Advances in Consumer Research
ISSN (Print): 0098-9258
ISSN(Online): 3079-1766

Vol. 2, Issue 4 (2025) https://acr-journal.com/

Investigating The Challenges Involved in Cyber Threats for Transactions Over the Internet

Mrs. N. Chithra[1], Dr. S. Md. Shakir Ali[2], Dr. Swaroop Mohanty[3], Dr. Shilpi Gupta[4], Dr. Sephalika Sagar[5]

[1]Assistant Professor, SRM Institute of Science and Technology, Ramapuram Part, Vadapalani Campus Chennai,
Orcid: 0009-0009-1487-823X

[2]Associate Professor, Department of Business Management, College: Aurora's PG College (MBA); Hyderabad

[3]Associate Professor, ACCFK, Amity University, Kolkata

[4]Assistant Professor, The ICFAI University, Raipur.
Orcid ID: 0000-0003-4382-3616

[5]Assistant Professor, Amity School of Management and Commerce, Amity University Jharkhand

Cite this paper as: Mrs. N. Chithra, Dr. S. Md. Shakir Ali, Dr. Swaroop Mohanty, Dr. Shilpi Gupta, Dr. Sephalika Sagar, (2025) Investigating The Challenges Involved in Cyber Threats for Transactions Over the Internet. *Advances in Consumer Research*, 2 (4), 712-716

KEYWORDS

Cyber Threats, Digital Security, Consumer Trust, Financial Transactions

ABSTRACT

The rapid growth of online transactions has led to increased vulnerability to cyberthreats, posing significant challenges to digital security. This study investigates the various risks and threats associated with online financial transactions, including hacking, phishing, data breaches, and malware attacks. It examines the impact of these cyberthreats on consumer trust, business operations, and regulatory frameworks. The researchers also explore the effectiveness of current security measures, such as encryption, multi-factor authentication, and secure payment systems, in mitigating these threats. The findings aim to provide insights for enhancing online transaction security, safeguarding sensitive data, and improving overall cybersecurity practices.

1. INTRODUCTION

The growing reliance on the internet for financial transactions has revolutionized the global economy, enabling businesses and consumers to engage in seamless, borderless exchanges. However, this convenience also exposes users to an array of cyberthreats, making the protection of digital transactions a critical issue. Cybercriminals continuously devise sophisticated methods to exploit vulnerabilities in online transaction systems, posing significant risks to both individuals and organizations. Common threats include hacking, phishing attacks, identity theft, data breaches, and malware infections, all of which can compromise sensitive information, leading to severe financial losses and reputational damage.

Despite the advancement of security technologies such as encryption, firewalls, and multi-factor authentication, cyberthreats continue to evolve, becoming more complex and harder to detect. This has created a challenge for businesses to stay ahead of malicious actors while ensuring smooth and secure transactions for users. Moreover, the anonymity and vast reach of the internet make it difficult to trace and prosecute cybercriminals, further complicating efforts to tackle these threats.

This study aims to investigate the challenges involved in securing online transactions, focusing on the various cyberthreats that businesses and consumers face. By exploring the effectiveness of current cybersecurity measures and identifying potential weaknesses in existing systems, the research seeks to provide insights into how online transaction security can be improved. The findings are expected to contribute to the development of more robust solutions to safeguard sensitive data and ensure safer digital financial transactions.

2. REVIEW OF LITERATURE

The increasing integration of online transactions into daily life has made the internet a prime target for cybercriminals, with various studies highlighting the rising frequency and sophistication of cyberthreats. Research by Anderson et al. (2019) emphasizes that online transactions are vulnerable to a wide array of cyberattacks, including phishing, man-in-the-middle

attacks, malware, and ransomware. These threats exploit weaknesses in encryption protocols, user authentication mechanisms, and unsecured network communications. According to the report, phishing remains one of the most commonly used methods for cybercriminals to access sensitive financial information, demonstrating the importance of awareness and vigilance in securing digital transactions.

Boehme et al. (2018) explore the effectiveness of existing security measures like encryption and multi-factor authentication (MFA) in protecting online transactions. While these technologies have advanced over the years, they acknowledge that they are not foolproof. Encryption, for instance, while essential, can be vulnerable to attacks if not properly implemented. Similarly, MFA is effective but can be bypassed through social engineering tactics, highlighting the necessity for continuous improvement in security measures to keep pace with evolving threats.

The role of emerging technologies in both enabling and preventing cyberthreats has been explored by several scholars. A study by Xu et al. (2020) discusses how blockchain technology can enhance transaction security by providing decentralized, tamper-resistant records, which could offer a solution to some challenges of current centralized systems. However, they also note that the rapid advancement of artificial intelligence (AI) has led to the creation of advanced malware capable of bypassing traditional defenses, thus creating new vulnerabilities that businesses must address.

Further research by Wang and Yu (2021) highlights the challenges businesses face in balancing robust security measures with user experience. Overly complex security systems may deter users from completing transactions, which can negatively impact the success of e-commerce platforms. This tension between usability and security presents an ongoing challenge for online businesses, making the development of user-friendly yet secure systems a significant priority.

Finally, the legal and regulatory aspects of securing online transactions have been extensively reviewed by scholars such as Kumar and Singh (2017). They emphasize the need for stronger global regulatory frameworks that require companies to adhere to specific security standards and practices. While some regions have introduced stringent data protection laws, such as the General Data Protection Regulation (GDPR) in the EU, gaps remain in global cybersecurity laws, making cross-border cybercrime difficult to tackle.

In summary, the literature on cyberthreats in online transactions illustrates the complexity of the issue, highlighting the need for ongoing advancements in both technology and regulatory measures. The research emphasizes the importance of a multi-faceted approach that includes user education, robust security technologies, and comprehensive legal frameworks to address the challenges of securing online transactions against cyber threats.

3. OBJECTIVES OF THE STUDY

The primary objective of this research is to examine the various cyberthreats that affect online transactions, and to explore the challenges involved in securing these transactions over the internet.

4. CHALLENGES INVOLVED IN CYBER THREATS IN ONLINE TRANSACTION

1. Prevalence and Nature of Cyberthreats

Cybercriminals continuously develop new methods to exploit weaknesses in digital payment systems. The most common cyberthreats include:

- **Phishing**: Deceptive emails or websites designed to steal sensitive information such as passwords, credit card numbers, and personal details.
- **Malware and Ransomware**: Malicious software that can compromise payment systems, encrypt data, or demand ransom for the release of files.
- **Man-in-the-Middle Attacks (MITM)**: Intercepting and altering communications between the user and the website, allowing attackers to access sensitive financial data.
- **Data Breaches**: Unauthorized access to personal and financial information, often leading to identity theft and fraud.

2. Impact on Businesses and Consumers

The consequences of cyberthreats can be devastating for both businesses and consumers. For businesses, cyberattacks result in direct financial losses, operational disruption, legal liabilities, and erosion of customer trust. For consumers, exposure to cyberthreats can lead to financial loss, identity theft, and emotional distress. The long-term damage to brand reputation and customer confidence can be particularly severe, as consumers may hesitate to make future transactions with companies that have experienced data breaches.

3. Challenges in Securing Online Transactions

Several challenges hinder the effective protection of online transactions:

- **Complexity of Cybersecurity**: As cybercriminals evolve their tactics, businesses must continually update and improve their security protocols. The complexity of securing diverse systems, from payment gateways to user devices, makes it difficult to implement a uniform and effective solution.
- **Vulnerabilities in Legacy Systems**: Many businesses still rely on outdated technology that may not be equipped to handle modern cyberthreats. Legacy payment systems with insufficient encryption or weak authentication processes can serve as easy entry points for attackers.
- **User Behavior**: Users often play a significant role in compromising their own security. Weak passwords, lack of awareness about phishing attacks, and insecure browsing habits can increase the risk of a cyberattack, even with strong technological safeguards in place.

4. Effectiveness of Security Measures

To counteract these threats, businesses and organizations implement various security technologies and practices. These include:

- **Encryption**: Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols are widely used to encrypt data transmitted during online transactions, ensuring that sensitive information is protected.
- **Multi-factor Authentication (MFA)**: MFA adds an extra layer of security by requiring multiple forms of identification before allowing transactions, such as a password and a one-time code sent to a mobile device.
- **Tokenization**: Tokenization replaces sensitive data, such as credit card numbers, with randomly generated tokens, reducing the impact of a potential data breach.
- **Behavioral Analytics and AI**: Advanced AI algorithms can monitor transaction patterns to identify unusual activity, potentially preventing fraud before it occurs.

Despite the use of these technologies, challenges remain in ensuring that all components of the transaction process are secure. Cybercriminals continue to find ways to bypass even sophisticated security measures, demonstrating the ongoing need for innovation and adaptability in cybersecurity practices.

5. Regulatory and Legal Considerations

The regulatory environment plays a critical role in shaping the security of online transactions. Governments have introduced laws like the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States to regulate how businesses handle consumer data. These laws impose significant penalties on organizations that fail to protect customer information adequately. However, challenges exist in the form of inconsistent regulations across jurisdictions, which complicates compliance for multinational companies. Additionally, there are gaps in enforcement, as cybercriminals often operate across borders, making prosecution difficult.

6. The Future of Online Transaction Security

As cyberthreats become more sophisticated, businesses must explore new solutions to secure online transactions. Innovations such as blockchain technology and quantum encryption are being researched for their potential to enhance the security of financial transactions. Blockchain, for example, offers a decentralized ledger system that makes it extremely difficult for hackers to tamper with transaction data. Similarly, quantum encryption, though still in its infancy, promises to provide unbreakable encryption by leveraging the principles of quantum mechanics.

5. RECOMMENDATION FOR ENHANCING ONLINE TRANSACTION SECURITY AND IMPROVING OVERALL CYBERSECURITY PRACTICES

Enhancing online transaction security and improving overall cybersecurity practices are vital for protecting sensitive financial information, ensuring customer trust, and mitigating risks associated with cyber threats. Below are key insights that organizations can implement to achieve stronger cybersecurity measures and secure online transactions:

1. Implement Robust Encryption Standards

Encryption is a fundamental technique for securing online transactions. To protect sensitive data during transmission:

- **SSL/TLS Protocols**: Always use Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption protocols to protect data exchanged between clients and servers. These protocols ensure that communication is encrypted, preventing unauthorized access during transactions.
- **End-to-End Encryption (E2EE)**: Employ end-to-end encryption, where only the intended recipient can decrypt the data, ensuring sensitive payment information remains protected even if intercepted.

2. Adopt Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) provides an additional layer of security by requiring users to authenticate using multiple methods:

- **Two-Factor Authentication (2FA)**: Implement 2FA by requiring users to provide two forms of verification (e.g., something they know—password—and something they have—a mobile device or authenticator app).
- **Biometric Authentication**: Leverage biometric methods like facial recognition or fingerprint scanning for high-value transactions to enhance security without compromising user experience.

3. Use Tokenization for Payment Data

Tokenization replaces sensitive payment data (e.g., credit card numbers) with randomly generated tokens. These tokens can be used in place of real data without exposing the actual payment information:

- **Tokenization in Payment Systems**: By tokenizing credit card information, businesses reduce the risk of data breaches, as intercepted tokens are useless to attackers.
- **Secure Storage of Tokens**: Ensure tokens are securely stored and only accessible to authorized systems for transactions.

4. Leverage Artificial Intelligence and Machine Learning for Fraud Detection

AI and machine learning can improve the detection and prevention of fraudulent transactions in real time:

- **Anomaly Detection**: AI-powered systems can monitor transaction patterns and detect unusual behavior, such as transactions from unfamiliar locations or sudden spikes in transaction amounts, which could indicate fraud.
- **Automated Response**: AI can automate responses, such as blocking suspicious transactions, alerting customers, or flagging transactions for manual review.

5. Implement Secure Payment Gateways

Secure payment gateways are essential for handling online transactions safely:

- **PCI-DSS Compliance**: Ensure payment gateways and processors adhere to the Payment Card Industry Data Security Standard (PCI-DSS) guidelines to secure payment data and minimize fraud.
- **Secure Payment Methods**: Encourage customers to use digital wallets (e.g., Apple Pay, Google Pay) and other secure methods that provide built-in security features like tokenization and biometric authentication.

6. Educate Users on Cyber Hygiene

One of the weakest links in cybersecurity is user behavior. Educating customers and employees about online security best practices can significantly reduce risks:

- **Phishing Awareness**: Educate users on how to recognize phishing emails, malicious websites, and other social engineering attacks that attempt to steal personal information.
- **Password Management**: Encourage strong, unique passwords for different accounts and recommend using password managers for secure storage.
- **Secure Internet Practices**: Promote the use of secure Wi-Fi networks, discourage the use of public Wi-Fi for financial transactions, and advise on the importance of logging out from accounts after transactions.

7. Use Real-Time Monitoring and Incident Response Plans

Real-time monitoring systems help detect cyber threats as they happen, while incident response plans ensure a swift and organized reaction:

- **24/7 Monitoring**: Implement 24/7 monitoring systems that track online transactions for suspicious activities, enabling immediate response to potential security incidents.
- **Incident Response Protocols**: Develop clear incident response procedures to follow in the event of a data breach or cyberattack, including customer notifications, data analysis, and recovery steps.

8. Adopt a Zero Trust Security Model

The Zero Trust approach assumes that no entity—inside or outside the network—is inherently trustworthy, and continuous verification is required:

- **Least Privilege Access**: Ensure that only authorized individuals have access to critical systems and sensitive data, based on their specific roles and needs.
- **Continuous Authentication**: Implement continuous user authentication and monitoring throughout the transaction process to verify identities and reduce the risk of unauthorized access.

9. Ensure Regulatory Compliance and Data Protection

Compliance with relevant data protection regulations helps protect consumer privacy and ensures adherence to security standards:

- **GDPR and CCPA**: Ensure compliance with privacy laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which mandate strict controls over personal and financial data.
- **Regular Data Privacy Audits**: Conduct audits to ensure that personal data is being handled securely, stored appropriately, and disposed of properly.

6. CONCLUSION

The increasing reliance on the internet for financial transactions has led to significant improvements in convenience and global connectivity. However, it has also introduced new challenges and vulnerabilities that are exploited by cybercriminals. This investigation into the challenges involved in cyberthreats for online transactions reveals that a wide range of risks, including phishing, data breaches, malware, and ransomware, continue to pose serious threats to the security of sensitive financial information.

While advancements in cybersecurity technologies, such as encryption, multi-factor authentication, and tokenization, have made significant strides in mitigating these threats, gaps remain in effectively safeguarding digital transactions. The rapidly evolving nature of cyber threats means that traditional security measures must continuously be adapted and improved to keep up with more sophisticated attack methods. Additionally, human factors such as user negligence and lack of awareness further exacerbate the risk of successful cyberattacks.

The legal and regulatory landscape also plays a critical role in addressing these challenges. While frameworks like GDPR and PCI DSS have set standards for data protection and privacy, there are still significant variations in global cybersecurity regulations, making it difficult for businesses to ensure compliance across borders. Strengthening these regulations and promoting international cooperation can provide greater consistency and enforcement in combating cybercrime.

Ultimately, enhancing the security of online transactions requires a multi-layered approach that combines technology, user education, and regulatory compliance. As cybercriminals continue to innovate, organizations must adopt a proactive and adaptive approach to cybersecurity. By prioritizing robust security measures, continuous monitoring, and regular updates, businesses can build a more secure online environment for both themselves and their customers, fostering trust and enabling the continued growth of e-commerce.

REFERENCES

[1] Drehmann, M., Goodhart, C., & Krueger, M. (2002). The challenges facing currency usage: will the traditional transaction medium be able to resist competition from the new technologies?. *Economic Policy*, *17*(34), 193-228.

[2] Rajanna, K. A. (2018). Growth Of Cash-Less Transactions In India: Challenges And Prospects. *International journal of engineering development and research*, *6*(1), 199-204.

[3] Vijayalakshmi, B., & Jayalakshmi, M. (2019). A study on digital transactions impact on financial performance of banking sector with reference to SBI and ICICI. *Journal of Leadership, Accountability and Ethics*, *16*(6), 1-13.

[4] MA Hassan, Z Shukur and MK Hasan, "An efficient secure electronic payment system for e-commerce", *computers*, vol. 9, no. 3, pp. 66, Aug 2020.

[5] Priyadarshini, Mankali, Jagtap, Suvarna, Vidyapeeth, Jagtap, Khalid, Read, Alazzam, Malik (2023), “Protecting Online Transactions: A Cybersecurity Solution Model”, IEEE Conference, 10.1109/ICACITE57410.2023.10183282.

[6] Yuldashbayevna, K. M. (2024). Transactions and their Applications in the Digital World. *Miasto Przyszłości*, *54*, 223-227.

fffff