7

Data Security in the Digital Era: Issues and Challenges

Dr. Jayanti Goyal [*]
Anjali Vijayvargiya[**]

Introduction

E-Commerce or electronic commerce is broadly considered as buying and selling the goods and services over the network. It includes a significant business area such as shopping, banking, tickets booking, paying bills and taxes, food delivery and much more other option available. E-commerce is subdivided into three categories: business to business or B2B (Cisco), consumer to consumer or C2C (eBay) and business to consumer or B2C (Amazon).E-commerce Security is a part of the Information Security framework and it includes Data security, Computer Security, and other wider areas of the IS framework.

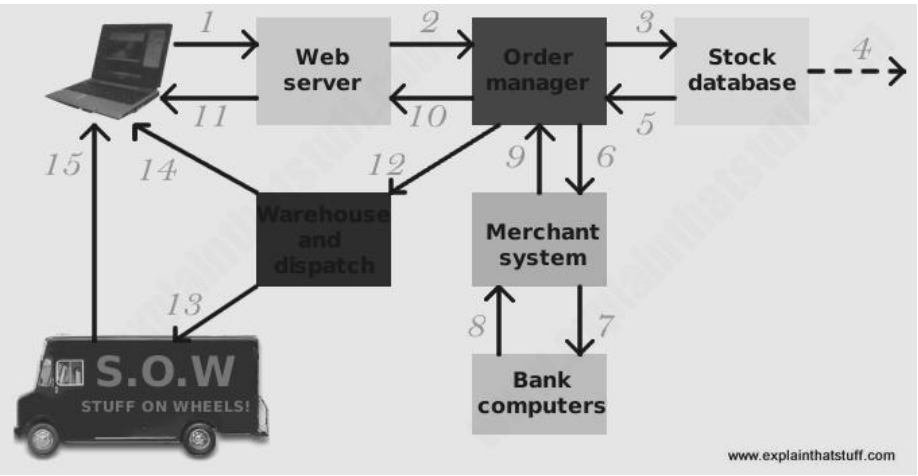
Web e-commerce applications that take care of payments such as electronic transactions using credit cards or debit cards, online banking, PayPal or other tokens have more compliance issues. Mule, Trojan horse and worms pose the greatest threat to e-commerce privacy and security because if they launched against client systems, they can threaten most of the authorization and authentication mechanisms used in an ecommerce transaction. To influence consumer behavior trust is an important element and has high significance toward merchants in internet-based environments. Therefore in E-commerce transactions trust would be favorably influenced by an increase in perceptions of security and privacy

[*] Head & Associate Professor, Kanoria Girls PG College, Jaipur, Rajasthan, India.
[**] Assistant Professor, Kanoria Girls PG College, Jaipur Rajasthan, India.

~ *The chapter is based on the paper presented in "**National Conference on Emerging Trends and Scope in Digital Banking, Cashless Economy & Innovations in Commerce and Modern Management & International Seminar on Global Economy: Opportunities and Challenges**" Organized by **Inspira Research Association (IRA),** Jaipur **& Shri Bhawani Niketan Girls P.G. College,** Jaipur, Rajasthan, India. **29-30 September, 2018**.*

E-commerce Working

- A customer wants to order a product online by his/her computer. The web browser then communicates with the web server that manages the e-commerce store's website.
- The Web server sends the order to the order manager which is the central computer that operates orders from submission to dispatch through every stage of processing.
- The order manager then queries the store database to check whether the customer wants is actually in stock or not.
- If the item is not found in the stock database then the system can order new supplies from the wholesalers or manufacturers.
- And if the item or product found in the stock database then the order manager continues to process it.
- Next, it communicates with the merchant system to make payment using the customer's credit or debit card number.



- The bank computer confirms whether the customer has enough funds.
- The merchant system authorizes the transaction to go ahead after done with payment.
- Then merchant system contacts to order manager after payment being done.
- The order manager confirms that the transaction has been successfully processed and then notifies the Web server.
- The Web server shows a Web page confirming that order has been processed and the transaction has been completed to the customer.
- The order manager then requests to the warehouse dispatch the goods to the customer.

- A dispatch truck then collects the goods from the warehouse.
- Once the goods have been dispatched, the warehouse computer e-mails the customer to confirm that goods are on the way.
- The goods are delivered to the customer.

Purpose of Study

The purpose behind this study is:

- To understand the process behind online shopping.
- To deal with the purpose of security in e-commerce.
- To discuss the different security issues which are faced during e-commerce transactions
- To discuss various security threats.

Purpose of Security in E-Commerce

E-commerce security is a crucial part of any online transactions that happens often and takes place over the network. There are various dimensions of e-commerce security:

- **Integrity:** It refers to prevention against unauthorized data modification. That means information or data should not be altered during its transmission which takes place online.
- **No Repudiation:** It refers to prevention against the denial of order or payment. Once a sender sends her transaction details, the sender should not be able to deny sending the message. Similarly, the receiver of the message should not be able to deny the receipt.
- **Authenticity:** It refers to the authentication of the data source. There should be a mechanism to give authentication only authorized person or user.
- **Confidentiality:** It refers to protection against unauthorized data disclosure. That means data or information should not be accessible or available to an unauthorized person. The data has to be between the client and server only. It should not be intercepted over the transmission.
- **Privacy:** It refers to the provision of data control and disclosure of data.
- **Availability:** It refers to prevention of data delays or removal of data. Information should be available whenever and wherever it required.

Various Security Issues in E-commerce

Data is transferred over the network by login or by transaction details. To secure those data from unauthorized access, E-commerce security provides a protection layer on e-commerce assets. Consumers hesitate by the fear of losing their financial data and e-commerce sites frighten about their financial losses and that

results in the bad impact on publicity. There are many security issues associated with e-commerce such as critical issues, social issues, and organizational issues. An online transaction requires a customer to disclose sensitive information to the vendor in order to make the purchase, placing him at significant risk. It basically deals with:

- Issues related to customers or Clients Security: if their data is not secured over the network, then it is an issue to think about. An organization has to provide security feature and take guarantee that data is secured by them, Techniques and practices that protect user privacy and integrity of the computing system.
- Issue related to Server Security: to protect web server, software and associated hardware from break-ins, damage from attacks. If there is an error in that software which implements security and for any reason, it is not providing that security so it is the second case which also takes seriously.
- Issue related to Transactions Security: to provide guaranteed protection against eavesdropping and intentional message modification such as tapping, intercepting and diverting the intended data.

Security Threats

The various types of security threats exist in e-commerce:

- **Malicious Code:** it is harmful code that harms the computer system and makes it useless after the attack. It includes virus, worms, Trojan horse etc.
- **Phishing and Identity Theft:** it is a type of attack in which user data such as login credentials and credit and debit card numbers stolen by the attacker by providing an email, instant message. By clicking on this malicious link and providing his/her details then, their data hack easily by the intruder.
- **Unauthorized Access:** it includes illegal access to data or systems for some malicious purpose. Two types of attack are included for unauthorized access, one is passive unauthorized access, in which the hacker keeps his eye only on the data that is over the network and further used it for their own illegal ambitions. However, in active unauthorized access, the hacker modifies the data with the intention to manipulate it. Home computer, point-of-sale, and handheld devices can easily get affected by this attack.
- **Denial of Service:** hackers flood a website with useless traffic to target a computer or a network and to stop them working properly. It may occur by spamming and virus. Spamming is an unusual email bombing on the targeted device by the hacker. By sending thousands of email one after the other, the system is affected by this attack.
- **Theft and Fraud:** fraud occurs when the stolen data is used or modified for illegal action. When a consumer makes an online purchase hackers break into insecure merchant web servers to harvest archives of credit card numbers

which is generally stored along with personal information. The merchant back-end and database is also susceptible to theft from third-party fulfillment centers and other processing agents.

Defensive Measures against Security Threats

The defensive measures used in transactions security are:

- **Encryption:** it's far the system of converting plain text or information into cipher text that can't be examined by using every person except the sender and receiver. It is accomplished with the help of mathematical algorithm the key's required to decode the message. In an asymmetric key encryption, each the sender and receiver use the same key to encrypt and decrypt the messages whereas symmetric or public key encryption makes use of two digital keys which are public and private to encrypt and decrypt the messages.
- **Secure Socket Layer:** SSL protocol provides data encryption, server authentication, client authentication and message integrity for TCP/IP connections. When data is transported over the internet between two applications SSL prevents from eavesdropping, tampering or forgery. It is used for securing connections between network application, clients and servers over an insecure network like internet.
- **Secure Hypertext Transfer Protocol:** An Internet protocol for the encryption of Hypertext Transfer Protocol (HTTP) traffic. S-HTTP is extending the HTTP protocol by adding encryption to Web pages. It additionally gives mechanisms for authentication and signatures of messages.
- **Digital Signature:** Digital Signature Certificate (DSC) is issued by a Certifying Authority (CA). It is a secure digital key that certifies the identity of the holder; Digital signature contains the user identity like name, email, country, account name and public key. Digital Certificates use Public Key Infrastructure. It means data that has been digitally signed or encrypted by a private key can only be decrypted by its corresponding public key. A digital certificate is just like credit card which establishes credentials when doing business or other transactions on the Web.

Challenges

Almost all data security issues are caused by the lack of effective measures provided by antivirus software and firewalls. Here are the following measures, on the basis of which security is being determined:

- Some organizations cannot provide access controls to divide the level of confidentiality within the company.
- Access control encryption and connections security can become inaccessible to the IT specialists who rely on it.

- Unethical IT specialists practicing information mining can gather personal data without asking users for permission or be notifying them.
- Automated data transfer requires additional security measures, which are often not available.
- Most distributed systems computations have only a single level of protection, which is not recommended.

Conclusion

Today, e-commerce is widely taken into consideration for the buying and selling of goods and services over the internet, however, any digital transaction that is completed entirely through digital measures can be considered in e-commerce. Day by day e-commerce playing the very good role in online retail marketing and peoples using this technology day by day increasing all over the world. Therefore for e-commerce transactions security parameter must be taken seriously which includes protection of assets from unauthorized access, destruction, use or alteration.

Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved. For that reason, the security concern at first place over the other from an e-commerce merchant's perspective and web servers have to provide the customer. Besides these sensitive servers should be kept highly specialized, it can be done by turning off and removing all inessential services and applications (e.g., FTP, email). Therefore the mechanisms such as encryption, protection, verification and authentication are used to implement security in a proper way. The marketplace can be trustworthy only when consumers sense to trust in transacting in those surroundings.

References

- "E-Commerce- Study of Privacy, Trust and Security from Consumer's Perspective"
- International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 5, Issue. 6, June 2016, pg.224 – 232
- "Security Issues over E-Commerce and their Solutions" https://www.researchgate.net/publication/317612828_Security_Issues_over_ECommerce_and_their_Solutions
- Website Link http://www.bbamantra.com/transaction-security-e-commerce/
- https://www.informatica.com/in/products/data-security.html#fbid=S9el7n64yeR
- Website Link http://www.datacenterknowledge.com/archives/2016/01/19/nine-main-challenges-big-data-security.

☯☯☯