**E-Commerce - Security Systems**

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised.

Following are the essential requirements for safe e-payments/transactions −

* **Confidentiality** − Information should not be accessible to an unauthorised person. It should not be intercepted during the transmission.
* **Integrity** − Information should not be altered during its transmission over the network.
* **Availability** − Information should be available wherever and whenever required within a time limit specified.
* **Authenticity** − There should be a mechanism to authenticate a user before giving him/her an access to the required information.
* **Non-Repudiability** − It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
* **Encryption** − Information should be encrypted and decrypted only by an authorized user.
* **Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

**Measures to ensure Security**

**Major security measures are following −**

* **Encryption** − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the same or a different secret code.
* **Digital Signature** − Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.
* **Security Certificates** − Security certificate is a unique digital id used to verify the identity of an individual website or user.

**Security Protocols in Internet**

We will discuss here some of the popular protocols used over the internet to ensure secured online transactions.

**Secure Socket Layer (SSL)**

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements −

* Authentication
* Encryption
* Integrity
* Non-reputability

"https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.

**Secure Hypertext Transfer Protocol (SHTTP)**

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiple security mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

**Secure Electronic Transaction**

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol. It has the following components −

**Card Holder's Digital Wallet Software** − Digital Wallet allows the card holder to make secure purchases online via point and click interface.

**Merchant Software** − This software helps merchants to communicate with potential customers and financial institutions in a secure manner.

**Payment Gateway Server Software** − Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.

**Certificate Authority Software** − This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.