Digital Payment Security: Threats, Challenges, and Modern Solutions

Sandhya Dahake[1] ; Neeraj Kumar Jha[2] ; Sanjana Jenekar[3]
[1]Department of Master in Computer Application, G H Raisoni College of Engineering and Management Nagpur, Maharashtra, India
[2]Department of Master in Computer Application, G H Raisoni College of Engineering and Management Nagpur, Maharashtra, India
[3]Department of Master in Computer Application, G H Raisoni College of Engineering and Management Nagpur, Maharashtra, India

Abstract
With the evolution of encryption, artificial intelligence-based fraud detection, block chain, and regulatory frameworks, the security of digital payments is evolving to counter new threats [1]. This study calls for robust authentication protocols, secure payment systems, and consumer education in safeguarding digital transactions [2]. In this paper Author insists that having strong security controls is necessary to establish trust and facilitate long-term growth of digital payments in a cashless economy [3].
Keywords
Electronic Payments, cyber security, fraud prevention, phishing, block chain.

1. Introduction

1.1 Definition of Digital Payments

Digital Payments, also called as electronic payments or e-payment done through digital or online mode, where exchange of hard cash (physical cash) is not involved [4]. It is the transfer of value from payer to payee where both uses a digital mode (device – mobile phone, computer, credit card, debit card, or prepaid card). This indicates that for digital payments to happen, the payer and payee both must have a bank account, any online banking method, a device from which they will be making the payments, and a medium [5].

1.2 Growth and Adoption

The adoption of e-payment (digital payment) systems has significantly accelerated over the decades, with the contribution of high Penetration of internet, technological advancement, global tilt towards cashless economies [6]. According to the recent study, statistics of global digital payment market is expected to reach $20 trillion by 2026, growing at A CAGR (compound annual growth rate) of 15% [7]. The turning point for the acceleration of this digital payments where the COVID-19 pandemics as contactless payment becomes a necessity for safety and hygiene reasons. Mobile payments app such as Google Pay, Phonepee, Apple pay has gained a wide usage, with billons of transactions happing daily [9].

1.3 Need for Security

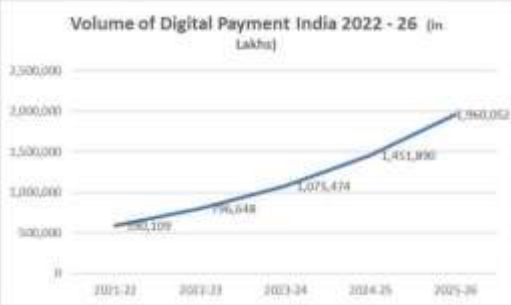
While digital payments provide various benefits like speed and accessibility, they also involve immense security threats [10]. Phishing, information hijacking, identity theft, and forgery of payments are top online issues both for users and banks [11]. Facilitating the security for e-payments is very critical to maintaining the trust of the users, preventing money losses, and keeping sensitive financial details private [2].

1.4 Objective of the Research

The primary purpose of this study is to research and address security issues in internet transactions. With the payment system of the internet changing at a very rapid rate, consumers and business are facing significant issues like fraud, hacking, identity theft, and data breaches [3]. The study will detail the detection process of overall security risks in online transactions and measuring the

DOI: https://doi.org/10.5281/zenodo.17452159

efficiency of existing security controls, including encryption, multi-factor authentication, and anti-fraud methods [4]. Furthermore, the study will investigate the new technologies of blockchain, AI, biometric verification, and quantum cryptography and how these can enhance the security of electronic payments [5]. Against the backdrop of studies on the emerging cybersecurity threats and advancement in payment technology, this study seeks to contribute towards the establishment of a stronger and more resilient digital payment system [6]. The results will equip business, banking, and policy-making communities with the guidelines and recommendations on how to secure transactions over the internet and safeguard users from probable cyber-attacks.



Source: Dart consulting and national informatics centre

2. Security Challenges in Digital Payments

2.1 Security Risks in Digital Payments

Digital payments are also vulnerable to hacking by cybercriminals who take advantage of loopholes in security features to obtain sensitive financial data [7]. The following are the most intense threats in digital payment systems at present [8].

2.1.1 Social Engineering and Phishing Attacks

Social engineering and phishing attacks are some of the most prevalent forms of attacks hackers initiate to manipulate customers into divulging their sensitive payment details [9].

- Phishing are spurious emails, SMS (smishing), or websites that imitate authentic financial institutions or payment gateways. The intention is to deceive users into divulging their login details, credit card numbers, or personal data [10].
- Social Engineering Attacks target psychological vulnerabilities instead of technical weaknesses [1]. Attackers impersonate bank officials, technical support personnel, or known individuals to deceive users into revealing their passwords, OTPs, or card PINs [2].

2.1.2 Payment Frauds (Card Fraud, Identity Theft)

Payment fraud is when card/debit or credit card information is stolen by hackers and/or utilized for unauthorized payments.

• **Card Fraud:** Card information is stolen by hackers using skimmers, malware, or data breach and utilize them to carry out unauthorized transactions.
• **Identity Theft:** Hackers use sensitive personal data such as names, addresses, and Social Security Numbers to open non-authorized accounts, obtain loans, or perform non-authorized transactions.

2.1.3 Malware and Ransomware

Ransomware and malware are major threats to payment digital security.

- Programs employed to target payment terminals with the aim of capturing account data, passwords, or authentication codes are referred to as malware.
- Ransomware locks accounts or payment systems out of access by encrypting sensitive information until a ransom is paid.

2.1.5 Data Breach by Unauthorized Access

Data breach by unauthorized access is a data breach where hackers exploit payment network security weaknesses to steal sensitive account information [1], [10].

2.2 Weaknesses in the Payment System

Despite technological advancements, many payment systems still suffer from security vulnerabilities, making them attractive targets for cybercriminals**.**

DOI: https://doi.org/10.5281/zenodo.17452159

2.2.1 Weak Authentication Controls

The initial defence against payment system security is authentication, but weak authentication controls are implemented on the majority of platforms [10].

- **Password Cracking**: The majority of users employ weak passwords such as "123456" or "password," which can be easily cracked by attackers.
- **Single-Factor Authentication (SFA):** The systems that implement a username and password only are vulnerable to credential capture.

2.2.2 Inadequate Encryption Practices

Encryption is necessary to secure payment transactions, but the lack of encryption practices makes the sensitive information open to attackers.

Payment Data: Data related to payments can be stored or sent to websites in a format that is easily readable. That makes easy for attackers to access.

Weak Encryption Algorithms: Encryption algorithms that are weak, such as MD5 or SHA-1, are highly susceptible to cryptographic attacks.

2.2.3 Insufficient Proper User Awareness

The security attacks are mainly caused by the user's forgetfulness or incompetence in the system. Due to some wrong practice users get phished and having personal payment details exposed [5].

- Using the same password for numerous websites.
- Not being able to identify scam or forgery payment sites.

Source: - Open-AI

Current Security Measures in Digital Payments

3.1. Encryption Techniques

End-to-end encryption E2EE: Is a security measure to ensure security without loss of confidentiality on payment data until they complete transmission.

SSL/TLS Protocols: Is a set of cryptographic protocols for regulating a secure channel from the user's device to the payment gateway while avoiding attacks from MITM. [1] [10]

3.2. Authentication Methods

Multi-Factor Authentication (MFA): Application refers to a technical scheme used in securing transactions in addition to MFA

One-Time Password (OTP): OTP means a temporary password sent from the server, or the issuer, to the user to validate the transaction.

Biometric authentication: Is a solution to identify users based on fingerprinting, recognition of the face, or retina scanning.

3.3. AI and Machine Learning for Fraud Detection

Real-time Fraud Monitoring-AI systems observe transaction patterns and identify alarming activities. - AI-based Anomaly Detection-The models of machine learning are able to see unusual spending behaviour that indicates fraud.

4 Future Technologies for Digital Payment Security

Digital payment security is a key concern

4.1 Block chain Technology

Decreasing potential for fraud and unauthorized changes is a benefit of using a distributed ledger for transactions. Smart Contracts are self-executing contracts that

DOI: https://doi.org/10.5281/zenodo.17452159

validate and enforce the terms of a contract automatically [9].

4.2 Quantum Cryptography

Future-Proof Security: Uses quantum mechanics to create unbreakable encryption methods. Post-Quantum Cryptography is a field under research at the moment. It aims to create cryptographic solutions that would be resistant to attacks from [10].

4.3 Advancements in Biometric Authentication

Voice Recognition: It is a system that identifies users by their voice patterns.

Retina Scanning: This is a process that involves the analysis of the unique patterns in

Behaviour-Based Authentication: This system examines keystroke patterns typing speed, and other behaviours to confirm the user.[10]

4.4 Zero Trust Security Model

Idea: Cyber security framework in which each access request is authenticated regardless of user location.

Implementation: Banks and payment service providers are implementing Zero Trust principles to reduce security risks [10].

Source: - Biz next

5. Digital Literacy for Payment Security

In the age of technology, awareness of payment security is necessary to prevent fraud and loss of money. Below is a concise summary of the key points [10].

1. Secure Transactions

Always check for HTTPS in the address of a webpage. Ensure that you use legit payment gateways to make payment. This will secure your money and personal information.

2. Scam and Phishing protection

Spammers typically send phony messages and emails with links that are malicious. Watch out for unsolicited requests for payment, mysterious senders and poor grammar in messages, these are typical fraud indications.

3. Secure Passwords & Authentication

Use strong, separate passwords and turn on multi-factor authentication (MFA) for greater security. Biometric authentication (like fingerprint or facial recognition) is another level of security.

4. Government & Institutional Initiatives

Governments and banks hold cyber security awareness programs. India's DISHA program and the European Union's cyber security programs, for example, make users aware of secure digital habits. Banks conduct awareness sessions to make customers secure online as well.

6. Regulatory and Compliance Factors

6.1 Global Standards & Frameworks

- **General Data Protection Regulation (GDPR):** Safeguards consumer data and mandates strict privacy regulations.
- **Payment Card Industry Data Security Standard (PCI DSS):** Secures handling of cre6. Aspects of Regulation and Compliance

6.2 The Role of Central Banks and Financial Institutions

- **Guidelines for the Security of Online Transactions:** Central banks implement security guidelines for electronic payments. Frameworks for cyber security: Financial institutions have stringent security guidelines to shield payment information. Card information.
- **Strong Customer Authentication (SCA):** An EU regulation mandating two-factor authentication for online transactions.

7. Conclusion and Recommendations

7.1 Summary of Findings

Finally Author concludes the Following

DOI: https://doi.org/10.5281/zenodo.17452159

• Although online payments have revolutionized money exchange, security threats still constitute a large deterrent.
• Multi-factor authentication, encryption, and AI-driven fraud detection are some of the security features.
• Secure web payment in the future will be influenced by technology such as block chain, quantum cryptography, and Zero Trust models [1], [2], [3].

7.2 Best Practices for Users and Organizations

•Multi-factor authentication and making the source of transactions trigger end users and other secure measures.
•Employing encryption, artificial intelligence-based security, and conducting regular cybersecurity audits.

7.3 Areas for Future Research

• Creating AI models to identify fraud.
• Creating post-quantum cryptography algorithms to address emerging threats [9], [10],

8. Acknowledgement

The authors gratefully acknowledge Dr. Sandhya Dahake for her valuable guidance and support during this research, and to Dr. Himanshu Sharma Dean, RND for his helpful suggestions and encouragement. Their encouragement from G H Raisoni College of Engineering and Management, Nagpur, has played a crucial role in the successful completion of this Study paper.

9. References

[1]Chaum, D. (1997). Security of electronic payment systems. Computer, 30(9), 28-35. IEEE. https://doi.org/10.1109/2.612244
[2]Shailza, & Sarkar, M. P. (2019). Literature review on adoption of digital payment system. Global Journal of Enterprise Information System, 11(3), 62-67. Retrieved from https://gjeis.com/index.php/GJEIS/article/view/14
[3]Bezhovski, Z. (2016). The future of the mobile payment as electronic payment system. European Journal of Business and Management. Retrieved from https://core.ac.uk
[4]Sujith, T. S., & Julie, C. D. (2017). Opportunities and challenges of e-payment system in India. International Journal of Scientific Research and Management. Retrieved from https://scholar9.com
[5]Ghosh, G. (2021). Adoption of digital payment system by consumer: A review of literature. International Journal of Creative Research Thoughts. Retrieved from https://researchgate.net
[6]Yu, H. C., Hsi, K. H., & Kuo, P. J. (2002). Electronic payment systems: An analysis and comparison of types. Technology in Society. Retrieved from https://elsevier.com
[7]Chaveesuk, S., Khalid, B., et al. (2021). Digital payment system innovations: A marketing perspective on intention and actual use in the retail sector. Innovative Marketing. Retrieved from https://researchgate.net
[8]Sivathanu, B. (2019). Adoption of digital payment systems in the era of demonetization in India: An empirical study. Journal of Science and Technology Policy. Retrieved from https://emerald.com
[9]Camenisch, J., Maurer, U., et al. (1997). Digital payment systems with passive anonymity-revoking trustees. Journal of Computer Security. Retrieved from https://journals.sagepub.com
[10] Biznext (2023). Digital security framework.