International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 713-716 www.ijaem.net ISSN: 2395-5252

Study on Cyber Security Issue and Solution in E-Commerce

Ho Wei Siang, Zolkipli MohamadFadli
School of Computing, University Utara Malaysia (UUM),
Sintok, 06100 Bukit KayuHitam, Kedah, MALAYSIA

Date of Submission: 05-02-2023 Date of Acceptance: 20-02-2023

ABSTRACT: Globally, e-commerce is becoming increasingly popular as a result of advancements in technology and consumer demands. However, the growth of online shopping does not correspond with platform security.In this paper the security issues that faced by the e-commerce platform will be discuss and the solution of current technology can provide to secure the system.

KEYWORDS:E-commerce, Security Issues, Solution.

I. INTRODUCTION

Electronic commerce (e-commerce) is the purchasing and selling of products, information, and services through online platform; many transactions might be completed with a few simple clicks on our own computer or smart phone [1].

Over the years of pandemic started from year 2019 the services of e-commerce is having a significant increase. People prefer shopping on an e-commerce platform over in a traditional market like a physical store due to convenience and other factors. Therefore, a trustworthy system is required to support e-commerce buying and selling operations.

The technology of cyber security has grown to be a serious issue that restricts the growth and acceptance of e-commerce platforms. But most of the developer and stakeholder always ignored the security aspect. They think the security aspect is not more important than the usability and reliability [2].

In this paper will discuss about the issue face by the e-commerce platform and it solutions. In second part we will discuss about the background of e-commerce and it security, when in third part the issues and solution of the e-commerce will be discussed, finally we will talk about the future research and conclusion.

II. BACKGROUND OF E-COMMERCE

E-commerce is a platform where people may use the internet to buy and sell goods and services. In addition, some consumers utilize this platform to do informational searches, compare costs amongst merchants, or look for the newest products that are on sale before deciding whether to buy them in person or online [3].In the year of 1990 every will think about Ecommerce this is because that in that year it face a significant development [5].In now days the e-commerce transaction occur in four categories which is:

1) **Business to Business (B2B):** This is an electronic trade between businesses is used to enhance their supply chain management procedures [4].
2) **Business to Consumer (B2C):** This the general public is sold goods and services through the use of catalogues and a shopping cart program [3, 20]. Such as Shopee.
3) **Consumer to Consumer (C2C):** It involve the trading between buyer and buyer [4]. For example mudah.my.
4) **Consumer to Business (C2B):** This is where the customers will try to advertise their own work or concept with a budget online, and entrepreneurs will review their requirements regarding the project and submit a bid if they are interested. The buyer will next review the bids and choose the organization that could carry out the task as a result. The organization will later introduce creative individuals, such as engineers and designers, and provide a platform and meeting place for the customer [3].

III. BACKGROUND OF E-COMMERCE SECURITY

E-commerce Security, which included data and computer, and other more detail domains inside the Information Security system, is a crucial part of the Information Security structure that is directly related to the segments that have an impact on web-based company. Currently, one of the biggest issues facing electronic technology is ensuring protection, privacy, and security. M-commerce poses security issues, much as other advancements in the field. In a number of contexts, including commerce, electronic device that record health records, e-recruitment technologies, and interpersonal connection, security and privacy problems have been uncovered, demonstrating a lack of confidence that has had a direct impact on users. Security is a major problem that keeps organisations and customers from participating in e-commerce. [6].

IV. E-COMMERCE SECURITY DIMENSIONS

E-commerce security is a kind of protection or we call safeguarding to prevent the user e-commerce asset from the security breaching, data manipulation or breakdown of their personal data. Inside e-commerce security there are 3of dimensions

1) **Integrity:**Integrity is the trustworthy and sureness of information. It depend to the data content, methods, and systems' accuracy, consistency, and reliability. This includes give ensuring to the users when they view back the data after last access provided the information are not damage[7].
2) **Confidentiality:**All the data of users must be encrypted by the system and only the one person that have the "KEY" can decode the data [8]. This mean the individuals who are not authorized should not have access to information. It must not be intercepted while in transit [19].
3) **Non-repudiation:**The intent of a party to fulfil its contractual duties. It also implies that no side to a transaction may deny receiving one, nor can the other party deny sending one. It is a legal term that frequently relate to provider that provide services of offering data origin certification in the context of information security. To reject a bargain or a purchase in online commerce is unacceptable [9].

V. E-COMMERCE SECURITY ISSUES

The security of e-commerce is threatened by a number of insider threats, including two different types of attacks: active and passive. While an active assault involves eavesdropping on the data, a passive attack involves changing the actual data. Worms and viruses—both of which need a host file to attack and cause resource loss—are examples of harmful code attacks used in the attacks. Denying a consumer access to resources is known as denial of service [11].

1) Information stealing

All data packet travel across the network in original text if no any encryption method is apply in it. When a data packet travel through our router or the gateway on the network, the unwelcome party can hijack the data packet that we send out. By repeatedly stealing and analysing the data, we can identify the legality and format of the data and then discover the content of the transmission data.Consequently, this may result in online transmission data leakage [10].

2) Denial of Service (DOS)

Spam and viruses are the two classic attacks of DOS. Spamming is the method of sending a large amount of commercial emails to random recipients, whereas email bombing is a method of a person sending an email by a huge number of amount to a single device or network. [6].

3) Unauthorized Access

If someone accessing a system without the authorization or known as illegal access. In order to gain an access to the private information they eavesdropping on the communication of the user. It might use the information for damaging ends, alters the message's intent, for as by bringing a transaction discussion to an early end or delaying it. [12].

4) Forgery of Information

The Ming channel is where the e-commerce platform transit the data when the process of forgery are complete. Some criminals utilise this weakness to fabricate user data because some organisations do not completely encrypt the customer data. By altering the email, fraudsters can send consumers a bogus email address and instruct them to make a payment, making it simple for customers to fall victim to network fraud [10, 13].

VI. E-COMMERCE SECURITY ISSUES SOLUTION

E-commerce security methods address two issues preserving the integrity of the company's kernel systems and network, and securing transactions between the company and their customers. The following are some ways to solve the issues faced:

1) Shop at Secure Website

Your personal Information is transferred from your device to the online merchant using encryption technology on secure sites. To prevent computer criminals from intercepting the data you submit, such as your credit card number, encryption scrambles it. Only those with authorised access privileges are able to decipher the code [11, 17].

2) Firewall

Once a device connect to an open network, it is a public target to attack by the attacker. Every data that coming into or going out of the network must went through the firewall, Thefirewall will examines each one and filters out those that don't meet the set security requirements. The ideal firewall setup is on the device software and hardware, however firewalls can be either. [8, 14].

3) Fernet Cipher Algorithm

The Fernet cipher and other asymmetric encryption methods ensure that the ciphertext can't decoded or changed without the key. Consistent resource locators are implemented via secure key encoding. For authentication, Fernet employs a hash-based MAC (message Authentication Code) using SHA (Secure Hash Algorithm) 256, 128 bit Advanced Encryption Standard in CBC mode, and PKCS7 padding. There are two parts to the Fernet Cipher algorithm: message encryption and decryption. [15].

4) Secure Socket Layer

Without the key, the encrypted communication cannot be decoded or changed thanks to asymmetric encryption methods like the Fernet cypher. For reliable resource locators, it employs secure key encoding. Fernet employs a hash-based MAC (message Authentication Code) using SHA (Secure Hash Algorithm) 256 for authentication, 128 bit AES in CBC mode, and PKCS7 padding. Encryption and decryption of messages are the two halves of the Fernet Cipher algorithm. [16].

VII. FUTURE RESEARCH

For the future research in this field the researcher want to study on the design of Secure Online Ordering System (SOOS) [18]. In order to solve the issues face by the current platform.

VIII. CONCLUSION

In conclusion, e-commerce is frequently associated with websites where products are sold and purchased, but any transaction that is carried out online or electronically can be categorised as e-commerce. Many individuals use e-commerce almost daily all around the world, and it has played a significant part in internet business.

In this paper the issues that face by the e-commerce and the solution how to prevent the issues to happen or to solving the issues have been mention. This paper will expose how important is the issues faced and the solution that can be use when some of the issues mentioned occur.

IX. ACKNOWLEDGMENTS

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Project. This work was supported by University Utara Malaysia.

REFERENCES

[1]. O. Najeem, Designing a conceptual Security Framework for Secure Online Ordering System (SOOS), Dec. 2020.

[2]. R. K. Jamra, B. Anggorojati, Kautsarina, D. I. Sensuse, and R. R. Suryono, “Systematic review of issues and solutions for security in e-commerce,” 2020 International Conference on Electrical Engineering and Informatics (ICELTICs), 2020.

[3]. C. H. I. N. Y. I. YUEN and Z. O. L. K. I. P. L. I. M. O. H. A. M. A. D. FADLI, Review on Challenges and Issues faces in E-commerce, Jun. 2021.

[4]. D. S. Gangele, D. Pathak, and D. D. Verma, The analysis of security issues and threat prevention model in e-commerce, 2017.

[5]. J. R. Shaikh, S. D. Babar, and G. lliev, “‘issues and solutions’ security in e-commerce,” E-commerce Development with Respect to its Security Issues and Solutions: A Literature Review, Jun. 2017.

[6]. D. R. K. Mahajan, Security Issues and Guidelines for a Successful E-Commerce System, Jun. 2018.

[7]. M. D. Kalamkar, A study of Ecommerce Security, 2017

[8]. S. S. Garash, “Overview Security in e-Commerce,” Overview of Electronic Commerce, Feb. 2022

[9]. N. Kuruwitaarachchi, P. K. W. Abeygunawardena, L. Rupasingha, and S. W. I. Udara, “A systematic review of security in electronic commerce- threats and Frameworks,” Global Journal of Computer Science and Technology, pp. 33–39, 2019.

[10]. S. Wang, “Study on the application of computer security technology in e-commerce,” Journal of Physics: Conference Series, vol. 1915, no. 4, p. 042044, 2021.

[11]. C. K. Kashinath, D. Chandrasekharan, T. R. Ravindran, and D. P, Security Issues in

E-Commerce: A Study, pp. 60–66, Apr. 2017.

[12]. M. D. Kalamkar, A study of Ecommerce Security, 2017.

[13]. S. Carta, G. Fenu, D. ReforgiatoRecupero, and R. Saia, “Fraud detection for e-commerce transactions by employing a prudential multiple consensus model,” Journal of Information Security and Applications, vol. 46, pp. 13–22, 2019.

[14]. P. D. Hatwar, A REVIEW ON NETWORK SECURITY PROTOCOLS, 2019.

[15]. D. P., S. S. Babu, and Y. Vijayalakshmi, “Enhancement of e-commerce security through asymmetric key algorithm,” Computer Communications, vol. 153, pp. 125–134, 2020.

[16]. D. P. Patil, Study on E-Commerce Security Issues and Solutions, Jan. 2017.

[17]. D. Kaushik, A. Gupta, and S. Gupta, “E-commerce security challenges: A Review,” SSRN Electronic Journal, 2020.

[18]. O. Najeem, Designing a conceptual Security Framework for Secure Online Ordering System (SOOS), Dec. 2020.

[19]. R. K. Jamra, B. Anggorojati, Kautsarina, D. I. Sensuse, and R. R. Suryono, “Systematic review of issues and solutions for security in e-commerce,” 2020 International Conference on Electrical Engineering and Informatics (ICELTICs), 2020.

[20]. S. Sahara and P. S. Kurniati, E-Commerce Risk During Transaction Process, 2019.