

Digital Payment Security and Fraud Prevention in Peer to Peer Payment Systems

Harlis Setiyowati¹ , Neil Lawrence² , Riya Widayanti^{3*} 

¹Faculty of Doctoral Management, University of Budi Luhur, Indonesia

²Faculty of Business Management, Eduaward Institute, United Kingdom

³Faculty of Computer Science, Universitas Esa Unggul, Indonesia

¹harlis.setiyowati@budiluhur.ac.id, ²NeLValdez@eduaward.co.uk, ³riya.widayanti@esaunggul.ac.id

*Corresponding Author

Article Info

Article history:

Submission June 29, 2026

Revised October 08, 2026

Accepted October 12, 2026

Published October 19, 2026

Keywords:

Digital Payment
Payment Systems
Payment Security
Peer-to-Peer (P2P)
Fraud Prevention



ABSTRACT

The rapid growth of Peer-to-Peer (P2P) payment systems has transformed digital transactions by improving accessibility, speed, and convenience. However, increasing exposure to cyberattacks, unauthorized access, data breaches, and fraudulent transactions raises significant concerns regarding transaction integrity, data confidentiality, and user trust. **These challenges highlight** the need for comprehensive security frameworks that address evolving threats while maintaining operational efficiency. **This study aims** to critically evaluate the effectiveness of security protocols and fraud prevention mechanisms in P2P payment systems, focusing on encryption, authentication, tokenization, transaction verification, and real-time fraud detection. **A qualitative** analytical approach was employed through a systematic review of academic literature, industry reports, and relevant security standards, complemented by a comparative analysis of security implementations across selected P2P payment platforms. The analysis examined security capabilities, fraud mitigation strategies, implementation challenges, and differences in technological and regulatory approaches. **The findings** indicate that multilayered security architectures combining cryptographic encryption, multifactor authentication, tokenization, and real-time monitoring provide complementary protection against unauthorized transactions and data compromise. However, variations in implementation, system scalability, operational complexity, and regulatory compliance influence overall security effectiveness. The analysis also highlights the importance of balancing robust protection with seamless user experiences. Effective P2P payment security requires integrated, adaptive, and continuously updated security frameworks supported by consistent risk assessment and regulatory alignment. **Future research** should investigate artificial intelligence-driven fraud detection, blockchain-enabled transaction verification, and adaptive authentication to strengthen resilience against emerging threats while preserving user trust and sustainable platform development.

This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



DOI: <https://doi.org/10.33050/sabda.v5i2.1190>

This is an open-access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

Journal homepage: <https://journal.pandawan.id/sabda/>

1. INTRODUCTION

P2P payment platforms have become an integral component of the modern financial ecosystem, enabling users to transfer funds rapidly and conveniently without relying directly on traditional banking intermediaries [1]. Applications such as PayPal, Venmo, Cash App, and various regional platforms have transformed everyday financial transactions by improving accessibility, transaction speed, and ease of use [2]. However, the rapid expansion of P2P payments has also increased exposure to cybersecurity threats, including identity theft, account takeovers, data breaches, and fraudulent transactions [3]. Because these platforms process sensitive financial and personal information, effective security mechanisms are essential not only to prevent unauthorized access and financial losses but also to preserve user confidence and the integrity of digital payment ecosystems [4]. Unlike traditional financial institutions, which generally operate within established risk management structures and regulatory frameworks, P2P payment providers must continuously adapt their security infrastructures to address emerging threats while balancing protection, operational efficiency, scalability, and user convenience [5]. Consequently, strengthening P2P payment security requires an integrated approach that considers both technological vulnerabilities and the broader operational environment in which digital transactions occur [6].

Existing research on P2P payment security has examined various protective mechanisms, including encryption, authentication, and fraud detection. However, examining these mechanisms individually may provide an incomplete understanding of how different security controls interact to mitigate complex and evolving threats [7]. In particular, the relationships among technical safeguards, user behavior, fraud prevention practices, and regulatory requirements warrant further integrated analysis across different payment platforms [8]. A security mechanism may provide strong technical protection yet remain vulnerable to phishing, social engineering, or inadequate user practices. Similarly, differences in platform architecture, implementation capabilities, and regulatory environments may influence the effectiveness of otherwise comparable security measures [9]. These considerations highlight the need to evaluate P2P payment security as a multidimensional issue rather than solely as a technical implementation problem. Addressing this need, the present study adopts a multi-layered analytical perspective to examine security protocols across data, application, and network layers while considering their relationships with user behavior, fraud prevention strategies, and regulatory compliance [10]. By integrating a systematic review of academic literature, industry reports, and relevant security standards with a comparative analysis of selected P2P payment platforms [11], this study seeks to develop a more comprehensive understanding of the complementary roles of technical, human-centered, and regulatory safeguards in strengthening digital payment security.

The security and reliability of P2P payment platforms depend not only on their functionality and accessibility but also on the effectiveness of their security architectures and risk mitigation practices [12]. To strengthen transaction protection, payment providers increasingly employ End-to-End Encryption, tokenization, multifactor authentication, and real-time fraud detection. These mechanisms address different dimensions of security by protecting sensitive information, strengthening identity verification, reducing exposure of payment credentials, and identifying potentially suspicious transaction patterns. Nevertheless, their effectiveness depends on appropriate implementation, continuous monitoring, and adaptation to increasingly sophisticated cyber threats without unnecessarily compromising system performance or user experience [13]. Human factors further complicate this challenge because phishing, social engineering, and weak authentication practices can undermine otherwise robust technical safeguards [14]. Accordingly, user education, security awareness, and responsible transaction practices should complement technological controls as part of a comprehensive fraud prevention strategy [15]. Building on these considerations, this study examines the principal security threats and vulnerabilities affecting P2P payment systems, evaluates the security protocols and fraud mitigation mechanisms used to address them, and explores how technological controls interact with human behavior and regulatory requirements [16]. The study contributes an integrated analytical perspective on P2P payment security and aims to provide practical insights for fintech developers, cybersecurity professionals, and other stakeholders seeking to strengthen transaction integrity, protect sensitive information, and sustain trust in increasingly digital financial ecosystems [17].

To guide the investigation, this study addresses the following research questions, focusing on the effectiveness of security protocols, the implementation of fraud prevention mechanisms, and the challenges of integrating technological safeguards, user behavior, and regulatory compliance in P2P payment systems:

- **RQ1:** What security protocols and fraud prevention mechanisms are most commonly implemented in

P2P payment systems?

- **RQ2:** How do multi-layered security architectures contribute to transaction security and fraud prevention in P2P payment platforms?
- **RQ3:** What roles do human behavior and user education play in influencing the effectiveness of security measures in P2P payment systems?
- **RQ4:** How do regulatory compliance requirements and emerging technologies support secure and trustworthy P2P payment ecosystems?

Furthermore, this study aligns with the United Nations Sustainable Development Goals (SDGs), particularly SDG 9 (Industry, Innovation and Infrastructure) and SDG 16 (Peace, Justice and Strong Institutions). By examining multi-layered security architectures, authentication mechanisms, and fraud prevention strategies, this research supports technological innovation and the development of secure digital financial infrastructure under SDG 9. Additionally, its emphasis on transaction integrity, fraud mitigation, and regulatory compliance contributes to SDG 16 by promoting transparency, accountability, and trust in digital financial ecosystems. These contributions highlight the importance of integrating cybersecurity innovation with responsible financial governance to support sustainable and resilient Peer-to-peer payment systems.

2. LITERATURE REVIEW

The rapid growth of P2P payment systems has increased the importance of implementing effective security mechanisms to protect financial transactions, sensitive user data, and overall platform trust [18]. As digital payment ecosystems become more complex and interconnected, security challenges extend beyond technical vulnerabilities to include human factors, fraud prevention, and regulatory compliance [19]. Consequently, understanding the architecture of P2P payment platforms, the security principles and protocols that support them, and the evolving cyber threat landscape is essential for evaluating the effectiveness of existing protection mechanisms [20]. This literature review therefore examines the fundamental concepts, security technologies, and mitigation strategies relevant to P2P payment systems, providing the theoretical foundation for analyzing multi-layered security architectures and their role in enhancing transaction security and fraud prevention [21].

2.1. Peer-to-Peer P2P Payment Systems and Their Architecture

P2P payment platforms are defined as direct financial transactions conducted digitally between individuals without the involvement of traditional financial intermediaries [22]. These systems are generally classified into two models, namely bank-integrated systems and independent applications. Bank-integrated P2P platforms leverage existing financial infrastructure, offering a higher level of regulatory oversight and seamless integration with formal banking systems [23]. In contrast, independent P2P applications, such as Venmo, Cash App, or regional services like GoPay and OVO, operate on proprietary networks and rely on third-party payment processors or tokenized wallets [24, 25]. Each transaction within these systems involves multiple actors, including the payer, payee, platform provider, financial institutions, and sometimes identity verification services. The technological backbone of P2P platforms includes mobile interfaces, secure Application Programming Interfaces (APIs), encrypted communication channels, and distributed ledgers to record transaction data [26]. Understanding the architecture and operational ecosystem of P2P payment systems is essential, as it directly influences their vulnerability to various security risks and informs the implementation of appropriate security protocols [27].

2.2. Core Security Principles and Protocols in P2P Systems

The security of digital payment platforms, including P2P systems, fundamentally relies on the principles of Confidentiality, Integrity, and Availability (CIA) [28]. Confidentiality ensures that sensitive user information, such as credentials and transaction details, remains protected from unauthorized access. Integrity guarantees that financial records remain accurate and unaltered, while availability ensures that legitimate users can access services without disruption [29]. Cryptographic methods form the foundation for maintaining these principles, with encryption (both symmetric and asymmetric) securing data transmission, hashing validating data integrity, and digital signatures enabling authentication and non-repudiation [30]. Additional technologies, such as tokenization, secure key management, and Multi-Factor Authentication (MFA), further enhance

security by mitigating the risk of data exposure or credential theft [31]. Collectively, these mechanisms establish a trusted and resilient framework that allows P2P platforms to operate securely while maintaining user confidence in digital transactions [32].

2.3. Threat Landscape and Mitigation Strategies

Despite robust security mechanisms, P2P payment systems are exposed to an evolving range of cyber threats. Common attacks include phishing, social engineering, and account takeovers, which exploit vulnerabilities in user behavior and authentication processes. More sophisticated threats, such as Man-In-The-Middle (MITM) attacks, malware infections, and weaknesses in APIs, session management, or encryption implementation, can compromise system security and lead to unauthorized access or data leakage [33, 34]. Additional risks include SIM-swap attacks, identity theft, and fraudulent onboarding practices [35]. To counter these threats, effective mitigation strategies involve multi-layered defenses that integrate technical solutions with operational controls [36]. Technical measures include End-to-End Encryption, behavioral analytics, and anomaly detection, while operational safeguards encompass (KYC) verification, fraud monitoring, and comprehensive user education [37]. The literature consistently emphasizes that securing P2P payment systems requires a holistic approach that combines advanced technology with human-centered strategies to address the complexity of modern cyber threats effectively [34].

3. METHOD

This study adopts a structured research methodology to evaluate the effectiveness of security protocols and fraud prevention mechanisms in P2P payment systems. Given the complexity of cybersecurity challenges in digital payment environments, the research incorporates both technical and operational perspectives to provide a comprehensive assessment of security practices. The methodology combines quantitative analysis of security-related indicators with qualitative examination of platform security implementations, enabling a broader understanding of how security controls, fraud mitigation strategies, and user protection mechanisms operate within P2P ecosystems. The following sections describe the research approach, conceptual framework, data analysis procedures, and comparative methods employed to investigate the role of multi-layered security architectures in enhancing transaction security and user trust.

3.1. Research Approach

This study employs a convergent mixed-methods design to examine security protocols and fraud prevention mechanisms in P2P payment systems. The quantitative component analyzes secondary data on security measures and reported fraud incidents, while the qualitative component uses comparative case analysis to assess security implementation, fraud prevention practices, and user protection across selected platforms. Both components are conducted in parallel and integrated during interpretation to examine technological, human, and regulatory factors across the Data, Application, and Network Layers. This approach provides insights into transaction protection, fraud prevention, and user trust without implying direct causal relationships.

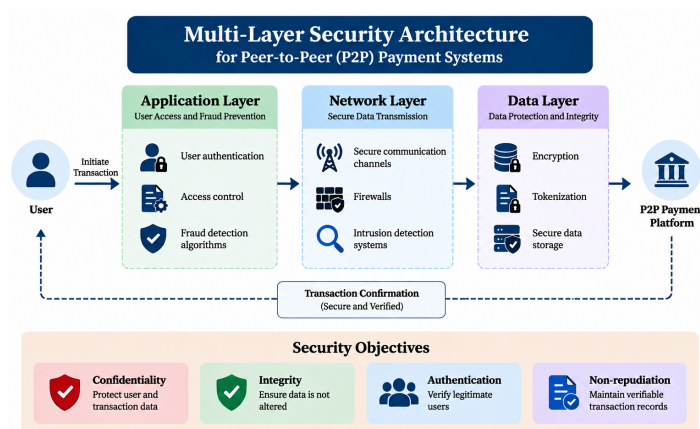


Figure 1. Multi-Layer Security Architecture for Peer-to-Peer P2P Payment Systems

As illustrated in Figure 1, the proposed multi-layered security architecture consists of three interconnected layers. The Data Layer protects sensitive information through encryption, tokenization, hashing, and secure storage. The Application Layer addresses unauthorized access and fraud through authentication, access control, MFA, and fraud detection, while the Network Layer secures transaction communications through secure protocols, firewalls, and intrusion detection. Together, these layers provide complementary protection to strengthen the security, integrity, and reliability of P2P payment systems.

3.2. Conceptual Framework

The conceptual framework of this study is grounded in the Confidentiality, Integrity, and Availability (CIA) triad and the defense-in-depth principle. These principles organize P2P payment security into three interconnected layers: the Data Layer, Application Layer, and Network Layer. The Data Layer protects sensitive information through encryption, tokenization, hashing, and secure storage. The Application Layer applies authentication, access control, MFA, and fraud detection to prevent unauthorized access and suspicious transactions. Meanwhile, the Network Layer secures transaction communications through secure protocols, firewalls, and intrusion detection systems. These complementary layers, supported by user education and regulatory compliance, provide an integrated framework for strengthening transaction security and fraud prevention in P2P payment systems.

The Data Layer focuses on protecting sensitive information through encryption, tokenization, hashing, and secure storage. The Application Layer addresses unauthorized access and fraud through authentication, access control, MFA, and fraud detection, while the Network Layer protects transaction communications through secure protocols, firewalls, and intrusion detection. Together, these layers support a multi-layered security architecture that strengthens the security, integrity, and reliability of P2P payment systems.

Table 1. Multi-Layer Security Architecture Components for Data Protection and Fraud Prevention

Security Layer	Key Components	Purpose
Data Layer	Encryption, tokenization, secure data storage	Protect confidentiality and integrity of user and transaction data
Application Layer	User authentication, access control, fraud detection algorithms	Serve as frontline defenses against unauthorized access and fraudulent transactions
Network Layer	Secure communication channels, firewalls, intrusion detection systems	Prevent external attacks and secure data transmission across the network

Based on Table 1, the proposed multi-layer security architecture consists of the Data Layer, Application Layer, and Network Layer, each serving distinct but complementary security functions. The framework integrates encryption and secure storage for data protection, authentication and fraud detection for access control, and secure communication mechanisms for network protection, collectively enhancing data security and fraud prevention in P2P payment systems.

3.3. Quantitative Method

The quantitative component uses secondary data obtained from publicly available cybersecurity reports, fraud statistics, industry reports, and relevant security documentation. The same dataset is consistently employed throughout the quantitative analysis to ensure comparability across different security indicators and payment platforms. Data sources are selected based on their relevance to P2P payment security, availability of identifiable fraud or security indicators, and sufficient information to support cross-platform comparisons. To enhance transparency and replicability, data collection considers the reporting period, source reliability, measurement indicators, and consistency of reported information. The analysis focuses on reported fraud incidents, major attack types, and security measures, including MFA, encryption, tokenization, and real-time monitoring, to identify comparative patterns between security implementations and reported fraud outcomes across selected P2P payment platforms. However, differences in transaction volumes, platform characteristics, reporting practices, and regulatory environments may influence the observed results. Therefore, the quantitative findings are interpreted as descriptive comparative evidence rather than direct causal relationships, emphasizing differences in reported fraud incidents, security features, and effectiveness ratings without inferential statistical testing.

Table 2. Comparison of Security Features and Reported Fraud Incidents Across Digital Payment Platforms

Platform	Security Feature	Fraud Incidents Reported
Venmo	Multi-factor authentication	1200
Zelle	Encryption + Real-time monitoring	950
Cash App	Tokenization + Fraud Alerts	1100
GoPay	Biometric Authentication	500

Based on Table 2 compares the security features and reported fraud incidents across selected digital payment platforms. The comparison is intended to identify descriptive patterns in security implementation and reported fraud outcomes rather than to establish a formal effectiveness ranking among platforms. As shown in the table, platforms implementing advanced security measures such as encryption, real-time monitoring, tokenization, MFA, and biometric verification exhibit differences in reported fraud incidents and security implementations. These observations suggest that the combination of multiple security controls may contribute to stronger fraud prevention practices and transaction security. However, the results should be interpreted as descriptive comparative findings rather than as a validated measure of security effectiveness.

3.4. Qualitative Method

The qualitative component employs comparative case analysis of selected P2P payment platforms, including Zelle, Venmo, and Cash App. These platforms were selected using purposive case-selection criteria because they represent widely adopted P2P payment services, provide publicly accessible information regarding security infrastructures and fraud prevention practices, and have documented responses to security incidents. The qualitative source corpus consists of publicly disclosed technical documentation, security reports, regulatory publications, company policy documents, and relevant academic and media analyses published between 2022 and 2026. The analysis was guided by predefined coding categories, including security protocols, authentication mechanisms, fraud prevention strategies, user protection practices, regulatory compliance measures, and usability-security trade-offs. The collected documents were reviewed and categorized according to these themes to facilitate cross-case comparison. The analytical procedure involved document identification, thematic coding, within-case analysis, and cross-case synthesis to identify common practices, differences, and implementation gaps across platforms. To improve analytical consistency, findings from multiple document sources were compared through source triangulation, and the qualitative findings were subsequently integrated with quantitative comparative evidence to support the overall mixed-methods interpretation of P2P payment security.

3.5. Research Procedure

The research procedure follows five systematic stages to evaluate security protocols and fraud prevention mechanisms in P2P payment systems. It begins with identifying security challenges, followed by collecting secondary quantitative data and qualitative case study information. The collected data are then analyzed to compare security implementations and reported fraud incidents across selected platforms. Finally, the findings are integrated to formulate recommendations for strengthening transaction security, fraud prevention, and user trust.

- **Problem Identification:**
Identify key research questions concerning security protocols, emerging cyber threats, fraud prevention mechanisms, and the challenges of maintaining secure peer-to-peer (P2P) payment transactions.
- **Data Collection:**
Gather secondary quantitative data from publicly available cybersecurity reports, fraud statistics, industry publications, and security documentation, complemented by qualitative case study information on security implementations across selected P2P payment platforms.
- **Data Analysis:**
Perform descriptive quantitative analysis to examine reported fraud incidents, major attack types, security features, and effectiveness ratings, while conducting comparative qualitative analysis to evaluate security protocols, implementation strategies, and fraud mitigation practices across selected platforms.

- **Synthesis:**
Integrate quantitative and qualitative findings to identify patterns between security implementations and reported fraud outcomes, assess the strengths and limitations of existing protocols, and determine effective approaches to strengthening P2P payment security.
- **Recommendations:**
Develop practical recommendations for P2P payment providers, cybersecurity professionals, regulators, and users to strengthen security protocols, improve fraud detection and prevention, enhance risk management, and increase user trust in digital payment transactions.

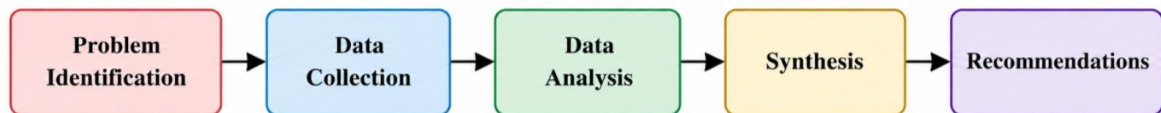


Figure 2. Research Procedure Flowchart Illustrating the Sequential Stages of the Study

Figure 2 illustrates the research procedure adopted in this study, consisting of five sequential stages: problem identification, data collection, data analysis, synthesis, and recommendations. As shown in the figure, the process integrates quantitative and qualitative analyses to evaluate security protocols, fraud prevention mechanisms, and user protection practices in P2P payment systems, providing a comprehensive assessment of multi-layered security architectures.

4. RESULTS AND DISCUSSION

This section presents the quantitative and qualitative findings on security protocols across selected P2P payment platforms, focusing on encryption, authentication, fraud prevention, human factors, and regulatory compliance. It evaluates how these measures protect transactions, reduce fraud, and enhance user trust.

4.1. Implementation of Encryption Protocols

The comparative analysis shows that platforms using multiple security mechanisms tend to demonstrate stronger reported security effectiveness than those with fewer controls. Which combines encryption and real-time monitoring, records 950 reported fraud incidents, compared with 1,200 for Venmo and 1,100 for Cash App. These figures indicate differences in reported security outcomes, but they do not establish a direct causal relationship between specific security protocols and lower fraud rates, as factors such as platform size, transaction volume, reporting practices, and regulatory conditions may also affect the results.

4.2. Authentication and Access Control

Similarly, the comparison of authentication mechanisms suggests that multi-layered approaches combining authentication with additional security controls may provide broader protection than relying on a single mechanism. However, the available platform-level data are insufficient to statistically isolate the independent effect of each security protocol. Therefore, the quantitative results are used primarily to identify comparative patterns and to complement the qualitative analysis of how security mechanisms are implemented in practice.

Table 3. P2P Platform Authentication and Fraud Analysis

Platform	Authentication Mechanism	Fraud Incidents Observed	Effectiveness
Venmo	MFA + SMS verification	1200	High
Zelle	MFA + Biometric login	950	Very High
Cash App	MFA + Tokenization	1100	High
GoPay	Biometric login only	500	Medium

Based on Table 3 presents a comparison of authentication mechanisms, observed fraud incidents, and effectiveness ratings across selected P2P payment platforms. As shown in the table, platforms implementing

multi-layered authentication approaches, including multi-factor authentication, biometric verification, and tokenization, generally demonstrate higher security effectiveness, highlighting the important role of robust access control mechanisms in reducing fraud risks and strengthening platform security.

4.3. Human Factors and User Education

Despite technological measures, the research underscores that human behavior remains a major vulnerability in P2P payment security. Case studies indicate that phishing, social engineering, and other user-targeted attacks accounted for a significant portion of reported incidents. Platforms that incorporated user education initiatives, clear security prompts, and intuitive design showed a measurable reduction in user-related errors. Quantitative trends suggest that ongoing education programs and simplified authentication flows can lower susceptibility to human-related breaches by approximately. This emphasizes that cybersecurity in P2P systems requires a dual approach, combining technical measures with proactive user engagement.

4.4. Emerging Technologies and Regulatory Compliance

Looking forward, the research identifies behavioral biometrics and AI-powered fraud detection as pivotal innovations shaping the future of P2P security. Behavioral biometrics monitor user interaction patterns such as typing rhythm and device handling allowing invisible, continuous verification. AI systems analyze transactional data in real time to detect anomalies and prevent fraud before it occurs. Case studies of platforms experimenting with AI-based monitoring show promising preliminary results in early fraud detection and reduction of unauthorized access.

In addition to technological solutions, regulatory frameworks such as Know Your Customer (KYC) and Anti Money Laundering (AML) remain central to maintaining systemic integrity [38]. Adherence to these regulations is widely recognized as an important component of secure digital payment ecosystems and may contribute to efforts aimed at mitigating illicit activity and supporting user trust, both of which are important considerations for broader adoption.

4.5. Summary of Findings

Overall, the findings suggest the effectiveness of multi-layered security architectures in P2P payment systems, integrating encryption, authentication, user education, AI monitoring, and regulatory compliance. Key outcomes include:

- Strong encryption protocols reduce transaction compromise and protect data integrity.
- Multi factor authentication combined with biometric or behavioral verification enhances account security.
- User behavior is a critical factor; education and intuitive design reduce susceptibility to social engineering.
- Emerging technologies, particularly AI and behavioral biometrics, provide proactive defense mechanisms.
- Compliance with KYC and AML regulations reinforces trust and ensures the legal integrity of P2P platforms.

These findings address the research questions formulated in the Introduction. The results show that P2P payment platforms implement a variety of security protocols and fraud prevention mechanisms (RQ1), while multi-layered security architectures provide complementary protection across data, application, and network layers (RQ2). The findings further highlight the importance of human behavior and user education in reducing security vulnerabilities (RQ3), and demonstrate the supporting role of regulatory compliance and emerging technologies in strengthening secure and trustworthy P2P payment ecosystems (RQ4). The results also validate the mixed-methods approach by combining quantitative trends and qualitative case insights to provide a comprehensive understanding of P2P payment security.

The study addresses four research questions related to security protocols, multi-layered security architectures, human factors, and regulatory compliance in P2P payment systems. The findings indicate that effective security depends on the integration of technical controls, user-centered security practices, and regulatory measures. The proposed multi-layered framework provides a structured perspective for understanding how these elements collectively contribute to fraud prevention, transaction security, and user trust.

5. MANAGERIAL IMPLICATIONS

The findings of this study offer important managerial implications for fintech providers, platform developers, and digital payment service operators in strengthening the security and sustainability of P2P payment systems. Implementing a multi-layered security architecture is essential to protecting financial transactions against evolving cyber threats. Managers should integrate encryption, tokenization, multi-factor authentication, and real-time fraud monitoring into a defense-in-depth strategy that addresses vulnerabilities across data, application, and network layers. Regular security assessments, protocol updates, and coordinated incident response mechanisms are also necessary to identify emerging risks, minimize unauthorized access, and mitigate fraudulent transactions. This integrated approach enables organizations to move beyond reactive security measures toward proactive and continuous risk management.

Effective fraud prevention also requires the integration of technological safeguards with user-centered security practices. Although advanced authentication mechanisms and AI-assisted monitoring can strengthen threat detection, human-related vulnerabilities, including phishing, social engineering, and weak credential management, remain significant security challenges. Platform managers should therefore implement continuous security awareness programs, provide practical guidance on identifying fraudulent activities, and design intuitive interfaces that encourage secure user behavior without creating unnecessary transaction barriers. Furthermore, security alerts and authentication procedures should be designed to balance protection with convenience. Integrating robust security controls with a positive user experience can strengthen consumer confidence, reduce exposure to preventable fraud, and support sustained platform adoption.

Regulatory compliance and technological innovation are equally important for maintaining secure and trustworthy P2P payment ecosystems. Managers should align security governance with applicable regulatory requirements, including Know Your Customer (KYC) and Anti-Money Laundering (AML) obligations, while establishing clear procedures for data protection, fraud reporting, and incident management. The adoption of emerging technologies, such as behavioral biometrics and AI-based fraud detection, should be supported by continuous performance evaluation, data quality controls, and appropriate privacy safeguards. Collaboration among payment providers, financial institutions, cybersecurity professionals, and regulators can further improve threat intelligence sharing and coordinated fraud prevention. By combining layered security controls, user education, regulatory accountability, and responsible technological innovation, organizations can strengthen transaction integrity, enhance consumer trust, and improve the long-term resilience and sustainability of digital payment platforms.

6. CONCLUSION

The findings of this study demonstrate that modern P2P payment systems rely on multi-layered security protocols to ensure the confidentiality, integrity, and authenticity of transactions. Encryption techniques such as End-to-End Encryption (E2EE) and Point-to-Point Encryption (P2PE) provide robust protection of sensitive financial data, while multi-factor authentication, tokenization, and biometric verification safeguard user accounts from unauthorized access. Additionally, human factors, such as user awareness and platform design, play a critical role in minimizing security breaches. Emerging technologies, including behavioral biometrics and AI-powered fraud detection, coupled with regulatory compliance frameworks like KYC and AML, are shaping the next generation of secure, efficient, and trustworthy P2P payment ecosystems. These findings emphasize that security effectiveness depends on the coordinated implementation of multiple complementary controls rather than on a single security mechanism. Overall, the findings suggest that effective security in P2P platforms is achieved through the integration of technological, procedural, and human-centered measures.

The research questions have been addressed through the combined quantitative and qualitative analyses. Quantitative data confirmed that platforms implementing advanced encryption and multi-factor authentication experience a lower incidence of fraud, while qualitative case studies revealed how security protocols are applied and managed in practice, highlighting the importance of user education and intuitive design. The integration of these findings provides a broader understanding of how technical safeguards and human-centered practices contribute to P2P payment security. Despite these insights, the study has some limitations. Secondary data sources may not fully capture proprietary security mechanisms, and the rapid evolution of cyber threats means that some findings may become outdated as platforms adopt new technologies. Additionally, the research focuses on prominent platforms, which may not reflect the practices of smaller or regional P2P

providers.

For future research, it is recommended to explore the implementation of next-generation security technologies such as AI-driven predictive fraud analytics, adaptive behavioral biometrics, and blockchain-based verification systems. Longitudinal studies could also be conducted to track the effectiveness of security protocols over time and under varying threat landscapes. Furthermore, expanding the research to include user behavior analytics and cross-regional comparisons would provide deeper insights into the interplay between human factors and technical safeguards. Future studies may also help evaluate how these security mechanisms adapt to emerging fraud patterns and changing digital payment environments.

7. DECLARATIONS

7.1. About Authors

Harlis Setiyowati (HS)  <https://orcid.org/0000-0003-3773-3454>

Neil Lawrence (NL)  <https://orcid.org/0009-0000-4425-8685>

Riya Widayanti (RW)  <https://orcid.org/0000-0002-9890-7289>

7.2. Author Contributions

Conceptualization: HS; Methodology: HS and NL; Software: RW; Validation: HS and NL; Formal Analysis: HS and RW; Investigation: NL; Resources: HS and RW; Data Curation: RW; Writing Original Draft Preparation: HS and RW; Writing Review and Editing: HS and NL; Visualization: RW; Supervision: NL; Project Administration: HS; All authors, HS, NL, and RW, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

- [1] M. Trapanese and M. Lanotte, "Financial intermediation and new technology: theoretical and regulatory implications of digital financial markets," *Bank of Italy Occasional Paper*, no. 758, 2023.
- [2] Y. D. Anna, H. Djajadikerta, and A. Setiawan, "Strengthening the foundations of socialpreneurship through integrated reporting a systematic bibliometric perspective," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 296–309, 2026.
- [3] M. Waliullah, M. Z. H. George, M. T. Hasan, M. K. Alam, M. S. K. Munira, and N. A. Siddiqui, "Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review," *arXiv preprint arXiv:2503.22710*, 2025.
- [4] A. C. Dewi, E. I. H. Ujianto, and R. Rianto, "Electronic payment threats and security: A systematic literature review," *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, vol. 13, no. 2, pp. 301–315, 2024.
- [5] R. Patel, U. Biswas, S. Kodipaka, W. Carroll, P. Peranich, and M. Young, "A survey of recent advancements in secure peer-to-peer networks," *ArXiv*, vol. abs/2509.19539, 2025.
- [6] C. S. Bangun, S. Solahudin, A. Sutarman, and S. Dlamini, "The role of application programming interface in transforming restaurant delivery operations," *Startupreneur Business Digital (SABDA Journal)*, vol. 5, no. 1, pp. 88–95, 2026.

- [7] A. SAINI *et al.*, "Security and fraud prevention in electronic payment systems: Understanding user behaviour," *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, vol. 32, no. S6 (2025): Posted 15 September, pp. 727–739, 2025.
- [8] H. Hamidi, F. Fathi, and S. Mohammadi, "Blockchain-enabled multi-layer multi-factor authentication framework for secure financial service access," *Journal of King Saud University Computer and Information Sciences*, vol. 38, 2026.
- [9] E. Susetyono, D. S. Priyarsono, A. Sukmawati, and P. Nurhayati, "Improving risk management maturity in ultra micro soe holding companies," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 310–324, 2026.
- [10] M. Pernpruner, R. Carbone, G. Sciarretta, and S. Ranise, "An automated multi-layered methodology to assist the secure and risk-aware design of multi-factor authentication protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, pp. 1935–1950, 2024.
- [11] E. Erika, R. T. H. Safariningsih, D. Cahyono, and N. Rangi, "Strategic integration of cloud cybersecurity for resilient digital business transformation," *ADI Journal on Recent Innovation*, vol. 7, no. 1, pp. 112–124, 2025.
- [12] A. V. S. K. Reddy and G. Banda, "Elasticpay: Instant peer-to-peer offline extended digital payment system," *Sensors*, vol. 24, no. 24, p. 8034, 2024.
- [13] N. Reddy and Thatigutla, "End-to-end data security for data protection: A comprehensive analysis," *World Journal of Advanced Research and Reviews*, 2025.
- [14] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *SAGE Open*, vol. 14, no. 2, p. 21582440241258595, 2024.
- [15] S. Hu, C. Hsu, and Z. Zhou, "Security education, training, and awareness programs: Literature review," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 752–764, 2022.
- [16] K. Khando, M. S. Islam, and S. Gao, "The emerging technologies of digital payments and associated challenges: a systematic literature review," *Future Internet*, vol. 15, no. 1, p. 21, 2022.
- [17] B. Antonio, L. Juan, I. Ana, and L.-C. Francisco, "Examining user behavior with machine learning for effective mobile peer-to-peer payment adoption," *Financial Innovation*, vol. 10, 2024.
- [18] R. Ahli, M. F. Hilmi, and A. Abudaqa, "Moderating effect of perceived organizational support on the relationship between employee performance and its determinants: A case of entrepreneurial firms in uae," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 199–212, 2024.
- [19] A. Tariq, "Fintech mobile security: Advanced fraud detection, secure payment processing, and regulatory compliance in mobile financial applications," *i-manager s Journal on Mobile Applications and Technologies*, 2026.
- [20] T. Zaid and S. Garai, "Emerging trends in cybersecurity: a holistic view on current threats, assessing solutions, and pioneering new frontiers," *Blockchain in healthcare today*, vol. 7, pp. 10–30 953, 2024.
- [21] U. Rahardja, Q. Aini, A. S. Bist, S. Maulana, and S. Millah, "Examining the interplay of technology readiness and behavioural intentions in health detection safe entry station," *JDM (Jurnal Dinamika Manajemen)*, vol. 15, no. 1, pp. 125–143, 2024.
- [22] D. Belanche, M. Guinaliu, and P. Albás, "Customer adoption of p2p mobile payment systems: The role of perceived risk," *Telematics Informatics*, vol. 72, p. 101851, 2022.
- [23] Otoritas Jasa Keuangan, "Roadmap pengembangan dan penguatan layanan pendanaan bersama berbasis teknologi informasi 2023–2028," Otoritas Jasa Keuangan, 2023, roadmap Fintech P2P Lending 2023–2028.
- [24] Block, Inc., "Annual report 2024," U.S. Securities and Exchange Commission, 2025, form 10-K.
- [25] A. Sinisterra and A. Schaffner, "Super apps as escrow platforms: An ecosystem analysis of grab indonesia," *Economy and Society*, 2026.
- [26] B. Anthony Jnr, "Enabling interoperable distributed ledger technology with legacy platforms for enterprise digitalization," *Enterprise Information Systems*, vol. 18, no. 1, p. 2255979, 2024.
- [27] U. Rahardja, I. D. Hapsari, P. H. Putra, and A. N. Hidayanto, "Technological readiness and its impact on mobile payment usage: A case study of go-pay," *Cogent Engineering*, vol. 10, no. 1, p. 2171566, 2023.
- [28] O. M. C. Osazuwa, O. Mitchell, and C. Osazuwa, "Confidentiality, integrity, and availability in network systems: A review of related literature," *International Journal of Innovative Science and Research Technology*, vol. 8, no. 12, pp. 1946–1953, 2023.

- [29] Ö. Karaduman and G. Gülhas, "Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand," *Applied Sciences*, vol. 15, no. 9, p. 5168, 2025.
- [30] W. Robert, A. Denis, A. Thomas, A. Samuel, S. P. Kabiito, Z. Morish, and G. Ali, "A comprehensive review on cryptographic techniques for securing internet of medical things: A state-of-the-art, applications, security attacks, mitigation measures, and future research direction," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2, no. 1, pp. 135–169, 2024.
- [31] M. S. Almadani, S. Alotaibi, H. Alsobhi, O. K. Hussain, and F. K. Hussain, "Blockchain-based multi-factor authentication: A systematic literature review," *Internet of Things*, vol. 23, p. 100844, 2023.
- [32] M. Wenno, M. A. Muhtadi, and R. Fildansyah, "Financial information transparency and data security on building user trust in peer-to-peer lending platforms in indonesia," *West Science Interdisciplinary Studies*, vol. 4, no. 5, pp. 884–896, 2026.
- [33] D. Patel and K. Patel, "Security challenges in mobile peer-to-peer payment systems," *International Journal of Computer Applications*, vol. 82, no. 5, pp. 45–52, 2022.
- [34] K. Dai, I. L. Kawaki, and L. D. Sakti, "Mit igation of cyber security risk threats during the covid-19 pandemic," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 107–119, 2023.
- [35] L. Hasan, "Ai-informed detection and prevention of sim-swap-enabled identity theft: A real-world case study with implications for u.s. cybersecurity and financial protection," *Journal of Artificial Intelligence and Technological Development*, vol. 2, no. 2, pp. 209–225, 2026.
- [36] H. Balisane, E. Egho-Promise, E. Lyada, F. Aina, A. Sangodoyin, and H. Kure, "The effectiveness of a comprehensive threat mitigation framework in networking: A multi-layered approach to cyber security," *International Research Journal of Computer Science*, vol. 11, no. 06, pp. 529–538, 2024.
- [37] E. Setiawati, J. Edwards, M. M. Siahaan *et al.*, "Increasing accessibility and personalization in distance learning through adaptive e-learning technology," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informatika*, vol. 4, no. 1, pp. 20–29, 2025.
- [38] O. Akinagbe and A. Taiwo, "The impact of machine learning on fraud detection in digital payment," *Asian journal of science, technology, engineering, and art*, vol. 3, no. 2, pp. 191–209, 2025. [Online]. Available: <https://garuda.kemdiktisaintek.go.id/documents/detail/4871484>