Security Vulnerability and Possible Attack Methods in e-commerce

Anjali Jolly

Abstract: E-Commerce Is The Process Of Selling Or Purchasing Of Goods Via Utilizing Online Services. Nowadays, E-Commerce Has Become An Integral Part Of Business Websites. In This, Third Party Services Are Being Used Most Commonly, Which Offer Ready To Use Setup For The Companies. Numerous Services And Technologies Are Used By The Firms Such As Applications For Payment-Processing (These Can Also Be Offered By Third Parties). Sometimes, Business Companies May Also Develop Their Own Customised Software At Specialised Price Or May Use Their Personal Software By Combining It With Third Party Software. Therefore, E-Commerce Websites May Succeed By Providing Secure Services To Their Customers, Such As Their Personal Information, Cards Details Etc. Must Be Secured With Trusted Encryption Technologies. But, At The Same Time, Widespread Use Of E-Commerce Is Accompanied With Certain Security Related Challenges. Hackers Try To Find Loopholes In The System Using Several Techniques. Hence, Taking The Preventive Measure And Educating Customers About The Threats May Help In Keeping The Customer Faith On Websites. Otherwise, If A Website Has Poor Encryption Technologies, Then It May Fail To Gain Customer Trust.

Keywords: E-Commerce, Nonrepudiation, Hackers, Security, Threats Techniques.

I. INTRODUCTION

Electronic commerce has grown considerably over the past few decades. As a result, several e-commerce companies have established in the marketplace. This revolution in digital commerce may get increase to a greater extent by crucially handling the security aspects on the websites [1]. Online businesses are facing several problems similar to conventional businesses such as network related security risks. These risks increases to a great extent in e-commerce as it involves online transactions as compared to physical transactions in traditional business practices. For an instance, transactions using credit cards are most commonly use to purchase goods and services. A vulnerability, in information technology, is a flaw in code or layout that creates a capacity point of security compromise for an endpoint or network. Vulnerabilities create feasible attacks, through which an interloper could run code or access a target gadget's reminiscence.

Manuscript published on November 30, 2019.
* Correspondence Author

Anjali Jolly*, Computer Deptt., DAV College Hoshiarpur(Pb.), India. Email: anjali_jolly@hotmail.com

The way with the aid of which vulnerabilities are exploited are numerous and consist of code injection and buffer overruns. It can be carried out through hacking scripts, applications and hand coding [8]. Due to expeditiously increasing threats, firms also hire new employees to reduce risks. Therefore, e-commerce environment is facing several vulnerabilities. To illustrate, while purchasing any online product using credit or debit card, customer's profile/ account information may be at risk due to any security issue. Consequently, such type of information may offer the hackers other methods to steal user's identification data. So, trust and customer expectations have become an important component of consideration in e-commerce environment. To create secure website servers, it becomes important to remove the sensitive applications and unnecessary services [2]. As data travels from one system to the other quite often, therefore, transmission channels should be capable enough to maintain customer privacy and security. In this paper, I will discuss the possible attack methods, various threats, components of security and its relation with e-commerce.

II. PROPOSED METHODOLOGY

Its an exploratory Research as datais secondary collected from various research papers , reports , International Journals and survays. Conclusion is according to the analysis of collected Data.

III. POSSIBLE ATTACKS IN E-COMMERCE ENVIRONMENT

E-commerce system may get exposed to several vulnerabilities at the entry and exit points mainly. For example, hackers may attack the system at its website server, software vendor, vendor's computer and even a network connection connecting website's server with the shopper. Some of the potential attacks methods on security are furtively attempting methods to find out shopper's private information. This may involve surveillance of vendor's behavior and then using this gathered information against him. To illustrate, setting up same password on different websites may put security at risk because a user's behavior on different websites can be tricked this way. Similarly, some phishing schemes may also be used by hackers against the shopper. This is the type of social engineering attack, which may be used by the attackers to steal user's sensitive data related to credit card details etc. Phishing attacks can be of several types. Sometimes, hackers put a link in e-mail to a scoundrel site which ultimately collects the user's data. Other than this, hackers may also use some other phishing techniques.

Sometimes, hardware and software vendors ship their products to the customers, without enabling the security features. As a result, a user having less knowledge about technical aspects may fail to enable all the security features due to lack of awareness. Hence, it may create a security breach because hackers may attempt to hack user's personal information. SATAN is one of the popular technique to get an entrance onto shopper's system. Attackers may scan the computer system to get user's personal information. Sniffing the network is another method used by hackers, in which the data (between server and buyer's computer) is monitored by the attackers [3].

IV. THREAT TECHNIQUES

Several techniques can be used by the attackers to invade the user's system, such as hardware, software, personal, physical and procedural. In hardware technique, a bug is implanted within the hardware controller in order to deny the system usage. Similarly, software attack method includes making the discrete alterations to compromise the system [4]. It is generally used to bring data destruction. IT industry is running diligently to mitigate vulnerabilities, called Meltdown and Spectre. These vulnerabilities are affecting nearly all computer systems, mobile phones and smart domestic gadgets within the world. The vulnerabilities ought to permit a hacker to steal statistics saved within the reminiscence of gadgets; together with passwords and other critical information. The crucial thing to observe is there are no recognised exploits for the vulnerabilities so far. The trouble is very demanding due to the fact it is able to affect many computers, consisting of non-public gadgets [6].

V. COMPONENTS OF SECURITY

In e-commerce, unauthorised access, fraud and denial of services can be three types of threats. While creating a security framework, it is important to cover all the security related aspects. Hence, it must include following components [5]:

- *Confidentiality*
- *Authenticity*
- *Utility*
- *Integrity*
- *Availability*
- *Nonrepudiation*

In case, if any of the above mentioned element is missing, then the security will be at risk. The main purpose of security framework is to protect customer privacy by lowering any impact on performance and controlling the security measures. Although, it may lead to certain negative impacts such as misuse, usage of false data and copying etc. The framework is utilized to protect such acts by detecting, investigating and preventing any errors in the system. Methods of safeguard functionality can be best selected by setting standards and regulations, which must be complied with the system.

Confidentiality can be defined as allowing the permitted users to access their sensitive information. This information is protected with the security framework, which may be enforced by building a classification system. Even though, users may require to clear some levels, before having final access to their information. For this, role base security methods or viewer authorization can be used to achieve confidentiality.

Authentication can be referred as a procedure which is used to confirm and ensure user's identity. It initiates at the time when use tries to get information. Hence, user is required to prove that he has right to access his data. Most commonly, setting up a username and unique passwords are used for this purpose. Unfortunately, such type of authentication may be at risk because it can be bypassed by the hackers. To prevent this, biometrics is most commonly used nowadays. Other than this, digital tokens or USB tokens can also be used.

Utility can be defined as something designed for use. For this, many technologies can be used, but one of the most widely trusted & protective mechanism is cryptography. It can be used to encrypt valuable information, which can be helpful in obtaining information copies (backup copies, in case if they get loose accidently.

Integrity is considered as a process of ensuring that information is accurate & real, hence is protected from unauthorized users to prevent any unauthenticated modifications. Therefore, data integrity is one of the main component of security framework, which ultimately helps to build customer trust. In simple words, it can be said that user data must not be changed or modified during transport or within computer system.

Availability, in context to e-commerce and computer system can be referred as accessing the data/ information in a meticulous format and that's too in a defined location. Availability is affected by time as information must be delivered efficiently. Therefore, it may be ensured by local or offsite storage. Apart from this, it should be properly functioning.

Nonrepudiation is a procedure of insuring message communication via using encryption technologies between two parties. In this, data hash is mainly obtained to prove that data is authentic. But, it is also to be noted here that encryption technology may also be at the risk of phishing. Therefore, in order to overcome this, digital signature may be used to prove message delivery and receiving.

VI. RESULTS: SECURITY & E-COMMERCE ENVIRONMENT AND SOLUTIONS

While using any e-commerce website, one of the prime concern is user's data and information related security because whole of such information is present online. Companies require to build the trust in customers that their information (related to purchase records, debit/credit card credentials and addresses) are secure with the firms they are dealing with and must be kept without making any changes. Hence, security process & systems are needed to be checked on consistent basis by setting the site security on top priority.

Other than this, some of the preventive measure are educating the customers that your framework is similarly as secure in light of the fact that
who the people are using it.

On the off chance that a customer picks a weak secret key, or does not remain their secret key mystery, at that point an aggressor will make as that client. This can be significant if the traded off secret word be in the correct spots to a director of the framework. Secondly, when interfacing your PC to a system, it progresses toward becoming in danger of possible attack. A private firewall shields your PC by restricting the classifications of traffic started by and coordinated to your PC. The intruder likewise can filter the hard drive to see any hang on passwords. Further, Secure Socket Layer could be a convention that encodes data between the customer's PC and the server. When a Secure Socket Layer ensured page is mentioned, the program distinguishes the server as a trusty and starts an affirmation to pass coding key information to and fro. Presently, on resultant solicitations to the server, the information streaming to and fro is scrambled so a programmer sniffing the system cannot peruse the substance. Similarly, a firewall is much the same as the channel including a manor. It guarantees that solicitations will just enter the framework. Intrusion recognition and audits of security logs are one of the foundations of a productive security system. This sees the character of the framework's traffic, or as a spot to start for lawful continuing against the assailants [9].

VII. CONCLUSION

In this era of information technology, security technologies are advancing, but at the same time, hacking tools are also flourishing. The net impact has been a boom in the range of cyber assaults, with a corresponding growth in losses to their sufferers. While few attacks had been attributed to foreign governments, these threats are worrisome due to their capacity to motive harm, if carried out towards critical infrastructures. The U.S. Government, along enterprise and academia, has initiated several applications to bolster our cyber protection capability and thereby mitigate this danger. They are crucial steps forward. However, there are numerous other targets to achieve in this concern. For an instance, we more statistical data is required to protect cyber incidents, such as occurrence and cost facts; records showing the correlation of incidents with operating modes and unique cyber defenses; and records showing the return on protection investment for distinct approaches. This data is essential so that businesses know what works and where to focus restricted resources. We want to increase our schooling and research tasks in order that there are more individuals capable of defending our networks and better tools at their disposal. Similarly, new structures may be designed with fewer vulnerabilities and mechanisms for limiting damages. We need to extend our worldwide projects so that cyber offenses may be correctly avoided, investigated, and prosecuted irrespective of the places of the perpetrators and sufferers. Finally, certain laws may be implemented to increase safety without sacrificing safety. Achieving these goals will not be viable with out considerable collaboration between the public and private sectors. Cyber protection cannot be always considered as an assignment for the government alone [7].

REFERENCES

1. UK. Essays, “Security Vulnerabilities in E Commerce Systems”, Retrieved from https://www.ukessays.com/essays/information-technology/security-vulnerabilities-in-e-commerce-systems-information-technology-essay.php?vref=1, November 2018
2. Huda Hamdan, Hasan Abdulrazzaq Jawad, “IJARCCE Security Vulnerabilities and Solution for Electronic Commerce in Iraq”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016
3. Tea Company, “Security Attacks and Defenses in an E-Commerce System”, Retrieved from https://www.teasoftware.com/articles/security-attacks-and-defenses-in-e-commerce-system
4. Wu Yanyan, “Research on E Commerce Security based on Risk Management Perspective”, International Journal of Security and Its Applications, Vol. 8, No. 3, pp. 153-162, 2014
5. Revathi C, Shanthi K, Saranya A.R, “A Study on E-Commerce Security Issues”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 12, December 2015
6. Purdue University Northwest, “Information Technology Security Vulnerabilities”, Retrieved from https://www.pnw.edu/information-services/information-technology-security-vulnerabilities/, February 1, 2018
7. Dorothy E. Denning, “Information Technology and Security”, Georgetown University Press, 2003, Retrieved from https://pdfs .semanticscholar .org/641d/fa3e4ae178705336 ecb35c442159ecde4b8d.pdf
8. Margaret Rouse, “Vulnerability (Information Technology)”, Retrieved from https://whatis.techtarget.com/definit ion/vulnerability
9. Dr. Pranav Patil , “Study on E-Commerce Security Issues and Solutions”, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.1, pg. 100-102, January- 2017

AUTHORS PROFILE

Ms Anjali Jolly, B.E(CSE),MSc(IT), NET qualified Presently working in DAV College Hoshiarpur as Asstt. Prof. She has published paper in IJERT, IJEAT and in BVICAM conference proceedings. She has also presented papers in Seminar related with topics like Big Data and Networking.