UNIT – 4
Web Security

* **Web Security :-** Web security is a branch of computer security specifically related to the internet often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.

* **Web Security Threats :-**

- Web security threats are that type of security threats which faced when using the web. One way to group these threats is in terms of passive and active attacks.
- Passive attacks include eavesdropping (to listen secretly) on network traffic between browser and server and gaining access to information on a website that is supposed to be restricted.
- Active attacks include impersonating another user altering messages in transmit between client and server and altering information on a website.
- Another way to classify web security threats is in terms of the threats, web server, web browser and network traffic between browser and server. Issues of server and browser security fall into the category of computer system security.

- Possible web security threats and their consequences. counter measures are as follows –

Page No :

	Threats	Consequences	Counter-measures
Integrity	(a) Modification of user data. (b) Trojan horse browser (c) Modification of memory (d) Modification of message traffic transmit.	Loss of info Compromise of machine Vulnerability to all other threats	Cryptographic checksums
Confidentiality	(a) Eavesdropping on the net. (b) Theft of information from server. (c) Theft of data from client. (d) Information about network configuration. (e) Information about which client talks to server	Loss of info Loss of privacy	Encryption, web proxies
Denial of Service	(a) Killing of user threats (b) Flooding machine with bogus threats (c) Filling up disk or memory. (d) Isolating machine by DNS attacks.	Disruptive Annoying Prevent user from getting work done.	Difficult to prevent.

Authentication	(a) Impersonation of legitimate users.	Misrepresentation of users.	Cryptographic techniques
	(b) Data forgery	Belief that false information is valid.	

* Secure Socket Layer (SSL) :-

SSL is the standard security technology for establishing an encrypted link between a web server and browser. This link ensures that all data passed between the web server and browsers remain private and integral.

- SSL Architecture :-

→ SSL is designed to make use of TCP to provide a reliable end to end ~~and~~ security services.

→ SSL is not a single protocol but rather two layers of protocols, as illustrated in figure.

→ The "SSL record protocol" provides basic security services to various higher-layer protocols.

→ In particular, the HTTP, which provides the transfer service for web client / server interaction, can operate on top of SSL.

→ Three higher-layer protocols can defined as part of SSL, the handshake protocol, the change cipher spec protocol and the alert protocol.

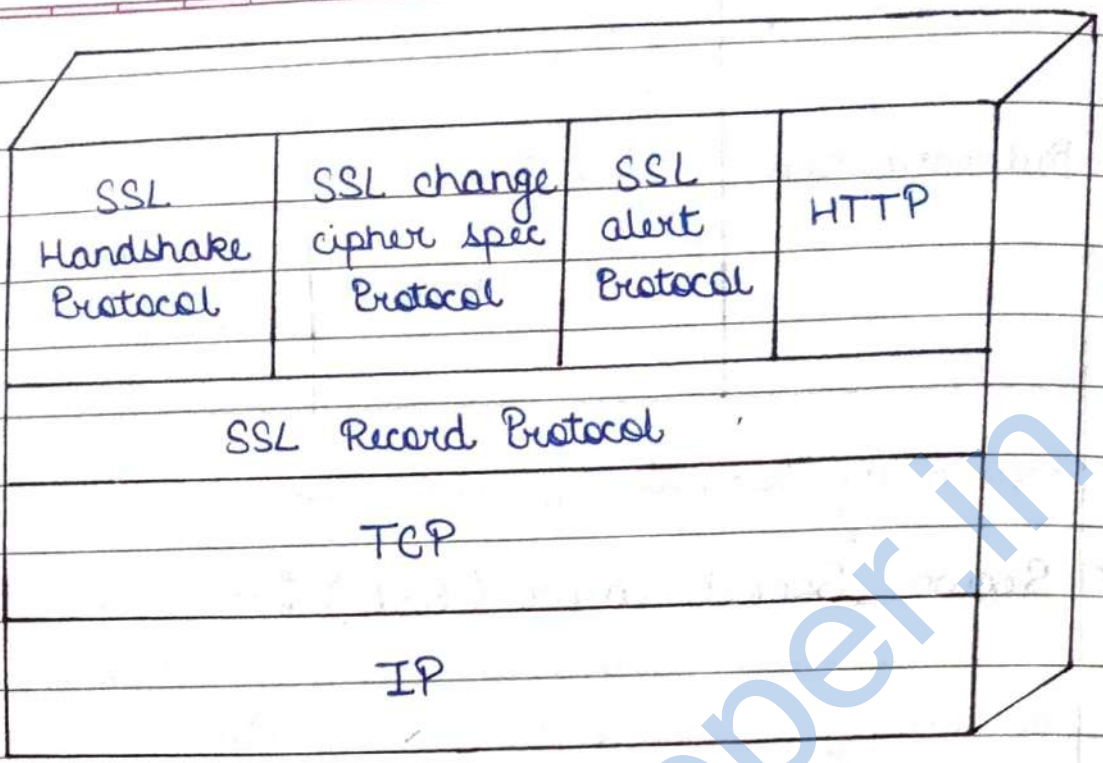


fig :- SSL Protocol Stack

- **SSL Session State :-**

→ SSL session is an association between a client and a server.

→ Sessions are created by the handshake protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections.

→ The session state is defined by the following parameters-

1- Session Identifier — An arbitrary type sequence chosen by the server to identify an active or resumable session state.

2- Peer Certificate — An X.509 v3 certificate of the peer. This element of the state may be null.

3- Compression method — The algorithm used to compress data prior to encryption.

4- Cipher spec — Specifies the bulk data encryption algorithm (such as null) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as hash- size.

5- Master secret — 48 byte secret shared between the client & server.

6- Is resumable — A flag indicating whether the session can be used to initiate new connections.

* SSL Connection State :-

→ A connection is a transport (in the OSI layer model definition) that provides a suitable type of service.

→ This is a logical client / server link, associated with the provision of a suitable type of service. In SSL, it must be a peer to peer connection with two network nodes.

→ A connection state is defined by the following parameters—

1- Server and client random — Byte sequence that are chosen by server and client for each connection.

2- Server write MAC secret — The secret key used in MAC operations on data sent by the server.

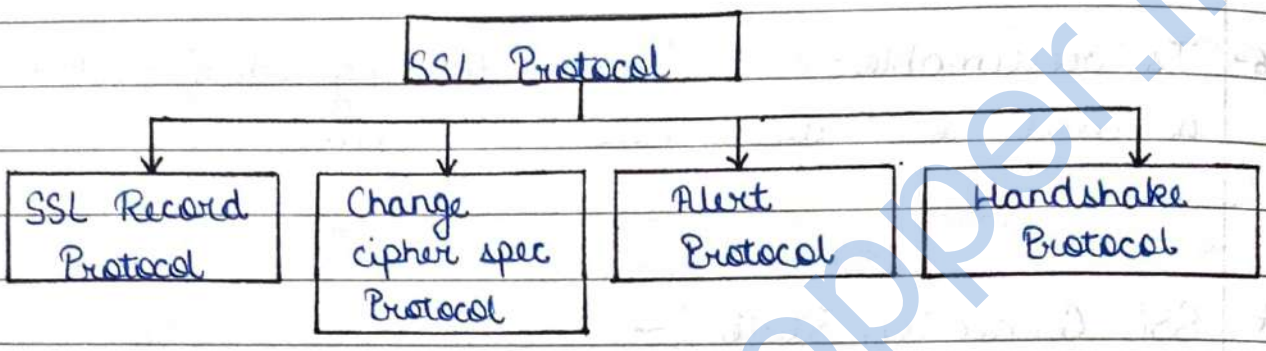
3- Client write MAC secret — The secret key used in MAC operations on data sent by the client.

4- Server write key — The conventional encryption key for data encrypted by the server and decrypted by the client.

5- Client write key — The conventional encryption key for data encrypted by the client and decrypted by the server.

★ SSL Protocols :-

There are four protocols used in SSL.

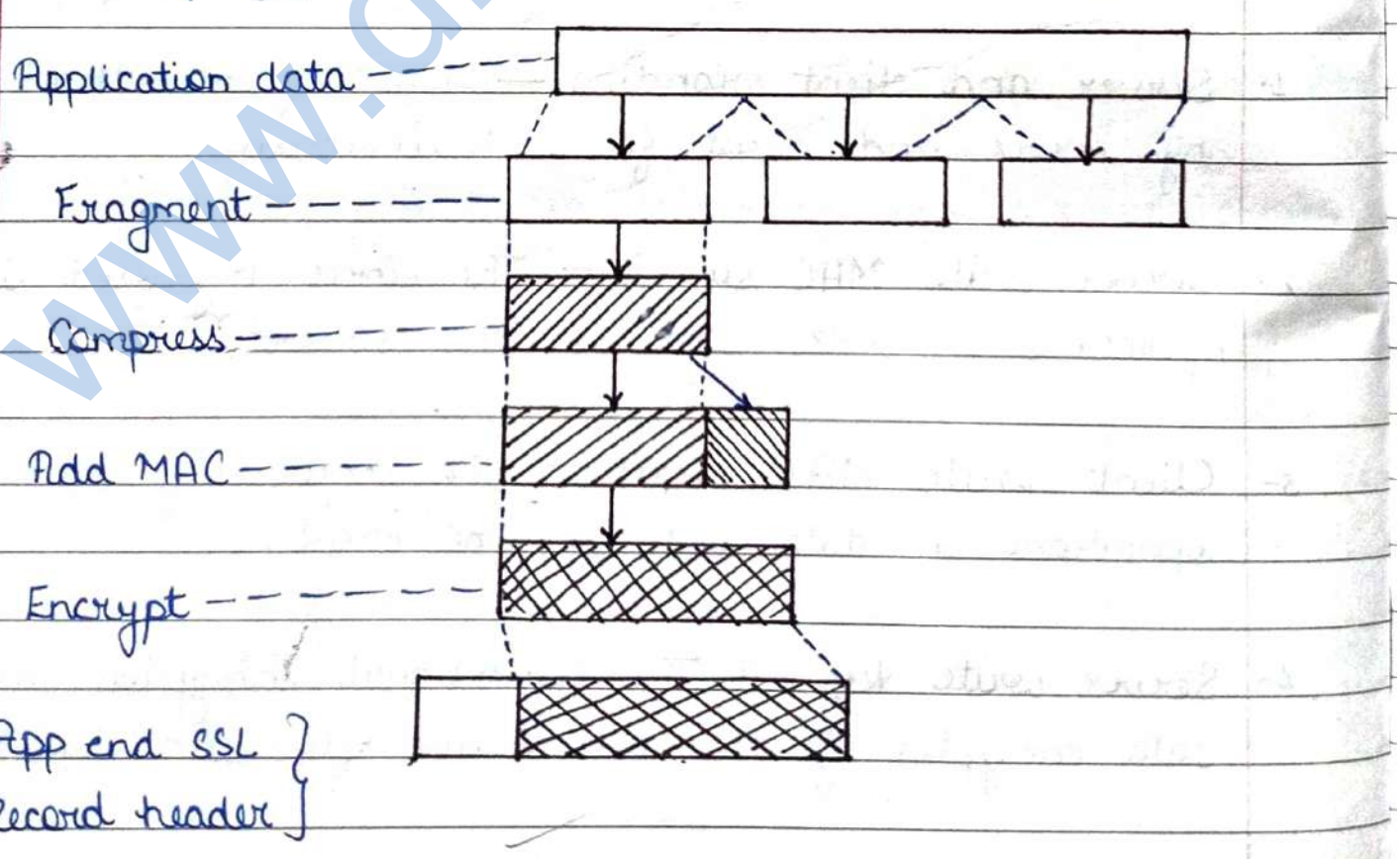


1. SSL Record Protocol :-

It provides two services for SSL connection —

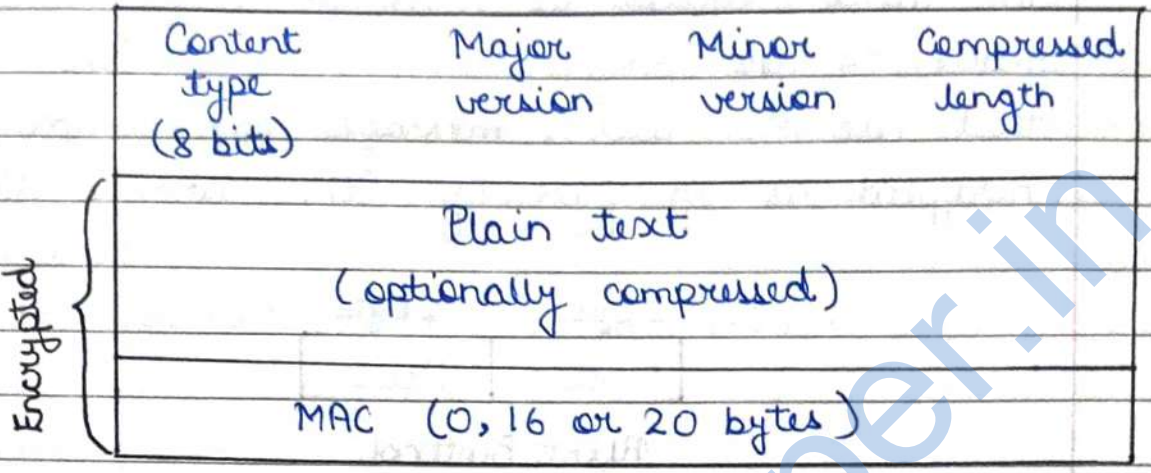
1- Confidentiality
2- Message Integrity

Following figure shows SSL Record Protocol operation —



Page No :

Following is SSL record format –



2- SSL change cipher spec protocol :-

→ The change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the just negotiated cipher spec and keys.

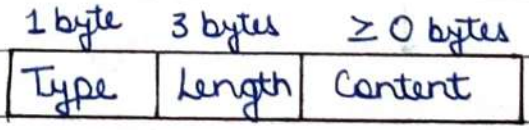
→ There are two states for the change cipher spec message –

(a) Read current

(b) Read pending

→ The sole purpose of this message is to cause the pending state to be copied into the current state.

(a) change cipher spec protocol

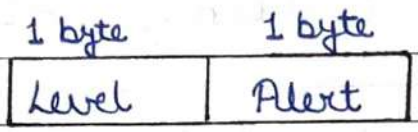


(b) Handshake Protocol

→ This change cipher spec message is normally sent at the end of the SSL handshake.

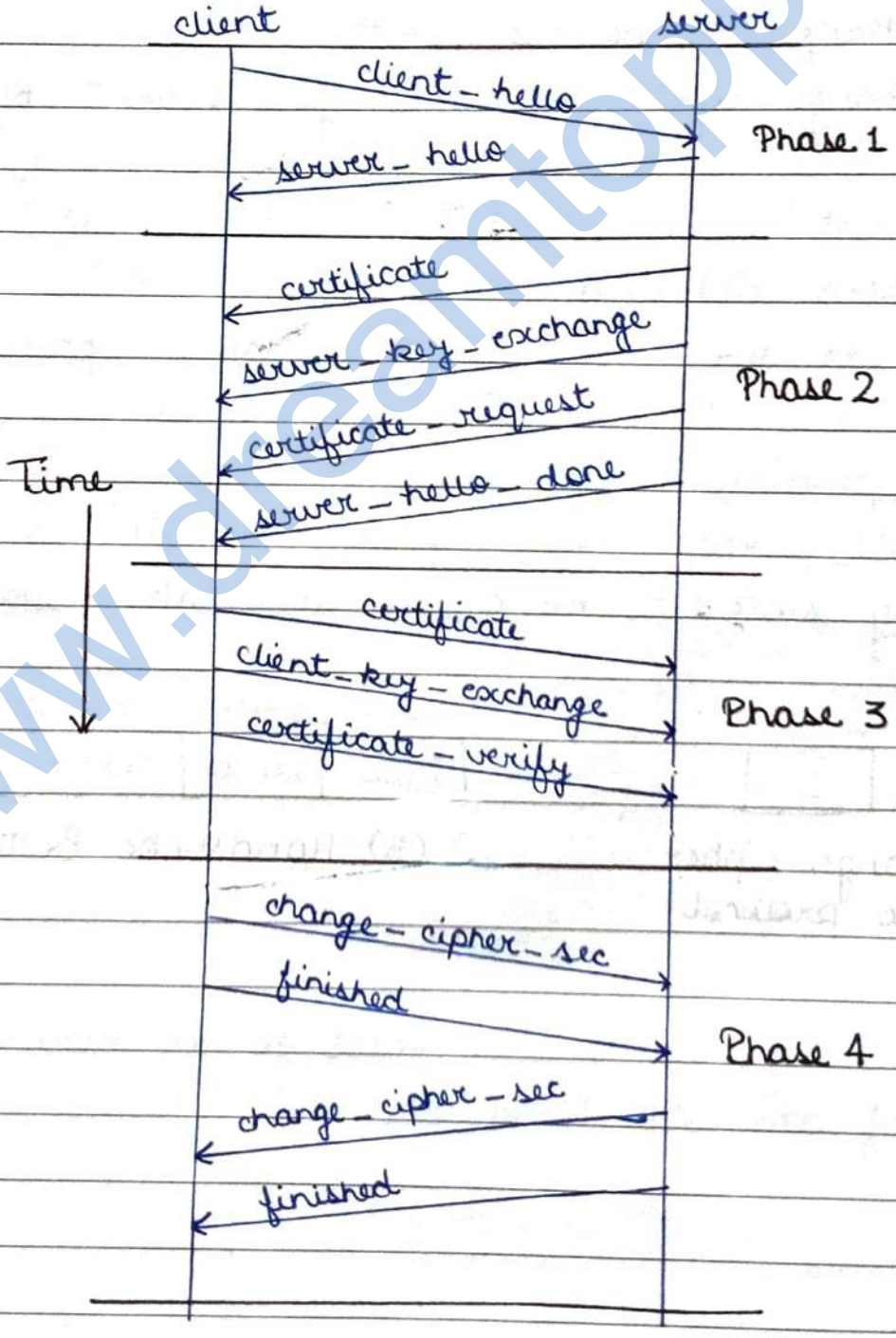
3. SSL Alert Protocol :-

The alert protocol is used to convey SSL related alerts to the peer entity. As with other applications that use SSL alert messages are compressed and encrypted as specified by the current state.



Alert Protocol

4. SSL Handshake Protocol :-



→ Handshake protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in a SSL record. Handshake protocol is used before any application data is transmitted.

→ Handshake protocol action is as follows —

★ Transport Layer Security (TLS) :-

1 → TLS is a protocol that provides communication security between client / server applications that communicate with each other over the internet.

2 → It enables privacy, integrity and protection for the data that's transmitted between different nodes on the internet.

3 → TLS primarily enables secure web browsing, applications access, data transfer and most internet based communication.

4 → It prevents the transmitted / transported data from being eavesdropped or tempered.

5 → TLS is used to secure web browsers, web servers, VPNs, database servers and more.

6 → TLS protocols consist of two different layers of sub-protocols :

(a) TLS Record Protocol

(b) TLS Handshake Protocol

(a) TLS Record Protocol ensures that the connection is private by using symmetric data encryption and it ensures that the connection is reliable.

(b) TLS Handshake Protocol allows authentication between the server and client, and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

★ Secure Electronic Transactions (SET) :-

→ SET is a standard that will enable secure credit card transactions on the internet.

→ SET has been endorsed by virtually all the major players in the electronic commerce arena, including microsoft, visa, netscape and mastercard.

→ SET provides three services :

(a) It provides a secure communication channel among all parties involved in a transaction.

(b) It provides trust by the use of X.509 v3 digital certificate.

(c) It ensures privacy because the information is only available to parties in a transaction when and where necessary.

→ SET is a system for ensuring the security of financial transactions on the internet.

→ It was initially supported by mastercard, visa, microsoft, netscape and others.

→ With SET, a user is given an e-wallet (digital signature) and a transaction is conducted and verified using a combination of digital certificates and combination of digital certificates and digital signature among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and

confidentiality.

→ SET is a specification defined in three books issued in May of 1997.
Book 1 : Business description (80 Pages)
Book 2 : Programmer's guide (629 Pages)
Book 3 : Formal protocol definition (262 Pages)

→ SET is not a payment system rather is security protocols.

- Key features of SET :-
SET incorporates the following features -

1- Confidentiality of information.
2- Integrity of data.
3- Cardholder account authentication.
4- Merchant authentication.

SET overview and its Requirements :-

→ Book 1 of the SET specification lists the following business requirements for secure payment processing with credit cards over the internet and other network.

1- Provide confidentiality of payment and ordering information.
2- Ensure the integrity of all transmitted data.
3- Provide authentication that a cardholder is a legitimate user of a credit card account.
4- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
5- Ensure the use of the best security practices and system

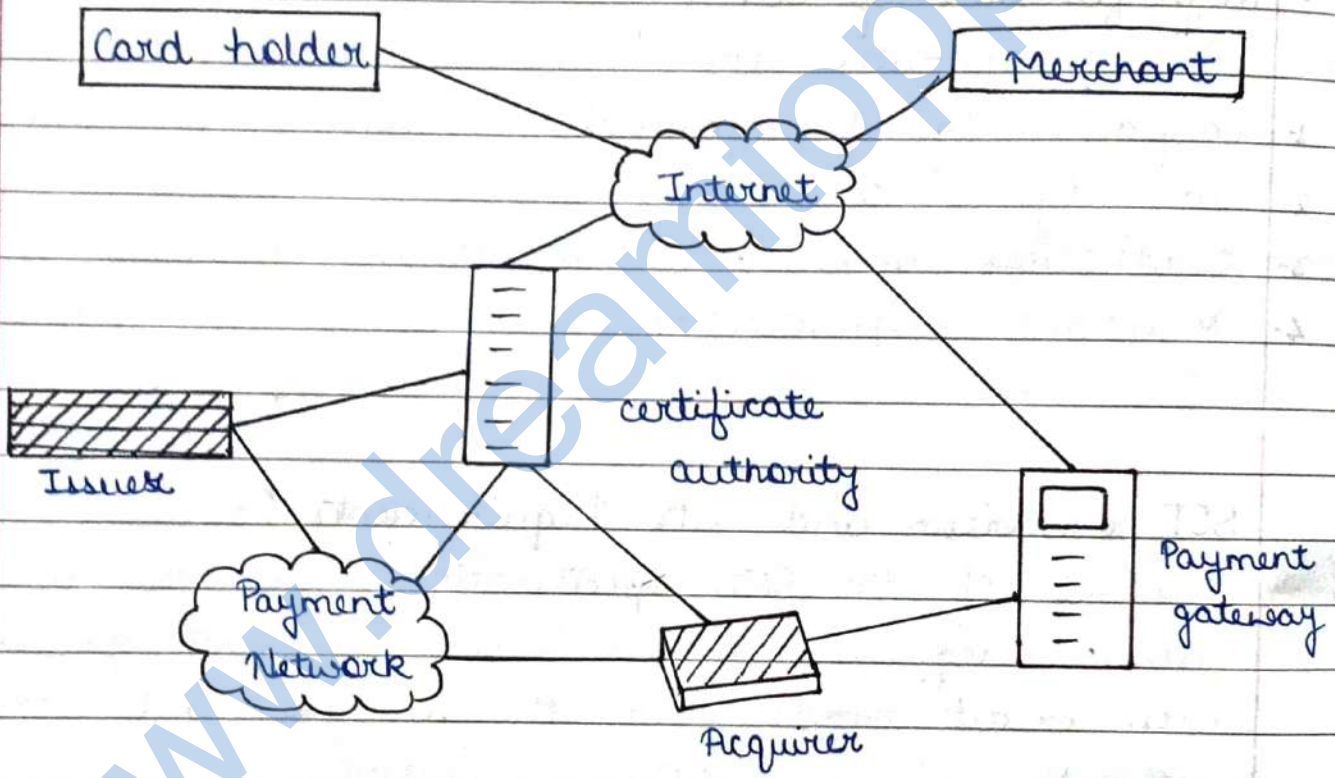
design techniques to protect all legitimate parties in an e-commerce transaction.

6- Create a protocol that neither depends on transport security mechanisms nor prevents their use.

7- Facilitate and encourage interoperability among software and network providers.

- Components of SET :-

Following figure indicates the component in SET system.



1. Card holder — In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the internet. A card holder is an authorised holder of a payment card (e.g. master card, visa) that has been issued by an issuer.

2. Merchant — A merchant is a person or organisation

that has goods or services to sell to the cardholder.

3- Payment Gateway — This is a function operated by the acquirer or a designed third party that processes merchant payment messages. It provides authorisation and payment functions.

4- Certification Authority (CA) — This is an entity that is trusted to issue X.509 v3 public key certificates for cardholders, merchants and payment gateways.

5- Issuer — This is a financial institution such as a bank, that provides the cardholder with the payment card. Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder.

6- Acquirer — This is a financial institution that establishes an account with a merchant and processes payment card authorisations and payments.

Acquirer provides authorisation to the merchant and that a given card account is active and that the proposed purchase does not exceed the credit limit.

Acquirer also provides electronic transfer of payments to the merchant's account.

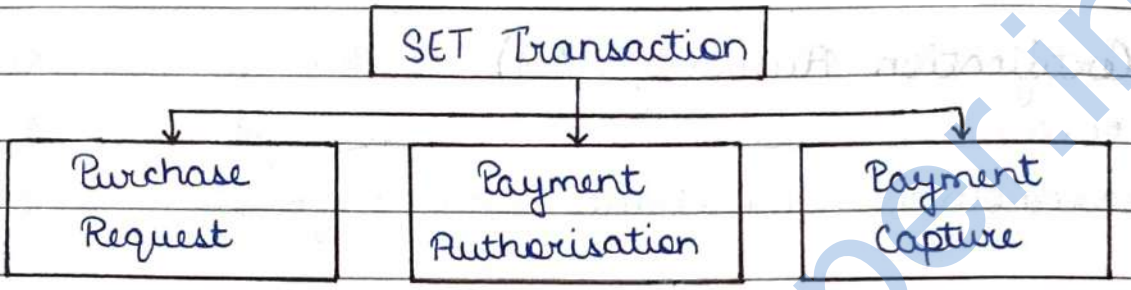
★ Dual Signature in SET :-

→ The purpose of the dual signature is to link two messages that are intended for two different recipients.

→ In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank.

→ The merchant does not need to know the customer's credit card number and the bank does not need to know the details of the customer's order.

★ SET Transaction Type :-



1- Purchase Request — Before the purchase request exchange begins, the cardholder has completed browsing, selecting and ordering. The end of this preliminary phase occurs when the merchant sends a completed order form to the customer. The purchase request exchange consists of four messages :
Initiate request, Initiate response
Purchase request, Purchase response

2- Payment Authorisation — During the processing of an order from a cardholder, the merchant authorises the transaction with the payment gateway.

The payment authorisation ensures that the transaction was approved by the issuer. The authorisation guarantees that the merchant will receive payment. The merchant can therefore provide the services or goods to the customer.

The payment authorisation exchange consist of two messages :
Authorisation request

Authorisation response
Purchase-related information
Authorisation-related information
Certificate

3- Payment Capture —

→ The merchant engages the payment gateway to obtain the payment in a payment capture transaction, consisting of a capture request and a capture response message.

→ For the capture request message, the merchant generates signs and encrypts a capture request block, which includes the payment amount and the transaction ID. The message also includes the encrypted capture token received earlier for this transaction, as well as the merchant's signature key and key-exchange key certificates.

→ When the payment gateway receives the capture request message, it decrypts and verifies the capture request block and capture token. It then creates a clearing request that is sent to the issuer over the private payment network.

→ The gateway then notifies the merchant of payment in a capture response message. The message includes a capture response block that the gateway signs and encrypts, also includes the gateway's signature key certificates.