Jump2Learn
PUBLICATION

www.jump2learn.com

E-COMMERCE & CYBER SECURITY

Jump2Learn - The Online Learning Place

Ms. Sonal R. Shah | Mrs. Krupali P. Patel | Mr. Nitesh G. Patel

3.1 E-commerce payment systems

When we purchase product or services online, then we pay for them with the help of an electronic payment system. In this method payment is done without using cash or paper cheque, it is known as e-commerce payment system or electronic payment systems.

An E-commerce payment system is a system that allows our customers to pay online for products as well as services over the internet, without the use of checks or cash.

Electronic payment systems refer to paperless financial transactions. Electronic payment systems have reformed the business handling by reducing the paperwork, cost of transaction and cost of labor.

Now a day, consumers have multiple e-commerce payment method options when they are making online purchase of goods and services.

There are different types of e-commerce payment modes are as follows:

3.1.1 Debit Card Based payment systems
3.1.2 Credit Card Based payment systems
3.1.3 E-Cash
3.1.4 E-Cheque
3.1.5 E-wallet
3.1.6 Smart card
3.1.7 Electronic Fund Transfer (EFT)
3.1.8 Risks and EPS

3.1.1 Debit Card Based payment systems:

Prerequisites for debit card, first you must have to require a bank account in bank before receiving a debit card from the bank. Bank provides the debit card to the bank account holder.

Debit card is a small plastic card. Debit card printed on both sides and it look like as follows.

Debit card Front side

Debit card Back side

Debit card has list of following basic components.

1) Bank name and Card holder name
2) The logo
3) The issue and expiration date
4) Processor chip
5) The card number
6) CVV number
7) Customer service number
8) The signature bar

1) **Bank name and Card holder name:**
Name of the bank and name of the card holder both printed on the debit card.

2) **The logo:**
The debit card has the logo of the bank that has issued card. It has one another logo that determine the type of the debit card such as Visa card, MasterCard, RuPay card.

3) **The issue and expiration date:**
The issue or Valid from date as well as expiration or valid upto date are also printed in the MM/YY format on the debit card.

4) **Processor chip:**
Debit card has one processor chip on front side of the card and this chip used to store the information of the card holder and Personal Index Number(PIN).

5) **The card number:**
Debit card has one unique 16-digit number which is printed on front side of a small plastic card. That one unique number all ways mapped with the bank account number of bank account holder. Debit card number is different from account number.

6) **CVV number:**
On the back side of the debit card one three digits CVV (Card verification Value) Number is printed, which will use to make the online payment transaction. CVV number is the unique number and it will be used for card verification. These number will be used at the time of online payment so that it provides an additional security layers.

7) **Customer service number:**
One toll-free number is also printed on the back side of the debit card. You are free to call this number in case of any question or theft of your card.

8) **The signature bar:**
   A signature bar is printed on the back side of the debit card. It is most important that you must sign as soon as you received the card. This signature bar will help you to prevent fraud payment transaction.

In case of payment through debit card, the amount gets deducted from the card's bank account immediately. To make the payment transaction, there should be enough balance in the bank account otherwise transaction will be failed. By using the debit cards customers are free to carry the cash and cheques and sellers accept a debit card freely to receive the payment from customers.

Debit card is most popular payment system for cashless transection. we can use the debit card at both retail and online store for any transection. We can also use the same card to withdraw the money from ATM machine. But debit card has following advantages and disadvantages.

Advantages of debit card

1) We can easily get the debit card for our account now a day.
2) Most of organization allow you to carry a debit card without any fees.
3) We can use the debit card for smallest purchases.
4) Many Reward programs come with debit cards today.
5) Free from error.
6) Easy to use.
7) Confidentiality in transaction.
8) Debit card services is very fast and efficient.
9) You can use the debit card at any time and from anywhere.
10) Debit card provide 24 hours, 7 days a week and 365 days a year services.

Disadvantages of debit card

1) Bank can take some charges for your debit card transaction.
2) If you not remember your PIN, then you are not able to complete a transaction.
3) You must have to maintain the balance before to make the transaction of debit card.
4) Credit card cannot allow the transaction on credit.
5) If card is stolen, then chances to miss use of card.

3.1.2 Credit Card Based payment systems

Payment using credit card is one of most common mode of electronic payment. A credit card is a system of payment named after the small plastic card issued to users of the system. 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. A credit card is different from a debit card in that it does not remove money from the user's account after every transaction.

When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. Credit cards have revolving credit arrangements that allow consumers to make purchases and be billed later. It is usually credit card monthly payment cycle. Most credit card accounts allow the consumer to carry a balance from one billing cycle to the next and make a minimum payment in each billing cycle rather than requiring payment of the full balance.

In the case of credit cards, the issuer lends money to the consumer (or the user) to be paid to the merchant.

Prerequisites for credit card, first you must have to require a bank account in bank before receiving a credit card from the bank. Bank provides the credit card to the bank account holder.

Credit card is a small plastic card same as debit card. Credit card also printed on both sides same as debit card and it look like as follows.

Credit card Front side

Credit card Back side

Credit card has list of following basic components same as debit card.

1) Bank name and Card holder name
2) The logo
3) The issue and expiration date
4) Processor chip
5) The card number
6) CVV number

7) Customer service number
8) The signature bar

1) **Bank name and Card holder name:**
Name of the bank and name of the card holder both printed on the credit card.

2) **The logo:**
The credit card has the logo of the bank that has issued card. It has one another logo that determine the type of the credit card such as Visa card, MasterCard, RuPay card.

3) **The issue and expiration date:**
The issue or Valid from date as well as expiration or valid upto date are also printed in the MM/YY format on the credit card.

4) **Processor chip:**
credit card has one processor chip on front side of the card and this chip used to store the information of the card holder and Personal Index Number(PIN).

5) **The card number:**
Credit card has one unique 16-digit number which is printed on front side of a small plastic card. That one unique number all ways mapped with the bank account number of bank account holder. Credit card number is different from account number.

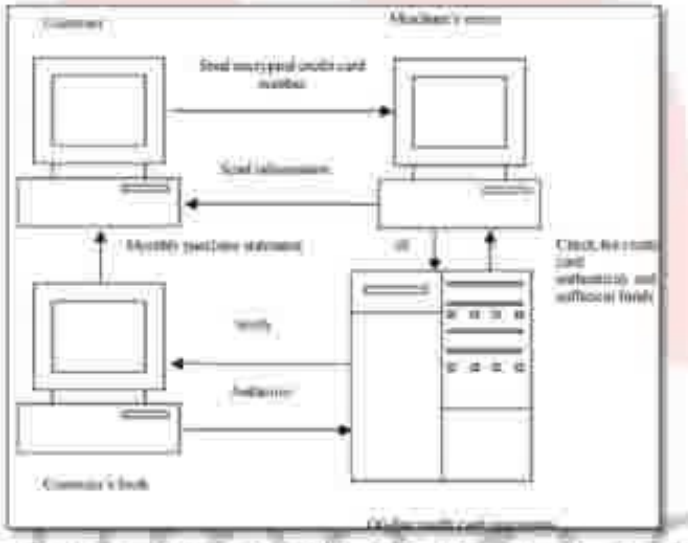
6) **CVV number:**
On the back side of the debit card one three digits CVV (Card verification Value) Number is printed, which will use to make the online payment transaction. CVV number is the unique number and it will be used for card verification. These number will be used at the time of online payment so that it provides an additional security layers.

7) **Customer service number:**
One toll-free number is also printed on the back side of the credit card. You are free to call this number in case of any question or theft of your card.

8) **The signature bar:**
A signature bar is printed on the back side of the credit card. It is most important that you must sign as soon as you received the card. This signature bar will help you to prevent fraud payment transaction.

Following are the actors in the credit card system.

- The card holder – Customer
- The merchant – seller of product who can accept credit card payments.
- The card issuer bank – card holder's bank
- The acquirer bank – the merchant's bank
- The card brand – for example, visa or MasterCard.



In case of payment through credit card, the amount gets deducted from the card's bank account immediately. To make the payment transaction, there is not enough balance in the bank account then also transaction will be successful. By using the credit cards customers are free to carry the cash and cheques and sellers accept a credit card freely to receive the payment from customers.

Credit card is most popular payment system for cashless transection. we can use the credit card at both retail and online store for any transection. Credit card has following advantages and disadvantages.

Advantages of credit card

1) We can easily get the credit card for our account now a day.
2) We can use the credit card for smallest purchases.
3) Many Reward programs come with credit cards today.
4) Free from error.
5) Easy to use.
6) Confidentiality in transaction.
7) Credit card services is very fast and efficient.
8) You can use the credit card at any time and from anywhere.
9) Credit card provide 24 hours, 7 days a week and 365 days a year services.
10) You should not maintain the balance before to make the transaction of credit card.
11) Credit card can allow the transaction based on credit.

Disadvantages of credit card

1) Bank can take some charges for your credit card transaction.
2) Fraud risk is high.
3) If card is stolen, then chances to miss use of card.

Difference of debit card and credit card:

The major difference between a debit card and a credit card are as follows.

No	Debit Card	Credit Card
1	Payment of transaction will be done based on amount available in account.	Payment of transaction will be done based on credit amount available in your credit card.
2	No penalty	Interest after the due date
3	Dose not impact on credit score.	Overdue payment impact on credit score.
4	The card holder can have credit for 30-45 days to make the payment.	Amount is debited immediately from account.
5	Possibility of Fraud risk is high as compare to debit card.	Possibility of Fraud risk is less as compare to credit card.

3.1.3 E-Cash

Definition of an E-cash:

E-cash is the sort form of electronic cash. it is a digital money product that provides a way to pay for products and services without resorting to paper or coin currency. Amount that is exchanged electronically using computer or telecommunications networks over the internet it is known as E-cash. E-cash is a new concept in on-line e-commerce payment system which is based on encryption.

Models of an E-cash:

There are two models developed for e-cash transactions now a day.

1) **Online form of e-Cash**
   The online form of e-Cash which will be worked for all types of Internet transactions.
2) **Offline form of e-cash**
   The offline form of e-cash involved a digitally encoded card that replaced paper money.

Working of an E-cash:

Step 1:

Consumer or wholesaler signs up with one of the participating banks or financial institutions.

Step 2:

Consumer obtains particular software to install on his or her computer. That software allows the customer to download and manages the electronic coins to his or her devices.

Step 3:

When we purchasing the services or product online then if that accepts e-cash, the consumer can simply Pay with e-cash using software. The wholesaler's software makes a payment request based on the items purchased by the consumer.

Step 4:

At the end of transaction, customer can accept or reject this payment request. When the customer accepts the payment request, then after the payment is subtracted from the software exist on the customer's devices and that is sent to the bank or financial institution of the wholesaler, and then is deposited to the wholesaler's account.

E-cash is the secure payment system. Digital signature is used to provide the security in E-cash transactions. E-cash on-line e-commerce payment system which is based on digital signature so that it uses the pair of keys to implement security. Bank give the public key to customer for decode the e-cash which is encoded by the bank's private key.

Properties of an E-cash:

1) Monetary value
2) Interoperability
3) Storable and Retrievable
4) Security

1) **Monetary(financial) value:**
E-cash has financial or monetary values and E-cash should be backed by a bank-certified cashier's check, hard currency or bank-authorized credit.

2) **Interoperability:**
E-cash must be interoperability. It is exchangeable or interoperable in the forms of payment for products, services, paper cash or any purpose for which currency is used.

3) **Storable and Retrievable:**
E-cash must be storable and retrievable. The e-cash stored on a remote computer's or devices memory, For example. smart cards, electronic wallets. The e-cash retrieval will permit users to exchange e-cash from anywhere like home, office.

4) **Security:**
E-cash is the secure payment system because of Electronic cash is not easy to modify or replica while being stored or exchanged.

3.1.4 E-Cheque

Definition of an E-Cheque:
E-Cheque is the digital form or representation of physical paper check. E-Cheque is an electronic money transfer from a bank account without the use of the physical paper check.
It contains the same information as the physical paper cheque. E-Cheque very useful to deposit the salary of employees.

Working of an E-Cheque:
E-Cheque payment transaction work as follows.
Step 1:
At very first customer sends electronic cheque to the person, merchant or organization for whom the payment is made. Electronic cheque can be send by email or any other communication medium.
Step 2:
When e-cheque is deposited by the receiver, then it will be send to account server for verification. After the verification of the e-cheque by the account server that is ready deposit into bank.

Step 3:
If the verification is completed successfully then amount that is specified in e-cheque which is transferred to the person, merchant or organization for whom the payment is made.

Finally, working of the e-cheque is same as physical paper cheque. E-cheque all information as the physical paper cheque. E-cheque also include the digital signature of the payers for verification.

Advantages of an E-Cheque:

1) Fast processing and time saving.
2) Reduce the paper work.
3) More Convenience than paper cheque.
4) Payment can have made at anytime and anywhere.
5) Transaction cost is very lower.
6) Expenses control for customer.
7) Expanded payment options.
8) Reduced back-office burden.

Disadvantages of an E-Cheque:

1) E-Cheque is Fraud potential because hackers can potentially get bank information.
2) Unauthorized transaction has great pain.
3) More chances of error than paper cheque because all work done by the machine.

3.1.5 E-wallet or digital wallet

Definition of an E-wallet:

E-wallet is nothing but an electronic version of a physical wallet, through which you can make the payments over the internet. When you use e-wallet in a smartphone then it is also referred to as a mobile wallet.

E-wallet is a type of electronic card which is used to make the payment online through a computer or a smartphone. E-wallet needs to be linked with the individual's bank account to make payments.

E-wallet is one type of pre-paid account in which a user can store money for online transaction. An E-wallet is always protected with a password.

Working of an E-wallet:

E-wallet payment transaction work as follows.

Step 1:

First log into e-commerce website or e-commerce App and add the particular product to a cart.

Step 2:

After the selecting product, to make the payment select "e-Wallet" payment mode.

Step 3:

After the selecting payment mode, then select the corresponding wallet.

Step 4:

After the selecting wallet, then make payment.

Application of an E-wallet:

E–wallet application are as follows.

1) Digital wallets can be used to make online purchases from e-commerce websites.
2) To pay various utility bills such as electricity bills, mobile bills, gas bills, booking movie tickets, etc.
3) E- wallet can be used to order food online.
4) E-wallet can be used to transfer the amount online.
5) So Many commercial products such as mutual funds as well as insurance can be purchased using e-wallet.

3.1.6 Smart card

Definition of a smart card:
Smart card is same as the credit card-size plastic card that stores digital information and that can be used for electronic payments in place of paper cash.
A smart card is a special type of plastic card like device which contains an integrated circuit chip embedded on it.

History: Roland Moreno patented the memory card in 1974.
By 1977, three commercial manufacturers Bull CP8, SGS Thomson, and Schlumberger, started developing smart card products.

In March 1979, Michel Hugon from Bull CP8 was the first to design and develop a microprocessor-based card combining a processor and local memory. He invented the computerized smart card.

Features: mart cards provide ways to securely identify and authenticate the holder and third parties who want to gain access to the card. A PIN code or biometric data can be used for authentication.
Types: To begin with, magnetic stripe cards are definitively not smart cards.

They also provide a way to securely store data on the card and protect communications with encryption. Smart cards provide a portable, easy to use form factor.

In smart card magnetic stripe replace with microchip that stores electronic cash to use for on-line and off-line payments. Smart cards can only be access with the help of PIN only. Smart card look likes as follows.

Memory vs. microprocessor

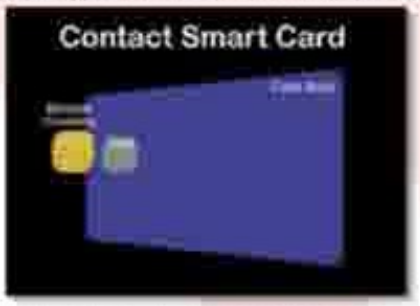
Smart cards come in two varieties: memory and microprocessor.

Memory cards store data and can be viewed as a small USB memory stick with optional security. On the other hand, a microprocessor card can add, delete, and manipulate information in its memory on the card.

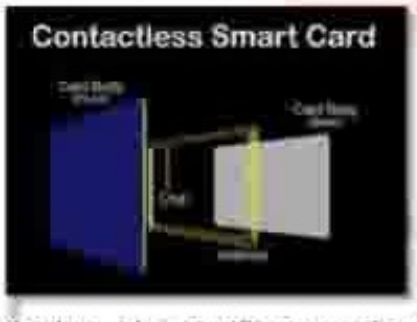
Like a miniature computer, a microprocessor card has an input/output port operating system and a hard disk with built-in security features such as encryption capabilities.

Contact vs. contactless:

Smart cards have two different types of interfaces: contact and contactless.



Contact smart cards are inserted into a smart card reader, making physical contact with the reader. However, contactless smart cards have an antenna embedded inside the card that enables communication with the reader without physical contact. You tap and pay.



Contactless is easy and convenient. It's a significant trend everywhere now in 2020 due to the recent pandemic.

Smart Card Technology:

There are two general categories of smart cards: contact and contactless.

A contact smart card must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card (typically gold plated).

Transmission of commands, data, and card status takes place over these physical contact points.

A contactless card requires only close proximity to a reader. Both the reader and the card have antennae, and the two communicate using radio frequencies (RF) over this contactless link. Most contactless cards also derive power for the internal chip from this electromagnetic signal. The range is typically one-half to three inches for non-battery-powered cards, ideal for applications such as building entry and payment that require a very fast card interface.

Two additional categories of cards are dual-interface cards and hybrid cards. A hybrid card has two chips, one with a contact interface and one with a contactless interface. The two chips are not interconnected. A dual-interface card has a single chip with both contact and contactless interfaces. With dual-interface cards, it is possible to access the same chip using either a contact or contactless interface with a very high level of security.

The chips used in all of these cards fall into two categories as well: microcontroller chips and memory chips. A memory chip is like a small floppy disk with optional security. Memory chips are less expensive than microcontrollers but with a corresponding decrease in data management security. Cards that use memory chips depend on the security of the card reader for processing and are ideal for situations that require low or medium security.

A microcontroller chip can add, delete, and otherwise manipulate information in its memory. A microcontroller is like a miniature computer, with an input/output port, operating system, and hard disk. Smart cards with an embedded microcontroller have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.

Smart Card has list of following basic components same as smart card.

1) Card holder name
2) The logo
3) The issue and expiration date
4) Processor chip
5) The card number

1) Card holder name:
Name of the card holder printed on the smart card.

2) **The logo:**
The smart card has the logo of the that has issued card.

3) **The issue and expiration date:**
The issue or Valid from date as well as expiration or valid upto date are also printed in the MM/YY format on the smart card.

4) **Processor chip:**
Smart card has one processor chip on front side of the card and this chip used to store the information of the card holder, Personal Index Number(PIN) and amount information.

5) **The card number:**
Smart card has one unique number which is printed on front side of a small plastic card.

Application of a smart card:

1) Financial uses.
2) Telephony uses.
3) Information technology uses.
4) Government uses.
5) Health care uses.
6) Identification uses.

Advantages of a smart card:

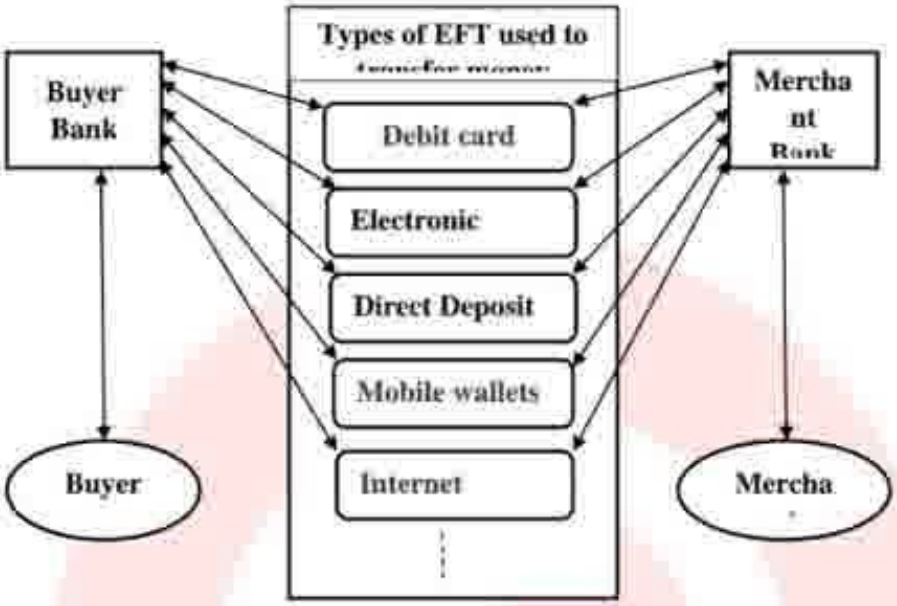
1) Processor chip stores the more data than magnetic stripe.
2) Processor chip is faster than magnetic stripe.
3) Smart card easily transfers the amount from one account to another account.
4) Smart card has high security using PIN.
5) Smart card is more reliable, reusable, disposable as well as multifunction.

3.1.7 Electronic Fund Transfer (EFT)

EFT stands for electronic funds transfer. An electronic funds transfer (EFT) is the digital transfer of money(amount) from one bank account to another within same bank or another bank account. EFTs require both the sender and receiver to have bank accounts. In electronic funds transfer money values is transfer with the help of computerized devices over the internet.
EFT transactions are also known as electronic banking.it it is used to debit one person's account and credit the other person's account so no paper money is needed.

Components of EFT

The components of electronic funds transfer are as follows.



Components of EFT

The components of electronic funds transfer are as follows.

1) Buyer
2) Bayer Bank
3) Merchant
4) Merchant Bank
5) Types of EFT

1) Buyer:

Buyer is the person, who wants to transfer the certain money amount from his/her account merchant account.

2) Bayer Bank:

Bayer Bank is the bank in which buyer bank account's available. Buyer can transfer the amount from buyer bank's account to merchant bank's account.

3) Merchant:

Merchant is the person or business organization, to whom account buyer wants to transfer the certain money amount from his/her account.

4) **Merchant Bank:**
Merchant Bank is the bank in which merchant bank account's available. Merchant can receive the amount from buyer bank's account to merchant bank's account.

5) **Types of EFT:**
Electronic funds transfer has different types and importance types are as follows.
1) **Debit card**
2) Electronic Cheque
3) Direct Deposit
4) **Mobile wallets**
5) **Internet banking**

1) **Debit card:**
Debit card is a small plastic card. It also allows you to make EFT transactions. Debit card is used to transfer money values from your bank account's to merchant account's when purchases any product or services online.

2) **Electronic Cheque:**
E-Cheque is the digital form or representation of physical paper check. E-Cheque is the one another type of electronic fund transfer which used to transfer money values from your bank account's to merchant account's when purchases any product or services online.

3) **Direct Deposit:**
Direct deposit also allows you to make EFT transactions. It lets you to electronic fund transfer as a salary to employees. your direct deposit service provider transfers that money from organization or institute's bank account to employee accounts on payday.

4) **Mobile wallets:**
Mobile wallets are one another types of electronic fund transfer. Mobile wallets used for different online payment and it used to transfer money values from one bank account to another bank account.

5) **Internet banking:**
Internet banking are one another types of EFT. With the help of Internet banking You can transfer the money values from one bank account to another bank account easily now a day. Internet banking electronic fund transfer become the more popular in current era of online payment system.

There some others types of EFT transactions are also used in current market place.

Advantages of EFT:
1) Everything is paperless, so there isn't a need for paper cash or paper checks.
2) Easy to use.

3) Confidentiality in transaction.
4) EFT provide 24 hours, 7 days a week and 365 days a year services.
5) EFT services is very fast and efficient.
6) EFT can be used to transfer the amount online.
7) Fast processing and time saving.
8) Reduce the paper work
9) transaction cost is very Lower.
10) Customers can set up automatic payments with EFTs.
11) EFT service is available almost anywhere in the world.

3.1.8 Risks and EPS

3.1.8.1 Risks in Electronic Payment System:

Electronic payment system allows you to transfer fund from one bank account to another bank account. In electronic payment system has following risk.

1) Risk of fraud
2) Risk of desire buying
3) Risk of payment clashes

1) **Risk of fraud:**
Some time there is the risk of fraud when you transfer fund from one bank account to another bank account. If your PIN known by any hackers, then there is a chance to fraud. When your card is stolen by others, then there is one another a chance to fraud.
2) **Risk of desire buying:**
In the environment of electronic commerce, you are able to purchase product or services on single click of mouse. When desire buying become the habitual that become the risk.
3) **Risk of payment clashes:**
In the environment of electronic payment system, you are not able to handle payment system but it will handle by the machine. So it may chance to generate the error when large amount of payment transaction carries out sequentially.

3.2 Security on Web

Security as well as privacy are most required before making financial transactions over the Internet. At present-day, financial information or records, and other important information are not encrypted. It can be interrupted by well knowledge hacker over the any network or internet. Now a day, so many commercial websites and applications are requiring security at client side as well as at server side for to make safe and authenticated online payment transaction.

In current era, so many types of data traveling over the different types of networks and internet such as private data, public data, copyright data, confidential data, secret data and so on. There is a chance of missuses or misconduct of all types data those traveling online. That's why you need to make secure our website or data.

A number of techniques that can be provide the securities in field of web and most used techniques are as follows.

1) S-HTTP
2) SSL
3) SHEN

1) S-HTTP:

S-HTTP stands for Secure Hypertext Transfer Protocol and it is the advanced version of HTTP. S-HTTP provided secure transactions over the Web. Secure-HTTP allows the secure exchange of files on the world wide web. SHTTP include different cryptography layouts such as DSA and RSA standards into both web client and web server. Secure-HTTP is an alternative of secure socket layer(SSL).

2) SSL

SSL stands for Secure Socket Layer and it protect the data collected by your website, like emails, credit card numbers and basic information of online payment, it transfer as it is from your website to a webserver. SSL include cryptography layout such as RSA security on TCP\IP protocol.

3) SHEN

SHEN one another security technique and it is similar to nature to SHTTP. SHEN security provide three security mechanisms such as week authentication with low maintenance, strong authentication using public key, strong encryption for message's data.

3.3 SSL

What is the SSL?

SSL stands for Secure Sockets Layer and it is a protocol designed by Netscape Communications to enable encrypted and authenticated communications over the Internet.

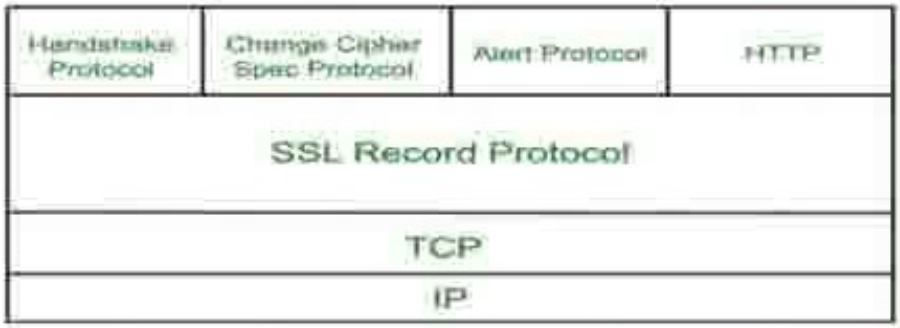
Secure Sockets Layer is the standard security tools for establishing an encoded link between a web browser and a server.

SSL is the encrypted connection between web server and a browser which guarantees that all data passed between them will be remain safe. SSL mainly used to provide three important things like, Privacy, Authentication, and Message Integrity.

Secure socket layer provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol



SSL Record Protocol:

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.

Handshake Protocol:

Handshake Protocol is used to establish sessions. This protocol allows client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- Phase-1: In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purpose.
- Phase-2: Server send his certificate and Server-key-exchange. Server end the phase-2 by sending Server-hello-end packet.
- Phase-3: In this phase Client reply to the server by sending his certificate and Client-exchange-key.

- Phase-4: In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

Change-cipher Protocol:

This protocol uses SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in pending state. After handshake protocol the Pending state is converted into Current state.

Change-cipher protocol consists of single message which is 1 byte in length and can have only one value. This protocol purpose is to cause the pending state to be copied into current state.

Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.
Level is further classified into two parts:

- Warning:
  This Alert have no impact on the connection between sender and receiver.
- Fatal Error:
  This Alert breaks the connection between sender and receiver.

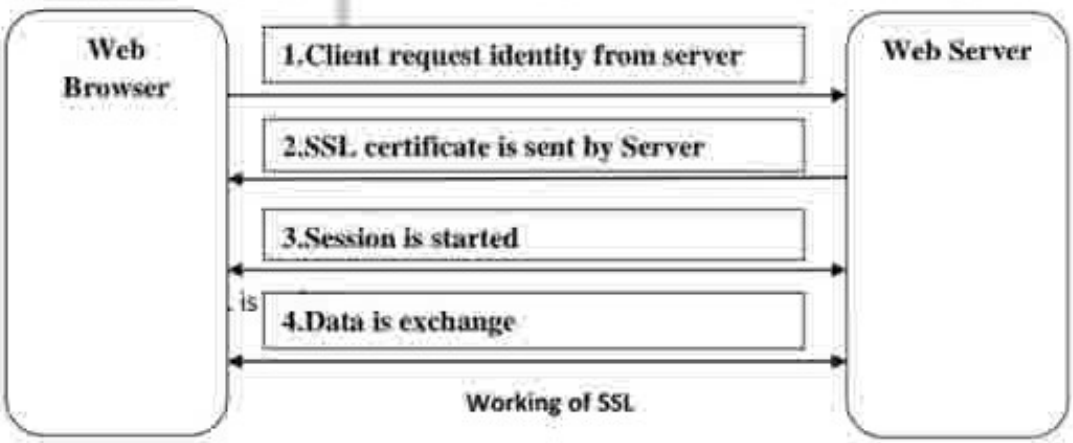
Features of Secure Socket Layer:

- Advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.

Working of SSL

With the help of SSL connection each side of the connection must have a Security Certificate.
Security Certificate must be required in each side (web server and web browser) of the SSL connection to make safe online transaction.

SSL security works based on public-key and private key cryptography. The working of SSL is as follows.



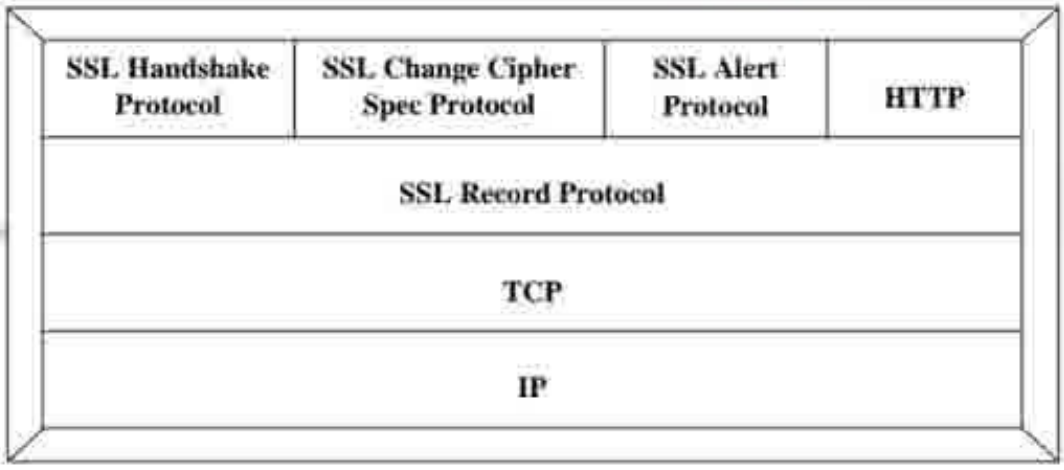
Working of SSL

Step 1:
The client sends the request to web server for identify itself.
Step 2:
The server sends copy of its SSL certificate with keys
Step 3:
The server acknowledges the client to start an SSL session.
Step 4:
The client uses the session keys generated in step 2 to encrypt its data and exchange it with the server.

What is SSL certificate?
SSL certificate is a type of digital certificate that provides authentication for a website and enables an encrypted connection. It consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decrypt information.
An SSL certificate helps to transfer secure information's such as:

1) Login identifications information.
2) Bank and credit card transactions information.
3) Personally identifiable information (such as name, address, date of birth, mobile number and so on.).
4) Proprietary(branded) information.
5) Authorized documents and agreements.
6) Medical records.

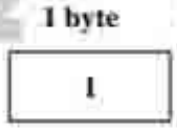
SSL Layered Architecture
SSL always runs on the top of TCP and it provides reliable and secure end-to-end connection service. SSL Layered Architecture Consists of two layers follows.



SSL Architecture

Secure Sockets Layer protocol has two layers (Layer1 and Layer2).

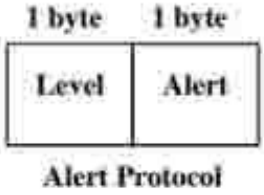
1) **First Layer Protocol:**
SSL Record Protocol included in first layers. The SSL Record Protocol Provides security to other higher level protocols like HTTP handshake protocol, change cipher protocol and alert protocol. The SSL Record Protocol Provides two services for SSL connections:
   1) **Confidentiality: -**
   A shared secret key that is used for conventional encryption of SSL payload.
   2) **Message Integrity: -**
   A shared secret key that is used to construct (Form) a message authentication code.
2) **Second Layer Protocol:**
There are three higher-layer protocols are included in second layer such as SSL Handshake Protocol, SSL Change Cipher Spec Protocol and SSL Alert Protocol.
   1) SSL Handshake Protocol
   2) SSL Change Cipher Spec Protocol
   3) SSL Alert Protocol
   1) **SSL Handshake Protocol:**
   SSL Handshake Protocol is the first protocal of the second layer. The most complex part of SSL is the handshake protocol. It allows the webserver and webclient to authenticate eachother, encryption, MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record. The handshake protocol is used before any application data are transmitted.
   2) **SSL Change Cipher Spec Protocol:**
   SSL Change cipher spec protocol is the second protocal of the second layer. It is one of the three SSL-specific protocols that use the SLL Record protocols. Change cipher spec protocol is the simplest protocol. Change cipher spec protocol is consists of a single message, which consists of a single byte with the value 1.



Change Cipher Spec Protocol

   3) **SSL Alert Protocol:**
   SSL Alert protocol is the third protocal of the second layer and it work on SSL Record protocol. SSL Alert protocol consists of a two bytes. The First

byte indicates **warning(1) or fatal(2).** A Fatal alert will terminate the connection. The Second byte indicate specific error code.



Alert Protocol

Application Protocols

Application Protocols like HTTP, FTP, SMTP, or whatever application is being used.