, based on this trust they would be willing to conduct commerce.

13. Usability: Paying with an electronic payment system should not be a complex task. Usability is an important characteristic and defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use". Payments should be automated and done in an easy, faultless way. The system must be easy to implement. The consumer requires the card issuer and merchant to provide a secure system that is not complex, while the merchant requires the acquirer and security software developers to provide a simple application that meets the security requirements.

ONLINE PAYMENT CATEGORIES

Online payment methods refer to the way shoppers can pay for their purchases over the Internet. There are quite a number of online payment services that have been developed within the payment system around the globe.

Several types of online payment system classification are available. The first level in the categorization is based on the way in which money transfer is organized. Existing payment mechanisms may be divided into two groups: electronic currency systems and credit-debit systems.

According to another classification it is divided into electronic currency and account-based systems. In account-based systems, users are allowed to pay using their own bank accounts while the latter allows consumers to pay only with the help of some electronic currency. Both the systems provide numerous payment methods such as i) Electronic payment cards (credit/debit and charge cards), ii) Mobile payments, iii) E-wallets, iv) Smart cards, v) Credit cards, vi) Stored value card payment, and vii) E-cash.

The third classification is based on the type of information that is exchanged. It distinguishes between token-based systems and account-base systems. Token based system correspond to credit-debit systems and account based system correspond to electronic currency. Therefore, existing payment mechanisms may be divided into two groups: electronic currency systems (or electronic cash) and credit-debit systems.

Electronic currency resembles conventional cash, when parties exchange electronic tokens that represent value, just as banknotes determine the value of paper money. The credit-debit approach in the context of electronic payments means that money is represented by numbers in bank accounts and these numbers are transferred between parties in an electronic manner over computer networks. Some writers put credit cards systems in a separate group; others consider them to be a variant of credit-debit system.

Going one step further in the classification in the group of account-based systems we can distinguish between debit and credit cards systems and specialized ones, e.g. those systems that use e-mail for money transfer or notification. Electronic currency, in its turn, can be divided on systems that support smart cards, and those that exist only in online environment. They can be called 'online cash' or 'Web cash'. Prepaid card and electronic purse systems can be also included in this category.

Digital Token Based Payment System

Electronic currency looks like conventional cash. When parties exchange electronic tokens gets a value, just as banknotes determine the value of paper money. When using electronic currency systems customers purchase electronic digital tokens from the issuing company. Electronic currency represents value in some form and can be spent with merchants, who deposit the currency in their own accounts or can spend the currency in other places. Electronic currency is stored in digital form and serves as a cash substitute for the Internet. It can be represented by electronic "bills and coins", certificates, packets of data, or, in other words, tokens. Customers can pay for tokens by using credit cards, electronic

cheques, or other means. Some of the systems allow converting electronic currency back in another form of money.

Benefit to Buyers

Digital token-based e-Payment systems have their own importance. Some of their benefits to buyers and sellers can be explained as below:

1. Convenience of global acceptance, a wide range of payment options, and enhanced financial management tools.
2. Enhanced security and reduced liability for stolen or misused cards.
3. Consumer protection through an established system of dispute resolution.
4. Convenient and immediate access to funds on deposit via debit cards.
5. Accessibility to immediate credit.

Benefit to Sellers

1. Speed and security of the transaction processing chain from verification and authorisation to clearing and settlement
2. Freedom from more costly labour, materials and accounting services
3. Better management of cash flow, inventory and financial planning due to speedy bank payment
4. Cost and risk savings by eliminating the need to run an in-house credit facility.

1. Electronic Tokens

An electronic token is a digital analogue of various forms of payment backed by a bank or financial institutions. There are two types of electronic tokens namely prepaid tokens and post paid tokens.

Prepaid or real-time tokens are exchanged between buyer and seller. The users may get prepaid token by making the payment in advance. Then transactions can be settled through these tokens. Digital cash or e-cash, debit cards, electronic purses are examples of this kind of tokens. In the case of post-paid tokens, fund transfer instructions are being exchanged between buyer and seller. Electronic cheques and credit cards are examples. The following are the important methods of making payment online.

2. Digital coins

In the absence of appropriate equipment for smart card on the consumer's computers, digital coins can be an appropriate method of payment for electronic transactions. The digital coin is based on the following principle: the bank provides consumers with the serial number of a coin encrypted with the bank's private key. If the consumer wants to spend the coin, the bank checks the serial number on the list of spent coins and, if the coin has not already been spent, the bank either credits the bank account or provides them with a new coin.

There are two main concerns for using digital coins: anonymity of the consumer and online verification.

With respect to anonymity, it is clear that each transaction using a digital coin allows the processing of personal data. However, anonymity could be preserved by blinded coins, which protects the details of the payer but not that of the payee.

The second concern of the consumer is related to online verification. In e-transaction between merchants and consumers, the merchant should verify if the coin offered to him has not previously been spent. It is possible to check the coin's digital signature via the public key corresponding to the coin. However, this verification seems to involve delay and expense. Obviously, the use of digital cash would enable the growth of e-commerce only if banks implementing this electronic system could ensure consumer privacy protection

Credit-Debit Instruments or Account-Based Systems

Account-based systems establishing accounts with payment service providers. Users can authorize charges against those accounts, as they would do with usual accounts. With the debit approach, the customer maintains a positive balance of the account and money is subtracted when a debit transaction is performed. With the credit approach, charges are posted against the customer's account and the customer is billed for this amount later or subsequently pays the balance of the account to the payment service.

One of the most widely used systems for electronic payment, the debit card, is a clear example of debit systems. A special group of account-based instruments that are currently in wide use employ credit cards systems. A majority of trade on the Internet is done using credit cards.

Advantages of the credit-debit model are its ease of use and scalability. Existing networks and a computer as a payment terminal is sufficient, there is no need for creating new hardware or infrastructure. Systems built by this model have the potential for good scalability, which allows more users to join the system without affecting its performance. The reason is that to support more users a system should only increase number of accounts that can be done relatively easy; there is no need to support large databases tracking all issued tokens as in electronic currency systems.

There are several limitations in these types of systems. They are usually traceable and not anonymous. Hence it is easy to observe spending and money flows. Account management is usually under the control of the company that provides this service. This can affect reliability and interoperability. These types of systems usually require a network connection and do not offer possibilities of offline payments, which is also a limitation in certain contexts of use.

CREDIT CARD AS E-PAYMENT SYSTEM

Credit cards are the most widely used and convenient method of making online 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 can pay the credit card bill.

Thus credit card is a financial instrument which can be used more than once to borrow money or buy products and services on credit. It is a small plastic sheet bearing the name and number of the holder. It also contains the validity period and other important particulars. The name of the bank, the name of the branch from which the card has been issued and card number are embossed on them.

Credit cards work around the globe regardless of the location or country of the issuing bank. They also handle multiple currencies and clear transactions through a series of clearing houses. There are two types of credit cards today namely credit card issued by credit card companies (e.g. MasterCard, Visa) and major banks.

Banks issue credit cards to their good customers. Cards are issued to customers on the basis of their income level, credit history and total financial soundness. By using these cards, customers can purchase goods and services either offline or online without making immediate payment. Payment to the merchants will be made by the customer's bank.

After the goods have been purchased, the buyer can make payment through his credit card. The customer is supposed to repay his debts during the payment period. Otherwise interest will accumulate. However credit cards are not suitable for very small and very large payments. In the case of very small payments, it is not cost justified and there are some security issues in very large payments.

To accept a credit card for payment, we have to open a merchant account with our bank. A merchant account allows sellers to accept and process credit card transactions. In these transactions, the card number and transaction details are processed with no

identification of the buyer. To implement the payments over the internet, the web merchant needs some form of secure and encrypted line using the Secure sockets Layer (SSL) that is standard on Netscape and Microsoft browsers. The merchant server needs an encryption key for the purpose.

Advantages

1. Convenience. The main advantage of credit cards is their convenience. Compared to cash, credit cards are easier to use in several ways.

2. Fast payment. It takes only a few seconds to swipe a credit card or insert it in a chip-enabled card reader. That means credit card can be used for making quick payments.

3. Easy access. User need not worry about the cash when use a credit card for shopping. At any time he can access his bank and make payments easily. For instance, if you are stranded late at night in a city far from home and have to pay for a hotel room. Instead of having to wander the dark and unfamiliar streets looking for a cash machine, you can just swipe your card for making payment.

4. More Shopping Options. It is not possible to make purchases over the phone with cash. In that situation, plastic card is the only way to go. A credit card is a necessity for shopping at many online retailers.

5. Consumer Protections. Another advantage of credit cards over debit cards is the increased consumer protection they provide. If someone steals your wallet full of cash, the money is simply gone. By contrast, if someone steals your credit or debit card number and uses it to make purchases, you are not required to pay for them.

6. Credit Score. Using a credit card regularly, and paying the bill on time, user will be able to develop a strong credit score. Credit score is a measure to know the creditworthiness of a user – that is, how likely he is to pay money back on time when he borrow it. The higher this score is, the more eager lenders are to make loans to them at favourable rates.

7. Record Keeping. When a person makes most of his purchases with a credit card, he gets an automatic record of his spending. Credit card bill lists all the purchases he made during the month, with their amounts, so he always able to know exactly how he spends his money. This information can be very useful for creating his personal budget.

Disadvantages

1. Over spending: The biggest disadvantage of credit cards is that they encourage people to spend money that they don't have. Most credit cards do not require paying off balance each month. While this may seem like 'free money' at the time, you will have to pay it off — and the longer you wait, the more money you will owe since credit card companies charge you interest each month on the money you have borrowed.

2. High Interest Rates and Increased Debt: Credit card companies charge an huge amount of interest on each balance at the end of each month. This is how they make their money and this is how most people get into debt trap and even bankruptcy.

3. Credit Card Fraud: Like cash, sometimes credit cards can be stolen. They may be physically stolen or someone may steal credit card and use the card to rack up debts. With advances in technology, it is possible to clone a card and gain access to confidential information through which another individual or entity can make purchases on your card. However, unlike cash, if you realize your credit card or number has been stolen and you report it to your credit card company immediately, you will not be charged for any purchases that someone else has made.

4. Hidden costs: Credit cards appear to be simple and straightforward at the outset, but have a number of hidden charges. Credit cards have a number of taxes and fees, such as late payment fees, joining fees, renewal fees and processing fees. Missing a card payment could result in a penalty and repeated late payments could even result in the reduction of credit limit, which would have a negative impact on credit score and future credit prospects.

5. High interest rate: if dues are not cleared before the billing due date, the amount is carried forward and interest is charged on it. This interest is accrued over a period of time on purchases that are made after the interest-free period.

Encryption and Credit Cards

When data is moving from one device or system to another it can be secretly copied and sent to a computer controlled by a thief. Data often must be stored somewhere for later use, or for archival purposes. Whether the storage medium is online such as a file server or, the data is vulnerable to accidental exposure or loss and to intentional theft.

Protecting stored cardholder data is essential for businesses. Probably the single most important measure that merchants can take to protect cardholder information is to encrypt it as soon as the data is captured and leave it in an encrypted state while it is transmitted to the payment processor. This is sometimes referred to as end-to-end encryption. As a result, the transaction is never transmitted in plain text in the frame relay, dial-up or Internet connection, where the potential exists for interception by fraudsters. If the data once encrypted, it is virtually useless to thieves.

Encryption refers to algorithmic schemes that encode plain text such as a cardholder number into a non-readable form called cipher text, thus providing privacy for the encrypted data. One or more "keys" are required to decrypt the data and return it to its original plain text format. The key is the trigger mechanism to the algorithm.

To be most effective, data encryption should take place at the POS terminal application, immediately after the magnetic-stripe reader (MSR) obtains the card data track. If data is not encrypted at the point of capture, it is vulnerable as it is transmitted in plain text to the POS server or the merchant's central server.

A merchant should send its transactions to the payment processor for approval in an encrypted form using industry standard, laboratory-tested algorithms. Using a key, the processor can decrypt the transaction and continue to process it as usual with the bank associations and networks. It is important to note that many encryption algorithms exist that are public or proprietary, and the resulting encryption will be only as effective as the

industry testing and validation of such algorithms. Proprietary algorithms do not go through necessary crypto-analysis scrutiny from industry experts, and one should be cautious when these untested algorithms are the basis of the encryption method used.

Once encrypted, the data can be safely stored on a merchant's POS server or host computer for the purpose of end-of-day reconciliation and other internal uses if needed. The processes of encrypting data immediately after capture and transmitting it to the payment processor in encrypted form provide great risk reduction. Even if a thief is able to intercept the data in transit, it will be in a format that is both unreadable and unusable to him.

The advantages and disadvantages of encryption

As with any security solution, there are advantages and disadvantages to the approach. On the positive side, encryption is a common technique that has proven to be very reliable over many years. It is not easy to break encryption. However, it takes a sophisticated thief to know how to penetrate an encryption algorithm to defeat it. Encryption technology continues to advance, making it far harder for someone to "crack the code."

DEBIT CARDS

Another important and popular method of making payment is through debit cards. Debit card is a prepaid card and also known as ATM card. An individual has to open an account with the issuing bank which gives debit card with a personal id number. This is a payment card that deducts money directly from a consumer's bank account to pay for a purchase. Debit cards eliminate the need to carry cash or cheques to make purchases.

A bank account is needed before getting a debit card from the bank. Banks issue debit cards to their customers who have maintained an account in the bank with sufficient credit balance. Each time the customer makes a purchase, an equal amount of the purchase is debited in his account. When using a debit card, consumers are drawing money in their account. But in the case of credit card, consumers are essentially borrowing money from banks. 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. Thus debit card is a kind of payment card that transfers funds directly from the consumer's bank account to the merchants account.

Debit cards serve a dual purpose. First, they allow the user to withdraw money from his bank account through an ATM or through the cash-back function many merchants offer at the point of sale. In addition they also allow the user to make purchases. ATM cards, by contrast, only allow the user to withdraw money from an ATM, while credit cards only allow purchases unless the credit card holder has a PIN-enabled cash advance feature. The cash advance will incur interest, unlike withdrawing cash from a bank account.

The transaction works much like a credit card transaction. For example a customer gives as ATM card to the seller for the purchase. The merchant read the card through a transaction terminal and the customer enters his personal identification number. Then the terminal route the transaction through the ATM networks back to the customer's bank for

authorization against customer's deposit account. The funds, are approved, are transferred from the customers bank to the seller's bank.

Advantages of a Debit Card

1. Easy to obtain. It is easy to obtain a debit card because most institutions will issue a debit card upon request once opening an account.

swiping the card rather than issuing out a bank cheque.

3. Quick purchase: Merchants like debit cards much more than cheques or credit cards because using a debit card is much faster than writing a cheque.

4. Comfortable: Payment of costly items or things can be easily bought using debit cards rather than writing a cheque or counting the cash. People can be relaxed while purchasing many items. They needn't take care of insufficient cash in their pocket.

5. Safety. Users need not have to carry cash or a cheque book with them for making purchase. Keeping debit cards are safer than keeping large amount of cash or cheque book.

6. Control on spending: Unlike credit cards, debit card won't allow to spend more than the amount of money in the bank account. This is very helpful to avoid accumulating debt.

7. Readily accepted. Debit card is a widely accepted payment medium and it can be used where ever user goes. Debit cards are accessible all over the world. So, people can simply swipe during the purchase instead of changing the currency for each country.

Disadvantages of a Debit Card

1. No grace period: Unlike a credit card, a debit card uses funds directly from bank account. A credit card allows borrow funds on credit, leaving disposable cash in the account.

2. Limited money access: Debit card takes money from the savings account. So, unlike credit card which gives unlimited money from its account debit cards has limited time period.

3. Less safety: Most financial institutions will try and protect their customer from debit card fraud. However, anyone who has the debit card and pin number can access the money. There is no high security for the debit cards since, any user can use it instead of the account holder. If someone gets debit card and PIN, user can lose all the money in the account and it will be much difficult to get it back.

4. Extra Fees: Debit cards can be accessed without any fee only in that specified bank ATM. Accessing from another bank's ATM will cost additional fee and it increases for each transactions. Since, the respective bank ATM cannot be available everywhere, this can be huge disadvantage for the user.

THE MOBILE PAYMENTS

Mobile payments are payments which can be initiated on a mobile device like a cell phone or tablet computer. In spite of its popularity, mobile payments have not been widely

adopted. Mobile payments gained attention because consumers have no access to other noncash forms of payment like cheques or credit cards. The potential benefits to consumers of mobile payments can be evaluated by comparing mobile payment methods to traditional payment methods in terms of key payment attributes. Some attributes, such as convenience, cost, security, and acceptance by merchants, apply to both mobile payments and traditional payment methods. The ability to receive targeted ads and monitor account balances from any location, are some special features of mobile payments.

Consumers can make three types of payments with a mobile device such as a cell phone or tablet computer. The first consists of person-to person transfer. These transfers include non-commercial payments from one consumer to another and commercial payments from a consumer to people like an electrician or plumber. The second type of payment is for goods and services purchased over the Internet on a mobile device. The third is mobile payments at a point of sale (POS), which are payments initiated from a mobile device at physical locations, such as a grocery store, restaurant, or gas station.

Mobile payments can be funded in a variety of ways. One is to fund the payment directly from a bank account or an account at a nonbank payment provider. When funded from a bank account, payments are typically processed over the automated clearing house (ACH), a system for direct electronic transfers between bank accounts. Another way is to fund the payment with a traditional credit, debit, or prepaid card. A final way is to pay for purchases through a mobile carrier, either by drawing on a prepaid account with the carrier or adding the purchase to the monthly phone bill. A consumer could also consolidate multiple funding options on a mobile device, through an application known as a "mobile wallet."

Several technologies are available for mobile payments at POS. Near field communication (NFC) chip technology enables wireless communication between devices over a short distance. Google is using NFC technology in its recently introduced mobile payment application, Google Wallet. Near field communications (NFC) is a short-range, high-frequency, standards-based wireless communication technology that enables exchange of data between devices in close proximity. When NFC is used for mobile POS payments, a mobile device embedded with a NFC chip sends encrypted data to an NFC-enabled POS device. Thus, instead of swiping a card or paying with cash or cheque, the consumer taps or waves his mobile device at the POS device. NFC can also be used for mobile person-to-person transfers if the sender's and receivers mobile devices are in close proximity.

While NFC is the best-known technology, there are also other technologies for making payments from a mobile device. Radio frequency identification (RFID) technology is similar to NFC, but with a longer transmission range. RFID is a technology that uses radio waves to transfer data from an electronic tag called an RFID tag. Some RFID tags can be read from several meters away. An RFID reader transmits an encoded radio signal to interrogate the tag. The tag receives the message and responds with its identification information. Similar to NFC, RFID can be used for both mobile POS payments and some mobile

person-to-person payments. However, because of the longer transmission range, some RFID-enabled mobile payments are considered less secure than NFC-enabled ones.

Another technology, 2D barcodes, has been used by merchants such as Starbucks and Target to allow consumers to make mobile payments from a prepaid account with the merchant. The consumer's mobile device displays a barcode, which is then scanned at the cash register to complete the purchase. 2D barcode is a two-dimensional barcode containing more information than a conventional one-dimensional linear barcode. A 2D barcode enables fast data access and is often used in conjunction with smart phones. A mobile device displaying a 2D barcode with the consumer's pre-funded account information is scanned by a POS device at checkout.

Finally, Wireless Application Protocol (WAP) is a technology for transmitting information over a mobile wireless network. WAP allows the consumer to log on to the payment provider's website through a mobile web browser or an application that can be downloaded and installed on the mobile device. Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile wireless network. The principal application is to enable access to the Internet from a mobile device (WAP browser). However, additional applications using WAP can be downloaded and installed on the mobile device. Similar to an Internet browser on a personal computer a WAP browser on a mobile device can be used to make remote consumer-to-business payments and person-to-person transfers. Applications downloaded and installed on the mobile device can also be used to make POS payments.

CLASSIFICATION OF NEW PAYMENT SYSTEM

Electronic commerce and electronic business require new payment systems for their further development. New payment system highlights the importance of user-related aspects in design and introduction of electronic payment systems for mass customers.

Smart Card Payment System

A smart card is similar to a credit card or debit card in size and shape. It is plastic card that contains an embedded computer chip–either a memory or microprocessor type–that stores and transacts data. The microprocessor is under a gold contact pad on one side of the card. It is a small plastic card that has a built-in microprocessor to store and process data and records.

Smart cards can be used with a smart-card reader attachment to a personal computer to authenticate a user. Smart card has the facility to store the details about customer. It encrypts digital cash on a chip and can be refilled by connecting to a bank. A smart card contains more information than in other types of cards. The ability of the chip to store more information in its memory makes the card smart. It can even make decisions as it has got powerful processing capabilities.

The cards can be used to purchase goods and services. Smart cards are very useful to merchants and consumers to settle the transaction between them. Smart card provides lot of benefits to consumers. It helps to manage expenditures more effectively, reduce the

paper work and ability to access multiple services and the Internet. A multiple application card can support services like health care, travel and financial data access.

Advantages

The benefits of smart cards for the consumer are the following.

1. ***Security:*** Smart cards are secured because unauthorised access is prevented by a lock function.

2. ***Convenience:*** Smart cards are also convenient to use since it is an easy method of payment.

3. ***Flexibility:*** Smart cards are flexible because smart cards can be used for all kind of purchases although certain limits are set within each country.

4. ***Control:*** Smart cards provide control on spending within the limits of an existing amount on the card.

5. ***International use:*** Smart cards are highly useful as it allow cardholders to use the card when travelling or transferring money abroad.

6. ***Interest free loan:*** Finally, in comparison with a credit card, a smart card allows consumers an interest free loan.

Disadvantages

1. ***Security:*** Level of security is another important disadvantage. They are more secure than other cards. However, they are not as secure as many of us would believe. This creates a false sense of security and someone might not be as diligent as protecting their card and the details it contains.

2. ***Chance of loss:*** Like a credit card, smart cards are small, lightweight and can be easily lost if not properly handled. Unlike credit cards, smart cards can have multiple uses and so the loss may be much more inconvenient.

3. ***Slow Adoption:*** If used as a payment card, not every store or restaurant will have the hardware necessary to use these cards. One of the reasons for this is since the technology is more secure, it is also more expensive to produce and use.

4. ***Possible Risk of Identify Theft:*** There is no risk when used smart cards correctly for identification purposes by authorised officials. However, for criminals seeking a new identity, they are like treasure, based on the amount of information it can contain on an individual.

MICRO PAYMENT SYSTEM

Merchants have to pay a fee for each credit card transactions they process. This is expensive when customers purchase goods involving small amount. The cost of certain items would be less than the processing fee which ultimately incurs loss to the merchants. Micro payments are made for small payments on the web. Most of these micropayment systems try to save costs, including financial risk-management costs, operational costs (including communication, processing, storage), and set-up costs. The process is very

similar to e-wallet technology where customers transfers some money into the wallet on his desktop and pays digital products by using this wallet.

Micro payment can be used to pay for one article published in a journal, a chapter from a scientific book or one song from the CD on the web. There are many vendors involved in micro payment systems. IBM offers micro payment wallet and servers. IBM micro payment system allows vendors and merchants to sell content, information and services over the web.

Characteristics of Micropayments

The important characteristics of micropayments are as follows.

1. The amount of payment in micropayment is very small. It could be as small as fractions of a rupee.
2. The payment is anonymous. The micropayment users intend to have a temporary relationship with vendor. The reason may be that they want to use micropayment without revealing their personal financial information or open an account just for making a small payment.
3. The efficiency and low cost are extremely important. The amount for each payment is very small and if the cost for handling each transaction is high, there will be no scope to for a vendor to make any profit and the whole system becomes worthless.
4. Finally, cheating on a small payment with big effort is not worth for a hacker to try. So Micropayment system can compromise some security to achieve the efficiency.

Different Micropayment Systems

There are different types of micropayment systems namely direct-to-bill, aggregation, pre-paid accounts and *direct* transfers.

1. Direct-to-bill

One form of micro payment system is direct-to-bill payment via telephony. It allows either to charge the telephony bill or to debit from pre-paid credit. An example is the Vodafone/ T-Mobile m-Pay Bill, which is intended for small transfers. Such payment systems are not widely offered and frequently do not permit international payments.

2. Aggregation

Cumulative collection/aggregation services are a frequently used for mobile payment. Individual transaction expenditures are summed once a month for payment. This service may be offered by a micropayment organisation connecting to a range of merchants. An alternative option is to add the cost of transaction to existing monthly bills usually telephone bills. A further mechanism consists in merchants themselves aggregating consumer expenditures.

3. Prepayment

Prepaid systems also have potential for micropayments. The card is for one time use only and contains no other information than a 16-digit PIN concealed under scratch foil. However none of these payment mechanisms have been widely used.

Peer –to- Peer Payments

P2P payments are person-to-person payments via a cell phone or email address. In some cases, users are also allowed pay the bills of merchants. This is gaining popularity because consumers can easily send or receive money anytime via their smart phone or online for a low, or no, fee.

Paypal is the most important peer-to-peer payment system, which is now owned by Ebay. These services have allowed individuals to make and receive payments through their own credit card and/or bank account. Furthermore, an increasing coverage offers a more or less faultless way to send and receive payments in many currencies, without having to incur further foreign exchange costs. PayPal, which launched in 1999, has offered P2P payments via the Web as a way for people to exchange money digitally. These days, we can use PayPal's downloadable mobile apps to send and receive money via a smart phone.

Electronic Cash or E-Cash

Electronic cash is a new concept to execute cash payment using computers connected with network. E-cash is an electronic medium for making payments. This refers to a system in which a person can securely pay for goods or services electronically without necessarily involving a bank to mediate the transaction. The primary function of e-cash is to facilitate transactions on the Internet. E-cash are also known as Digital Cash and Cyber cash.

E-cash involves at least three parties, issuer not necessarily financial institutions, consumer as the end-user who uses the E-cash and merchant who accept E-cash in exchange with products or services provided. The following procedure is followed to implement e-cash.

1. Consumer needs to open an account with a bank. Merchants who want to participate in e-cash transaction need to have accounts with various banks in order to support consumer's transactions. The banks on the other hand will handle both consumers' and merchants' accounts.

2. In an e-cash transaction the consumer is required to download and install software called electronic wallet on his computer (PC). So, as to get DigiCash, an electronic wallet is used by consumer to create digital coins, and thus, these created coins are sent to the bank to get signed. And after the coins are signed, the equivalent amount of money is withdrawn from the person's (customers) account of concerned bank.

3. In case of when the person interested in making a purchase, he suppose to send signed digital coins to the Vendor. On the contrary the vendor cross-verifies the bank's signature and performs the deposit of the coins into the bank, where they are credited to the vendor's account in the respective bank.

When consumer decides to purchase, he will transfers the E-cash from his bank account to his electronic purse (on-line system) or E-cash token (off-line system). The E-cash can then be transferred to the merchant in exchange with the merchant's products or services. The E-cash payment can be in term of softcopy (via software) or token based. Transactions via Internet are normally encrypted.

4. Upon receiving E-cash payment from consumer, merchant will get confirmation from the bank. The bank will then authenticate the E-cash transaction. At the same time the bank will debit consumer's account based on the agreed amount. The merchant will then delivers the products or services and instructs the bank to deposit the agreed amount to the merchant's bank account.

Properties of E-Cash

An e-cash system should have the following properties.

1. ***Security***: Security is one of the main concerns that need to be considered while using e-cash. The originality of the message being transferred among consumers, merchants and banks need to be secured to avoid any unauthorized individual intercepting or changing the content of the messages. It should ensure a high-level of security through complex authenticated techniques, which means it should not be copied or reused by the payer, the payee or anyone else.

2. ***Portability***: E-cash should be portable, similar to the conventional money where it does not depends on physical location. The transactions can be carried over computer networks and into storage devices and vice versa.

3. ***Anonymity***: It should be able to maintain the anonymity of the person, i.e. the transaction carried out should not be traceable. Similar to coins and paper notes there should not be any link or trace to individual who uses the e-cash for any transaction. This feature is needed in order to protect consumers' privacy from being monitored for the purpose of financial surveillance.

4. ***Transferability***: Transferability features allow consumers to transfer e-cash from one person to another without a need to refer to the bank. Similar to conventional cash where coins or paper notes can be transferred easily, E-cash should be able to do the same. The user can spend the money received in payment without having to contact a bank for authentication.

5. ***Divisibility***: This allows the digital cash to be sub-divided into smaller denominations. It means e-cash should possess the ability to make change where e-cash can be divided into small denominations to allow small value transaction possible. This is known as micropayment. The challenge for divisible system is to be able to divide the e-cash value to small values where the total of the small E-cash value is equal to the original value.

6. ***User friendly***: Both the payer and payee should be able to use it easily so that it would widely acceptable.

Advantages of E-Cash

1. ***Convenience to consumers:*** E-cash is more than a convenient way of carrying cash to consumers, since it also provides opportunity for e-commerce to take place. Consumer only needs to have smart card like devices to initiate transaction, either on-line or off-line.

2. ***Consumer privacy:*** Anonymity implementation gives consumer a privacy to use e-cash just like the conventional coins and paper notes. Consumers are also able to make transactions without the need of third party verification.

3. ***Purchase in small lots***: E-cash environment enables consumers to purchase small item over the Internet, which is difficult in other implementations such as credit cards.

4. ***Global market:*** To merchant, E-cash provides an opportunity to expand their businesses across the globe without the barrier of different currencies.

5. ***Security:*** By using identified approach, merchant can be protected against fraud because each transaction needs verification from financial institutions or banks.

6. ***Efficiency of banks:*** For the banks, E-cash implementation does reduce cost in maintaining cash in the bank and therefore increase bank management efficiency. Furthermore with E-cash, banks are now able to provide their services to the world via the Internet more easily.

Disadvantages of E-Cash

1. ***Existence of counterfeiters:*** One of the disadvantages of E-cash is the existence of counterfeiters who are able to recreate E-cash either stored in smart card or softcopy based. All parties involve, consumers, merchants and banks/issuers, are affected by this counterfeit activity.

2. ***Lack of Infrastructure:*** Although the number of Internet users is increasing in number, there are many others who do not have the opportunity to own computers and get connected to the Internet. These are the people who will be left behind even further with the introduction of the E-cash.

3. ***Computer literacy:*** Consumer needs to learn new things such as installing software on the computer and understand how e-cash software operates.

4. ***Less popularity:*** Furthermore, the numbers of participating companies are still low and it seems companies are not willing to accept e-cash system in order to attract more consumers. This phenomena might relate to the fact that additional fee is incur as processing charges by banks to merchant and consumer. These additional charges are non-issue in conventional payment system but can mounting to a huge sum in E-cash implementation.

5. ***Difficulty in monitoring:*** Other issue of E-cash is money monitoring by the government. With the conventional coins and paper notes, government can monitor money flow to stabilized economy, but with E-cash, there is no foreseeable way for the government to control the flow of E-cash in and out of a country.

CHEQUE PAYMENT SYSTEM ON THE INTERNET

E-cheques are a mode of electronic payments. Integration of the banking and the information technology industry has benefited the consumers in many aspects with respect to time, cost and operational efficiency. Cheque is the most widely accepted Negotiable Instrument to settle transactions in the world. Paper cheques provide consumers an important payments mechanism.

ELECTRONIC CHEQUE

Cheque is the most widely accepted negotiable instrument to settle transactions in the world. An e-cheque is an electronic document which substitutes the paper cheque for online transactions. Electronic cheques are very similar to ordinary paper cheques except that they are initiated electronically. E-cheques work the same way as paper cheques and are a legally binding promise to pay. The payer/account holder writes an e-cheque using a computer or other type of electronic device and transmits the e-cheque to the payee electronically. Digital signatures are used for signing and endorsing electronic cheques. Public networks such as the Internet deliver electronic cheques. Electronic Payment (deposits) are gathered by banks and cleared through existing banking channels, such as automated clearing houses.

In India, Negotiable Instrument Act 1881 has amended in 2002 and substituted new section for Section 6 as follows-

A "cheque" is a bill of exchange drawn on a specified banker and not expressed to be payable otherwise than on demand and it includes the electronic image of a truncated cheque and a cheque in the electronic form.

An e-cheque uses the same legal and business protocols associated with traditional paper cheques. It is a new payment instrument that combines high security, speed, convenience and processing efficiencies for online transactions. The e-cheque system is designed with message integrity, authentication and non repudiation features, strong enough to prevent fraud against the banks and their customers.

Payers and payees can be individuals, businesses, or financial institutions such as banks. E-cheques are transferred directly from the payer to the payee, so that the timing and the purpose of the payment are clear to the payee.

The payer writes an e-cheque by structuring an electronic document with the information legally required to be in a cheque and digitally signs it. The payee receives the e-cheque over email or web, verifies the payer's digital signature, writes out a deposit and digitally signs it.

The payee's bank verifies the payer's and payee's digital signatures, and then forwards the cheque for clearing and settlement. The payer's bank verifies the payer's digital signature and debits the payer's account. Like paper cheques, e-Cheques can bounce or be returned, for stop payment instructions, insufficient funds or accounts being closed.

Advantages of E-Cheque

1. Faster Processing: Faster processing of e-cheques is much beneficial to business people. Paper cheques require many steps before the money moves from the customer's account to the merchant's account, which can take several days. An electronic cheque can process within few hours, which means the business gets its money faster. This allows businesses to more easily manage their bills and creates a more stable financial situation for the business.

2. Lower Costs: The cost of an electronic cheque is much cheaper than that of a paper check. Processing payments online with electronic cheques eliminates the need for stamps and envelopes, which saves time and money for customers. Processing electronic cheques also saves money for merchants in processing costs, especially in the elimination of deposit and transaction fees. Electronic cheques can also be an environmentally conscious choice, since less paper is involved in printing and processing the cheques.

3. Customer Payment Options: Some customers do not possess a debit or credit card. This limits purchasing options, especially from online vendors. Business that accepts electronic cheques will sell goods or services that might otherwise remain unavailable to customers.

4. Security and Reliability

The electronic cheque is far more secure than a paper cheque, with an encryption feature that verifies the account number, amount, and even uses a digital signature to check against the name of the account.

Disadvantages of E-Cheque

1. Fraud Potential: As computers process electronic cheques, hackers can potentially get access to users banking information. Some fraudulent businesses also offer electronic cheques as a means to steal banking information.

2. Errors: The computer-driven nature of electronic cheques also makes them subject to computer errors. For example, a fault in the processing might lead to a double withdrawal from account or an incorrect withdrawal amount.

3. Absence of Float: Customers who opt to pay with e-cheques are often at a disadvantage as the money is immediately debited from their account, in contrast to paper cheques that provide individuals with a "float" time during which they can debit sufficient funds into their bank account.

4. Bouncing: Due to the insufficient funds in many individual's bank accounts, their e-cheques are often "bounced" or returned. This not only causes delays in the payment transaction but its increases the amount of time involved in returning and refunding payment transactions

E-WALLETS

E-wallet is a type of electronic card which is used for transactions made online through a computer or a smart phone. Its utility is same as a credit or debit card. An E-wallet needs to be linked with the individual's bank account to make payments.

E-wallet is a type of pre-paid account in which a user can store his money for any future online transaction. An E-wallet is protected with a password. With the help of an E-wallet, one can make payments for groceries, online purchases, and flight tickets, among others.

E-wallet has mainly two components, software and information. The software component stores personal information and provides security and encryption of the data. The information component is a database of details provided by the user which includes their name, shipping address, payment method, amount to be paid, credit or debit card details, etc.

For setting up an E-wallet account, the user needs to install the software on his device, and enter the relevant information required. After shopping online, the E-wallet automatically fills in the user's information on the payment form. To activate the E-wallet, the user needs to enter his password. Once the online payment is made, the consumer is not required to fill the order form on any other website as the information gets stored in the database and is updated automatically.

Type of M- Wallets in India

According to RBI, there is three kinds of mobile wallets – closed wallets, semi-closed and open wallets.

1. Closed mobile wallets: Closed mobile wallet doesn't provide services like redemption or cash withdrawal. It can only be used for goods and services for that specific company. Online merchants like MakeMyTrip, Jabong, etc. are some examples of closed wallets. In case of any cancellation or to return product your registered MakeMyTrip or Jabong accounts credited with the refund amount. This can only be used with that merchant itself.

2. Semi-closed wallets: Semi-closed wallets are also similar like closed wallets. It also doesn't permit to redeem or withdraw cash. But it allows users to purchase goods and services with listed merchants who have a contract with Wallet Company to receive payment. Paytm, PayUMoney, MobiKwik, Oxigen, etc. are examples of semi-closed e-wallets. Moreover, they are the most downloaded and trending mobile wallets in India.

3. Open Wallets The wallets that allow users to redeem plus withdraw cash name as Open Wallets. Vodafone Powered M-Pesa wallets is the perfect example.

Electronic Purse

Cash has been around us for many thousands of years and has worked reasonably well. However, with the introduction of Internet and consequent development of e-business and e-commerce, there arises a genuine need for secure transactions together with a support from the financial service sector to increase the services to users.

Electronic Purse is a card with a microchip that can be used instead of cash and coins for everything from vending machines to public transportation. The Electronic Purse would consist of a micro-chip embedded in a credit card, debit card, or stand alone card to store value electronically. The card would replace cash and coins for small-ticket purchases

such as gasoline stations, pay phones, road/bridge tolls, video games, school cafeterias, fast food restaurants, convenience stores, and cash lanes at supermarkets. Cardholders can "reload" the microchip and control the amount of value stored in the card's memory The Electronic Purse provides cardholders with the security and convenience of carrying less cash and coins, eliminating the need for exact change.

Electronic purse is a term applied to a number of formats, each with different applications. At the moment, smart card based systems are used as a direct replacement for money that the user would have in his pocket and software based systems are used for online purchases. There are already some systems on the market that make use of a smart card based electronic purse and combine it with a reader to enable the user access to Internet based commerce through their PCs. The main advantage of this type of system is that it is able to use the smart card in shops as well.

One of the biggest advantages to the banks of transferring transactions to an electronic based medium is that it will avoid the requirement to transport large quantities of metal and paper currency around the country and reduce the number of staff required to interact with customers. In addition, replacing cheques with their long delays with electronic money will speed up the processing of accounts, giving users access to their own funds.

Advantages

1. As the customer requires new services, the various open card framework structures allow secure installation of facilities on the card. If the programming team have done their job and ensured that the code works well and is secure, the user knows that his card will perform as expected.
2. A secured purse for larger amounts of cash - such transactions requiring a PIN - and an unsecured purse for immediate, small value transactions such as buying a newspaper and so on make this very convenient.
3. Assuming that the user does not lose the card or get it stolen, others cannot borrow money from the wallet without the authorised user's knowledge.
3. The use of Internet purchasing in this way may provide a means of bypassing the practice of price chains. Users will be able to purchase goods at a lower cost, legally, even when all the appropriate taxes and duties have been paid.

BITCOIN - CRYPTOCURRENCY

Bitcoin is a digital payment currency that utilizes cryptocurrency and peer-to-peer technology to create and manage monetary transactions as opposed to a central authority. The open source Bitcoin P2P network creates the bitcoins and manages all the bitcoin transactions.

Bitcoin is a digital currency which is traded on applications based virtual exchanges throughout the world. Bitcoin is often quoted in dollar terms but is widely traded in local currencies of the respective nation. Bitcoin is considered the biggest cryptocurrency and it was first introduced in 2009 by Satoshi Nakamoto.

Cryptocurrency is nothing but a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Cryptocurrencies are also a fast and comfortable means of payment worldwide, and they are private and anonymous enough to serve as a means of payment for black markets and any other outlawed economic activity. They are called cryptocurrencies because it is secured by strong cryptography. They are not secured by people or by trust, but by math.

New bitcoins are created by a competitive and decentralized process called "mining". Bitcoin miners are processing transactions and securing the network using specialized hardware and are collecting new bitcoins in exchange. The Bitcoin protocol ensures new bitcoins are created at a fixed rate, making the process of bitcoin mining a very competitive business. Bitcoin is traded on virtual exchange based applications. Bitcoin neither have an intrinsic value nor it is derived from an underlying asset. With a huge difference in the number of people participating on different exchanges, the price of Bitcoin varies accordingly.

In India, there are several Bitcoin applications which facilitate Bitcoin trading, for example, Zebpay, Unocoin and Coinsecure. Bitcoin can be bought and sold very easily after creating an account with the trading partner filling in your necessary details. In India, the mandatory things needed to start Bitcoin trading are an active email account, a bank account, a mobile number, an aadhaar card and a pan card.

In India, credit and debit cards are rarely accepted in rural and even in few semi-urban areas, imagine yourself how much Bitcoin can be accepted. Though there have been few places which have started accepting Bitcoins but with a very high volatility and price fluctuations people refrain from transacting in Bitcoin.

Bitcoin is a legal currency in over 60 major nations including the United States, China, Japan, United Kingdom, Mexico, Canada, Hong Kong, South Korea, Singapore, Germany, Switzerland. Interestingly, Bitcoin has not been legalised in India but many Indians are after it, in order of quick millionaire dream. Apart from India, Bitcoin is also stated as illegal tender in Pakistan, Bangladesh and Nepal.

In the absence of legality, there are risks of losing money. Another major risk associated with it is that there is no governing body, no regulator, no centralised check, no government intervention. As Bitcoin exchanges are very vulnerable to hacking and security risks, even personal data is at a risk.

Properties of Bitcoin

Following are the main features of Bitcoin .

1. Irreversible: After confirmation, a transaction cannot be reversed by anybody. If money is sent, it is sent. It cannot be taken back. If you sent your funds to a scammer or if a hacker stole them from your computer, it is lost. There is no safety net.

2. Pseudonymous: Neither transactions nor accounts are connected to real-world identities. Bitcoins are received on so-called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyze the transaction

flow, it is not necessarily possible to connect the real world identity of users with those addresses.

3. Fast and global: Transactions are propagated instantaneously in the network and are confirmed within minutes. Since they are created in a global network of computers they are completely indifferent of person's physical location. It doesn't matter if Bitcoin is sent to a neighbour or to someone on the other side of the world.

4. Secure: Cryptocurrency funds are created in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers make it impossible to break this scheme. A Bitcoin address is more secure.

5. No Permission: No permission from anybody is needed to use cryptocurrency. It is only a software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There are no restrictions at all.

6. Controlled supply: Most cryptocurrencies limit the supply of the tokens. In Bitcoin, the supply decreases in time and will reach its final number somewhere in around 2140. All cryptocurrencies control the supply of the token by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today.

7. No debt but bearer: Cryptocurrencies don't represent debts. They just represent themselves. They are money as hard as coins of gold.

INTERNET BANKING

Internet banking refers to any banking transaction that can be conducted over the internet, generally through a bank's website under a private profile, and with a desktop or laptop computer. These transactions include services traditionally offered at local branches without having to go to one. Internet banking is generally defined as having the following characteristics:

1. Financial transactions are conducted over the internet through a bank's secure website.
2. The bank may have physical branch locations or it may exist only online.
3. The user must register with the financial institution online and create a login ID and password.

Internet banking is performed through a computer system or similar devices that can connect to the banking site via the internet. Net banking is a facility provided by bank to its customers who have no sufficient time to visit bank. Customers can do transaction from their place.

Banking is now no more limited in going and visiting the bank in person for various purposes like depositing and withdrawing money, requesting for account statement, stop a payment,

etc. Customer can do all these tasks and many more using the online services offered by the banks. He can also keep a track of his account transactions and balance all the time. They can request for cheque book, balance inquiry, downloads statement, and can check the record of last so many years. This service is provided free of cost by banks. They can have all the advantages of the bank just from their mobile or computer.

The Internet provides a secure medium for transferring funds electronically between bank accounts, and also for making banking transaction over the Internet. All banking activities that were conventionally carried by visiting a bank can now be done through a computer with Internet access. Internet banking is highly useful for making payments for the goods and services purchased online.

Advantages of Internet Banking

Internet Banking has several advantages over traditional one which makes operating an account simple and convenient. Some of the advantages of internet banking are:

1. Simplicity: Online account is simple to open and easy to operate.

2. Convenient: It is quite convenient to customers because he can easily pay bills, transfer funds between accounts, etc. Customers need not have to stand in a queue to pay off bills; also do not have to keep receipts of all the bills as he can now easily view your transactions.

3. Any time anywhere: It is available all the time, i.e. 24x7. Customers can perform their tasks from anywhere and at any time; even in night when the bank is closed or on holidays. The only thing need to have is an active internet connection.

4. Fast and efficient: It is fast and efficient. Funds get transferred from one account to the other very fast. He can also manage several accounts easily through internet banking.

5. Safety: Through Internet banking, it is possible to keep an eye on all transactions and account balance all the time. This facility also keeps account **safe**. This means that by monitoring the account at anytime, customers can get to know about any fraudulent activity or threat to account before it can lead account to severe damage.

6. Promotion: It also acts as a great medium for the banks to endorse their products and services. The services include loans, investment options, and many others.

RISKS AND E- PAYMENT SYSTEMS

Before the introduction of computers, people manage payment systems directly and valuable information of business organisations was kept safely in paper records and files. However, in e-commerce environment, information related to payments is transmitted through internet and as such it can easily be accessible to any number of people including outsiders. Hence, the data in computers are more liable to destruction, fraud, error, and misuse. Since payment information is so valuable its security is all the more important Therefore it is highly essential to protect valuable payment information against loss, damage or disclosure. Though only the positive aspects about e-payment systems are always highlighted, we cannot ignore the disadvantages of electronic payment systems.

Users must be aware of the privacy and security concerns raised by electronic payment systems. The risk involved in electronic payment systems can be classified as customer's risks and merchant's risks.

Customer's Risks

Electronic payment raises the following issues to customers

1. Stolen credentials or password: One of the major disadvantages of e-payments is that customers need to register with the institution in order to be authorized to perform money transactions with them. There is no way of verifying the true identity of the maker of the transaction. As long as the password and security questions are correct, the system assumes you are the right person. If this information falls into the hands of a fraud, he will be able to steal customer's money. A dishonest individual will steal customers' personal data, enabling him to set up illegitimate credit card accounts, bank accounts and other accounts. This is called identity theft. Merchant may misuse information provided for transactions by customer.

2. Dishonest merchant: The bigger risk to the customer is the dishonest merchant who accepts credit-cards for payment for legitimate sales and then gives these numbers to others. This type of risk also occur over-the-counter sales. Even then, there will be a limit for customer's liability of a credit card, so the risks are generally quite manageable.

3. Disputes over transaction: One of the great problems of e-payments is the lack of authentication, repudiation of charges and credit card fraud. Conflicts over payments often arise because the payments are not done manually but by an automated system that can cause errors. This is especially common when payment is done on a regular basis to many recipients. Disputes involving credit card transactions are relatively common, usually involving unauthorized transactions like using stolen cards, account statement errors, and dissatisfaction regarding goods and services. These disputes are dealt with in the context of the system operator agreements.

4. Inappropriate use of transaction details: Inappropriate use of transaction details is another major risk faced by customers in electronic payments. Merchant may use personal data and many individuals may not expect or understand the way their information is used. Customers are not generally not aware of this because it happens 'behind the scenes' and may use techniques they are not familiar with. If, for example, personal data is going to be used to offer targeted pricing – i.e. offering the same goods to different people at different prices, depending on their previous online behaviour.

Merchant s Risk

Merchants also face several types of risks in electronic payment system. The important among them are the following.

1. Forged or copied instruments: Forged instruments may be used for making payment in e-commerce. Theft of goods and services through credit card fraud is the most important form of fraud. Merchants are not meeting their customers' face-to face and hence, it difficult to know whether the credit card payment that has accepted is really from a valid

customer. It results in the loss of both the product and the payment. And while credit card holders usually have limited liability, merchants need to bear the full cost of a fraudulent transaction and related fees.

2. Disputed charges: Customers may return goods or services when they are dissatisfied with them, when they never received the merchandise or service, or when they never authorized the charge. In such cases dispute may arise with customers and merchants are bound to pay back the money. In the event of a chargeback, the customer's banks will repay the funds immediately and it is the burden of the merchant to seek remedy for the funds. If your customer feels that they have been charged wrongly or without their authorization they may dispute this directly through their bank with a refund.

3. Insufficient funds in customers account: The risks associated with accepting electronic cheques or credit card is a major concern for merchants. The funds from an electronic cheque transaction remain in electronic cheque account until the funds have cleared or until the transaction is "returned" or "charged back". The e-commerce system will inform a merchant of a returned transaction and the cause thereof usually within 2 to 3 days of the original transaction date. The two most common reasons a transaction is returned are Insufficient Funds (NSF) or Invalid Acct due to the bank account number and routing number were typed incorrectly.

4. Main issue: Secure payment scheme: A payment must always be authorized by the payer. It needs payer authentication through physical, PIN, or digital signature. A payment may also need to be authorized by the bank

DESIGNING E- PAYMENT SYSTEMS

It includes several factors:

1. Privacy

A user expects trust in a secure e-payment system. Customer information has to pass through several hands so security and privacy of the information are a major concern. The safety and security of a customer's personal information lies within the hands of the business. Therefore businesses have to give the customer first their guarantee, and second peace of mind that the information passed over is of no risk to any invading eyes.

2. Security

A secure system verifies the identity of two-party transactions through user authentication and reserves flexibility to restrict information/services through access control. Websites should provide the customers with choices regarding the use of their personal information, and incorporate security procedures to limit access to customer information by unauthorised parties.

3. Intuitive interfaces

The payment interface must be as easy to use as a telephone.

4. Database integration

With home banking, for example, a customer wants to play with all his accounts.

5. Brokers

A network banker is needed to broker goods and services, settle conflicts and financial transactions electronically. Customers may be concerned about how their complaints may be handled. They also may be concerned about warranty disputes. Customers may be in another country and it is very difficult to safeguard their rights. Court action is expensive for all concerned. Instead, third party dispute resolution can be the answer. An independent third party could be used to adjudicate to the betterment of all.

6. Pricing

One fundamental issue is how to price payment system services. All costs to the customer must be displayed including any taxes such as CST, before the customer presses the final button to confirm the order. A facility to allow printing of the order could be given to the customer if they wish to have a hard copy of the order.

7. Standards

Without standards, the bringing together of different payment users into different networks and different systems is impossible.

CRYPTOGRAPHY - the key to security

Many organisations depend on encryption technique to protect their valuable information sent over the Internet and other networks. Encryption is the process of coding and scrambling of messages to prevent unauthorised access to or understanding of the data being transmitted. A message can be encrypted by applying a secret numerical code, called an encryption key, so that it is transmitted as a twisted set of characters. The key consists of large number of letters, numbers and symbols. In order to be read, the message must be decrypted with a matching key. When data are encrypted, the hackers' are not able to understand its real meaning and hence hacking becomes difficult.

As long as there has been communication, there has been the need for privacy and safe, secure methods of information transmission. Cryptography is used to keep transmissions privacy through the use of data encryption techniques.

Cryptography has been around us for centuries. Cryptography is an algorithmic process of converting a plain text or clear text message to a cipher text or cipher message based on an algorithm that both the sender and receiver know, so that the cipher text message can be returned to its original, plain text form. In its cipher form, a message cannot be read by anyone but the intended receiver. The act of converting a plain text message to its cipher text form is called enciphering. Reversing that act (i.e., cipher text form to plain text message) is deciphering. Enciphering and deciphering are more commonly referred to as encryption and decryption, respectively.

Forms of Cryptography

There are two main forms of cryptography:

1. Secret Key Cryptography (SKC) or symmetric: Uses a single key for both encryption and decryption

2. Public Key Cryptography (PKC) or asymmetric: Uses one key for encryption and another for decryption

1. Secret-key cryptography or Symmetric cryptography

Secret-key cryptography, also known as symmetric cryptography is the more traditional form, and has been used for all kinds of communications throughout the ages. In this method, one "key" is used to both encrypt and decrypt the data. A key can be anything from a secret-decoder to a highly complex mathematical algorithm. In secret-key cryptography, the sender and receiver must have the same key for the transmission to work correctly.

Secret-key cryptography suffers from two important limitations. First, any two people that want to communicate with each other must first agree on the key to use. This makes it more difficult to send information to people that we do not already know and hence large-scale communication becomes difficult.

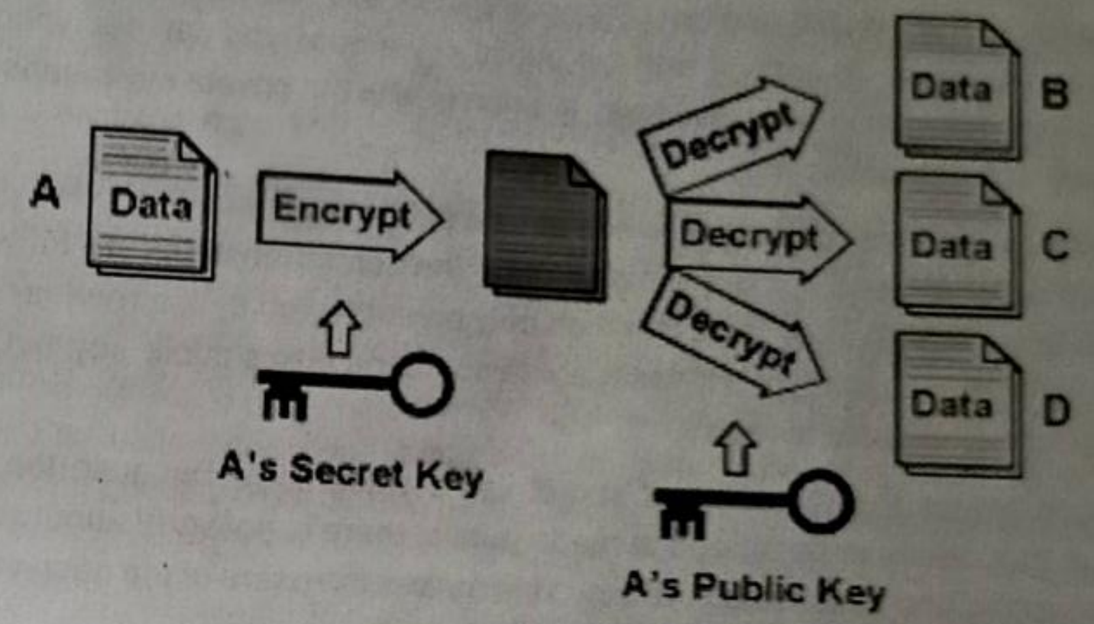
The second important issue is that of "key management". A key is to be agreed between communicating partners and for this purpose some prior communication need to take place between them. This communication itself can be eavesdropped. Then all further communications between the two parties are no longer secure and private. The initial parties might have no way of knowing that the key was stolen.

The most widely used symmetric key cryptographic method is the Data Encryption Standard (DES), published in 1977 by the National Bureau of Standards. DES is still the most widely used symmetric-key approach. It uses a fixed length, 56-bit key and an efficient algorithm to quickly encrypt and decrypt messages. It can be easily implemented in hardware, making the encryption and decryption process even faster. In general, increasing the key size makes the system more secure. A variation of DES, called Triple-DES or DES-EDE (encrypt-decrypt-encrypt), uses three applications of DES and two independent DES keys to produce an effective key length of 168 bits [ANSI 85].

The International Data Encryption Algorithm (IDEA) was invented by James Massey and Xuejia Lai of ETH Zurich, Switzerland in 1991. IDEA uses a fixed length, 128-bit. It is also faster than Triple-DES. In the early 1990s, Don Rivest of RSA Data Security, Inc., invented the algorithms RC2 and RC4. These use variable length keys and are claimed to be even faster.

Symmetric key cryptography, it has a fundamental weakness. Since the same key is used for encryption and decryption, it must be kept secure. If an enemy knows the key, then the message can be decrypted. At the same time, the key must be available to the sender and the receiver and these two parties may be physically separated. Symmetric

key cryptography transforms the problem of transmitting messages securely into that of transmitting keys securely. Nevertheless, ensuring that the sender and receiver are using the same key and that potential adversaries do not know this key remains a major stumbling block. This is referred to as the key management problem.



2. Public-key cryptography or Asymmetric key cryptography

The key management problem inherent to secret-key cryptography needed to be addressed in order for large-scale, secure use of data encryption techniques. In 1976, Whitfield Diffie, a cryptographer and privacy advocate, and Martin Hellman, an electrical engineer, working together discovered the concept of public-key encryption, otherwise known as asymmetric cryptography. In public cryptography, Instead of using one secret key by both users, each user has a public/private key pair. A user makes the public key open and available to anyone, and keeps the private key secret.

Asymmetric encryption uses different keys for encryption and decryption. Under this method, two keys are created namely a private key and a public key. The public key is distributed among the message senders and they use the public key to encrypt the message. The recipient uses their private key any encrypted messages that have been encrypted using the recipient's public key.

Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption key pairs. Having knowledge of one key, say the encryption key, is not sufficient enough to determine the other key - the decryption key. Therefore, the encryption key can be made public, provided the decryption key is held only by the party wishing to receive encrypted messages hence the name public/private key cryptography. Anyone can use the public key to encrypt a message, but only the recipient can decrypt it with private key.

RSA is a widely used public/private key algorithm is, named after the initials of its inventors, Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman [RSA 91]. It depends on the

difficulty of factoring the product of two very large prime numbers. Although used for encrypting whole messages, RSA is much less efficient than symmetric key algorithms such as DES. ElGamal is another public/private key algorithm [El Gamal 85]. This uses a different arithmetic algorithm than RSA, called the discrete logarithm problem.

The mathematical relationship between the public/private key pair permits a general rule: any message encrypted with one key of the pair can be successfully decrypted only with that key's counterpart. To encrypt with the public key means you can decrypt only with the private key. The converse is also true - to encrypt with the private key means you can decrypt only with the public key.

The private key is mathematically derived from the public key, and thus the two are linked together. In order to send someone a message, the sender encrypts the transmission with the receiver's public key. This can then only be decrypted by the receiver's private key. Thus, anyone can encrypt a message with someone else's public key, but only that person would ever be able to read it.

This method solves the problems of secret-key cryptography. Because the only key information that needs to be shared is made public, there is no worry about some third party intercepting and possessing the key. This makes the users of the encryption surer that their transmissions are secure and private.

DIGITAL SIGNATURE

Digital Signature is a process that guarantees that the contents of a message have not been altered in transit. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital document. A valid digital signature gives the recipient reason to believe that the message was created by a known sender in a way that they cannot deny sending it and that the message was not altered in transit. A digital signature is basically a way to ensure that an electronic document like e-mail, spreadsheet, text file, etc. is authentic.

Authentication means that recipient knows who created the document and that it has not been altered in any way since that person created it. Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures.

When sender digitally signs a document, he adds a one-way hash (encryption) of the message content using his public and private key pair. Recipient client can still read it, but the process creates a "signature" that only the server's public key can decrypt. The client, using the server's public key, can then validate the sender as well as the integrity of message contents.

Digital signatures provide the following benefits:

***1. Authentication*:** Digital signature authenticates a document and which enables to identify the sender and sender cannot later say he didn't sign the document.

***2. Non-repudiation*:** Signing takes place through a series of steps and tracks all of those steps. This eliminates the possibility of a signer suggesting he made a mistake in signing or never 'clicked' a button.

***3. Integrity*:** Documents signed with digital signature alert the reader in real time if anything has been changed or if there is any reason not to trust the document.

Signature and the Law

The traditional signatures are hand written and are uniquely representative of one's identity. The use of signature is mandatory in law in certain cases and holds an important legal position in the document as it signify two things, the identity of the person and its intent to it. The Signature is one's identity on a document and is used in day to day transaction and in case of illiterate persons its fingerprint is considered as his signature. The handwritten signature is prone to forgery and tampering hence insufficient for online transaction and contracts. The online transaction requires unique and strong protection which is served by electronic signature.

The concept of digital signature was introduced through Information Technology Act 2000 in India, which is enhanced with hybrid concept of electronic signature which is based on UNCITRAL Model Law on Electronic Signatures 2001. The electronic signature is a technologically neutral concept and includes a digital signature. The object and purpose of electronic signature are similar to that of traditional signature. In cyber world electronic signature ensures that the electronic records are authentic and legitimate as electronic signature are safer and cannot be forged and is convenient as the sender himself does not have to be present personally at the place to contract to sign the document. For example a person can sign a contract in India and send it to any part of the world to complete the transaction.

Legal Position of Digital Signature

Digital signature is electronically generated and can be used to make sure the honesty and legitimacy of data. The introduction of information technology revolutionized the whole world. India is not an exception to it.

Section 3 of the Information Technology Act 2000 provides for authentication of electronic records. It provides that the electronic records can be authenticated by using digital signatures. It prescribes technology requirements for digital signatures. It prescribes the use of an asymmetric crypto system and hash function for authentication of electronic records. Authentication of an electronic document is important as it ensures that the message has not been tampered and confirms the creator's identity, making it non repudiable, i.e., the sender cannot deny its creation. The object of authentication is achieved by the use of asymmetric system and hash function which convent the electronic message into an unreadable format to prevent tampering of electronic record.

A hash function is the method or scheme used for encrypting and decrypts digital signatures. A hash function produces a hash value which is also known as a message digest. It plays an important role in ensuring that the message has not been tampered and information is safe and secure.

Section 4 made the provision for Legal recognition of electronic records — where any law provides that information or any other matter shall be in writing, typewritten or printed form then not-withstanding anything contained in such law, given requirement shall be deemed to have been satisfied if such information or matter is

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference

Section 5 Legal recognition of [electronic signatures] — where law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of [electronic signatures] affixed in such manner as may be prescribed by the Central Government.

Digital Signature Vs. Digital Certificate

Digital signatures are based on three pointers for authentication – Privacy, Non repudiation and Integrity in the virtual world, while the objectives of digital certificate are the authentication of documents, and bind the person who is putting the digital signature, which based on public key cryptography requires two separate keys, as secret and public. However, both the keys are linked together, one key encrypts the plain text, and another decrypts the cipher text, and neither key can perform both the functions. The other difference is digital signature is an electronic process of signing an electronic document while a Digital Certificate is a computer based record which is the identification of certifying agency or the identity of subscriber

How Digital Signature Works?

The private key of the originator is used as input to the algorithm which transforms the data being signed (or its hash value). This transformation can only be reversed, and the data decrypted and accessed, by use of the originator's public key, which is provided to the recipients by the originator.

Verifying a digital signature created with a private key

The recipient must decrypt the digital signature using the public key of the originator and recalculate the hash value of the corresponding digital object. If the calculated hash value does not match the result of the decrypted signature, either the object has been altered since being signed, or the signature was not generated with the corresponding private key of the originator.

Let us illustrate how this is being done. For example, Mr. Dinesh wants to send a secure message to Mrs. Divya. Using this, we can demonstrate how digital signatures work.

From Dinesh's point of view, the signing process operation is simple. But few steps are happening while signing process is started. For digitally sign documents, Dinesh needs to obtain a Private and Public Key – a one-time process; it is done by Secured Signing Service while user registered. The Private Key is not shared and is used only by Dinesh sign documents. The Public Key is available for all, used for validate the signatory's digital signature.

Dinesh sends the signed document to Divya. Divya uses Dinesh's public key which is included in the signature within the Digital Certificate to authenticate Dinesh's signature and to ensure the document didn't alter after it was signed.

1. Document validation process starts
2. Decrypts Dinesh's digital signature with his Public Key and gets sent document
3. Compares Dinesh's document hash with Divya calculated Hash –Divya calculates the document hash of the received document and compares it with the hash document in the digital signature. If both hashes are same, the signed document has not been altered.

Certificate Authority (CA)

CA issues certificates to ensure the authenticity of the signatories. Certificates are similar to ID Document. When we want to identify a user in the system we check his certificate. This certificate issued in registration process once all require information filled in. In PKI world the CA uses the CA's certificate for authenticating user's identity.

Public key certificate

A public key certificate is a digitally signed document that serves to validate the sender's authorization and name. The document consists of a specially formatted block of data that contains the name of the certificate holder which may be either a user or a system name and the holder's public key, as well as the digital signature of a certification authority for authentication. The certification authority attests that the sender's name is the one associated with the public key in the document. A user ID packet, containing the sender's unique identifier, is sent after the certificate packet. There are different types of public key certificates for different functions, such as authorization for a specific action or delegation of authority. Public key certificates are part of a public key infrastructure that deals with digitally signed documents. The other components are public key encryption, trusted third parties such as the certification authority, and mechanisms for certificate publication and issuing.

An alternative approach to the above is the use of certificates that can be used by participants to exchange keys without contacting a public-key authority. Each certificate, containing a public key and other information, is created by a certificate authority and is given to the participant with the matching private key. A participant conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority. Four requirements can be placed on this particular scheme:

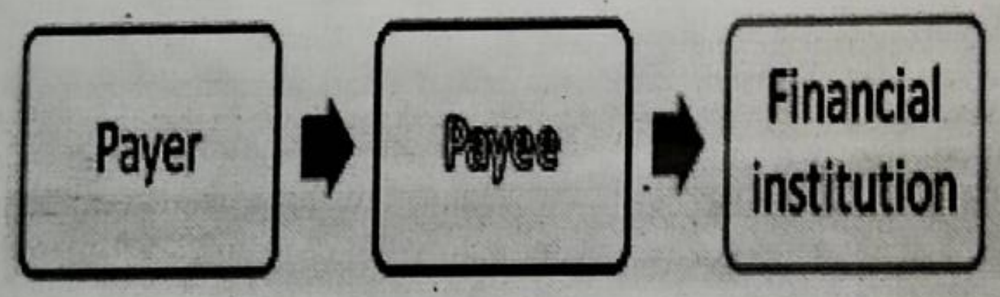
1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
3. Only the certificate authority can create and update certificates.
4. Any participant can verify the currency of the certificate.

The Secure E-payment Process Method

Due to the nature of Internet, security and authenticity of payments and participants cannot be guaranteed with technologies that are not specifically designed for e-commerce. We need an e-payment system that would not only provide secure payments but should also have properties like online customer and merchant authentication, solid proof of transaction authorization by the customer both to the merchant and the bank, privacy of customer and transaction data.

Over the years there are many e-commerce technologies that have been developed. This helps the customers in many ways in terms of convenience and accessibility. But still the security of their valuable money is left unanswered. Now an e-commerce technology is developed known as the Secure Payment System. It is a mode of operation wherein the security of financial transactions done on the Internet is ensured to be safe and confidential.

The secure e-payment process method should keep the customers of an online company coming back because they view the online store as safe and reliable. It will provide them a sense of safety and security of their financial transactions. SET or the Secure Electronic Transaction is one of these types of e-commerce technology. The SET uses the unique process of encrypting the information obtained between the customers-and-the-online-store. Transaction participant's scenario assumes the existence of three participants a customer (the payer), a merchant (the payee) and a financial institution (e.g. a bank).



The All participants are connected with communication links as shown in figure 1. In order to perform the purchase, the participants need to exchange certain information over those links. If the information is transmitted over the links in plain text, there is a possibility of eavesdropping. Anyone listening to the network traffic could gain access to sensitive information, such as card numbers, card type and whole detail of card holder. Credit card-such as a Visa or Master, has a preset spending limit based on user's credit limit. Debit Cards-removes the amount of the charge form the cardholder's account and transfers it to

the seller's bank. In electronic payment system, server stores records of every transaction. When the electronic payment system eventually goes online to communicate with the shops and the customers who can deposit their money and the server uploads these records for auditing purposes.

Secure electronic payment system uses different cryptographic algorithms and techniques to achieve: privacy, integrity, authentication and non-repudiation. The primary goal of cryptography is to secure important data as it passes through a medium that may not be secure itself. Usually, that medium is a computer network. There are many different cryptographic algorithms, each of which can provide one or more of the following services to applications. It is generally accepted that, in order to be considered secure, a payment system must satisfy the following fundamental security requirements.

1. Authentication

Both parties should feel comfortable that they are communicating with the party with whom they think they are communicating. Applications usually perform authentication checks through security tokens or by verifying digital certificates issued by certificate authorities. Cryptography can help establish identity for authentication purposes.

2. Access Control

The prevention of unauthorized use of a resource i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.

3. Data Confidentiality (Secrecy)

Confidentiality is needed for the protection of data from unauthorized disclosure. Confidentiality is an essential component in user privacy, as well as in the protection of proprietary information, and as prevention to theft of information services. The only way to ensure confidentiality on a public network is through strong encryption. Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium

4. Data Integrity (Anti-tampering)

The assurance that data received are exactly as sent by an authorized entity i.e., contain no insertion, deletion, or alteration. It should prevent the unauthorized medication of data. Financial messages travel through multiple routers on the open network to reach their destinations. We must make sure that the information is not modified in transit.

5. Non-Repudiation

It provides protection against denial by one of the entities involved in a communication of having participated in all or part of communication.

Secure Socket Layer (SSL)

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted links between a server and a client—typically a web server (website) and a browser. SSL allows traffic to be encrypted.

The Secure Socket Layer (SSL) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. SSL protocol is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet.

SSL allows transmitting sensitive information such as credit card numbers, and login identifications securely. Normally, data sent between browsers and web servers is sent in plain text allow misusing information. If an attacker is able to catch all data being sent between a browser and a web server they can see and use that information.

SSL secures millions of data on the Internet every day, especially during online transactions or when transmitting confidential information. Internet users have come to associate their online security with the lock icon that comes with an SSL-secured website or green address bar that comes with an extended validation SSL-secured website. SSL-secured websites also begin with https rather than http.

SSL has two main objectives:

1. To ensure confidentiality, by encrypting the data that moves between the communicating parties (client and the server).
2. To provide authentication of the session partners, using RSA algorithm. The SSL protocol f two protocols.

Secure Electronic Transaction (SET)

To carry out transactions successfully and without compromising security and rust, business communities, financial institutions and companies offering technological solutions need a protocol that works very similar to the way how a credit card transactions work. Visa and MasterCard, leading credit card companies in the world formed a consortium with computer vendors such as IBM and developed an open protocol which emerged as a standard in ensuring security, authenticity, privacy and trust in electronic transactions.

SET encrypts payment card transaction data and verifies that both parties in the transaction are genuine. SET, originally developed by Mastercard and Visa in collaboration with leading technology providers, has a large corporate backing and is perceived to be more secure as a result of its validation from card companies.

ELECTRONIC FUNDS TRANSFER-EFT

Electronic fund transfer system is one of the oldest electronic payment systems. EFT is a payment system through which cash and cheque payments are totally eliminated. EFT is used for transferring money from one bank account to another directly without involving cash or cheque. In EFT money is directly deposited in an account electronically. EFT is considered to be a safe, reliable and convenient way to conduct business.