Security Analysis for E-Commerce Business

Sagor Sen[1], Charlie Natarajan[1]

[1]Student, Department of Computer Engineering, Indian Institute of Technology, Kanpur, India.

Corresponding Author: sagor@theperfectreview.com

Abstract: - One of the essential parts of the Information Security framework is E-commerce Security. It is primarily used for the features that impact e-commerce, including Data Security, Computer Security, and other broader realms of the Information Security framework. E-commerce security has individual nuances and is one of the most visual safety components influencing the end user through regular payment interaction with business. E-commerce safety protects e-commerce assets from unapproved entry, use, alteration, or demolition—measurements of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, and Availability. ECommerce gives the banking industry a great chance but develops new threats and vulnerabilities such as safety weaknesses. Moreover, data security is an important control and technological essential for efficient and adequate Payment transaction actions over the internet. Still, its description is difficult to work due to the stable technical and business shift and needs a coordinated match of algorithm and technological resolutions. In this article, we explained a summary of E-commerce protection, Understand the Online Shopping Steps to place an order, the Purpose of Security in E-commerce, Various safety issues in E-commerce, and Secure online shopping guidelines.

Key Words— *Security measures, Online Shopping, Digital E-commerce cycle, Security Threats, Secure online shopping guidelines, E-Commerce Security Issues.*

I. Introduction

The advantages of E-commerce, including availability, ease to access, various selections of products and services, and international reachability, continue to attract online customers to join the eCommerce business [1]. For example, e-commerce sales worldwide reached 1.2 trillion US dollars in 2013 [2], and it is estimated that e-commerce sales will reach 1.92 trillion US dollars in 2016 [3]. Due to such growth, business owners should realize that improving the online services provided to their customers is vital. Currently, many companies are gathering customers' information (e.g., name, address, interest, etc.) through registration, online transactions, or cookies to improve provided services [4].

Manuscript revised October 17, 2022; accepted October 18, 2022. Date of publication October 20, 2022.

This paper available online at www.ijprse.com

ISSN (Online): 2582-7898; SJIF: 5.59

This collected information helps companies study their customers' behaviors and trends. Accordingly, they are being able to make better advertising decisions and potential target customers effectively [5]. While online customers can trade data collected about them with some benefits (i.e., financial benefits), 95% of online customers refuse to provide their personal information to e-commerce websites [6].

Safety and privacy are strong barriers to adopting e-commerce services [7, 8, and 9]. Hoffman and Novak [6] mentioned that 63% of online customers refuse to share their personal information such as name, gender, date-of-birth, phone number, and email address with e-commerce organizations, because of the lack trust in such websites. Furthermore, 67% to 75% of online customers refuse to exchange their personal data for financial benefits. Moreover, 72% of online customers believe that providing personal information to e-commerce organizations is too risky and does not worth privacy and security risks associate with it. Additionally, 69% of customers decline registration in e-commerce websites, because they do not know how the organizations will handle their personal information [6]. Privacy and security concerns associated with e-commerce are not a new subject. It has been existed a long time ago; because ecommerce services require multiple transactions of sensitive and personal data between different networks [10]. To decrease these concerns and attract online clients, e-commerce institutions should manage factors impacting clients' beliefs, such as security and privacy concerns and clients' perceived threats.

In this article, we suggest a primary method to believe clients' privacy issues, security concerns, and how they can affect their perceived risk. We will also study the relationship between the mentioned elements and customers' trust and behavior in online shopping/transactions. This model is developed based on an existing model, the privacy-trust-behavioral intention model, founded in [4], which investigated the relationship between privacy concerns and how it would affect consumers' trust and behavioral intentions. That model does not involve a vital aspect considered a precursor to trust, perceived risk [11]. Since we believe that perceived risk is critical in controlling customers' trust, we developed a new model that studies the relationship between privacy and security concerns and perceived risk and how it would relate to customers' confidence level in e-commerce.

II. Literature Review

Security is a principal and continuing concern that restricts customers and organizations from engaging with eCommerce. Besides the advantage of threat-adjusted expenses, open dataset's resource helps institutions benchmark their inner cyber attitude and cybersecurity measures [18]. This paper explores the perception of security in e-commerce B2C and C2C websites from both customer and organizational perspectives. [7] With the rapid growth of E-commerce, safety issues are rising from people's concentration. The safety of the transaction is the core and significant point of the development of E-commerce. This article about the safety issues of Ecommerce functions put forward a solution strategy from two aspects: technology and system, to improve the environment for E-commerce development and promote E-commerce's further development. [8] Web applications growingly combine third-party services. Introduces new safety challenges due to an application's difficulty coordinating its inner states with the feature services and the web customer across the Internet [9].

Ecommerce website owners, on one side, are thinking of how to attract more customers and how to make visitors feel secure when working on the site. On the other side, how the end utilizers should review an e-Commerce website and what need do to give safety as one among the online groups. Our objective in writing this research analysis journal is to provide the readers with clarity of thinking on the approaches that give safe transactions and security tips. And how e-Commerce site owners must create their online visitors of much comfort or Trust an eCommerce site via Trust marks and their safety techniques. [10].

The typical authentication techniques are based on identity to give safety or access control systems; standard encryption and authentication algorithm need the high computing power of computer equipment. Therefore, improving the authentication mechanism and optimizing the traditional encryption and authentication algorithm may be the focus of P2P e-commerce [11].

E-Commerce offers the banking industry great opportunity but also creates new risks and vulnerabilities such as security threats. Therefore, information security is an essential management and technical requirement for efficient and effective Payment transaction activities over the Internet. Still, its definition is a complex endeavor due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions [12].

The online transaction requires consumers to disclose sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce.[13] In online shopping, electronic payment is the main point to confirm the clients are fast and suitable. We have to ensure the security and secrecy of the clients during a transaction, which needs total electronic trading strategies [14].

III. The Proposed Model

E-commerce services have grown dramatically in recent years. Understanding what motivates customers to shop online will ease the adoption of such services and help organizations gain profits. Researchers have found different aspects that would affect the adoption of e-commerce services, such as security [16, 17], privacy concerns [15, 18], risk [17, 19, 20], and trust [15].

According to Liu [15], e-commerce firms should provide customers with detailed explanations regarding data use and collection, and in return, the customers should be willing to provide their data. By doing so, e-commerce companies will earn loyal clients, and clients will be pleased to receive targeted promotions and proposals. Since that risk differs from one individual to another, we decided to consult perceived threats in our system. Kim et al. in [18] suggested that understanding perceived risk, its precursors, and its outcomes can help eCommerce providers build a solid relationship with their customers. Similarly, Pennanen et al. in [17] have found that a high level of perceived risk and uncertainty of adverse outcomes can decrease customer trust in e-commerce businesses. Results of their study suggested different relationships between perceived risk and security, privacy concerns, and trust. In addition, the study's results supported the assumption that risk is an antecedent of trust. Trust is deemed a robust idea when talking about online trade. Hoffman et al. in [16] proposed that customers refuse to be involved in e-commerce and never provide their credit card information because of the lack of trust in such services. Thus, to build a strong relationship with customers and gain profits, e-commerce vendors should consider the concept of trust and understand the relationship of trust with other important concepts (i.e., perceived risk, security, and privacy) that would affect the adoption of e-commerce services. Therefore, research by Liu et al. in [15] offered that the level of trust will positively impact the behavioral intention of online customers. So, if a customer has a high level of trust, they will revisit the website, purchase again, recommend it to others, or give positive comments. We took this relation between trust and behavioral intention from a tested and validated study in [15] and used it in our model.

Although several researchers investigated different relationships between aspects that would affect the adoption of e-commerce services [17, 19, 21], none have addressed perceived risk as a significant precursor of trust. In addition, few studies have been developed to investigate the relation between security and privacy concerns, perceived risk, and trust with each other as distinct aspects. Our objective was to create and test a theoretical model which suggests that security and privacy concerns have a negative relationship with perceived risk, which in return have a negative association with the level of trust that would impact the customer's behavioral intention. Our theoretical model is based on the privacy-trust-behavioral model proposed by Liu et al. in [4]. We added the concept of perceived risk because, for e-commerce, it is essential to address such a concept, as some studies showed that perceived risk is the precursor of trust.

IV. Limitations

Future research will be required to improve the proposed model and validate some of the rejected hypotheses. This section will discuss some limitations that may result in leaving some of the ideas. First, participants in the study showed essential clients of e-commerce, but not all.

For example, multi-cross participants would be a better choice for aspects like privacy and trust that may differ from one region to another. Second, we assumed that privacy and security would indirectly affect the level of trust through perceived risk. Still, other researchers believe that privacy and security directly affect the level of trust [15]. Therefore, we should consider other possible models to understand the relationship between these aspects better.

V. Digital-E-Commerce Cycle

Security is essential in online trading sites. Recently, a large amount is being traded online because it’s easy and more suitable. Anything can be purchased, like food, clothing, music, toys, cars, etc. Some of these tradings are illegal; we will concentrate on all the items you can purchase legally on the internet. Few famous websites are Amazon, AliExpress, eBay, iTunes, HMV, Mercantila, dell, Best Buy, and many more.

VI. E-commerce Security Tools

- Firewalls – Software and Hardware
- Public Key Infrastructure
- Encryption software
- Digital certificates
- Digital Signatures
- Passwords.

VII. Purpose of Security

1. Data Secrecy – is delivered by encryption or decryption.
2. Authentication and Identification – ensuring that someone is who they claim to be is implemented with digital signatures.
3. Access Control – governs what sources a utilizer may access on the method. Uses valid IDs and passwords.
4. Data Integrity – confirms data has not been tampered with. It is implemented by message digest or hashing.

5. Non-rejection – not to refuse a sale or buy. Implemented with digital signatures.
    - Plaintext/Cleartext – message humans can read.
    - A cryptographic algorithm is called a cipher. Most attacks are emphasized discovering the key.

VIII. Security Issues

E-commerce security protects e-commerce assets from illegal entry, utilize, alteration, or demolition. While safety attributes do not guarantee a safe method, they are essential to develop a closed method. Safety features have the following parts:

- Authorization: This permit only client to exploit clients' sources in exact paths. This protects client from growing the balance of clients account or removal a bill.
- Pairing: Contract with data hiding. It confirms client can't spy on others during Online banking transactions.
- Auditing: Save a data of system. A businessman uses auditing to confirm that clients purchase exact merchandise.
- Integrity: Protection against illegal data edit
- Non-repudiation: Protection against any one client from reneging on an agreement after the reality
- Availability: Protection against data pauses or delete.

IX. Conclusion

Safety, perceived risk, secrecy, and trust issues are essential in eCommerce. Understanding the connection between this system is even crucial. In this article, we have focused some insights into eCommerce's safety, perceived risk, secrecy, and trust method. Therefore, we analyzed the significance of each technique for e-commerce. The article also studied the relationships between the four said concepts. Furthermore, we offered a security-privacy-perceived risk-trust primary hypothetical method for clients in e-commerce. The technique shows the relationship between secrecy, safety, perceived threat, and confidence. The provided process in this article gives a basis for further analysis on defining and knowing the connection between trust and other ideas in e-commerce. With proper verification technology, the approach will lead to a more helpful understanding of the significance of safety, secrecy, perceived threat, and confidence in accepting e-commerce.

References

[1]. Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I., 2012. The effect of online privacy policy on consumer privacy concern and trust. Computers in human behavior, 28(3), 889-897.

[2]. E-Commerce - Statistics & Market Data, Statista. Retrieved October 9, 2015.

[3]. B2C e-commerce sales worldwide 2018, Statista. Retrieved October 9, 2015.

[4]. Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S., 2005. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. Information & Management, 42(2), 289-304.

[5]. Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y., 2014. Information Security in Big Data: Privacy and Data Mining. Access, IEEE, 2, 1149-1176.

[6]. Hoffman, D.L., Novak, T.P., and Peralta, M. Building customer trust online. Communication of the ACM, 42 (4). 80-85.

[7]. Mohanad Halaweh, Christine Fidler - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449.

[8]. Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.

[9]. Md Haris Uddin Sharif, Ripon Datta, Mounicasri Valavala (2019), Identifying Risks and Security Measures for E-Commerce Organizations, International Journal of Engineering Applied Sciences and Technology. Vol. 4, Issue 5.

[10]. Rui Wang, Shuo Chen "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P '11 proceedings.

[11]. V.SRIKANTH "Ecommerce Online Security and Trust Marks". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July-September (2012).

[12]. Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011).

[13]. RAJU BARSKAR, ANJANA JAYANT DEEN" The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology"(IJCSIS)-Vol. 8, No. 1, April 2010.

[14]. Pradnya B. Rane, Dr. B.B.Meshram. "Transaction Security for Ecommerce Application" IJECSE -ISSN- 2277-1956. 2012.

[15]. Yang Jing "On-line Payment and Security of E-commerce". ISBN 978-952-5726-00-8, 2009 International Symposium on Web Information Systems and Applications (WISA '09).

[16]. Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S., 2005. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. Information & Management, 42(2), 289-304.

[17]. Hoffman, D.L., Novak, T.P., and Peralta, M. Building customer trust online. Communication of the ACM, 42 (4). 80-85.

[18]. Md Haris Uddin Sharif and Mehmood Ali Mohammed, (2022), A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(01), 138–156.

[19]. Yousafzai, S.Y., Pallister, J.G., and Foxall, G.R., 2003. A proposed model of e-trust for electronic banking. Technovation, 23. 847-860.

[20]. Kim, D.J., Ferrin, D.L., and Rao, H.R., 2008. A trust-based customer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decision Support Systems, (44) 2. 544-564.

[21]. Featherman M.S. 2003, and Pavlou, A. Predicting e-service adoption: a perceived risk facets perspective. International Journal of Human Computer Studies – Spatial issue on HCI and MIS, 59 (4). 451-474.

[22]. McKnight, D.H., Choudhury, V., and Kacmar, C., 2002. Developing and validating trust measures for e-commerce: an integrative typology. Information System Research, 13 (3).334-359.