Security Issues in E-Commerce: Need and Concept

In spite of its advantages and limitations E-commerce has got some security issues in practical. E-commerce security is nothing but preventing loss and protecting the areas financially and informational from unauthorized access, use or destruction. Due the rapid developments in science and technology, risks involved in use of technology and the security measures to avoid the organizational and individual losses are changing day to day. There are two types of important cryptography we follow for secured E-commerce transactions.

Symmetric (private-key) cryptography: This is an encryption system in which sender and receiver possess the same key. The key used to encrypt a message is also used to decrypt the encrypted message from the sender.

Asymmetric (public-key) cryptography: In this method the actual message is encoded and decoded using two different mathematically related keys, one of them is called public key and the other is called private key.

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 unauthorized 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.

E-COMMERCE SECURITY CAN BE DIVIDED INTO TWO BROAD TYPES:

(1) Client-Server Security

Client-server securities are popular because they increase application processing efficiency while reducing costs and gaining the maximum benefit from all resources working together. These

benefits are gained by splitting processing between the client machine/software and server machine/software. Each process works independently but in cooperation and compatibility with other machines and applications (or pieces of applications).

All independent processing must be performed to complete the requested service. Cooperation of application processing produces another client-server advantage, it reduces network traffic. Since each node (client and/or server) performs part of the processing within itself, network communication can be kept to a minimum. For example, static processes, like menus or edits, usually take place on the client-side. The server, on the other hand, is responsible for processes like updating and reporting.

(2) Data and Transaction Security

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others. With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality. SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Terisa System's Secure Hypertext Transfer Protocol (S-HTTP). SET uses some but not all aspects of a public key infrastructure (PKI).

Security threats in E-Commerce Environment

In the past few years it's seemed like there has been a new widespread security breach every other week. High profile incidents such as Heartbleed and WannaCry and hacks of notable entities including Sony Pictures and the Democratic National Committee have brought cyber security to the front of people's minds. The magnitude of Distributed Denial of Service (DDoS) attacks has risen with the increased number of devices connecting to the internet, and as more of the population engages with these devices the risk of sensitive information being taken advantage of continues to rise.

E-COMMERCE THREATS

Some of the common security threats we may come across:-

(i) Malware

Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or

hijacking core computing functions and monitoring users' computer activity without their permission.

(ii) Virus

A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems. As of 2005, even though no currently existing antivirus software was able to uncover all computer viruses (especially new ones), computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.

(iii) Spam

Spam is the electronic equivalent of the 'junk mail' that arrives on your doormat or in your postbox. However, spam is more than just annoying. It can be dangerous – especially if it's part of a phishing scam.

Spam emails are sent out in mass quantities by spammers and cybercriminals that are looking to do one or more of the following:-

(a) Make money from the small percentage of recipients that actually respond to the message.

(b) Run phishing scams – in order to obtain passwords, credit card numbers, bank account details and more

(c) Spread malicious code onto recipients' computers,

(IV) Spyware threats

Spyware is generally loosely defined as software that's designed to gather data from a computer or other device and forward it to a third party without the consent or knowledge of the user. This often includes collecting confidential data such as passwords, PINs and credit card numbers, monitoring keyword strokes, tracking browsing habits and harvesting email addresses. In addition to all of this, such activities also affect network performance, slowing down the system and affecting the whole business process. It is generally classified into four main categories: Trojans, adware, tracking cookies and system monitors.

(V) Trojan Horse

A Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses into your system.

(VI) Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.[1] Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Elements of Good E-Commerce Security

In order to protect information, a solid, comprehensive application security framework is needed for *analysis* and *improvement*. This application security framework should be able to list and cover all aspects of security at a basic level. It should incorporate the following six parts:

- Security elements that need to be preserved: availability, utility, integrity, authenticity, confidentiality, nonrepudiation
- Sources of loss of these elements: abuse, misuse, accidental occurrence, natural forces
- Acts that cause loss: use of false data, disclosure, interference with use, copying, misuse or failure to use
- Safeguard functionality used to protect from these acts: audit, avoidance, detection, prevention, recovery, mitigation, investigation
- Methods of safeguard functionality selection: diligence, comply with regulations and standards, meet needs
- Objectives to be achieved by the application security framework: avoid negligence, protect privacy, minimize impact on performance

The six essential security elements

In the proposed framework, six security elements are considered essential for the security of information. If one of these six elements is omitted, information security is deficient and protection of information will be at risk.

Availability

Looking at the definition, availability (considering computer systems), is referring to the ability to access information or resources in a specified location and in the correct format. When a system is regularly not functioning, information and data availability is compromised and it will affect the users. Besides functionality, another factor that effects availability is time. If a computer system cannot deliver information efficiently, then availability is compromised again. Data availability can be ensured by storage, which can be local or offsite.

Utility

Considering the definition, utility refers to something that is useful or designed for use. Normally, utility is not considered a pillar in information security, but consider the following scenario: you encrypt the only copy of valuable information and then accidentally delete the encryption key. The information in this scenario is available, but in a form that is not useful. To preserve utility of information, you should require mandatory backup copies of all critical information and should control the use of protective mechanisms such as cryptography. Test managers should require security walk-through tests during application development to limit unusable forms of information.

Integrity

In the context of computer systems, integrity refers to methods of ensuring that the data is real, accurate and guarded from unauthorized user modification. Data integrity is a major information security component because users must be able to trust information. Untrusted data compromises integrity. Stored data must remain unchanged within a computer system, as well as during transport. It is important to implement data integrity verification mechanisms such as checksums and data comparison.

Authenticity

Regarding computer systems, authenticity or authentication refers to a process that ensures and confirms the user's identity. The process begins when the user tries to access data or information. The user must prove access rights and identity. Commonly, usernames and passwords are used for this process. However, this type of authentication can be circumvented by hackers. A better form of authentication is biometrics, because it depends on the user's presence and biological features (retina or fingerprints). The PKI (Public Key Infrastructure) authentication method uses digital certificates to prove a user's identity. Other authentication tools can be key cards or USB tokens. The greatest authentication threat occurs with unsecured emails that seem legitimate.

Confidentiality

Defining confidentiality in terms of computer systems means allowing authorized users to access sensitive and protected information. Sensitive information and data should be disclosed to authorized users only. Confidentiality can be enforced by using a classification system. The user must obtain certain clearance level to access specific data or information. Confidentiality can be ensured by using role-based security methods to ensure user or viewer authorization (data access

levels may be assigned to a specific department) or access controls that ensure user actions remain within their roles (for example, define user to read but not write data).

Nonrepudiation

Nonrepudiation refers to a method of guaranteeing message transmission between parties using digital signature and/or encryption. Proof of authentic data and data origination can be obtained by using a data hash. While the method is not 100 percent effective (phishing and Man-in-the-Middle attacks can compromise data integrity), nonrepudiation can be achieved by using digital signatures to prove the delivery and receipt of messages.

Each of the six elements can be violated independently of the others. The elements are unique and independent and often require different security controls. Maintaining availability of information does not necessarily maintain its utility: information may be available, but useless for its intended purpose. In order to identify threats, we can pair the six elements into three pairs, which can be used to identify threats and select proper controls:

Availability and utility → Usability and usefulness

Integrity and authenticity → Completeness and validity

Confidentiality and nonrepudiation → Secrecy and control

E-Commerce Security Plan

Measures to ensure Security

- **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.

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 unauthorized 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.