International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1117-1120 www.ijaem.net ISSN: 2395-5252

A Review on Cyber Attacks and Countermeasures in the Online Payment System

Sahil Baghla[1], Kamalpreet Kaur[2]
[1]*Department of Management, CT University, Ludhiana, India*
[2]*Department of Management, CT University, Ludhiana, India*

Date of Submission: 15-05-2023 Date of Acceptance: 30-05-2023

ABSTRACT: Due to the advancement in the banking system, the popularity of the online payment systems is increased exponentially. In the online payment system, the user transfers the money electronically from one place to another using the internet as a communication media. However, the online payment system is prone to numerous attacks on the internet. Therefore, a security system is required for secure transactions. In this paper, we have studied and analyzed the various cyber-attacks and countermeasure methods are used for online payment system. From the analysis, we found that the most popular online cyber-attacks on the online system are phishing, malware, SQL injection, man-in-the-middle, and denial-of-service. Further, to overcome these attacks, encryption, two-factor authentication, and fraud detection systems have been implemented in the online payment system.

Keywords: Cyber-Attacks, Denial-of-service (DoS) Attacks; Encryption; Malware; Man-in-the-middle Attacks; Online Payment Systems; Phishing Attacks; Security Measures; SQL Injection Attacks; Two-factor authentication.

1. INTRODUCTION

Online payment systems are a type of electronic payment system that allows individuals or businesses to transfer money electronically over the internet. The first online payment system, called Electronic Funds Transfer (EFT), was developed in the 1970s and used by banks to transfer funds between accounts (Mueen, U., 2021). However, it was not until the mid-1990s that online payment systems began to gain widespread use with the growth of e-commerce (Hisham, N. R., 2021).

The rise of online shopping and the increasing number of transactions conducted over the internet led to the development of various online payment systems, including PayPal, Skrill, Stripe, and others. These systems allow users to make purchases online and transfer funds between accounts quickly and securely.

Today, online payment systems have become an essential part of the e-commerce landscape, with millions of transactions being conducted daily. They offer convenience, flexibility, and security, making them a popular choice for individuals and businesses around the world. As online payment systems continue to evolve, new technologies and security measures are being developed to keep up with the ever-changing threat landscape and protect users from cyber attacks (Botheju, D., 2017).

- **Online Payment System in India:** Online payment systems in India have seen significant growth in recent years due to the increasing adoption of digital payment methods (Arora, A., 2019). The Indian government's demonetization efforts in 2016, which aimed to reduce cash transactions and promote digital payments, helped accelerate the growth of online payment systems in the country. Some of the popular online payment systems in India include Paytm, Google Pay, PhonePe, Amazon Pay, and BHIM. These systems allow users to make payments for a wide range of services and products, including utility bills, online shopping, and mobile recharges (Wang, X., 2018). The adoption of online payment systems in India has been driven by various factors, including the increasing availability of affordable smartphones and internet access, government policies, and the rise of e-commerce. The COVID-19 pandemic also accelerated the adoption of digital payment methods as people turned to online shopping and contactless payments to avoid physical contact (Zhou, Y., Liu, D., 2020). However, the growth of online payment systems in India has also led to various challenges, including security concerns, transaction failures, and user privacy issues. In the literature, the most popular cyber attacks on the online system are phishing attacks, malware, denial-of-service attacks, SQL injection attacks, and man-in-the-middle attacks (Liu, Y., 2019). However, attackers continually find new ways to exploit vulnerabilities in the system, making it essential to update and improve security measures continually. Cyber-attacks on online payment systems pose a significant threat to both users and payment system providers, making it crucial to be vigilant when using online payment systems and report any suspicious activity to the payment system provider immediately. Therefore, the government and payment system providers are taking steps to address these challenges, including the implementation of security measures such as two-factor authentication, fraud detection systems, and encryption (Liu, Y., 2020).

The main contribution of this paper is to study and analyze the various cyber-attacks on the online payment system and countermeasure methods are deployed to overcome it. Initially, this paper discusses the various types of cyber-attacks on the online payment system ((Yaraghi, N., Du, 2017). After that, it gives a detailed description of the countermeasure methods such as two-factor authentication, encryption, and fraud detection system are deployed in it (Abuhamad, A. 2018, Zhang, Y., 2020). Additionally, the paper emphasizes the importance of continually updating and improving security measures to protect against evolving threats.

The rest of the paper is organized as follows. Section 2 gives a detailed description of the cyber attacks on the online payment system. Section 3 shows the countermeasure methods are deployed for overcome the cyber-attacks. Finally, conclusion is drawn in Section 4.

II. TYPES OF CYBER ATTACKS ON ONLINE PAYMENT SYSTEM

There are various types of cyber attacks that are commonly directed towards online payment systems, including:

- **Phishing Attack**: This type of attack involves tricking users into providing personal or financial information through fake websites or emails that appear to be from a legitimate payment system.
- **Malware**: Malware can be used to infect a user's device and steal their payment information or carry out unauthorized transactions.
- **Denial-of-Service (DoS) Attack**: DoS attack involves overwhelming the payment system with traffic, making it impossible for legitimate users to access the system or carry out transactions
- **SQL Injection Attack**: SQL injection attack involves exploiting vulnerabilities in the payment system's database to gain unauthorized access or steal sensitive information.
- **Man-in-the-Middle Attack**: Man-in-the-middle attack intercepts communication between the user and the payment system to steal sensitive information.
- **Cross-site Scripting (XSS) Attack**: This type of attack involves injecting malicious scripts into a website's code to steal user information or carry out unauthorized transactions.
- **Brute Force Attack:** Brute force attack involves trying every possible combination of usernames and passwords to gain unauthorized access to a payment system.
- **Social Engineering Attack:** Social engineering attack involves manipulating users into divulging sensitive information by posing as a trustworthy entity. Attackers may use tactics such as impersonating customer support or creating fake promotions to trick users into providing their payment information.
- **Insider Attack**: Insider attack involves individuals with authorized access to the payment system who use their privileges to carry out fraudulent activities, such as stealing sensitive information or carrying out unauthorized transactions.
- **Supply Chain Attack**: Supply chain attack involves exploiting vulnerabilities in third-party software or hardware components used in the payment system to gain unauthorized access or steal sensitive information.

These attacks pose a significant threat to the security and integrity of online payment systems and can result in financial losses for users and payment system providers. It is essential to be aware of these types of attacks and take necessary precautions, such as implementing strong passwords, using two-factor authentication, and keeping security software up to date, to protect against them (Yeboah-Boateng, 2019). It is important for online payment systems to implement robust security measures to protect against these types of attacks. This includes implementing strong authentication methods, encrypting sensitive data, monitoring for suspicious activity, and regularly conducting security audits and assessments. Additionally, users should be vigilant and take necessary precautions such as regularly checking their account activity and reporting any suspicious activity to the payment system provider (Kizza, J. M. 2017).

2.1 Countermeasure Methods to Overcome Cyber-Attacks in the Online Payment System

In recent years, cyberattacks have become a growing concern for individuals, businesses, and governments (Zhu, Y., Li, X., 2019). These attacks can cause significant financial losses, damage to reputation, and in some cases, even physical harm. The good news is that there are several security methods that can be used to overcome cyberattacks (Wei, Q., 2020). In this article, we will discuss some of the most effective methods.

- **Strong Passwords and Multi-Factor Authentication:** One of the easiest and most effective ways to prevent cyberattacks is to use strong passwords and multi-factor authentication (MFA). Strong passwords should include a combination of upper and lowercase letters, numbers, and symbols, and they should be changed regularly. MFA adds an extra layer of security by requiring users to provide two or more forms of identification, such as a password and a fingerprint or a security token.
- **Regular Software Updates:** Cybercriminals often exploit vulnerabilities in software to gain access to systems. Regular software updates can patch these vulnerabilities and prevent cyberattacks. Therefore, it is essential to keep all software up to date, including operating systems, web browsers, and third-party applications.
- **Firewalls and Antivirus Software:** Firewalls and antivirus software can help prevent cyberattacks by blocking malicious traffic and detecting and removing viruses and other malware. Firewalls can be hardware-based or software-based, and they work by filtering network traffic to prevent unauthorized access. Antivirus software can scan files and programs for viruses and other malicious code (Olawale, F., 2018).
- **Data Encryption:** Encryption is the process of converting data into a coded language that can only be accessed with a specific key or password. Encrypting sensitive data can help prevent cybercriminals from accessing it, even if they manage to breach a system's defenses.
- **Regular Backups:** Regular backups can help protect against cyberattacks by ensuring that data is not lost in the event of a breach. Backups should be stored in a separate location, and they should be tested regularly to ensure that they are working correctly.
- **Employee Training:** Employees are often the weakest link in a company's cybersecurity defenses. Therefore, it is essential to provide regular training to educate them on how to recognize and respond to cyber threats. This training should cover topics such as phishing scams, password security, and safe browsing practices.
- **Incident Response Plan:** Even with the best cybersecurity measures in place, it is still possible for a cyberattack to occur. Therefore, it is important to have an incident response plan in place. This plan should outline the steps that should be taken in the event of a cyberattack, including who to contact and what actions to take to minimize damage.

From the above analysis, we found that cyberattacks are a growing threat, but there are several security methods that can be used to overcome them (Li, J., 2020). By using strong passwords and multi-factor authentication, regularly updating software, using firewalls and antivirus software, encrypting data, regularly backing up data, providing employee training, and having an incident response plan in place, individuals, businesses, and governments can significantly reduce the risk of cyber-attacks (Zargar, S. T., 2013).

CONCLUSION AND DISCUSSION

In conclusion, cyber-attacks on online payment systems have become a significant concern in recent years, with many individuals, businesses, and governments falling victim to these attacks. These attacks can result in financial losses, data breaches, and damage to reputation. However, there are several security methods that can be used to overcome cyberattacks and prevent them from occurring in the first place. One of the most effective methods is the use of strong passwords and multi-factor authentication. Regular software updates, firewalls, and antivirus software can also help prevent cyberattacks. Additionally, encrypting sensitive data, regularly backing up data, providing employee training, and having an incident response plan in place can further enhance cybersecurity measures. It is important to note that cyberattacks are constantly evolving, and therefore, cybersecurity measures must also evolve to keep up with these attacks. Therefore, individuals, businesses, and governments must stay up to date with the latest cybersecurity trends and invest in effective cybersecurity measures to protect themselves against cyberattacks.

REFERENCES

[1]. Abuhamad, A. (2018). Cyber Security Risks and Mitigation Techniques for Online Payment Systems. International Journal of Computer Science and Network Security, 18(2), 121-131.

[2]. Arora, A., & Sharma, M. (2019). Cyber Security in E-payment System: A Review. International Journal of Innovative Technology and Exploring Engineering, 8(11S), 137-141.

[3]. Botheju, D., & Liyanage, J. P. (2017). A multi-level security framework for mobile payment systems. Journal of Telecommunication, Electronic and Computer Engineering, 9(1-2), 11-17.

[4]. Cao, Y., & Shang, Y. (2021). The impact of cyberattacks on online payment platforms: Evidence from China. Telematics and Informatics, 60, 101532.

[5]. Hisham, N. R., Yahya, A. S., Hashim, H., & Razak, S. A. (2021). A study on security factors of online payment systems in Malaysia. IEEE Access, 9, 25133-25145.

[6]. Kizza, J. M. (2017). Guide to Computer Network Security. Springer.

[7]. Li, J., Li, Y., Li, T., & Li, J. (2020). Exploring the determinants of online payment security: A perspective of perceived control. Journal of Business Research, 109, 308-318.

[8]. Liu, Y., & Yu, B. (2020). A cyber security analysis of online payment in China. Journal of Cyber Security Technology, 4(2), 103-113.

[9]. Liu, Y., Wang, H., & Zeng, D. D. (2019). Towards comprehensive understanding of cyber attack and defense. Information Systems Frontiers, 21(2), 259-262.

[10]. Mueen, U., & Lu, W. (2021). Cybersecurity and risk assessment in online payment systems: A review. Journal of Information Privacy and Security, 17(2), 96-112.

[11]. Olawale, F., &Adetunmbi, A. (2018). Cybersecurity and online payment system: a review. International Journal of Computer Applications, 181(19), 11-17.

[12]. Wang, X., Jiang, Y., Guo, C., & Yu, Y. (2018). Design and implementation of online payment system based on the Internet of Things. Journal of Physics: Conference Series, 1065(4), 042043.

[13]. Wang, Z., Li, J., Liu, S., & Li, Z. (2020). Online payment security assessment based on analytic hierarchy process and grey clustering. Journal of Ambient Intelligence and Humanized Computing, 11(3), 1113-1123.

[14]. Wei, Q., & Zhang, Y. (2020). Research on the risk assessment of online payment security. Advances in Information Sciences and Service Sciences, 12(3), 274-287.

[15]. Yaraghi, N., Du, A. Y., Sharman, R., & Gopal, R. (2017). An empirical analysis of data breach litigation. MIS Quarterly, 41(4), 1153-1176.

[16]. Yeboah-Boateng, E. O., &Nyanzu, F. O. (2019). Cybersecurity and online payment systems: A conceptual review. Journal of Innovation and Entrepreneurship, 8(1), 1-18.

[17]. Zargar, S. T., Joshi, J. B., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046-2069.

[18]. Zhang, Y., & Kim, M. (2020). Cybersecurity threats in online payment systems: A review of literature. Sustainability, 12(20), 8515.

[19]. Zhou, Y., Liu, D., & Wang, Y. (2020). An analysis of online payment security based on deep learning. Journal of Ambient Intelligence and Humanized Computing, 11(3), 1383-1393.

[20]. Zhu, Y., Li, X., & Fan, X. (2019). An analysis of cyber security issues in online payment platforms. Journal of Information Security and Applications, 46, 273-284.