International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

xx

COPY RIGHT

IJIEMR Transactions, online available on 27th May 2024. Link
https://www.ijiemr.org/downloads/Volume-13/ISSUE-5

10.48047/IJIEMR/V13/ISSUE 05/49

TITLE: CYBERSECURITY CHALLENGES IN E-COMMERCE TRANSACTIONS

Volume 13, ISSUE 05, Pages: 474-481

Paper Authors TVL kedareshwari, Dr M Chandra Sekhar Reddy

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

CYBERSECURITY CHALLENGES IN E-COMMERCE TRANSACTIONS

TVL kedareshwari, Dr M Chandra Sekhar Reddy

Svck college of engineering, kadapa.

ABSTRACT

The term "e-commerce," which is often referred to as "electronic commerce," describes the act of purchasing and selling goods and businesses, as well as the transmission of assets or information, through the utilisation of an electronic network that is essentially analogous to the internet. Business-to-business (b to b), business-to-consumer (b to c), consumer-to-consumer (c to c), and consumer-to-business (c to b) transactions are the many kinds of commercial transactions that can take place. The process of exchanging products or services through the utilisation of computer networks such as the Internet or informal communities that can be discovered online is referred to as the process of doing business online. The most significant challenges that are working to impede the growth of online businesses are identity theft and fraudulent activity on the internet. There is a basic issue that needs to be solved in order to support the rapid spread of e-commerce, and that issue is inadequate security on web servers used for e-commerce and the use of computers. Hackers are those who are responsible for breaking into computer systems. With the goal of boosting customer confidence in online shopping, this paper offers some guidelines for ensuring the safety of online transactions.

Keywords: E-Commerce, Cyber-security, fraud and identity.

1. INTRODUCTION

There is a part of the Information Security framework called "security in e-commerce" that is specifically used for parts of the framework that affect e-commerce. Computer security and data security are two of these parts. In order to be successful, e-commerce requires high-security components that have an impact on the end user through their regular interactions with businesses regarding payments. E-commerce necessitated the establishment of a dependable infrastructure and framework in order to facilitate prosperous and risk-free e-commerce [1]. At the present time, the protection and security of electronic technologies are a big concern for the industry. To give one example, the security problems that are associated with M-commerce (Mobile Commerce) are similar to those that are associated with e-commerce for enterprises and associations. There are a greater number of compliance challenges and technologies in the area of online commerce applications that handle payments. Some examples of these applications include online savings accounts, electronic exchanges, or the use of debit cards, credit cards, PayPal, E-money, prepaid cards, master cards, visa cards, or other tokens. Concerns regarding protection have been identified, revealing a lack of confidence in a variety of settings. These situations include commerce, electronic health records, e-recruitment technology, and long-range interpersonal contact. As a result, users have been directly impacted by this [2].

Security is one of the most important reasons that restricts the participation of customers and associations in e-commerce. This is because security is one of the variables that prevents customers and associations from engaging in activity. Currently, businesses that engage in e-commerce are making efforts to gradually fix security vulnerabilities that exist on their internal networks. Standards of this kind for the protection of systems and networks are accessible for anyone working on e-commerce platforms to understand and put into practice. These standards are available for both individuals and organisations.

It is still in its early stages to educate consumers about security concerns because a significant number of customers who use online shopping are illiterate, while others are literate. This means that the education of customers on security concerns is still in its phases. Despite this, it will end up being the most important component of the security architecture for online commerce it is intended to protect. The practice of shopping online, which is also referred to as the transaction of products or services through the use of the Internet, is gaining popularity and has a substantial amount of space for growth.

This is due to the fact that computing equipment and communication technologies are undergoing rapid developments and getting more cost efficient everyday [4]. The tremendous potential that mobile computing possesses to make online buying a very popular way of shopping is astonishing. In order to preserve the trust of their clients and offer them with great service, business owners want to make sure that their e-commerce web platforms have high availability, sufficient capacity, and satisfactory performance. The primary concern of customers is security, which is a factor that is slowing down the rapid rise of online commerce transactions. Finding answers to security issues such as the destruction, disclosure, and modification of data, as well as denial of service, fraud, waste, and misuse of network resources, is important in order to earn the trust of customers in electronic commerce. This is why it is necessary to develop solutions to these security issues. [5] An e-commerce environment is comprised of a number of components, including web pages on the front end, databases on the back end, web servers, and an internal network architecture.

In order to lessen the likelihood of security problems occurring, it is necessary to locate and fix the weak spots that are present in an electronic commerce system.

1.1 E-Skimming

Due to the fact that it involves criminals recording the information that customers type into online shopping checkout pages in real time, e-skimming is a serious security problem for websites that are involved in e-commerce. Because of this, there is a major risk to both safety and security. The most typical way for attackers to gain access to an e-commerce website is through the use of phishing. However, they may also be able to achieve this goal through the use of cross-site scripting (XSS), third-party compromise, and brute force attacks.
Once the cybercriminal has obtained access to the system, they are able to introduce malicious skimming code that either directs customers to a false website or directly gathers credit card information in real time. Both of these methods are potentially harmful.

1.2 **Phishing**

Phishing is the most popular method that hackers employ to attack organisations, particularly those that deal in online commerce but also other types of businesses. Phishing and social engineering are two techniques that are aimed to trick users into giving personally identifiable information (PII). This information includes passwords, account numbers, and credit card numbers. Phishing and social engineering include both of these techniques. Phishing and social engineering are two forms of social engineering that are frequently carried out through the exchange of fake communications with the intention of deceiving recipients into giving sensitive information. Cybercriminals have the ability to make use of this information in order to gain unauthorised access to one or more user accounts. A number of significant security challenges are presented by phishing. One of the most serious of these challenges is the chance that a successful phishing attempt may result in a significant data breach that would lead to the distribution of access credentials on the web. Phishing provides a number of significant security challenges. The successful completion of a phishing attempt is typically a precursor to the infection of a computer with malware. Phishing was a form of social engineering. In the event that there are insufficient security procedures and systems in place, it is possible that these attacks will not be noticed. A credential-stuffing attack is an attempt to acquire unauthorised access to one or more websites by using credentials. After that, fraudsters can purchase lists of usernames and passwords and use bots to carry out the attack. This attack involves attempting to gain access to the websites by using credentials.

1.3 Malware

Malware refers to any piece of malicious software that is designed to infect a computer or mobile device. Malware can be found on both desktop and mobile devices. Obtaining personally identifiable information (PII), which includes login credentials, redirecting people to alternate websites, stealing money, and restricting access to the website and its services are all examples of successful applications of this technique.

E-commerce websites are frequently the focus of hackers' attention for a number of reasons, one of which is the fact that hackers can use malware to target clients of a business. By employing an XSS attack to exert influence over an e-commerce website or by delivering emails to customers that look to be genuine but are actually communicated through hacked access credentials, they are able to accomplish this goal.

These messages are often delivered by email. When an e-commerce company is subjected to a ransomware attack, the virus that represents the cybercriminal encrypts the essential data of the company. A ransom payment is then demanded by the cybercriminal in exchange for the decryption key, which the cybercriminal may or may not supply.

2. LITERATURE REVIEW

Technology makes a significant contribution to our day-to-day lives. The applications of technology to the manner in which business is conducted are one of the key contributions that technology has made [6]. The conventional approaches to conducting business have been elevated to a higher level as a result of this. The quality and pricing of products and services, as well as the means by which businesses operate, are impacted by new technology [7].

The term "business" refers to the act of trading one item for another; to be more particular, it is specific to the act of selling and purchasing goods or services in exchange for monetary compensation [8]. As was said previously, the use of technology has resulted in a change in the manner in which business is conducted. In the context of business, the term "e-commerce" or "e-business" refers to any activity that involves the utilisation or application of electronic technology [9].

E-commerce refers to the practice of doing business transactions online by utilising the internet to carry out those transactions. Other technologies, such as email, can also be utilised in the process of conducting business online; however, the most prevalent method of conducting business online is through the usage of a website. When it comes to the world of electronic commerce, the three most significant components are the electronic market, online shopping, and online auctions. A customer is able to make a purchase of a product or service from a distance if they make use of the application or technology that is providing the opportunity to do so [10]. Researchers from a wide range of disciplines, such as business and technology, have been drawn to the field of e-commerce in order to enhance the process and make it more advantageous and profitable at the same time.

E-commerce is still in the process of developing as a result of the creation of new technology and its applications. At the same time, however, these innovations have also presented the sector with a few obstacles [11]. E-commerce is confronted with a number of issues, one of which is "the cyber security concern" [12], which is undoubtedly one of the most significant and widespread worries it faces.

Customers and commercial entities involved in e-commerce are always the focus of hackers and cyberattacks [13]. A survey indicates that 83 percent of the retail establishments in the United States are susceptible to attack and might be easily targeted [14].

In most cases, attackers target the private information of clients, which is the most valuable asset in the realm of online commerce. On the other hand, this can be accomplished by the utilisation of malicious software, ransomware, e-skimming, or the theft of data from the databases of online retailers. [15] [15] They are also able to launch attacks in the form of distributed denial of service attacks, which are more commonly referred to as DDoS attacks. It is undeniable that the proliferation of businesses that have been made possible by technological advancements, such as e-commerce and e-business, has led to an increase in the number of options that are open to us.

However, this does not mean that there are no problems of any kind, such as cyber security, etc. In the same way as e-commerce organisations are continuously working to improve their technology and expertise, cybercriminals are also continually working to uncover weaknesses in the present system of e-commerce and then exploit those holes [16]. In light of this, it is necessary to do so in order to study the advantages and disadvantages of technology and to find solutions to the issues that have been identified.

3. E-COMMERCE SECURITY THREATS AND THEIR SOLUTIONS

The field of electronic commerce has grown to become one of the most significant sectors in the world. Because of the rapid development of technology and the internet, there has been a significant increase in the number of channels via which companies can communicate with their clients located in different parts of the world. Nevertheless, the risk is proportional to the size of the company, which is a significant factor.

Moreover, this is also the situation with regard to online business. As a company or a brand, it is not only your duty but also your responsibility to safeguard all of your customers and yourself from potential dangers. In the past few years, there has been an increase in the number of people who are concerned about safety and privacy on the internet. The consumer and the brand are both exposed to information that is available to the public, which leaves them susceptible to security concerns.

3.1 Electronic Payments Threat

It is now possible to apply the concept of everything taking place online to the banking and financial industry as well. As a means of payment, the usage of online wallets and electronic transactions has become increasingly prevalent over the course of the past several years. On the other hand, interacting with money on a network exposes one to additional dangers due to the fact that hackers might be able to break through the cybersecurity measures. Furthermore, there are other dangers, such as the following:

1. Fraud

For the purpose of making an online transaction easier, the users have either pins or passwords. However, the authorization of payments based solely on passwords and security questions does not guarantee that the person being authorised is who they claim to be. In the event that another individual has access to our credentials, this could result in a case of fraud. The third party will have an easier time stealing money in this manner.

2. Tax Evasion

For the purpose of verifying the collection of taxes, the companies offer the invoice in the form of paper records. On the other hand, when things are done online, the issue becomes more confusing, and the Internal Revenue Service is confronted with the challenge of dealing with it. As a consequence of this, it becomes more challenging for them to handle the collection of taxes and to ascertain whether or not the company exhibits ethical behaviour.

3. Payment Conflicts

The users and the automated electronic systems are the parties involved in these transactions. There is a possibility of making mistakes when processing payments due to the fact that it is a machine at the end of the day. The users end up losing their money as a result of these errors and abnormalities, which occur when there are conflicts of payment.

4. E-cash

By utilising internet wallets such as PayPal, GooglePay, Paytm, and others, the paperless cash system can be implemented. Given that the entirety of the financial information is contained within the application, a single security breach has the potential to result in the revelation of private information as well as monetary loss.

3.2 Personal Information Threats

1. Scraping

This method is commonly used by a large number of firms that are in direct competition with one another in order to acquire sensitive data and important internal key performance indicators (KPIs). Despite the fact that the companies maintain a high level of security about such information, it is still feasible for hackers or bots to break into the system and acquire access to the necessary information.

2. Spam

It is possible to accomplish this goal in the majority of instances by sending out enticing baits in order to gather personal information. Additionally, it is feasible for spammers to take use of contact forms and blog pages in order to fool organisations into clicking on links that actually contain dangerous content.

They are able to cause harm to the website's speed, security, and customers as a result of this access.

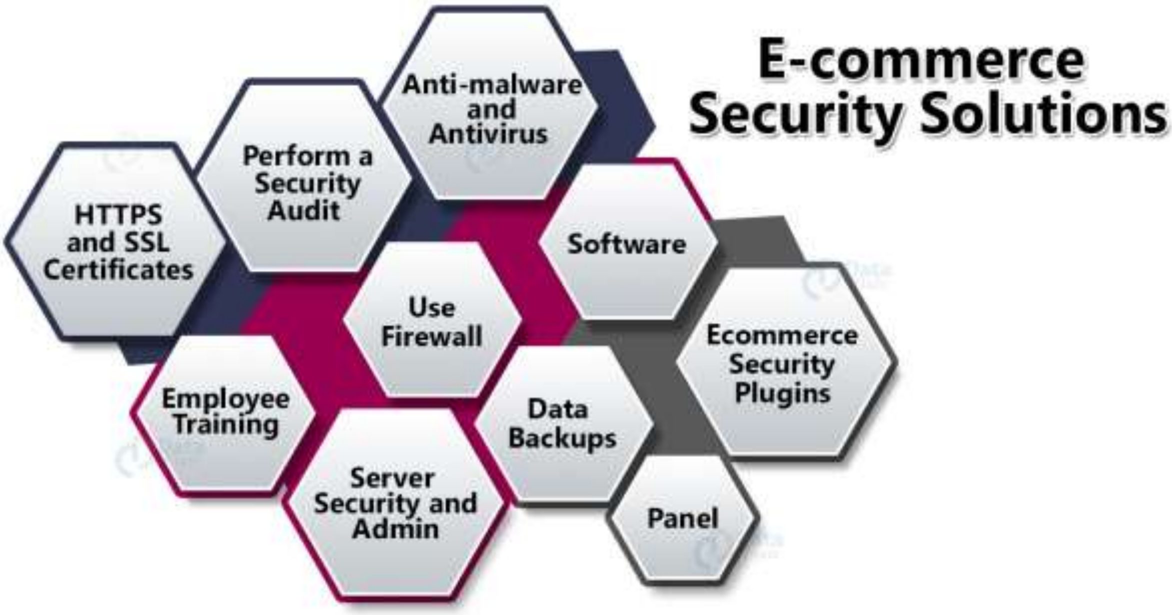
3. SQL Injection

For the purpose of gaining access to databases, hackers employ a method that involves the use of query submission forms. Through the use of viruses, they corrupt all of the information and make it an infectious disease. One option available to them is to make a copy of the data for their own personal use, after which they can remove it from the primary system in an irreversible manner.

4. Bots

This is software that uses web crawlers to determine the ranks of websites based on the pages that are already there on the internet. These crawlers can be utilised by hackers in order to monitor the policies and strategies of competitors, which might result in unfair market practices. There is a possibility that this will be exploited against the corporation or in favour of the rival.

3.3 E-commerce Security Solutions


E-commerce Security Solutions
HTTPS and SSL Certificates
Perform a Security Audit
Anti-malware and Antivirus
Software
Use Firewall
Ecommerce Security Plugins
Employee Training
Data Backups
Server Security and Admin
Panel

1. Secured Payment Gateway

During online transactions, the most prudent guideline to follow is to make sure that you exclusively use safe payment getaway techniques. Additionally, these gateways have improved security and nondisclosure policies, which are designed to safeguard all of the customers.

2. Use firewall

It is a highly prevalent method that involves following predetermined rules in order to regulate network traffic and prevent security concerns from occurring. This particular piece of software is a type of network security software that functions in a manner that is consistent with the security measures that are suggested by the administrators. This provides protection against the vast majority of cyber threats, including cross-site scripting (XSS), SQL injection, trojan horses, and other varieties of malicious software.

3. HTTPS and SSL certificates

Both SSL certificates and HTTPS certificates adhere to a common protocol that encrypts personal data before it is transmitted to websites that support online commerce. This protocol is known as the encryption protocol.

If a website possesses both certificates, then the consumers will continue to be protected. Despite having access to information, hackers are unable to accomplish much with data that has been encrypted.

4. Encryption

A technique that transforms regular English into a coded form, making it impossible for hackers to decipher the message. For the sake of preventing any kind of data leak, it is absolutely necessary for websites to implement encryption. The decryption of this cypher text should be possible only by a small group of highly trained persons, ensuring that safety is maintained at all times.

5. Server Security and Admin Panel

The requirements for the passwords that are supplied on a variety of websites ought to be adhered to by the users in the most stringent manner possible. By utilising a combination of charters, symbols, and numbers, users are able to generate passwords that are more secure than those that are created individually. The restriction of access to various websites on the internet is something that they ought to be aware of and take into consideration.

In order to prevent security breaches, make sure to follow the instructions on the administrative panel.

6. Anti-malware and Antivirus Software

In order to avoid the modification of files or software, it is possible to install anti-malware and virus software that can identify and remove infections. By taking this precaution, you can rest assured that your data and personal information will be protected against threats such as worms, viruses, and Trojan horses.

CONCLUSION

The accessibility of the internet and technology did open up many doors that led to a simpler way of life, but this came at a costly price. When treated casually, these security dangers are extremely serious and have the potential to cost businesses of a significant size a lot. On the other hand, this does not imply that you, as a buyer, can disregard them. Due to the fact that you are equal shareholders in this cycle, you are responsible for ensuring your own safety. By according to this set of recommendations, businesses and individuals will be able to use the internet in a more secure manner while simultaneously preserving their privacy.

REFERENCES

1. Abdel Hakeem, S. A., Hussein, H. H., and Kim, H. (2022). Security requirements and challenges of 6G technologies and applications. Sensors 22:1969. doi: 10.3390/s22051969

2. Abdelhamid, M., Kisekka, V., and Samonas, S. (2019). Mitigating e-services avoidance: the role of government cybersecurity preparedness. Inform. Comput. Secur. 27, 26–46. doi: 10.1108/ICS-02-2018-0024

3. Ahmad, S. F., Alam, M. M., Rahmat, M. K., Mubarik, M. S., and Hyder, S. I. (2022). Academic and administrative role of artificial intelligence in education. Sustainability 14:1101. doi: 10.3390/su14031101

4. Ahmad, S. F., Rahmat, M. K., Mubarik, M. S., Alam, M. M., and Hyder, S. I. (2021). Artificial intelligence and its role in education. Sustainability 13:12902. doi: 10.3390/su132212902

5. Ahmadian, S. (2021). Review of e-commerce service delivery models. Arman Process J. 2, 14–20.

6. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., and Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network 2, 123–138. doi: 10.3390/network2010009

7. Alavi, R., Islam, S., and Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. Inform. Comput. Secur. 24, 205–227. doi: 10.1108/ICS-01-2016-0006

8. Al-Ghamdi, M. I. (2021). Effects of knowledge of cyber security on prevention of attacks. Mater. Today Proc. doi: 10.1016/j.matpr.2021.04.098

9. Anderson, R. J. (2008). “A guide to building dependable distributed systems,” in Security engineering, 2nd Edn, (Hoboken, NJ: Wiley).

10. Anshari, M., Almunawar, M. N., and Al-Mudimigh, A. (2022). “Digital marketplace as a new frontier of electronic commerce,” in Handbook of research on big data, green growth, and technology disruption in asian companies and societies, (Hershey: IGI Global), 122–137. doi: 10.4018/978-1-7998-8524-5.ch007

11. Anvari, R. D., and Norouzi, D. (2016). The Impact of E-commerce and R&D on economic development in some selected countries. Proc. Soc. Behav. Sci. 229, 354–362. doi: 10.1016/j.sbspro.2016.07.146

12. Bigcommerce (2022). What you need to know about securing your ecommerce site against cyber threats. Available online at: https://www.bigcommerce.com/articles/ecommerce/ecommerce-website-security/ (accessed April 10, 2022).

13. Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. Netw. Secur. 2016, 5–9. doi: 10.1016/S1353-4858(16)30086-1

14. Burton, W. (2007). Burton’s legal thesaurus, 4 Edn. New York, NY: McGraw-Hill Education.

15. Castagna, F., Centobelli, P., Cerchione, R., Esposito, E., Oropallo, E., and Passaro, R. (2020). Customer knowledge management in SMEs facing digital transformation. Sustainability 12:3899 . doi: 10.3390/su12093899

16. Centobelli, P., Cerchione, R., Esposito, E., and Oropallo, E. (2021a). Surfing blockchain wave, or drowning? Shaping the future of distributed ledgers and decentralized technologies. Technol. Forecast. Soc. Change 165:120463. doi: 10.1016/j.techfore.2020.120463