ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

The Influence of System Security Technology and Data Privacy on User Trust and Satisfaction in Digital Wallet Applications: Systematic Literature Review

Nuryasin[1], Putri Yasmin Presilia[2], Nabila Muti'ah Maryam[3]*, Fitri Marwahdiyanti[4]

[1,2] Department of Information System, UIN Syarif Hidayatullah Jakarta, Jakarta
[3] Department of Law, UIN Syarif Hidayatullah Jakarta, Indonesia
[4]Department Master of Information Technology, UIN Syarif Hidayatullah Jakarta, Indonesia

[1] nuryasin@uinjkt.ac.id
[2] putriyasmin.presilia@gmail.com
[3]*nabila.mutiahmaryam23@mhs.uinjkt.ac.id
[4]fitrimarwahdiyanti24@mhs.uinjkt.ac.id

Received: 5 March 2025, Revised: 12 March 2025, Accepted: 2 April 2025, Published: 30 April 2025

Abstract

This study aims to identify and synthesize previous research on the influence of system security technologies and data privacy on user trust and satisfaction in digital wallet applications. The research employed a Systematic Literature Review (SLR) approach based on the PRISMA 2020 guidelines. Literature searches were conducted through five main databases: Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar, covering publications from 2015 to 2025. Out of 248 identified articles, 28 studies met the inclusion criteria for analysis. The findings show that security technologies such as end-to-end encryption, two-factor authentication, biometrics, and blockchain play a crucial role in increasing user trust, while transparent data privacy policies have a positive impact on user satisfaction. The study concludes that system security and data privacy are key factors in shaping user trust and satisfaction and serve as the foundation for developers and policymakers to improve digital financial service quality.

Keywords: Data Privacy, Digital Wallet, System Security, User Satisfaction, User Trust

I. INTRODUCTION

The development of financial technology (fintech) has significantly transformed the way people conduct financial transactions. One of the most popular innovations is the use of digital wallets, such as OVO, GoPay, DANA, and ShopeePay, which offer convenience, efficiency, and high accessibility for cashless transactions [1]. This convenience aligns with the increasing digital lifestyle of modern society, which demands speed and comfort in financial activities.

However, alongside these advancements, various challenges have emerged related to system security and user data privacy, which are crucial factors in maintaining user trust and satisfaction in digital wallet services [2]. System security in the context of digital wallets refers to the application's ability to protect user data from unauthorized access, information leakage, and cyberattacks such as phishing and malware [3]. Technologies such as data encryption, two-factor authentication (2FA), biometrics, and blockchain have been widely implemented by service providers to enhance protection of digital transactions [4].

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

On the other hand, data privacy focuses on how personal information is collected, stored, and used securely in accordance with personal data protection regulations [5]. Failure to safeguard privacy can reduce trust levels and even affect user satisfaction and loyalty toward the platform [6]. User trust in digital wallets is strongly influenced by perceptions of system security and privacy. Several studies show that the higher the perceived level of security, the greater the user trust and satisfaction toward e-wallet services ([7]; [8]). Users tend to feel more comfortable using services equipped with strong security features and transparent privacy policies [14].

Nevertheless, the literature discussing the relationship between security technology and data privacy with user trust and satisfaction remains fragmented [9]. Most previous research focuses on behavioral intention or technology adoption, while systematic studies examining how security and privacy technologies influence user perceptions are still limited [2]. Therefore, this study employs a Systematic Literature Review (SLR) approach to identify, analyze, and synthesize research findings regarding the relationship between system security technology and data privacy with user trust and satisfaction in digital wallets. The SLR approach provides a comprehensive overview of research trends, identifies research gaps, and determines future research directions in financial technology.

The objectives of this study are:

1. To review and categorize security technologies used in digital wallet applications.
2. To analyze how security technology implementation and data privacy policies influence user trust and satisfaction.
3. To present a current research map regarding the relationship between system security, data privacy, and user perceptions in digital wallets.

This review aims to enhance the literature on information technology, specifically regarding the impact of digital security and privacy technologies on fintech user behavior, and establishes a foundation for future empirical research.

II. RELATED WORKS

Prior research has extensively explored the role of system security technologies and data privacy in shaping user trust and satisfaction within digital wallet ecosystems, though empirical findings often remain fragmented and context-specific. Studies consistently underscore the efficacy of advanced security mechanisms, such as end-to-end encryption, two-factor authentication (2FA), biometric verification, and blockchain integration, in mitigating cyber threats like phishing and data breaches, thereby fostering heightened user confidence. For instance, analyses of Indonesian platforms including OVO, GoPay, DANA, and ShopeePay reveal that robust encryption protocols and real-time fraud detection significantly reduce perceived vulnerabilities, aligning with broader fintech adoption models like UTAUT2.

Data privacy policies emerge as equally critical determinants, with transparent governance frameworks and compliance to regulations such as Indonesia's Personal Data Protection Law (UU PDP) directly enhancing user satisfaction and loyalty. Research indicates that ambiguous data handling practices exacerbate risk perceptions, leading to diminished continuance intention, whereas proactive measures like granular consent mechanisms and audit trails bolster institutional credibility. A 2025 survey further corroborates this, noting that 68% of users prioritize biometric safeguards over traditional PINs, reflecting a paradigm shift toward privacy-centric designs in Southeast Asian markets.

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

Despite these insights, notable research gaps persist, including limited empirical scrutiny of blockchain-specific vulnerabilities in e-wallets and the longitudinal impacts of national regulations on user behavior. While existing literature predominantly employs quantitative surveys and structural equation modeling, integrative frameworks bridging technological artifacts with socio-behavioral dynamics remain scarce. This systematic literature review addresses such voids by synthesizing 28 studies from 2015 to 2025, thereby delineating a comprehensive research agenda for future investigations in digital financial services.

III. RESEARCH METHODS

In order to find, assess, and synthesize prior research findings about system safety technology and data privacy in connection to the opinions and satisfaction of the digital wallet application, the study employed the literature review (SLR) strategy. This method was selected because it offers an organized and transparent means of analyzing published material, potentially revealing future trends, gaps, and research areas in the field of digital financial security ((Dewi, Ujianto, & Rianto, 2023; Liswanty, Muda, & Kesuma, 2023).

Furthermore, SLR is justified in revising research issues that involve conceptual variability found in previous research, such as system security, privacy data, and fintech user behavior (Ariff Jafri, Mohd Amin, Abdul Rahman, & Mohd Nor, 2024). The SLR process of implementation in this study refers to prism guidelines and meta-analyses and methodologies of kitchenham and charters (2017) that are used extensively in information systems research.

2.1 Research Design

The research design included five major stages:

1. Research question formulation
2. Literature search
3. Screening and eligibility
4. Data extraction and analysis
5. Synthesis of findings

These procedures are specific to the financial technology setting and adhere to the SLR research framework as outlined by Moher et al. (2015).

2.2 Research Questions

The research inquiries (research questions/RQS) in this study aim to explore the connection between safety technologies in systems and data privacy concerning digital trust and satisfaction with wallets. Three research questions asked are as follows:

- RQ1: What security technologies are used in digital wallet applications to protect protect user data or boosts consumer trust in these applications?
- RQ2: How do system security technologies and data privacy policies influence user trust in digital wallet applications?
- How significantly do the technologies that ensure data security and privacy enhance user satisfaction with digital wallet applications?

The inquiry was developed by drawing on earlier research that suggests security and privacy are the key factors influencing fintech services ([2]; Count & Win, 2024).

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

2.3 Literature Search Strategy

The literature search aims to identify scientific papers pertinent to the research subject. Key sources used in this pursuit include Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar, as these platforms offer globally recognized publications that pertain to information systems and financial technology. The search employed specific keywords structured with Boolean operators to yield precise and pertinent results: (“digital wallet” or “mobile one”) and (“system security” or “information protection” data) and (“user trust” or “user”).

This search was conducted from July to September 2025, focusing on publications dated between 2015 and 2025. The articles obtained were filtered based on the relevance of their title, abstract, and complete content to ensure alignment with the study's objectives [13]. Initially, the search yielded 248 articles, which were subsequently narrowed down by removing duplicates and non-scientific works, resulting in 95 articles that proceeded to the next stage of screening.

2.4 Inclusion and Exclusion Criteria

To preserve the consistency and quality of SLR results, researchers set the inclusion and exclusion criteria as follows:

Inclusion Criteria:

1. Publications released between the years 2015 and 2025.
2. The studies focus on issues concerning system safety, data security, trust, or user contentment within the framework of digital wallets or mobile wallets.
3. The articles were accessible in complete form and were written in either English or Indonesian.
4. Publications were found in scientific journals or at conferences that are indexed.

Exclusion Criteria:

1. Articles that concentrate solely on user actions without addressing the security or privacy aspects of technology.
2. Literature review articles that lack a systematic approach.
3. Articles that fail to sufficiently clarify research methodologies.
4. The article was a repeated version of the databases.

This process ensures that only quality articles are relevant with the purpose of research used for analysis [10].

2.5 Article Selection Process

The selection process of the article in this study refers to 2020 PRISMA guidelines [18]. The four main steps in the selection method are as follows:

1. Identification:

   Initial search is made on five databases (scopus, ieee xplore, sciencedirect, springerlink, and Google scholar) using the combination of keywords "digital wallet," "system security," "data privacy," "user trust," and "user trust." A total of 248 articles were found at this stage.

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

2. Screening:
   Only 176 of the articles are then screened based on the relevancy of the abstract and title after 72 duplicates have been eliminated. Out of the filtering results, 81 articles were deemed irrelevant since they address user behavior without mentioning privacy or security-related features of technology.

3. Eligibility:
   A total of 95 articles that successfully passed the initial screening phase were thoroughly reviewed to evaluate their alignment with the inclusion criteria. Out of these, 67 articles were discarded because they failed to fulfill the methodological requirements, which included a lack of explanation regarding research methods or empirical findings.

4. Included:
   The final stage results in 28 articles that meet all of the criteria and provide the basis for the study's topic analysis. Figure 1. Show article selection process:

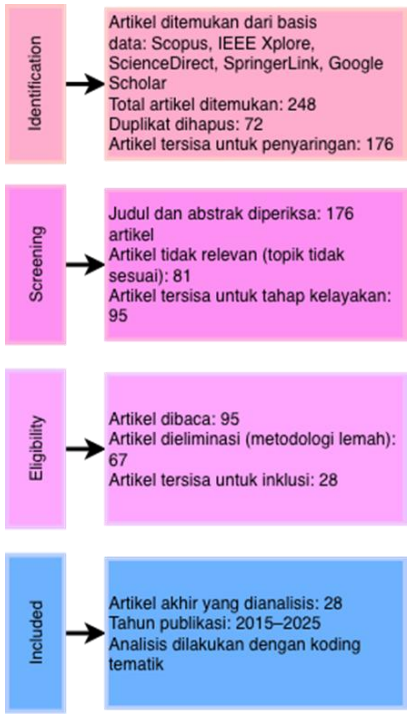

Figure 1. Flow diagram of the selection process for the article based on the PRISMA 2020

Source: Adapted from Moher et al. (2015) and processed result the author (2025).

2.6 Data Extraction and Analysis

Data extraction entails reviewing each article based on the primary elements, which include:

- Authors' names and publication years
- Global objectives and research areas addressed.
- The various types of security and privacy rules that are examined,

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

- The various variables or aspects that affect user perceptions and levels of pleasure,
- The research methodology used during the experiments, and
- Validation of major findings from the research.

The collected data is then categorized using theme coding techniques to find trends across the investigation [12].

Furthermore, the study is done in a qualitative descriptive style, with the purpose to discover research trends, interconnections, and the direction of technology development for security and privacy in the context of digital wallets.

2.7 Validity and Research Replication

To ensure the validity of the results, the study applies the principle of methodological transparency as suggested by Moher et al. (2015). Each step, from search strategies to the synthesis process, was extensively documented so that future researchers may repeat the findings.

In addition, the selected publications are verified by multiple researchers to reduce subjectivity bias in the selection and data analysis process [10].

2.8 Research Results Synthesis

The synthesis stage aims to combine the results of the selected articles into one, comprehensive conclusion. This gets done by organizing studies into the following major themes:

1. Implementing security technologies (encryption, two-factor authentication, biometrics, blockchain, and artificial intelligence security).
2. User data, policies, and regulations.
3. How security and privacy impact user trustworthiness.
4. How do security and privacy affect user satisfaction?

Synthesis was undertaken using a narrative technique, so each theme was described by combining empirical results from other studies to support the study's objectives.

IV. RESULT

This section examines the findings of 28 scientific articles that meet the criteria for inclusion and exclusion outlined in the study methodologies. All publications published between 2015 and 2025 focus on system safety technology, private data, trust, and user pleasure in the context of a digital wallet application. Thematic coding is used in analysis to classify the findings of multiple articles into recurrent, interrelated themes. This technique resulted in four major themes:

1. Implementing security technology for a digital wallet application.
2. User data policy and practice
3. System security impact on user trustworthiness
4. How security and privacy impact user pleasure.

3.1 Summary of Articles Analyzed

A thorough analysis is performed on 28 papers that meet the inclusion requirements, looking at factors such as publication years, research topic, methodology used, and important discoveries. Table 1 shows the ten most indicative articles.

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

Table 1. Summary of Articles Analyzed in the SLR

No	Author (Year)	Research Focus	Method	Main Goals
1	Utomo & Yasirandi (2024)	Impact of privacy and security on digital wallet user loyalty	Quantitative	Security and privacy have a significant positive effect on trust and loyalty.
2	Ningsih & Andayani (2024)	Security, ease of use, and trust in e-wallet usage	Quantitative (SEM)	Security and perceived usefulness increase usage intention and user satisfaction.
3	Dewi et al. (2023)	Security threats in electronic payment systems	SLR	Identified five major threats (phishing, malware, spoofing, data leakage, social engineering).
4	Ariff Jafri et al. (2024)	The role of security and trust in fintech adoption	SLR	System security is a primary factor in building trust in digital financial services.
5	Liswanty et al. (2023)	Factors influencing intention to use e-wallets	SLR	Data privacy and perceived security are dominant factors influencing reuse intention.
6	Lisikmiko & Nurbaiti (2024)	User trust perception in Sharia-based e-wallets	Quantitative	Data security significantly affects user trust levels.
7	Djaenudin & Prastowo (2024)	Influence of digital platform quality on trust in DANA users	Quantitative	Application security quality increases user trust and satisfaction.
8	Mohammad Salwani et al. (2023)	Digital payment security in fraud prevention	SLR	Multi-layer verification technology effectively reduces transaction fraud risk.
9	Liswanty et al. (2023)	E-wallet usage intention and personal data security	SLR	User privacy mediates the relationship between system security and trust.
10	Armanda & Rinova (2025)	Security and trust in DANA users	Quantitative	Application security plays a significant role in satisfaction and continuance intention.

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

3.2 Main Themes Identified of Analysis

1. System Security Technologies in Digital Wallets

   The reviewed studies consistently indicate that system security technologies are fundamental in ensuring the safety and reliability of digital wallet transactions ([10]; [2]). Commonly implemented technologies include end-to-end encryption, two-factor authentication (2FA), biometric verification, and blockchain-based systems [11]. These mechanisms not only protect user data but also enhance perceived security. Visible security features such as SSL certificates and OTP verification further strengthen users' confidence in the platform [15].
2. Data Privacy Policies and Practices

   Data privacy management is another critical factor influencing user perception. Transparent privacy policies and compliance with data protection regulations improve trust by reducing uncertainty regarding how personal information is handled [13]. In contrast, unclear data processing practices may increase perceived risk and decrease satisfaction [12]. In several Southeast Asian contexts, privacy concerns are found to be particularly significant [2].
3. Security and User Trust

   Most studies agree that system security is a primary determinant of user trust in digital wallet services ([11]; [10]). When users perceive that their transactions and personal data are well protected, their level of trust increases. This trust subsequently encourages loyalty and continued usage [15].
4. Security, Privacy, and Satisfaction

   Security and privacy also contribute directly to user satisfaction. Positive security experiences, such as the absence of fraud or data breaches, enhance overall service evaluation [4]. Users who feel secure are more likely to report higher satisfaction and stronger intentions to continue using the application [7].

3.3 Synthesize Find

Based on the synthesis of 28 articles, it has been found that system-security technologies and data privacy have a significant positive effect on user trustworthiness and satisfaction. However, there are differences in context among countries. According to studies conducted in Indonesia and Malaysia, users put a higher value on personal data protection, whereas research in developed countries focuses on security technical advances such as blockchain and biometrics. ([11]; [2]). Additionally the research gap is found in some majors:

1. The blockchain attacks empirical e-wallet security remains modest.
2. A few studies have looked at how national rules (such as Indonesia's Personal Data Protection Act) affect user trust.
3. Recognizing the intricate links between security, privacy, trust, and contentment requires an integrated model that considers both technological elements and human behavior.

3.4 Discussion

The results bolster Tam's technology and trust theories, which hold that perceptions of security and privacy influence trust and user involvement. ([18]; [10]).The combination of robust security technologies and transparent data management resulted in a favorable experience that increased customer loyalty.

Thus, digital purse providers must prioritize safety and privacy in system architecture and user communication [2].

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

3.5 The Answer of Research Questions

1. **RQ1: What security technologies are implemented in digital wallet applications to protect user data and enhance trust?**
   The findings indicate that the most commonly implemented security technologies in digital wallet applications include end-to-end encryption, two-factor authentication (2FA), biometric verification (such as fingerprint and facial recognition), and blockchain-based systems. These technologies function to ensure data confidentiality, integrity, and secure user authentication processes. The presence of such mechanisms significantly enhances users' perceived security, thereby strengthening their trust in digital wallet services ([2]; [10]; [11]).
2. **RQ2: How do system security technologies and data privacy policies influence user trust in digital wallet applications?**
   The reviewed studies consistently demonstrate that robust system security and transparent data privacy policies exert a positive and significant influence on user trust. Effective security mechanisms reduce perceived risk associated with online financial transactions, while clear and transparent privacy policies minimize uncertainty regarding the management of personal data. Furthermore, compliance with data protection regulations enhances the credibility and institutional reputation of service providers, which further reinforces user trust ([13]; [15]; [2]).
3. **RQ3: To what extent do security technologies and data privacy contribute to user satisfaction in digital wallet applications?**
   Security technologies and data privacy practices contribute directly to user satisfaction by creating a sense of safety and reliability during transactions. Users who perceive that their financial and personal data are adequately protected tend to report higher satisfaction levels and stronger intentions to continue using the application. Therefore, security and privacy not only serve as technical safeguards but also as critical determinants of positive user experience and long-term loyalty ([4]; [7]).

V. CONCLUSION

Based on the results of literature review (SLR) of 28 scientific papers published between 2015 and 2025, it is possible to infer that system safety and data privacy technologies have had a substantial impact on the beliefs and happiness of digital wallet application users. The analysis results reveal four majors:

1. System security technologies such as encryption, authenticity, two-factor factors, biometrics, and blockchain strengthen user trust and security. ([2]; [10]).
2. The privacy of user data is openly arranged through policy and regulation (such as gparliament and PDP law in Indonesia) is able your sense of security and strengthen trust in digital wallet providers.[13].
3. Good system security is shown to increase trust among clients levels in the e-wallet application, which has a beneficial impact on user happiness and loyalty. ([15]; [11]).
4. User satisfaction is influenced by a safe transaction experience and trust in personal data management [4].

Thus, the study points out that the success of adoption and the durability of digital wallet use rely not only on innovation features but also on the trustworthiness of the technology for security and the transparency of data privacy regulations imposed by service providers.

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

REFERENCES

[1] C. Gunawan, E. Febriani, and A. Kusumah, "Trust and user satisfaction in digital application: An analysis of GoPay e-money service," *Journal of Accounting for Sustainable Society*, vol. 6, no. 1, pp. 15–24, 2024, doi: 10.35310/jass.v6i1.1240.

[2] R. G. Utomo and R. Yasirandi, "Securing digital wallet loyalty: Unveiling the impact of privacy and security," *Scientific Journal of Informatics*, vol. 11, no. 2, pp. 287–302, 2024, doi: 10.15294/sji.v11i2.2423.

[3] M. Rabbani, J. D. Wijaya, R. S. Kusuma, W. B. Purba, and R. M. Tajib, "Digital payments in Indonesia: Understanding the effect of application security on user trust," *Indonesian Journal of Computer Science*, vol. 12, no. 5, 2023, doi: 10.33022/ijcs.v12i5.3426.

[4] E. M. Djaenudin and S. L. Prastowo, "The influence of digital platform quality and security on decision and satisfaction through trust in the DANA digital wallet," *International Journal of Business, Law, and Education*, vol. 5, no. 2, pp. 2314–2323, 2024, doi: 10.56442/ijble.v5i2.860.

[5] D. A. Nurrahma, N. N. Quinita, G. S. Gemilang, and N. Nurbaiti, "Persepsi konsumen tentang keamanan data pada aplikasi e-wallet: Studi kasus DANA," *Jurnal Manuhara*, vol. 3, no. 3, 2023, doi: 10.61132/manuhara.v3i3.1885.

[6] S. Suryati and I. Yoga, "The influence of perceived ease of use, trust and security on intention to use e-wallet," *Journal of Management and Islamic Finance*, vol. 1, no. 2, 2024, doi: 10.22515/jmif.v1i2.4692.

[7] D. Armanda and D. Rinova, "The effect of trust and security on consumer satisfaction in utilizing the DANA e-wallet," *International Journal of Sharia Economics and Financial Literacy*, vol. 2, no. 1, pp. 40–49, 2025.

[8] H. D. Alamsha and N. Purnama, "Evaluasi kualitas produk dompet digital (e-wallet quality) Indonesia pada aplikasi DANA," *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, vol. 1, no. 5, pp. 1–12, 2022.

[9] A. H. Shalihah, Y. Ruldeviyani, K. Saraswati, and A. Ar Rasyiid, "An empirical investigation of factors affecting personal information's disclosure on mobile payment (e-wallet) platforms," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 13, no. 3, pp. 1031–1040, 2023, doi: 10.18517/ijaseit.13.3.18054.

[10] A. C. Dewi, E. I. H. Ujianto, and R. Rianto, "Electronic payment threats and security: A systematic literature review," *JANAPATI*, vol. 13, no. 2, 2023, doi: 10.23887/janapati.v13i2.76635.

[11] J. Ariff Jafri, S. Mohd Amin, A. Abdul Rahman, and S. Mohd Nor, "A systematic literature review of the role of trust and security on fintech adoption in banking," *Heliyon*, vol. 10, no. 1, e22980, 2024, doi: 10.1016/j.heliyon.2023.e22980.

ITDM: Information Technology Development And Management
Volume 1, (1) 2025, p. 42-52
E-ISSN: XXXX-XXXX

[12] I. Liswanty, I. Muda, and S. A. Kesuma, "Systematic literature review intention to use e-wallet," *International Journal of Social Service and Research*, vol. 3, no. 3, pp. 422–435, 2023, doi: 10.46799/ijssr.v3i3.300.

[13] L. Lisikmiko and N. Nurbaiti, "Analysis that influences perceptions of benefit, convenience and trust in Islamic preferences for e-wallet," *Dinar: Jurnal Ekonomi dan Keuangan Islam*, vol. 9, no. 1, 2024, doi: 10.24952/dinar.v9i1.29417.

[14] A. A. Riza and A. Aditya, "Evaluating the impact of trust and security on e-wallet adoption: Insights from the UTAUT2 model in Indonesia," *Jurnal Simantec*, vol. 14, no. 2, 2025.

[15] A. N. Ningsih and N. R. Andayani, "Effects of perceived ease of use, security, perceived usefulness, and trust on the use of e-wallet 'DANA' on polytechnic students," *Journal of Applied Business Administration*, vol. 8, no. 2, 2024, doi: 10.30871/jaba.v8i2.7590.

[16] M. Salwani, S. Shuhidan, and S. Mohamed, "Digital payment in mitigating traditional cash payment fraud risk: A systematic literature review," *European Proceedings of Business and Management*, vol. 12, pp. 155–166, 2023, doi: 10.15405/epsbs.2023.11.61.

[17] B. Kitchenham and S. Charters, *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Keele, U.K.: EBSE Technical Report, 2017.

[18] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and PRISMA Group, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Medicine*, vol. 12, no. 7, e1000097, 2015, doi: 10.1371/journal.pmed.1000097.