
**INDIVIDUAL ASSIGNMENT**

| | | |
|---|---|---|
| **NAME (TP NUMBER)** | **:** | Koo Wai Kit (TP081761) |
| **INTAKE CODE** | **:** | APUMF2406CYS |
| **MODULE TITLE** | **:** | Security Audit and Assessment (102024-YWR) |
| **MODULE LECTURER** | **:** | Yogeswaran A/L Nathan |
| **PROJECT TITLE** | | Security Audit and Assessment: Individual Assignment Section 1 (Research Proposal Work) |
| **DATE ASSIGNED** | **:** | 21 October 2024 |
| **DATE COMPLETED** | **:** | 3 February 2025 |

# Contents



# List of Figures

# 1. Abstract

The growth of digital payments has led the way for global commerce to be revolutionized, but it has also introduced complex security concerns that threaten the transactional integrity and trust in users. In order to identify critical issues and recent innovations in security audit assessments of the digital payment industry, this research proposal conducts a systematic literature review of several recently published papers. The key findings point out that the persistent vulnerabilities, such as sophisticated cyber-attacks, weak authentication mechanisms and gaps in the regulatory compliance make the digital payment ecosystems not very resilient. While blockchain, artificial intelligence, and machine learning have potential to improve audit processes, little research exists on using such emerging technologies and how they can be effectively included in security audit frameworks. By synthesizing current challenges and future directions, this research provides actionable insights to strengthen security audits, safeguard sensitive financial data and bolster trust in digital payment systems.

# 2. Introduction

As the industries move from the traditional face-to-face transactional model to platforms that are making their services available online, the growth of digital payment systems have been exponential. This shift has made possible unprecedented convenience and efficiency in processing payments, while simultaneously exposing all the financial ecosystems to new cyber threats. For instance, vulnerabilities in areas like user authentication, data encryption and network integrity continue to be a concern in security audit assessments regarding digital payment (Solat, 2017).

Since digital payments are becoming an undeniably key part of modern day commerce, the need to analyze and improve their security in rigorous audit processes has never been more important. Even with clear benefits of digital transformation brought by these systems, there are lots of challenges that these systems are facing, from sophisticated fraud techniques to the failure of protecting consumer's privacy, which can damage the integrity of consumer's trust and financial transactions.

This research proposal intends to review recently published papers systematically in order to map the main challenges and innovations in security auditing of the digital payment industry.

By doing so, it gives a clear concise view of the challenges to be understood to improve the security and resilience of digital payment systems.

# 3. Proposal

The core elements of the research proposal are specified in this section. The central inquiry of the study is presented in Section 1.3.1, and a rationale in Section 1.3.2 that explains why this topic is worth studying.

## 3.1 Research Question

The central research question of this study is:

- What are the major problems and challenges in the security audit assessment of the digital payment industry as described in recent literature?

## 3.2 Justification

A large number of security challenges have appeared from the rapid adoption of digital payment systems. Recent media reports have shown a sharp increase of sophisticated cyber-attacks against these platforms, resulting in massive financial damage and damages to the consumer trust. For example, in Ireland, payment fraud shot up by 26%, reaching €126 million in fraudulent transactions in 2023 alone (Kavanagh, 2025).

In reaction of these increasing threats, digital payment providers are also being subject to increased oversight by regulatory bodies. In the United States, the announcement was made by the Consumer Financial Protection Bureau (CFPB) that it is planning to regulate major fintech companies, such as Venmo and PayPal in the same way as traditional banks do (Hyatt, 2024). This shows how securing the complex interlinked digital payment sector has become extremely crucial.

Security audits for any digital payment system are very important because they will help to find vulnerabilities in the system. These play a critical role to assess risks and get a better overall security posture of these platforms. Audits help organizations to actively plan how to protect sensitive financial data and to protect consumer confidence by systematically assessing security environments (Martin, 2022).

As cyber threats are dynamic and the fields of digital payments are evolving, it is important to investigate the major issues and challenges of security audit assessment. This kind of research can guide more effective security strategies and policies to strengthen the digital finance system's resilience and trustworthiness.

# 4. Literature Review

This section synthesizes recent studies on security audit challenges in the digital payment industry with the analysis of the vulnerabilities, methodologies, emerging technology and research gap proposed for future directions of optimum audit practice. An overview of this section is illustrated in Figure 1.

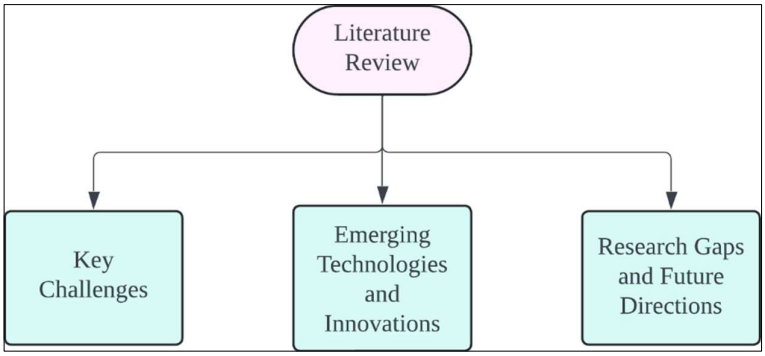


*Figure 1: Overview of literature review*

## 4.1 Key Challenges in Conducting Security Audits in the Digital Payment Industry

Security challenges in the digital payment industry are very important and can have a big influence on user trust, integrity of the transactions and overall system reliability. The challenges that arise from these are due to factors like technological vulnerabilities, user behaviour and regulatory compliance.

First, there are some serious technological challenges faced by digital payment systems. Cyber-attacks such as hacking, phishing and malware are serious threats to digital payment systems. Since these attacks are becoming more sophisticated, this makes it a major threat to user data and financial transactions. For instance, Zitha and Penceliah (2022) point to the fact that organisations need to invest in good security measures to protect user's information in online shopping platforms since failure to do so can result in a big data breach. Also, the reliance on mobile and internet connectivity can result in transaction failures and delays especially in areas with unstable connections (Musyaffi et al., 2022).

Second, the issue of data privacy is a crucial issue in digital payment systems, especially in the exposure of sensitive user data during transactions. Khan et al. (2024) points out that public exposure of data in financial transactions threatens user's privacy to such an extent that it is highly insecure. On the other hand, integrating technologies, such as blockchain, that give rise to increased security features also brings about new privacy challenges which have to be catered to (Usmiati, 2024).

Third, user trust and perception play a crucial role in the adoption of digital payment systems, as they are heavily influenced by perceived security. Zehra et al. (2024) finds that convenience, security and trust are all factors that influence consumers in this sector. Despite this, many users are still skeptical about security of their financial transactions, and making digital payment solutions popular remains an uphill task (Ramli et al., 2024). This is particularly important because, according to Vijayan and Duraisamy (2021), the security perception plays a direct role in the consumers' purchase intention when paying online.

Fourth, it is essential that the integrity of digital payment systems should be maintained through regulatory compliance and keeping to security standards such as Payment Card Industry Data Security Standard (PCI DSS). Nevertheless, there is a question about the effectiveness of these regulations on real world applications. Al-Qubati and Al-Shaibany (2024) stresses the need for the use of robust security measures such as encryption and protection of data to protect users' sensitive information. The problem is that all stakeholders must do the same thing consistently to keep the digital payment environment secure.

Fifth, new security challenges arise with emerging threats that are evolving at the same time as the digital payment systems. Ahmed et al. (2021) highlights that the rise of mobile payment platforms have introduced new vulnerabilities, as there are various security models that need to adapt continuously in the face of these threats. Furthermore, artificial intelligence in the payment systems does not only bring many opportunities but also comes with challenges which are aiming to secure the transactions and protect data at the same time (Nanda et al., 2024).

Lastly, digital payment ecosystems are complex and pose challenges in terms of security and conducting comprehensive audits. The varied security protocols and standards that exist in the organizations today create discrepancies in security protocols and practices due to the existence of numerous stakeholders such as the banks, payment processors, and the merchants. Ishrat

(2020) notes that effective auditing depends on strong collaboration and communication among stakeholders, but this level of coordination is hard to achieve.

### 4.2 Emerging Technologies and Innovations in Security Audits for the Digital Payment Industry

To further enhance the security, efficiency and reliability of financial transactions in the digital payment industry, it is imperative that new technologies and innovations of security audits for the industry continue to emerge. With the development of digital payment, several new technologies and approaches are increasingly being adopted in the security audit processes in order to cope with the growing challenges brought to the market from the cyber threats and regulatory requirements.

First, with the rise of the use of Artificial Intelligence (AI) and Machine Learning (ML) technologies, the security audits are now augmented through the automation of anomaly detection and possible fraud detection. These technologies analyze massive amounts of transaction data to find patterns related to possible fraud, and thus, allowing proactive risk management (Nanda et al., 2024). Moreover, AI-driven analytics can also be used by auditors to determine compliance to security standards and regulations, resulting in enhanced audit process (Wang et al., 2023).

Second, with the concept of tamper-proof ledger, blockchain is an emerging technology which provides a solution to keep the transactions secured and authenticated in a decentralized manner. The fact that it is inherently transparent and immutable makes for more efficient auditing processes. Utilizing the concept of blockchain, transactions can be tracked in real time, thus resulting in higher accountability and decreasing of the risk of fraud (Norbu et al., 2024). Besides, blockchain integration in digital payment systems greatly enhances trust and security because verification of the transactions does not depend on a central authority (Guntara et al., 2023).

Third, biometric technologies like fingerprint recognition and facial recognition are being increasingly used in digital payments with the intent of securing payments. These methods offer a higher level of security against the traditional password-based system as each of them is unique and difficult to replicate (Iqbal et al., 2020). Adding biometric authentication to payment systems will increase the trust of users and reduce the possibility of unauthorised access, thus improving the security audit process (Varalakshmi et al., 2024).

Lastly, Self Sovereign Identity (SSI) technologies enable users to control their digital identities and share only the information required during a transaction. It improves privacy and security by decreasing the amount of personal data delivered to payment systems (Satybaldy et al., 2022). Hence, SSI frameworks can be used by auditors to check whether data protection regulations are being followed and to verify users' identities without compromising on sensitive information.

### 4.3 Research Gaps and Future Directions of Security Audits in the Digital Payment Industry

There are several research gaps and future directions in the security audits of digital payment industry that should be addressed to make the audits more effective and reliable.

To start off, there lies a big potential to integrate emerging technologies like blockchain, AI, and ML as the integration of these technologies into security audit frameworks in the digital payment industry offers a great opportunity to boost the performance of the audit. However, few comprehensive studies have been conducted to assess how these technologies are integrated into an effective manner. Zitha and Penceliah (2022) affirm that organizations must focus on security in the face of advancing technologies. Future research should aim at integrating these technologies in the auditing processes, in order to improve fraud detection and risk management.

Apart from that, given the growing importance of data privacy and protection, there is an increased need for specific research guided on how to assure security audits guarantee compliance to regulations like GDPR and CCPA. The studies by Poudel (2023) indicate that security and privacy matter a lot in terms of adoption of digital payment systems. Future research should determine what are best practices on how to perform security audits prioritizing data privacy and adherence to the applicable regulations.

Furthermore, although security audits in digital payment systems are critical to security, there is lack of a comprehensive study of the factors of security and privacy risks in this domain. The existing literature primarily addresses perceived risks and user acceptance, without understanding the basic source of security vulnerabilities (Sahi et al., 2022).

# 5. Conclusion

In conclusion, this research proposal emphasizes the need to tackle the evolving security issues of digital payment systems. The systematic literature review uncovers large weaknesses which compromise the integrity as well as user's trust in these platforms due to technological drawbacks and data privacy problems, regulatory compliance problems and new cyber threats. Although emerging technologies such as blockchain, artificial intelligence or machine learning show huge potential for improving current security auditing framework, there are significant research gaps about how to integrate these technologies effectively to audit frameworks.

This study tries to provide the necessary basis for more solid security strategy development by mapping the present security audit challenges and key areas of further investigation. This research will not only provide the academic understandings of securing digital payment but will also provide some practical guidance value to industry practitioners and regulators working to improve the security and reliability of digital financial transactions.

# 6. References


Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). Security in next generation mobile payment systems: A comprehensive survey. *IEEE Access, 9*, 115932-115950.

Al-Qubati, S. A. and Al-Shaibany, N. A. (2024). E-wallet security readiness: a survey. *International Journal of Computer Science and Mobile Computing, 13*(3), 20-26. https://doi.org/10.47760/ijcsmc.2024.v13i03.003

Guntara, R. G., Nurfirmansyah, M. N., Ferdiansyah. (2023). Blockchain implementation in e-commerce to improve the security online transactions. *Journal of Scientific Research Education and Technology (Jsret), 2*(1), 328-338. https://doi.org/10.58526/jsret.v2i1.85

Kavanagh, M. (2025). *Fraudsters are outwitting us to steal our cash – spot the signs and stay safe online with these top tips*. The Irish Sun. https://www.thesun.ie/tech/14598908/online-fraud-scams-michael-kavanagh-customers-digital-safe-tips/?

Hyatt, D. (2024). *CFPB Will Treat Payment Apps Like Banks*. Investopedia. https://www.investopedia.com/cfpb-will-treat-payment-apps-like-banks-8749003?

Iqbal, S., Irfan, M., Ahsan, K., Hussain, M., Awais, M., Shiraz, M., … & Alghamdi, A. (2020). A novel mobile wallet model for elderly using fingerprint as authentication factor. *IEEE Access, 8*, 177405-177423. https://doi.org/10.1109/access.2020.3025429

Ishrat, Z. (2020). Compendious research of Escrow Payment - Focusing on Future Considerations, Trends and Applications. *European Journal of Business and Management Research*, *5*(4). https://doi.org/10.24018/ejbmr.2020.5.4.347

Khan, S., Rezk, W. M. E., Halim, M. A. A., & Qazaq, A. J. (2024). Navigating the bitcoin wave: an in-depth examination of its advantages and drawbacks in the contemporary economic landscape. *International Journal of Religion, 5*(10), 1884-1897. https://doi.org/10.61707/z1k2q603

Martin, C. (2022, March 23). *An integrated approach to security audits*. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2022/an-integrated-approach-to-security-audits?

Musyaffi, A., Gurendrawati, E., Afriadi, B., Oli, M., Widawati, Y., & Oktavia, R. (2022). Resistance of traditional smes in using digital payments: development of innovation resistance theory. *Human Behavior and Emerging Technologies, 2022*, 1-10. https://doi.org/10.1155/2022/7538042

Nanda, A. P., Veluri, K. K., & Beura, D. (2024). Role of ai in enhancing digital payment security. *African Journal of Biomedical Research*, 2112-2119. https://doi.org/10.53555/ajbr.v27i3s.2546

Norbu, T., Park, J. Y., Wong, K. W., & Cui, H. (2024). Factors affecting trust and acceptance for blockchain adoption in digital payment systems: a systematic review. *Future Internet, 16*(3), 106. https://doi.org/10.3390/fi16030106

Ramli, A. A., Mazlan, N. I. b., Harun, Z. F., & Mohd Yusof, Y. L. B. (2024). Factors influencing customers on the use of e-payment in klang valley. *Information Management and Business Review, 16*(2(I)S), 18-23. https://doi.org/10.22610/imbr.v16i2(i)s.3765

Sahi, A. M., Khalid, H., Abbas, A. F., Zedan, K., Khatib, S. F. A., & Al Amosh, H. (2022). The Research Trend of Security and Privacy in Digital Payment. *Informatics*, *9*(2), 32. https://doi.org/10.3390/informatics9020032

Satybaldy, A., Subedi, A., & Nowostawski, M. (2022). A framework for online document verification using self-sovereign identity technology. *Sensors, 22*(21), 8408. https://doi.org/10.3390/s22218408

Solat, S. (2017). Security of electronic payment systems: A comprehensive survey. *arXiv preprint arXiv:1701.04556*.

Shukla, A. (2022). Innovative way of using ai and ml to create and audit crypto token smart contract addresses in any block chain. *Journal of Artificial Intelligence & Cloud Computing*, 1–4. https://doi.org/10.47363/jaicc/2022(1)137

Usmiati, U., Huda, N., & Claudia, M. (2024). Qris, blockchain, ai, and iot: enhancing e-commerce transaction security. *International Conference of Business and Social Sciences*, 1013-1023. https://doi.org/10.24034/icobuss.v4i1.584

Varalakshmi, D., S, A., Baheti, A., Dugar, P., Pentala, P., & D, M. S. (2024). Cyber security in digital payments: an empirical study. *Asian Journal of Management and Commerce, 5*(1), 305-310. https://doi.org/10.22271/27084515.2024.v5.i1d.274

Vijayan, P. and Duraisamy, D. (2021). Effect of online payment security on the buying behaviour of the online shoppers in chennai city. *Journal of Contemporary Issues in Business and Government, 27*(02). https://doi.org/10.47750/cibg.2021.27.02.251

Wang, Q., Zong, B., Lin, Y., Li, Z., & Wang, L. (2023). The application of big data and artificial intelligence technology in enterprise information security management and risk assessment. *Journal of Organizational and End User Computing, 35*(1), 1-15. https://doi.org/10.4018/joeuc.326934

Zehra, F., Khan, F. S., Mazhar, S. S., Akhlaue, N., Haque, E., & Singh, A. (2024). Exploring consumer preferences and behaviour toward digital payment gateways in india. *International Journal of Experimental Research and Review, 41*(Spl Vol), 158-167. https://doi.org/10.52756/ijerr.2024.v41spl.013

Zitha, T. and Penceliah, D. (2022). Perceptions regarding digital payments in online shopping amongst millennials in kwazulu-natal, south africa. *African Journal of Inter/Multidisciplinary Studies, 4*(1), 338-349. https://doi.org/10.51415/ajims.v4i1.1047