Banking Strategies for Maintaining Customer Security and Trust in Digital Services: A Literature Review

Drajat Sugiarto[1], Hwihanus[2]
[1,2]Universitas 17 Agustus Surabaya, Indonesia
Email: 20201052600013@surel.untag-sby.ac.id

Abstract

The rapid digitalization of banking services has expanded customers' access to financial transactions, but at the same time, it has exposed banks and customers to increasing cyber threats, fraud, and misuse of personal data, which directly challenge the foundation of customer trust. This study aims to synthesize banking strategies for maintaining customer security and trust in digital services and to formulate an integrated conceptual model that explains how security strategies are transformed into sustainable customer trust. Using an integrative literature review approach, this study examines peer-reviewed journal articles, policy reports from international institutions, and Indonesian regulatory instruments addressing digital banking security, cyber risks, fraud prevention, data protection, and customer trust. The synthesis results show that perceived security consistently functions as a primary antecedent of customer trust and the continued use of digital banking services. The reviewed evidence also indicates that multilayered technological security measures, including multifactor and biometric authentication as well as machine learning-based fraud detection, constitute the operational core of security strategies. Regulatory compliance and data governance, particularly cyber resilience requirements and personal data protection principles, provide institutional assurance that strengthens customer confidence beyond technological features. The findings also indicate that customer education and transparent crisis responses are essential because social engineering exploits human vulnerabilities, while security incidents can rapidly erode trust if banks respond inadequately. Based on these findings, this study proposes an integrated security–trust strategy model consisting of technological, institutional, and human-relational layers that collectively shape perceived security, trust, and continued use. This model contributes to the digital banking literature by consolidating fragmented findings into a coherent framework for subsequent empirical validation, while also offering practical guidance for bank managers, regulators, and policymakers in building a resilient and trustworthy digital banking ecosystem.

Keywords: *Digital Banking, Cybersecurity, Customer Trust, Perceived Security, Banking Strategy.*

A. INTRODUCTION

The digital transformation of the banking industry has fundamentally changed the way customers access financial services, shifting most transactions from physical branch offices to mobile applications, internet banking, and other digital channels. Mobile banking has become a primary channel for customers to manage accounts, transfer funds, and make payments, and its adoption is increasingly influenced by factors beyond functional convenience (Merhi et al., 2019). In emerging markets, mobile banking is also positioned as an instrument for expanding financial access, and research in Indonesia shows that banks continue to seek strategies to accelerate adoption among communities that remain underserved by conventional banking

services (Sebayang et al., 2024). The expansion of digital channels enables banks to reduce operational costs, improve service speed, and offer more personalized financial products.

At the same time, the shift of financial activities to digital environments means that customers increasingly entrust their funds, identities, and personal data to systems that they cannot physically observe. This condition makes digital banking a service domain in which the relationship between banks and their customers depends heavily on perceptions of the reliability and protection provided by the underlying technology. Research on mobile banking adoption across various national contexts consistently shows that security, privacy, and trust have become integral elements in customers' decisions to use digital banking services (Merhi et al., 2019; Apau et al., 2025). The growth of digital banking is not merely a technological shift but also a transformation of the fundamental basis on which customers evaluate and maintain their relationships with financial institutions. Banks are no longer evaluated solely on the diversity of their products and the convenience of their services, but also on their ability to ensure that every digital interaction takes place securely. This development indicates that the strategic value of digital banking services increasingly depends on the effectiveness of banks in managing security and trust as inseparable components of the customer experience.

Behind its benefits in expanding digital banking, this development is accompanied by a significant increase in cyber threats and digital fraud. A systematic review of online banking security reported that the increasing use of digital banking technology has coincided with a surge in online banking fraud, which has evolved into an organized global problem involving phishing, denial-of-service attacks, Trojan horses, malware, identity theft, and computer viruses (Ahmad et al., 2024). Another systematic review identified identity theft, malware attacks, phishing, and vishing as recurring threats that hinder digital banking adoption (Cele & Kwenda, 2025). In the Indonesian context, social engineering schemes such as malicious application files, phishing, pretexting, baiting, and quid pro quo have caused actual financial losses for digital banking customers, while existing consumer protection provisions have not fully addressed the specific circumstances of social engineering victims (Utami & Purwanti, 2025). The vulnerability of the banking sector is also evident in the cyberattack against Bank Syariah Indonesia in May 2023, which triggered intense public discussion on social media regarding the perpetrators of the attack and the alleged data breach (Timur et al., 2024).

Such incidents demonstrate that security failures are not merely technical disruptions but events that directly affect customers' confidence in institutions. Empirical evidence from mobile banking users in Indonesia also shows that some customers have personally experienced security issues, including the risks of data theft and online fraud, and that perceived security significantly influences the continued use of mobile banking (Sahata Sitanggang et al., 2024). This situation places banks in a difficult position because the digital channels that create competitive advantages also introduce new points of vulnerability. The intangible nature of digital

transactions makes customers dependent on banks' ability to detect, prevent, and respond to threats that they cannot see. Understanding these challenges is an important starting point for examining the strategies employed by banks to maintain security and trust in digital services.

Customer trust and perceived security emerge as two interrelated and central constructs in understanding customer behavior in digital banking. Trust has long been conceptualized as the willingness of one party to be vulnerable to the actions of another party based on the expectation that the other party will perform actions that are important to the trusting party, and this willingness is shaped by perceptions of the ability, benevolence, and integrity of the trusted party (Mayer et al., 1995). In electronic commerce, trust has been integrated with technology acceptance models, demonstrating that trust works alongside perceived usefulness in shaping usage intentions and that institutional assurances contribute to trust formation (Gefen et al., 2003). In the context of mobile banking, perceived security, perceived privacy, and trust have been shown to significantly influence behavioral intentions to adopt mobile banking in both developing and developed countries (Merhi et al., 2019).

More recent evidence indicates that security, institutional trust, and technology trust influence users' intentions to adopt mobile banking applications, while stronger security and privacy protections are recommended as central components of adoption strategies (Apau et al., 2025). Perceived risk has also been shown to negatively affect customer trust and attitudes toward mobile banking, whereas perceived security and trust play key roles in increasing adoption (Almaiah et al., 2023). Trust and perceived risk also moderate the relationship between behavioral intentions and actual mobile banking use (Kumar et al., 2023). These findings indicate that security and trust are not peripheral considerations but fundamental mechanisms determining whether customers begin and continue using digital banking services. Security provides an objective and perceptual basis for confidence, while trust transforms that confidence into a willingness to rely on banks under conditions of uncertainty. The interaction between these two constructs establishes a strong theoretical foundation for examining banking strategies in digital services.

Previous studies have substantially advanced the understanding of security and trust in digital banking; however, the existing body of knowledge remains fragmented across various disciplinary perspectives. Behavioral studies have largely examined perceived security, perceived risk, and trust as determinants of adoption and continued use within extended technology acceptance frameworks (Merhi et al., 2019; Almaiah et al., 2023; Apau et al., 2025). Technical studies have focused on the development and evaluation of machine learning models for detecting fraudulent financial transactions, often without examining how these technologies shape customer perceptions (Ali et al., 2022; Hernandez Aros et al., 2024). Legal studies in Indonesia have concentrated on consumer protection, social engineering, and personal data protection in the banking sector, emphasizing regulatory gaps and banks' responsibilities toward customers (Utami & Purwanti, 2025; Yudha, 2025). Other studies have examined customer responses to specific cyber incidents, such as

public sentiment and the potential for customer switching following the cyberattack against Bank Syariah Indonesia (Timur et al., 2024). These fragmented perspectives provide valuable insights but limit the development of an integrated explanation of how technological, institutional, and customer-oriented strategies collectively contribute to customer trust. Behavioral literature often treats security as a perception without detailing the strategic measures that generate it, while technical and legal literature frequently describes these measures without explaining how they translate into customer trust. This separation makes it difficult for academics and practitioners to understand the combination of strategies required to sustain trust in an increasingly complex digital banking environment. The absence of an integrative framework is a critical concern because cyber threats simultaneously exploit technological weaknesses and human vulnerabilities. Addressing this gap requires a broader conceptual perspective capable of connecting security strategies, institutional assurances, customer capabilities, and trust outcomes within a single explanatory structure. This unresolved issue provides a strong rationale for synthesizing the literature on banking strategies for maintaining customer security and trust in digital services.

Based on these research gaps, this study aims to synthesize banking strategies for maintaining customer security and trust in digital services and to develop an integrated conceptual model that explains how these strategies shape customer trust and continued use. Rather than examining technological, regulatory, and customer-oriented measures separately, this study conceptualizes them as complementary layers within a single security–trust strategy. This study employs an integrative literature review approach, which is suitable for evaluating, critiquing, and synthesizing literature on a research topic, thereby enabling the emergence of new theoretical frameworks and perspectives (Snyder, 2019). This approach is particularly appropriate because the research topic draws on behavioral, technical, legal, and managerial research streams that employ different methods and units of analysis. This study is guided by three research questions. First, how does the literature explain the relationship between security and customer trust in digital banking services? Second, what strategies are used and recommended for banks to maintain customer security in digital services? Third, how can these strategies be integrated into a conceptual model that explains the formation and maintenance of customer trust?

The answers to these questions are expected to clarify how security strategies are translated into perceived security and trust, as well as how trust can be maintained when security incidents occur. This study pays particular attention to the Indonesian context, where the rapid growth of digital banking, major cyber incidents in the Islamic banking sector, and the enactment of personal data protection legislation provide a relevant background for examining these strategies (Law No. 27 of 2022; Timur et al., 2024). The resulting model is expected to serve as a conceptual reference for subsequent empirical research on digital banking security and trust across various institutional and cultural contexts.

This study offers both theoretical and practical contributions to the digital banking literature. From a theoretical perspective, this study consolidates behavioral, technical, legal, and managerial findings into an integrated model that explains how banking strategies are transformed into perceived security, trust, and continued use. This integration extends adoption-oriented models that emphasize perceived security and trust as determinants of intention by detailing the strategic sources that generate these perceptions (Merhi et al., 2019; Apau et al., 2025). This study also extends trust theory in digital banking by explaining how banks' ability, integrity, and benevolence can be signaled through security technologies, regulatory compliance, customer education, and crisis communication (Mayer et al., 1995). Furthermore, this study incorporates the dimension of post-incident trust, which has received less attention in adoption studies but becomes crucial when cyberattacks and data breaches occur (Kuipers & Schonheit, 2022; Timur et al., 2024).

From a practical perspective, the findings of this study can help bank managers design security strategies that combine authentication, fraud detection, data governance, customer education, and incident response, rather than relying on isolated measures. Regulators and policymakers can use these conceptual insights to strengthen implementing regulations, cyber resilience requirements, and customer protection mechanisms in digital banking (Financial Services Authority, 2022; Utami & Purwanti, 2025). The proposed model can also serve as a reference for researchers seeking to validate the relationships between security strategies, perceived security, trust, and continued use across various banking sectors, including Islamic banking. Overall, this study provides a comprehensive conceptual understanding that bridges academic research and managerial practice while supporting the development of a secure and trustworthy digital banking ecosystem.

B. METHOD

This study employs an integrative literature review to synthesize banking strategies for maintaining customer security and trust in digital services and to develop a conceptual model of the relationships among these strategies. An integrative review was selected because it aims to evaluate, critique, and synthesize literature on a research topic, allowing new theoretical frameworks and perspectives to emerge, and is suitable for developing preliminary conceptual models in emerging research areas (Snyder, 2019). The literature search was conducted through Google Scholar, publisher platforms hosting Scopus-indexed journals, including Emerald Insight, MDPI, Springer Nature, Palgrave Macmillan, and Elsevier, the RePEc/IDEAS bibliographic database, and Indonesian journal portals. The search used combinations of keywords, including "digital banking," "mobile banking," "internet banking," "perceived security," "customer trust," "perceived risk," "cybersecurity," "fraud detection," "biometric authentication," "social engineering," "phishing," "data breach," and "personal data protection," as well as their Indonesian equivalents, such as "security," "customer trust," and "digital banking".

The inclusion criteria required sources to be peer-reviewed journal articles, official regulatory instruments, or reports from international institutions; directly address security, fraud, data protection, or trust in digital banking or closely related digital financial services; and have bibliographic details that could be verified through publisher websites or DOIs. This review prioritized publications from 2019 to 2025 to capture recent developments, while also including seminal works on trust that remain foundational to theoretical development (Mayer et al., 1995; Gefen et al., 2003). Sources that could not be verified, were insufficiently relevant to the research questions, or had not undergone peer review, such as unpublished undergraduate theses and preprints, were excluded from the analysis. The final corpus consisted of 25 sources, comprising 22 peer-reviewed journal articles, one World Bank policy report, and two Indonesian regulatory instruments, namely the Personal Data Protection Law and the Financial Services Authority Regulation on the Implementation of Information Technology by Commercial Banks.

Each source was read iteratively to extract its research context, theoretical perspective, methodology, and main findings. The extracted information was then thematically coded according to the strategic dimensions discussed, resulting in five themes: security as the foundation of trust, technological safeguards, regulation and data governance, customer education and crisis response, and integrative strategies. The mapping of sources to these themes is presented in Table 1. The analysis emphasized conceptual interpretation rather than statistical aggregation because the objective of the study was theory development rather than hypothesis testing. Convergent findings, divergent findings, and unresolved issues were compared across studies, after which complementary insights were linked into an integrated conceptual model expressed through a series of propositions for subsequent empirical validation.

Table 1. Thematic Mapping of the Reviewed Literature

Theme	Synthesis Focus	Sources
Security as the Foundation of Trust	Perceived security, privacy, risk, and trust as drivers of adoption and continued use	Mayer et al. (1995); Gefen et al. (2003); Merhi et al. (2019); Almaiah et al. (2023); Kumar et al. (2023); Che et al. (2023); Ansori & Nugroho (2024); Sahata Sitanggang et al. (2024); Apau et al. (2025)
Technological Safeguards	Authentication, biometrics, and machine learning-based fraud detection	Ali et al. (2022); World Bank (2023); Bhat et al. (2024); Hernandez Aros et al. (2024); Sebayang et al. (2024); Dichev et al. (2025)
Regulation and Data Governance	Cyber resilience regulations, personal data protection, and	Law No. 27 of 2022; Financial Services Authority (2022); Utami & Purwanti (2025); Yudha (2025)

	consumer protection	
Customer Education and Crisis Response	Cyber threats that exploit customers, financial literacy, incident communication, and post-attack responses	Kuipers & Schonheit (2022); Ahmad et al. (2024); Isaia et al. (2024); Rahman et al. (2024); Timur et al. (2024); Cele & Kwenda (2025)

Source: Author's Synthesis

C. RESULTS AND DISCUSSION

1. Security as a Fundamental Determinant of Customer Trust in Digital Banking Services

The literature synthesis identifies security as a fundamental determinant underlying customer trust in digital banking services. Across various national contexts, perceived security consistently emerges as a significant predictor of customers' intentions to adopt mobile banking and the trust they place in these services. Evidence from Lebanon and the United Kingdom indicates that perceived security, perceived privacy, and trust significantly influence behavioral intentions in both countries, suggesting that the role of security is not limited to any particular level of economic development (Merhi et al., 2019). Studies extending technology acceptance models also demonstrate that perceived security and trust play key roles in increasing the adoption of mobile banking applications, whereas perceived risk weakens both trust and attitudes toward use (Almaiah et al., 2023). This synthesis also reveals that the influence of security does not end at the initial adoption stage but continues into the stage of sustained use. Continued trust in mobile banking applications is predicted by privacy assurances, security features, organizational reputation, customer service support, and customers' previous experiences, indicating that trust must be continuously reinforced through customers' ongoing interactions with banks (Che et al., 2023).

In Indonesia, customers' perceptions of transaction security significantly influence the continued use of mobile banking, and security remains a major challenge despite the convenience offered by these services (Sahata Sitanggang et al., 2024). Evidence from mobile payment users in Indonesia also indicates that security and reputation positively influence trust, while trust positively influences continued usage intentions (Ansori & Nugroho, 2024). The reviewed literature further indicates that trust and perceived risk determine whether customers' intentions are translated into actual usage (Kumar et al., 2023). Overall, these findings indicate that customers interpret security as evidence of a bank's competence and integrity, which are core dimensions of trustworthiness (Mayer et al., 1995). These findings establish security as the primary foundation of customer trust, implying that banks' strategies for maintaining trust in digital services must begin with credible and visible protection of customers' funds, identities, and data.

2. Multilayered Technological Safeguards: Authentication, Biometrics, and Intelligent Fraud Detection

The literature review reveals that multilayered technological safeguards constitute the operational core of banking strategies for protecting customers in digital services. Authentication represents the first layer because it determines whether the party initiating a transaction is the legitimate customer. A study of mobile banking users in Indonesia recommends measures such as two-step verification, one-time passwords, real-time transaction notifications, and single-device security to strengthen protection against cyberattacks and fraud (Sebayang et al., 2024).

However, this synthesis indicates that conventional authentication methods have weaknesses that banks must address. The World Bank's focus note on customer authentication explains that SMS-based one-time passwords have become less secure because fraudsters can intercept them, obtain them through social engineering, or redirect them through SIM-swap fraud. Therefore, it recommends combining one-time passwords with other factors, shortening their validity periods, and implementing risk-based authentication alongside multifactor authentication (World Bank, 2023). Biometric authentication emerges as the second layer, offering both convenience and stronger identity binding. Empirical evidence from bank customers indicates that attitudes toward biometric authentication shape perceived ease of use and perceived security, which subsequently influence perceived usefulness and intentions to use biometric banking services. Accordingly, banks are recommended to integrate facial recognition, fingerprint recognition, and iris scanning into their applications (Bhat et al., 2024). World Bank (2023) notes that biometrics raise privacy and data-handling concerns and cannot be replaced in the same way as compromised passwords. Therefore, banks need to manage biometric data with particular care.

The third layer involves intelligent fraud detection. Systematic reviews indicate that machine learning has become a major approach to financial fraud detection, with support vector machines and artificial neural networks among the most frequently used algorithms (Ali et al., 2022; Hernandez Aros et al., 2024). Empirical testing involving approximately 1.5 million transactions also indicates that tree-based machine learning methods have greater discriminatory power than logistic regression and can complement rule-based fraud detection systems (Dichev et al., 2025). This suggests that an effective technological strategy does not rely on a single tool but instead involves a multilayered architecture that combines strong authentication, carefully managed biometrics, and adaptive fraud detection.

3. Regulatory Compliance and Data Governance as Institutional Assurances

Regulatory compliance and data governance emerge from the synthesized literature as strategies that provide institutional assurances beyond the technological features visible to customers. The reviewed sources indicate that banks operate in an increasingly regulated environment that establishes minimum standards for cyber resilience and data protection. In Indonesia, Financial Services Authority Regulation No. 11/POJK.03/2022 concerning the Implementation of Information Technology by

Commercial Banks strengthens information technology governance and requires banks to improve their cyber resilience through cybersecurity testing, self-assessment of cybersecurity maturity levels, and cyber incident reporting (Financial Services Authority, 2022). The enactment of Law No. 27 of 2022 on Personal Data Protection further establishes data subjects' rights and personal data controllers' obligations, including those of financial institutions that process large volumes of customer data (Law No. 27 of 2022).

Legal studies argue that banks need to implement the principle of data minimization by collecting only data that are relevant, limited, and related to legitimate processing purposes, because collecting customer data beyond what is necessary may violate customers' privacy rights (Yudha, 2025). The same study recommends that banks disclose the types of data collected, periodically map and evaluate their data needs, and implement selective and secure information technology systems (Yudha, 2025). This synthesis also indicates that existing regulations are not yet fully adequate to address evolving threats. Consumer protection provisions in the banking sector establish basic principles but do not sufficiently address the needs of social engineering victims, leading to recommendations for more detailed implementing regulations (Utami & Purwanti, 2025).

From the perspective of trust theory, regulatory compliance and data governance function as structural assurances that signal institutional integrity, a mechanism recognized in models integrating trust and technology acceptance (Gefen et al., 2003). Customers rarely directly observe a bank's internal controls, but they can rely on the existence of regulatory oversight and transparent data management practices as evidence of the bank's accountability. This positions regulatory compliance and data governance as the institutional layer of banking strategies that transforms legal obligations into credible assurances of customer protection.

4. Customer Education and Transparent Crisis Response as Strategies for Maintaining Trust

The synthesis reveals that customer education and transparent crisis response are essential strategies because digital banking security depends not only on systems but also on human behavior and institutional responses when incidents occur. Systematic reviews indicate that phishing, vishing, identity theft, and malware remain the most common threats to digital banking, and many of these attacks succeed by manipulating customers rather than breaching technical controls (Cele & Kwenda, 2025; Ahmad et al., 2024). Therefore, Ahmad et al. (2024) emphasize the importance of continuous training and awareness programs for both bank employees and customers as part of a comprehensive security response. Legal research in Indonesia also recommends bank-organized financial literacy programs and greater customer vigilance when sharing sensitive information as important measures for addressing social engineering (Utami & Purwanti, 2025).

Evidence supporting the protective role of knowledge reinforces these recommendations, as basic financial knowledge has been found to be negatively

associated with the likelihood of becoming a victim of online fraud, whereas excessive confidence in one's own financial literacy increases vulnerability (Isaia et al., 2024). The literature also indicates that education contributes to trust formation because informing users about the available security measures can strengthen their confidence in mobile banking services (Sebayang et al., 2024). The second component of this strategy concerns banks' responses when security incidents occur. An analysis of public responses to the 2023 cyberattack on Bank Syariah Indonesia indicates that the attack triggered intensive discussions about the perpetrators and data exposure and estimated a potential short-term customer migration of 1.60 percent of the customer base. The study concluded that strong cybersecurity and rapid response strategies are necessary to protect customer trust (Timur et al., 2024).

Research on corporate data breaches indicates that detailed instructions for affected consumers, acknowledgment of responsibility, consistency in communication strategies, and voluntary disclosure can reduce reputational damage, whereas denial is the most detrimental response (Kuipers & Schonheit, 2022). Subsequent research in Indonesia's Islamic banking sector has also examined the relationship between perceived risk, service quality, and customer trust with customer loyalty following cyberattacks (Rahman et al., 2024). This synthesis indicates that customer education reduces the likelihood of successful attacks, while transparent crisis response limits the erosion of trust when incidents cannot be prevented.

5. An Integrated Security–Trust Strategy Model for Digital Banking

The final outcome of this literature synthesis is an integrated security–trust strategy model that combines the preceding findings into a single conceptual framework, as illustrated in Figure 1. This model consists of three strategic layers that collectively shape customers' perceived security. The technological layer includes multifactor and risk-based authentication, biometric authentication, encryption, and machine learning-based fraud detection, which protect transactions at the operational level (World Bank, 2023; Bhat et al., 2024; Dichev et al., 2025). The institutional layer encompasses compliance with cyber resilience regulations, personal data protection, data minimization, and transparent data governance, which signal banks' integrity and accountability (Financial Services Authority, 2022; Yudha, 2025). The human-relational layer includes customer education, security awareness, customer service support, and transparent crisis communication, which reduce human vulnerability and maintain relationships between banks and their customers (Utami & Purwanti, 2025; Kuipers & Schonheit, 2022).

These three layers are proposed to influence perceived security, which subsequently shapes customer trust, while trust then promotes continued use and loyalty toward digital banking services (Merhi et al., 2019; Che et al., 2023; Ansori & Nugroho, 2024). Perceived risk is positioned as an inhibiting force that weakens trust and the conversion of intentions into actual usage (Almaiah et al., 2023; Kumar et al., 2023). Security incidents are positioned as disruptions that can rapidly erode trust,

with the extent of the decline depending on the quality of the bank's crisis response (Timur et al., 2024).

Based on this structure, the model proposes six propositions. P1: Multilayered technological safeguards positively influence customers' perceived security in digital banking services. P2: Regulatory compliance and transparent data governance positively influence perceived security and trust by signaling institutional integrity. P3: Customer education and security awareness reduce customers' vulnerability to social engineering and strengthen perceived security. P4: Perceived security positively influences customer trust, which subsequently has a positive effect on continued use of digital banking services. P5: Perceived risk negatively influences customer trust and weakens the conversion of behavioral intentions into actual usage. P6: Transparent and timely crisis response moderates the negative effect of security incidents on customer trust. This model conceptualizes customer trust as an outcome of a coordinated strategic system rather than the result of a single security measure.

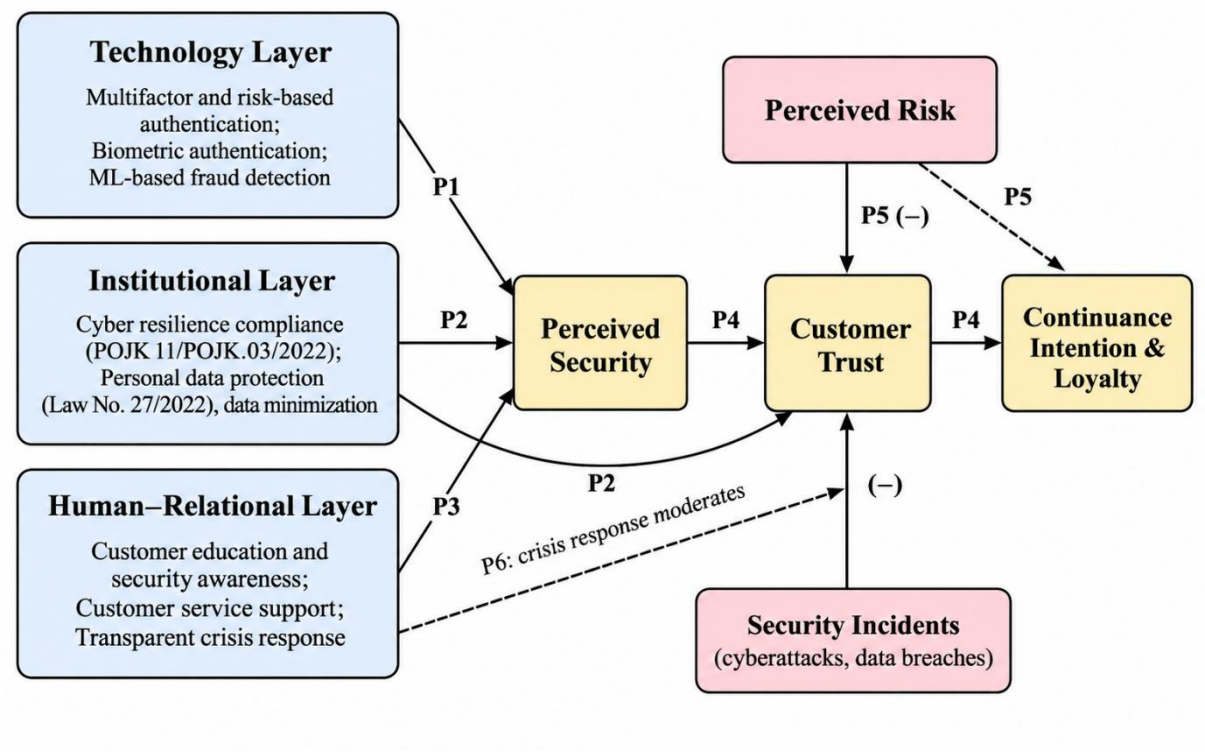


Figure 1. Integrated Security–Trust Strategy Model for Digital Banking

Source: Author's Synthesis

This study establishes security as a fundamental determinant of customer trust in digital banking services, and this conclusion reinforces and extends several previous empirical studies. Merhi et al. (2019) demonstrated that perceived security, perceived privacy, and trust significantly influence intentions to use mobile banking among Lebanese and British consumers, confirming that security is a determinant of adoption across cultures. This synthesis extends that perspective by arguing that security is not merely one of several parallel predictors of intention but rather the foundation upon which trust is established and continuously renewed. A similar conclusion emerges from the study by Che et al. (2023), which found that continued

trust in mobile banking applications is predicted by privacy assurances, security features, organizational reputation, customer service support, and previous experiences.

Unlike these studies, which group predictors into application, organizational, and customer factors, this synthesis connects each factor to a specific strategic layer that banks can manage, thereby translating trust predictors into actionable strategies. These findings are also consistent with evidence from Indonesia reported by Sahata Sitanggang et al. (2024), who found that customers' perceived security significantly influences continued mobile banking use and that security remains a major challenge for these services. Nevertheless, this literature review extends that explanation by positioning security within a trust theory framework, which views visible protection as a signal of a bank's competence and integrity (Mayer et al., 1995). This interpretation explains why customers may remain hesitant to use convenient digital services when they perceive weaknesses in protection, and why convenience alone cannot replace security. Evidence from mobile payment users in Indonesia, which indicates that security and reputation positively influence trust while trust promotes continued usage intentions, further supports this sequential interpretation (Ansori & Nugroho, 2024). This study provides a broader conceptual understanding by explaining that security serves as the psychological and institutional foundation upon which sustained customer trust in digital banking develops.

The findings identify multilayered technological safeguards as the operational core of banking security strategies, and this interpretation both supports and extends previous research. Bhat et al. (2024) demonstrated that attitudes toward biometric authentication shape perceived ease of use and perceived security, which subsequently influence intentions to use biometric banking services, confirming that authentication technology affects customer perceptions and not merely technical protection. This synthesis extends that perspective by arguing that biometric authentication should be understood as one layer within a broader architecture, as World Bank (2023) highlights that biometric data raise privacy concerns and cannot be replaced once compromised. Comparable conclusions can be drawn from the recommendations of Sebayang et al. (2024), who found that privacy and financial risks were considered highly important by mobile banking users in Indonesia but were perceived to be inadequately addressed, and recommended two-step verification, one-time passwords, real-time notifications, and single-device security. Whereas that study focused on prioritizing attributes for adoption, this synthesis indicates that these measures need to be complemented by stronger authentication approaches, given the documented vulnerabilities of SMS-based one-time passwords to interception and SIM-swap fraud (World Bank, 2023).

These findings are also consistent with the study by Dichev et al. (2025), which found that tree-based machine learning models outperformed logistic regression in detecting fraudulent banking transactions and could complement rule-based systems. However, Dichev et al. (2025) acknowledged that interpretability was not the focus of their study, whereas this synthesis argues that interpretability becomes important

when fraud detection decisions, such as transaction blocking, directly affect customer experiences and trust. Systematic reviews by Ali et al. (2022) and Hernandez Aros et al. (2024) confirm the increasing use of machine learning for fraud detection, but most primarily evaluate algorithm performance rather than customer outcomes. By linking technological safeguards to perceived security and trust, this study offers a more comprehensive explanation than previous studies that examine technological performance or customer perceptions separately.

The findings position regulatory compliance and data governance as institutional assurances that strengthen perceived security and trust, and this conclusion is consistent with and extends previous research. Gefen et al. (2003) integrated trust into a technology acceptance model and acknowledged that institutional assurances contribute to trust formation in online environments. This synthesis extends that insight to digital banking by identifying cyber resilience regulations and personal data protection as concrete forms of institutional assurance in the Indonesian context (Financial Services Authority, 2022; Law No. 27 of 2022). A similar argument was advanced by Yudha (2025), who found that banks often collect more customer data than necessary and recommended data minimization, disclosure of data types, periodic data mapping, and secure information technology systems.

Whereas that study addresses the issue from a normative legal perspective, this synthesis interprets data minimization as a trust-building strategy because collecting less data reduces potential harm from data breaches and demonstrates banks' respect for customer privacy. These findings are also consistent with Utami and Purwanti (2025), who found that Indonesia's banking consumer protection framework remains inadequate in addressing the needs of social engineering victims. This literature review extends that conclusion by arguing that regulatory gaps are not merely a legal issue but also a trust issue, because customers who experience losses without clear recovery mechanisms may generalize their disappointment to the digital banking system as a whole. Integrating these legal findings with behavioral evidence on trust explains why compliance needs to be communicated to customers as part of a bank's value proposition rather than treated solely as an internal obligation. This interpretation provides stronger theoretical coherence than studies that examine regulation and customer behavior separately. This study strengthens the understanding of trust in digital banking by demonstrating that institutional assurances complement technological safeguards in shaping customer confidence.

Customer education and transparent crisis response have been identified as strategies for maintaining trust, and this interpretation both reinforces and extends previous scholarly discussions. Ahmad et al. (2024) concluded that banks need to combine advanced security measures with continuous training and awareness programs for employees and customers, emphasizing that the human factor is central to digital banking security. This synthesis extends that argument by linking education to trust formation, supported by the observation of Sebayang et al. (2024) that informing users about available security measures can build confidence in mobile banking. A similar conclusion was reported by Isaia et al. (2024), who found that basic

financial knowledge reduces the likelihood of becoming a victim of online fraud, whereas excessive confidence increases that likelihood.

Although that study was conducted among the general population in Italy rather than specifically among bank customers, this synthesis argues that the same mechanism is relevant to banks seeking to reduce the success of social engineering attacks. This implies that education should target accurate knowledge rather than confidence alone. These findings are also consistent with the study by Timur et al. (2024), which analyzed public responses to the cyberattack on Bank Syariah Indonesia and concluded that strong cybersecurity and rapid response strategies are necessary to protect customer trust and limit customer attrition. This literature review extends that conclusion by incorporating evidence from Kuipers and Schonheit (2022), who demonstrated that acknowledgment of responsibility, detailed instructions, consistency, and voluntary disclosure reduce reputational damage following data breaches, whereas denial is the most detrimental approach. Although Kuipers and Schonheit (2022) focused on reputation rather than trust and examined corporations outside the banking sector, their findings provide a reasonable basis for designing banks' incident communication strategies. This integrated interpretation offers a more comprehensive explanation of trust maintenance than adoption studies that implicitly assume a stable environment without security incidents.

Based on the above findings, an integrated security–trust strategy model and conceptual framework are proposed, reinforcing and extending previous scholarly perspectives on digital banking. Unlike previous studies that primarily examine security, trust, and risk as direct predictors of adoption, the proposed model explains how technological, institutional, and human-relational strategies collectively shape perceived security, trust, and continued use. This integrative perspective complements the study by Apau et al. (2025), which extended UTAUT2 by incorporating security, risk, institutional trust, and technological trust and found that the extended model explained substantially more variance in behavioral intentions than the original model. However, this study advances that framework by specifying the strategic antecedents of these constructs, thereby connecting customer perceptions with decisions that banks can implement. The proposed model is also consistent with the systematic review by Cele and Kwenda (2025), which identified identity theft, malware, phishing, and vishing as major threats to digital banking adoption and called for cybersecurity risk management strategies. Whereas that review focused on identifying threats, this synthesis translates those insights into a structured strategic model that pairs threats with multilayered responses.

The model is also consistent with the findings of Kumar et al. (2023), who demonstrated that perceived risk and trust moderate the relationship between behavioral intentions and actual mobile banking use. Nevertheless, this study extends that conclusion by positioning perceived risk as an inhibiting force that banks can mitigate through the three strategic layers, while also incorporating security incidents and crisis response as dynamic elements absent from most adoption models. The resulting framework therefore reduces conceptual fragmentation among behavioral,

technical, and legal research on digital banking security. By integrating these dimensions into a coherent structure expressed through testable propositions, the model provides a solid conceptual foundation for future empirical research involving conventional and Islamic banks, different customer segments, and various regulatory environments.

D. CONCLUSION

This study synthesizes the literature on banking strategies for maintaining customer security and trust in digital services and develops an integrated security–trust strategy model. The literature review indicates that security functions as a fundamental determinant of customer trust and continued use of digital banking services across different national contexts, including Indonesia. The findings show that banks' security strategies operate through three complementary layers. The technological layer consists of strong and risk-based authentication, carefully managed biometric authentication, and machine learning-based fraud detection. The institutional layer comprises compliance with cyber resilience regulations, personal data protection, data minimization, and transparent data governance, which provide assurances of bank integrity. The human-relational layer consists of customer education, security awareness, customer service support, and transparent crisis response, which reduce human vulnerability and maintain trust when incidents occur.

These findings confirm that customer trust in digital banking results from the interaction of multiple strategies rather than a single security measure. The proposed model explains how these strategies shape perceived security, how perceived security shapes trust, and how trust promotes continued use, while perceived risk and security incidents act as forces that may weaken this process. This integration reduces fragmentation among behavioral, technical, and legal research on digital banking security. This study also demonstrates that technological sophistication alone cannot guarantee sustained customer trust without accountable governance and well-informed customers.

Several limitations should be acknowledged. This review relies on a limited number of verified sources, some of which were accessible only at the abstract level, and the proposed relationships have not yet been empirically tested. Future researchers could empirically validate the six propositions using quantitative methods, such as structural equation modeling, across conventional and Islamic banks, different customer segments, and various countries. Future studies could also expand the model by examining emerging issues such as artificial intelligence-based fraud, deepfake-based identity attacks, and the role of Islamic ethical values in shaping trust in Islamic digital banking. Bank managers can use this model to design coordinated security strategies that integrate technology, governance, and customer engagement. Regulators and policymakers can utilize these insights to strengthen implementing regulations, customer protection mechanisms, and incident response standards. Ultimately, this study demonstrates that maintaining customer security

and trust in digital banking requires the harmonious integration of technological safeguards, institutional assurances, and human-relational strategies within a resilient and customer-centered digital banking ecosystem.

REFERENCES

1. Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: Unmasking online threats and fortifying e-banking security, a systematic review. *Journal of Financial Crime, 31*(6), 1485–1501. https://doi.org/10.1108/JFC-11-2023-0302
2. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences, 12*(19), 9637. https://doi.org/10.3390/app12199637
3. Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Abu Alghanam, O. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability, 15*(13), 9908. https://doi.org/10.3390/su15139908
4. Ansori, A. D., & Nugroho, S. S. (2024). The role of trust on the continuance usage intention of Indonesian mobile payment application. *Gadjah Mada International Journal of Business, 26*(2), 233–259. https://doi.org/10.22146/gamaijb.70452
5. Apau, R., Titis, E., & Lallie, H. S. (2025). Towards a better understanding of mobile banking app adoption and use: Integrating security, risk, and trust into UTAUT2. *Computers, 14*(4), 144. https://doi.org/10.3390/computers14040144
6. Bhat, S. A., Islam, S. B., & Mir, M. F. (2024). Consumers' attitude toward biometric banking services: An empirical evaluation of determinants and outcomes. *Journal of Financial Services Marketing, 29*(4), 1572–1588. https://doi.org/10.1057/s41264-024-00285-5
7. Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime, 32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263
8. Che, M., Say, S. Y. A., Yu, H., Zhou, Q., Shu, J., Sun, W., Luo, X., & Xu, H. (2023). Investigating customers' continuous trust towards mobile banking apps. *Humanities and Social Sciences Communications, 10*, 1–10. https://doi.org/10.1057/s41599-023-02483-3
9. Dichev, A., Zarkova, S., & Angelov, P. (2025). Machine learning as a tool for assessment and management of fraud risk in banking transactions. Journal of Risk and Financial Management, 18(3), 130. https://doi.org/10.3390/jrfm18030130
10. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90. https://doi.org/10.2307/30036519
11. Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications, 11*, 1–22.

https://doi.org/10.1057/s41599-024-03606-0
12. Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance, 44*, 100977. https://doi.org/10.1016/j.jbef.2024.100977
13. Kuipers, S., & Schonheit, M. (2022). Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. *Corporate Reputation Review, 25*(3), 176–197. https://doi.org/10.1057/s41299-021-00121-9
14. Kumar, R., Singh, R., Kumar, K., Khan, S., & Corvello, V. (2023). How does perceived risk and trust affect mobile banking adoption? Empirical evidence from India. *Sustainability, 15*(5), 4053. https://doi.org/10.3390/su15054053
15. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. https://doi.org/10.2307/258792
16. Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society, 59*, 101151. https://doi.org/10.1016/j.techsoc.2019.101151
17. Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Otoritas Jasa Keuangan.
18. Rahman, B. S., Prabawani, B., & Nugraha, H. S. (2024). Analysis of the effect of perceived risk, service quality and customer trust toward customer loyalty after a cyber-attack (Study in Bank Sharia Indonesia). *Jurnal Ilmu Administrasi Bisnis, 13*(4), 1092–1101. https://doi.org/10.14710/jiab.2024.44725
19. Sahata Sitanggang, A., Lestari, S., Cika Febrianti, N., Az-zahra, A., & Nurazizah Fitriadi, M. (2024). Analisis tingkat kepercayaan nasabah pada keamanan transaksi perbankan melalui mobile banking (M-Banking). *Jurnal Masharif al-Syariah: Jurnal Ekonomi dan Perbankan Syariah, 9*(3). https://doi.org/10.30651/jms.v9i3.23067
20. Sebayang, T. E., Hakim, D. B., Bakhtiar, T., & Indrawan, D. (2024). The investigation of preference attributes of Indonesian mobile banking users to develop a strategy for mobile banking adoption. *Journal of Risk and Financial Management, 17*(3), 109. https://doi.org/10.3390/jrfm17030109
21. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
22. Timur, Y. P., Ridlwan, A. A., Fikriyah, K., Susilowati, F. D., Canggih, C., & Nurafini, F. (2024). How should Bank Syariah Indonesia respond to cyber-attacks? Churn, sentiments, and emotions analysis with machine learning. *Journal of Islamic Economics Lariba, 10*(1), 439–470. https://doi.org/10.20885/jielariba.vol10.iss1.art24
23. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
24. Utami, P. D. Y., & Purwanti, N. P. (2025). Strengthening legal protections against social engineering in digital banking: Challenges, gaps, and recommendations. *Masalah-Masalah Hukum, 54*(2), 214–226.

https://doi.org/10.14710/mmh.54.2.2025.214-226
25. World Bank. (2023). *Customer authentication 2.0: Approaches and challenges in fast payments (Focus Note)*. World Bank.
26. Yudha, W. A. (2025). Urgensi penerapan minimalisasi data dalam upaya pencegahan penyalahgunaan data pribadi nasabah di sektor perbankan berdasarkan Undang-Undang Pelindungan Data Pribadi. *Mahkamah: Jurnal Riset Ilmu Hukum*, *2*(3), 273–285. https://doi.org/10.62383/mahkamah.v2i3.935