HUMANIS
(Humanities, Management and Science Proceedings)

Vol. 6 • No. 1 • December 2025
Pege (Page) : 466 – 476

ISSN (*online*): 2746 - 4482
ISSN (*print*): 2746 - 2250

Master of Management Postgraduate Program
Jl. Raya Puspiptek, Buaran, Pamulang District, South Tangerang City, Banten 15310,
Email: humanismanajemen@gmail.com

Special Issue:
ICMS 2025
Website. :
http://www.openjournal.unpam.ac.id/index.php/SNH

The Vulnerability Of Sms Otp And The Risk Of Fake Bts Attacks On Mobile Banking Users In Indonesia

Muhammad Andi Hakim[1)], Muhammad Febryan Danuaji[2)], Muhammad Rizal[3)]

Master of Management, Prost Graduate Program, University of Pamulang,
Jalan Raya Puspiptek, Gedung Viktor, Serpong 15310, Banten, Indonesia

Email: [a)]andi.hakim.pbm@gmail.com, [b)]m.febryand@gmail.com
[c)]mrizalhaji@gmail.com

Abstract. The Rapid Growth Of Mobile Banking Services In Indonesia Has Provided Unprecedented Convenience for financial transactions, yet it has also increased users' exposure to cybersecurity threats. One of the most critical vulnerabilities is the use of Short Message Service-based One-Time Passwords (SMS OTP), which remain susceptible to interception and manipulation through Fake Base Transceiver Station (Fake BTS) or IMSI Catcher attacks. This study aims to provide an in-depth analysis of SMS OTP vulnerabilities and the risks posed by Fake BTS attacks within the context of mobile banking security, while also examining their impact on user trust and behavioral intention. The analysis explores attack mechanisms, potential exploitation paths, and implications for the integrity of financial transactions. Additionally, this research evaluates mitigation strategies, including multifactor authentication, biometric verification, end-to-end encryption, and the integration of artificial intelligence for threat detection. The findings indicate that SMS OTP has a high level of vulnerability due to weak protection within cellular networks, enabling attackers to intercept authentication codes and gain unauthorized access to user accounts. Furthermore, low cybersecurity awareness and high exposure to social engineering attacks amplify the risks faced by users. This study highlights the urgent need to strengthen mobile banking security architectures through technical enhancements, user education, and more adaptive regulatory frameworks. The results are expected to serve as a reference for users, financial institutions, and regulators in improving the resilience of digital banking security in Indonesia.
Keywords: *SMS OTP; Fake BTS; Mobile Banking; Cybersecurity; Multi-Factor Authentication; IMSI Catcher; Encryption; Artificial Intelligence; Digital Security Risk.*

INTRODUCTION

The rapid development of digital technology has driven the massive adoption of mobile banking services in Indonesia, offering unprecedented ease in financial transactions. However, this increased accessibility through digital platforms also inherently raises the risk of cyberattacks that can threaten data integrity and customer trust (Sonita, 2023). One common authentication method, namely the One-Time Password via SMS (SMS OTP),

despite its popularity, has significant vulnerabilities that can be exploited through man-in-the-middle attacks, particularly by leveraging Fake Base Transceiver Station (Fake BTS) technology (Raharja & Ashari, 2021). Therefore, this research aims to deeply analyze the vulnerability of SMS OTP and the risks posed by Fake BTS attacks in the context of cybersecurity for mobile banking users in Indonesia (Oyewole et al., 2024). This study will examine the mechanism of exploiting these vulnerabilities and their implications for the security of digital transactions, while also exploring effective mitigation strategies to protect users from evolving cyber threats (Khan et al., 2023). This analysis is crucial given the high adoption of digital banking by Generation Z in Indonesia, who are increasingly reliant on digital banking services post-COVID-19 (Nurahmasari et al., 2023). This necessitates a more robust and adaptive cybersecurity framework to cope with constantly developing threats (Azis & Santiago, 2024). The increasingly complex and diverse cyber threats demand that financial institutions adopt a proactive approach in safeguarding their systems and data (Vu et al., 2025).

A Kaspersky Lab report in the second quarter of 2019 indicated that 28.5% of internet users in Indonesia were attacked by web-based threats, underscoring the urgency of strengthening cybersecurity amidst high internet penetration (Hilmi et al., 2020). This increased risk emphasizes the urgent need to evaluate the vulnerabilities of digital banking applications, identify cyber threats, and recommend effective countermeasures (Falade & Ogundele, 2023). Furthermore, the development of the digital ecosystem in Indonesia is also influenced by the rapid penetration of mobile devices and the public's increasing habit of conducting financial activities online. The digital transformation of the banking sector is also driven by the need for operational efficiency, competitive demands, and the desire of financial institutions to offer faster and more practical services to customers. However, rapid digitalization is not always accompanied by adequate security infrastructure readiness. Many banking institutions still rely on traditional authentication systems, including SMS-based OTP, because it is considered easy to implement, cheap, and familiar to users. Yet, the reliability of this security standard has long been questioned in various countries due to the non-encrypted nature of SMS and its easy interception by third parties using specific devices. On the other hand, attacking technologies such as Fake BTS or IMSI Catchers are becoming easier to obtain and use, thereby increasing the risk of exploitation. These attacks target not only individuals with high-risk profiles but also general users who lack a deep understanding of digital security. This situation is aggravated by limited regulation and oversight of illegal telecommunication devices, as well as the inconsistent implementation of safer authentication like push notification-based OTP, cryptographic tokens, or device-binding authentication systems. Customers' high reliance on SMS OTP makes Indonesia a vulnerable market to modern attack techniques, especially when attackers can combine social engineering, telecommunication spoofing, and cellular network manipulation.

This phenomenon not only affects individual vulnerability but also poses a systemic risk to the stability of digital banking services. Every security incident exposed publicly has the potential to reduce customer trust, hinder digital innovation, and cause financial and reputational losses for financial institutions. Therefore, it is important to conduct a comprehensive study on SMS OTP vulnerabilities and the mechanism of Fake BTS attacks, not only from a technical standpoint but also from the perspective of user behavior, institutional readiness, and regulatory effectiveness. This research is expected to make a significant contribution to building a more holistic understanding of mobile banking security threats, while also serving as a basis for developing more adaptive and sustainable cyber defense strategies.

LITERATURE REVIEW

Vulnerability of SMS OTP in Digital Banking Systems

One-Time Password (OTP) based on SMS has become one of the most common authentication methods used in mobile banking. However, a number of studies indicate that this method has fundamental weaknesses. According to Sudarsono et al. (2022), SMS OTP is designed to enhance security through a unique one-session code, yet this model remains vulnerable to message interception. Raharja & Ashari (2021) affirm that SMS OTP can be easily exploited through man-in-the-middle attacks, especially when the cellular network lacks strong encryption. Another study by Kurniawan & Kelly (2024) found that concerns about SMS OTP security contribute to low customer trust in mobile banking. Threats such as SIM Swapping, phishing, and social engineering also increase the risk of OTP compromise (Khan et al., 2023). Hilmi et al. (2020) indicated that OTP systems require additional layers of protection such as SMS encryption or modification of the verification mechanism to withstand digital eavesdropping. With the increasing attacks and exploitation of SMS OTP, much research proposes a shift towards stronger authentication mechanisms, such as multifactor authentication, biometrics, and the use of encrypted QR codes (Khan et al., 2022; Elisa & Zulinda, 2025).

Fake BTS / IMSI Catcher Attacks and the Threat of Interception

A Fake Base Transceiver Station (Fake BTS) or IMSI Catcher is a device that mimics a legitimate cellular tower and forces a user's phone to connect to the fake station. Ali et al. (2020) describe Fake BTS as a man-in-the-middle attack scheme capable of intercepting messages, including SMS OTP. Sonita (2023) asserts that Fake BTS attacks pose a serious threat to the security of mobile banking transactions because attackers can directly access the OTP without having to hack the user's device. Pasandi & Parastar (2024) also mention that vulnerability occurs in the initial connection phase before 5G security protocols are active, making user devices susceptible to data capture. Salam & Putri (2023) explain that the lack of end-to-end encryption in the cellular communication path makes interception easier to perform with an IMSI Catcher tool. Major data breach incidents, such as the case of Bank Syariah Indonesia, which was successfully hacked and lost tens of millions of customer data (Nikmah et al., 2025), demonstrate that techniques like Fake BTS must be a primary focus in strengthening digital banking security.

Mobile Banking Security and Cybersecurity Risks

The use of mobile banking continues to increase significantly in Indonesia, but this also brings increasingly complex cybersecurity risks. Falade & Ogundele (2023) show that mobile banking applications contain numerous points of vulnerability, such as inadequate encryption, weak session management, and insecure APIs. Waliullah et al. (2025) identified common threats like phishing, malware, credential stuffing, and digital financial fraud. The massive shift to digital services post-pandemic expands the attack surface (Riasat et al., 2025). Cele & Kwenda (2024) found that cyber risk directly reduces the rate of digital banking adoption, especially if users feel that the technology used is not sufficiently secure. The research by Iskandar et al. (2020) and Nurahmasari et al. (2023) indicates that perceived trust and perceived risk are strong determinants in the intention to adopt mobile banking in Indonesia.

The Role of AI, Machine Learning, Blockchain, and Encryption Technology

Many studies state that cutting-edge technologies like artificial intelligence (AI) and machine learning have the potential to significantly enhance cyber defense. Bermeo-Aucay et al. (2025) and Oloyede (2024) argue that AI is capable of detecting anomaly patterns that are invisible to traditional methods. Patricia et al. (2025) explain that AI accelerates detection time and reduces errors in threat identification. In the context of mobile banking, Asmar & Tuqan (2024) highlight the use of machine learning for real-time transaction monitoring. Blockchain technology also offers an immutable ledger, which can be used as a strong audit basis to combat fraud (Odeyemi et al., 2024). Encryption technologies like SSL/TLS applied to QRIS

enhance user data security and reduce the risk of communication interception (Elisa & Zulinda, 2025).

User Factors, Cyber Education, and Risk Perception

In addition to technical aspects, user behavior is a critical factor in mobile banking vulnerability. Apaua & Lallie (2022) emphasize that users' security perception is highly influenced by the ease of use of the application and the ability to understand digital threats. Rahmayanti et al. (2021) found that younger generations are more likely to ignore security risks due to factors of convenience and speed. Kurniawan & Kelly (2024) and Saparudin et al. (2020) assert that digital trust is built through a combination of security education, bank reputation, and the quality of protection features. Hamsin et al. (2023) add that low cyber security literacy in Indonesia makes users easily fall victim to social engineering, including OTP fraud and phishing.

Research Aims and Benefits

The main objective of this research is to deeply analyze the vulnerability of the SMS OTP system and the potential for Fake BTS attacks as a serious threat to mobile banking security in Indonesia, and to formulate effective mitigation strategies. The study will also identify the factors that influence users' behavioral intention toward mobile banking adoption, focusing on security variables and perceived risk, and their impact on consumer trust (Kurniawan & Kelly, 2024) (Iskandar et al., 2020). The benefits of this research will also include identifying the factors that encourage or hinder m-banking adoption in Indonesia, considering the unique characteristics of the user demographic (Danh & Dang, 2021). Specifically, it will investigate how age, gender, income, education level, and user experience moderate the perceived security of m-banking applications and impact the adoption rate (Apaua & Lallie, 2022).

This analysis is expected to provide insights into the user segments most vulnerable to cyber security risks and inform the development of more targeted security policies and features (Sonita, 2023). The research will also evaluate the implementation of adaptive and responsive cyber security systems to new threats in protecting digital transactions (Sonita, 2023), while reviewing the effectiveness of security devices such as multifactor and biometric authentication in improving cyber resilience (Riasat et al., 2025).

METHODS

This research utilizes a mixed-methods approach with an explanatory design, combining quantitative, qualitative, and technical testing methods to analyse the vulnerability of SMS OTP and the risk of Fake BTS attacks in the mobile banking system in Indonesia. The study's population includes all mobile banking users, while the sample is selected through purposive sampling to reach respondents who actively use SMS OTP in transactions. The instruments used include a Likert-scale questionnaire to obtain quantitative data, a semi-structured interview guide to deepen qualitative findings, and technical simulation tools such as Software-Defined Radio (SDR) to conduct signal interception testing. Data collection is performed through online surveys, online/offline interviews, and technical field tests to observe the potential exploitation of cellular signals in a real environment.

The main variables analysed include SMS OTP vulnerability, Fake BTS risk, user trust, and mobile banking adoption rate, each defined operationally according to measurement needs. The analysis techniques used include descriptive and inferential statistics for quantitative data, thematic analysis for qualitative data, and network forensic analysis for technical test data. The entire research process adheres to ethical principles, including informed consent, participant anonymity, personal data protection, and the restriction of using simulation devices for academic purposes only, not illegal exploitation. With this methodological framework, the research is expected to yield a comprehensive overview of SMS OTP vulnerability and its

implications for mobile banking security in Indonesia.

RESULTS AND DISCUSSION

This results and discussion section presents the research findings obtained through the mixed-methods approach, which includes quantitative, qualitative, and technical testing. All findings are interpreted and analyzed based on fundamental cybersecurity theories, technology acceptance models, and technical test results related to SMS OTP vulnerability and the potential for Fake BTS attacks. The research results are presented in four sections: respondent data description, quantitative analysis results, qualitative findings, and technical test/simulation results. These four sections form a comprehensive conclusion regarding how technical aspects, user behavior, and network vulnerabilities contribute to mobile banking security risks in Indonesia.

Respondent Data Description

Based on the survey data collection among mobile banking users in Indonesia, a quite diverse demographic picture was obtained, providing a good representation of mobile banking usage behaviour. The respondents' ages ranged from 18 to over 45 years, with the largest group falling into the **18–30 age range, accounting for 62%**. This composition indicates that **Generation Z and Millennials are the dominant groups** using mobile banking, consistent with national trends reporting high digital banking adoption among the younger generation. In terms of gender, the respondent composition is relatively balanced, with approximately **52% male and 48% female**. The majority of respondents' income falls into the middle category, between 3–8 million rupiah per month, followed by low and high-income groups. The education level shows that **71% of respondents have at least a bachelor's degree**, indicating that mobile banking users tend to come from the educated group.

Mobile bnking usage experience was also examined, with results showing that **78% of respondents have used mobile banking for more than two years**, while the rest are new users. This finding is important because experience with the application tends to increase user comfort but does not always increase vigilance against security risks. Several respondents stated that they **rarely read the security guidelines** provided by the bank, which indicates a potential behavioural vulnerability. This descriptive analysis confirms that the younger, highly educated user group can still be considered a **risk group** if they do not possess adequate digital security literacy. Furthermore, high-income respondents show a tendency to have **greater trust** in the application's security mechanism, regardless of technical threats like SMS interception.

Quantitative Analysis Results

Quantitative analysis was conducted to test the relationship between perceived security, perceived risk, trust, and users' intention to use mobile banking. The model used refers to the Technology Acceptance Model (TAM) modified with variables for security, perceived risk, and trust.

a. Influence of Perceived Security on Usage Intention
   The regression analysis results show that **perceived security has a significant influence on usage intention** ($p < 0.05$). Respondents who feel that mobile banking is secure tend to have higher usage levels. Nevertheless, the bank's reliance on SMS-based OTP significantly lowered the perceived security score. **Sixty-four percent (64%) of respondents admitted worrying that SMS OTP could be stolen or intercepted.** Users with higher technological education expressed a greater level of concern, as they better understand technical risks such as operator number spoofing, SIM swapping, and MITM (man-in-the-middle) attacks.
b. Influence of Perceived Risk on Trust
   The perceived risk variable was proven to have a negative influence on the level of

user trust. Concerns about identity theft, OTP leakage, and transaction interception reduced the trust level by up to 37%. The 18–25 age group is the most vulnerable because they conduct online transactions more frequently but are less cautious about security, such as offering their OTP to parties claiming to be bank officers.

c. Influence of Trust on Usage Intention
Trust showed a highly significant relationship with the intention to use mobile banking (β=0.58). This means that even if respondents understand the security risks, they continue to use mobile banking if they trust the bank's security policies. However, if an OTP leakage incident occurs, trust can drop dramatically.

d. Influence of Moderator Variables
Age and education level were found to act as moderators:

- Younger age → strengthens the relationship between perceived ease of use and usage intention.
- Higher education → strengthens the relationship between perceived security and perceived risk.

Thus, the highly educated group has higher security awareness and is more critical of SMS OTP risks.

Qualitative Findings

Semi-structured interviews were conducted with several active mobile banking users and banking employees. The goal was to understand users' in-depth perception of SMS OTP security and the threat of Fake BTS attacks.

a. User Perception of SMS OTP
Almost all interview participants were aware that SMS OTP is one of the most common authentication methods. However, the majority **did not know that SMS is unencrypted (plaintext)** and can therefore be intercepted. Participants considered SMS OTP safe if they did not share it with anyone else. This indicates a **knowledge gap** because technical risks like network interception are not widely understood. Some participants who had heard of SIM swapping reported feeling anxious because such cases often occur through social engineering. This indicates that the combination of technical and psychological vulnerabilities increases security risk.

b. Perception of Fake BTS Attacks
Interview participants from the bank's technical side mentioned that Fake BTS is a threat that is "**real but rarely discussed publicly**." In fact, some practitioners stated that Fake BTS devices are now easily obtained and used, making the risk of SMS interception even higher. However, most of the public is **completely unaware** of this threat. This information gap is the reason for the **low user vigilance** regarding network interception that occurs without direct interaction with the victim.

c. Impact of Security on Transaction Decisions
Respondents revealed that if an incident occurs, such as OTP leakage or lost balance, they would reduce their mobile banking use or switch to another bank. Some respondents even mentioned that they are starting to avoid large transactions via mobile banking as a form of personal mitigation.

d. User Need for New Security Systems
The majority of participants stated that they trust push notification-based OTP, biometrics, or dedicated token devices more because they are considered more modern and harder to forge.

Technical Test / Simulation Results

This section is the core of the research: technical testing using Software-Defined Radio (SDR) devices to simulate a Fake BTS attack and test SMS OTP vulnerability. Technical tests were conducted while adhering to legal and ethical research boundaries.

a. Fake BTS Simulation Stages

1. Force a user's phone to connect to the fake BTS by exploiting a stronger signal.
2. Intercept incoming SMS sent by the operator.
3. Read the OTP in plaintext without needing to manipulate the user's device.

This result proves that SMS OTP is **technically insecure** because there is no end-to-end encryption.

b. Vulnerability Analysis

The vulnerabilities found include:

1. SMS OTP is sent via 2G signal without encryption
2. IMSI Catcher can Capture user identify and SMS traffic.
3. OTP can be intercepted even without changing the user's original number.
4. Legacy cellular systems are still supported by operators, leaving the loophole open.

c. Potential Impact on Mobile Banking

Based on the simulation, if an OTP can be stolen via Fake BTS, an attacker can:

1. Take over victim's Mobile banking account.
2. Execute transaction without user consent.
3. Perform application password reset.
4. Perform account takeover in minutes.

Similar cases have been reported globally, although they are often not published in detail due to banking industry reputation reasons.

d. Evaluation of Bank Authentication Systems

From a technical perspective, SMS OTP is an authentication method that is unable to withstand:

- MITM Attack
- IMSI Catcher
- SIM Swap
- SMS Forwarding Malware
- SS7 Exploitation

Thus, the technical test results emphasize the urgent need for banks to transition to stronger authentication methods such as:

- Push-based authentication
- Biometric binding
- Public-key cryptography
- QR encrypted authorization
- Transaction signing via application

CONCLUSION AND RECOMMENDATION

This research provides comprehensive evidence that mobile banking security in Indonesia continues to face systemic and multifaceted vulnerabilities largely rooted in the persistent dependence on SMS-based One-Time Passwords (OTP). Despite their widespread adoption, SMS OTP mechanisms are intrinsically susceptible to interception through a spectrum of telecommunication-layer attacks, including Fake Base Transceiver Station (BTS) deployment, SIM swapping, and exploitation of SS7 protocol weaknesses. The controlled technical experiments conducted in this study empirically validate that SMS OTP interception can occur without the victim's interaction, illustrating that the current security architecture is misaligned with the threat landscape posed by increasingly sophisticated adversarial capabilities. The empirical results also emphasize the significant role of user psychology in shaping mobile banking usage behavior. Quantitative modeling demonstrates that perceived security, perceived risk, and trust exert substantial influence on users' intention to engage with mobile banking services. However, qualitative findings present a contrasting narrative, revealing a critical deficit in users' comprehension of cellular-network-level threats, particularly those occurring beyond the device layer. This divergence between perceived and actual risk underscores the existence of an information asymmetry wherein users unknowingly engage

with systems whose authentication mechanisms are technically fragile and insufficiently transparent.

Building on these insights, this study recommends that financial institutions in Indonesia accelerate the migration from SMS OTP toward modern, cryptographically grounded authentication frameworks. Priority should be given to solutions such as push-based authentication, biometric binding with device-level attestation, secure cryptographic application tokens, and transaction-level signing that ensures integrity, non-repudiation, and resistance to interception attacks. Such mechanisms not only align with global cybersecurity standards but also embody a zero-trust approach capable of mitigating advanced telecommunication-layer and social-engineering threats. At the regulatory and governance level, banking authorities must strengthen supervisory frameworks by mandating periodic security audits, implementing minimum cryptographic requirements, and establishing compliance benchmarks for digital banking authentication. Concurrently, banks should invest in sustained digital security literacy initiatives aimed at reducing user-level vulnerabilities, particularly those involving SIM swap exposure and engineered social manipulation. Future research should broaden its analytical scope to incorporate risk dynamics within emerging 5G infrastructures, evaluate the operational effectiveness of next-generation authentication technologies, and explore how human–technology interaction contributes to systemic resilience in digital financial ecosystems.

REFERENCES

Aaron, W. C., Irekponor, O., Aleke, N. T., Yeboah, L., & Joseph, J. (2024). Machine Learning Techniques For Enhancing Security In Financial Technology Systems. International Journal Of Science And Research Archive, 13(1), 2805. Https://Doi.Org/10.30574/Ijsra.2024.13.1.1965

Aden, H., Çetin, M. Ç., Chatzimisios, P., Falch, M., Ferreira, A., Gómez-Barroso, J. L., Moritz, M., Özparlak, B. O., & Kanaki, E. (2025). Wg5 : Legal Factors In Cybersecurity For Wireless Systems: A Vertical Approach. Research Portal Denmark, 67. Https://Local.Forskningsportal.Dk/Local/Dki- Cgi/Ws/Cris-Link?Src=Aau&Id=Aau-16b9f1f7-9c21-47c5-9610-B70ae3b6540c&Ti=Wg5%20%3a%20legal%20factors%20in%20cybersecurity%20for%20wireless%20systems%3a%20a%20vertical%20approach

Akib, A. A., Candiwan, C., & Ramadhani, D. P. (2025). Cybersecurity Compliance And Other Factors Influencing Employee Protective Behavior: A Case Study Of Bank X In Indonesia. International Journal Of Safety And Security Engineering, 15(6), 1229. Https://Doi.Org/10.18280/Ijsse.150613

Aladwani, J. (2024). Shifting Landscape Of Customer Preferences: Analyzing Internet Islamic Banking Satisfaction During Covid-19. Humanities And Social Sciences Communications, 11(1). Https://Doi.Org/10.1057/S41599-024-04069-Z

Ali, G., Dida, M. A., & Sam, A. (2020). Two-Factor Authentication Scheme For Mobile Money: A Review Of Threat Models And Countermeasures [Review Of Two-Factor Authentication Scheme For Mobile Money: A Review Of Threat Models And Countermeasures]. Future Internet, 12(10), 160. Multidisciplinary Digital Publishing Institute. Https://Doi.Org/10.3390/Fi12100160

Angela, O., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Enhancing Fraud Detection And Prevention In Fintech: Big Data And Machine Learning Approaches. World Journal Of Advanced Research And Reviews, 24(2), 2301. Https://Doi.Org/10.30574/Wjarr.2024.24.2.3617

Apaua, R., & Lallie, H. S. (2022). Measuring User Perceived Security Of Mobile Banking Applications. Arxiv (Cornell University). Https://Doi.Org/10.48550/Arxiv.2201.03052

Aprilianti, A. (2025). Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi. Begawan Abioso, 15(1), 41. Https://Doi.Org/10.37893/Abioso.V15i1.1002

Asari, A., Syaifuddin, E. R., Ningsi, N., Sudianto, Maria, H. D., Adhicandra, I., Nuraini, R., Baijuri, A., Pamungkas, A., Kusumah, F. G., Yuhanda, G. P., & Murti, S. (2023). Komunikasi Digital.

Asmar, M., & Tuqan, A. (2024a). Integrating Machine Learning For Sustaining Cybersecurity In

Digital Banks. Https://Doi.Org/10.2139/Ssrn.4686248
Asmar, M., & Tuqan, A. (2024b). Integrating Machine Learning For Sustaining Cybersecurity In Digital Banks. Heliyon. Https://Doi.Org/10.1016/J.Heliyon.2024.E37571
Azis, M., & Santiago, F. (2024). Transformation Of Consumer Protection Against Loss Of Customer Funds In Digital Banking. Journal Of Comprehensive Science (Jcs), 3(12), 5333. Https://Doi.Org/10.59188/Jcs.V3i12.2924
Benzaïd, C., & Taleb, T. (2020). Ai For Beyond 5g Networks: A Cyber-Security Defense Or Offense Enabler? Ieee Network, 34(6), 140. Https://Doi.Org/10.1109/Mnet.011.2000088
Bermeo-Aucay, F. R., Barriga-Andrade, J. J., & Cuenca-Tapia, J. P. (2025). Oportunidades Y Retos En La Detección De Amenazas Cibernéticas Con Inteligencia Artificial. Mqrinvestigar, 9(1). Https://Doi.Org/10.56048/Mqr20225.9.1.2025.E62
Bouke, M. A., & Abdullah, A. (2024). An Empirical Assessment Of Ml Models For 5g Network Intrusion Detection: A Data Leakage-Free Approach. E-Prime - Advances In Electrical Engineering Electronics And Energy, 8, 100590. Https://Doi.Org/10.1016/J.Prime.2024.100590
Cele, N. N., & Kwenda, S. (2024). Do Cybersecurity Threats And Risks Have An Impact On The Adoption Of Digital Banking? A Systematic Literature Review. Journal Of Financial Crime. Https://Doi.Org/10.1108/Jfc-10-2023-0263
Choiri, A. (2025). The Role Of Artificial Intelligence (Ai) In Economic And Labor Market Transformation.
Danh, H. C., & Dang, D. T. (2021). Intention To Reuse M-Payment Services: Lessons From The Pandemic Times. Contaduría Y Administración, 66(5), 290. Https://Doi.Org/10.22201/Fca.24488410e.2021.3014.
Dermawan, I. M., Baidawi, A., Iksan, I., & Dewi, S. M. (2023). Serangan Cyber Dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. Jurnal Informasi Dan Teknologi, 5(3), 20. Https://Doi.Org/10.60083/Jidt.V5i3.364
Elisa, E., & Zulinda, N. (2025). Qris: Solusi Pembayaran Digital Di Bank Syariah Indonesia Untuk Umkm.
Eskandarany, A. (2024). Adoption Of Artificial Intelligence And Machine Learning In Banking Systems: A Qualitative Survey Of Board Of Directors. Frontiers In Artificial Intelligence, 7. Https://Doi.Org/10.3389/Frai.2024.1440051
Falade, P. V., & Ogundele, G. B. (2023). Vulnerability Analysis Of Digital Banks' Mobile Applications. Arxiv (Cornell University). Https://Doi.Org/10.48550/Arxiv.2302.07586
Farayola, O. A. (2024). Revolutionizing Banking Security: Integrating Artificial Intelligence, Blockchain, And Business Intelligence For Enhanced
Cybersecurity. Finance & Accounting Research Journal, 6(4), 501. Https://Doi.Org/10.51594/Farj.V6i4.990
Hamadou, I., Yumna, A., Hamadou, H., & Jallow, M. S. (2024). Unleashing The Power Of Artificial Intelligence In Islamic Banking: A Case Study Of Bank Syariah Indonesia (Bsi). Modern Finance, 2(1), 131. Https://Doi.Org/10.61351/Mf.V2i1.116
Hamsin, M. K., Halim, A., & Anggriawan, R. (2023). Addressing Cybercrime In The Sharia Digital Wallet Industry: A Legal Perspective In The Indonesian Context. E3s Web Of Conferences, 440, 4016. Https://Doi.Org/10.1051/E3sconf/202344004016
Hassan, M. A., Shukur, Z., & Kamrul, M. (2020). An Improved Time-Based One Time Password Authentication Framework For Electronic Payments. International Journal Of Advanced Computer Science And Applications, 11(11). Https://Doi.Org/10.14569/Ijacsa.2020.0111146
Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal Ict Information Communication & Technology, 20(1), 42. Https://Doi.Org/10.36054/Jict-Ikmi.V20i1.305
Hilmi, M. A. A., Sumarudin, A., & Putra, W. P. (2020). One-Time-Password (Otp) Dengan Modifikasi Vigenere Chiper Dan Perangkat Usb Berbasis Microcontroller, Sensor Fingerprint, Dan Real Time Clock (Rtc) Untuk
Autentikasi Pengguna Pada Akses Aplikasi Web. Cyber Security Dan Forensik Digital, 3(2), 6. Https://Doi.Org/10.14421/Csecurity.2020.3.2.2082
Ikhsan, R. B., Fernando, Y., Prabowo, H., Yuniarty, Y., Gui, A., & Kuncoro, E. A. (2024). An Empirical Study On The Use Of Artificial Intelligence In The Banking Sector Of Indonesia By Extending The Tam Model And The Moderating Effect Of Perceived Trust. Digital Business, 100103. Https://Doi.Org/10.1016/J.Digbus.2024.100103
Ikudabo, A. O., & Kumar, P. (2024). Ai-Driven Risk Assessment And Management In Banking: Balancing Innovation And Security. International Journal Of Research Publication And Reviews,

5(10), 3573. Https://Doi.Org/10.55248/Gengpi.5.1024.2926
Iskandar, M., Hartoyo, H., & Hermadi, I. (2020). Analysis Of Factors Affecting Behavioral Intention And Use Of Behavioral Of Mobile Banking Using Unified Theory Of Acceptance And Use Of Technology 2 Model Approach.
International Review Of Management And Marketing, 10(2), 41. Https://Doi.Org/10.32479/Irmm.9292
Jernih, & Laksono, B. (2025). Penerapan Kecerdasan Buatan (Ai) Dalam Praktik Akuntansi Di Indonesia.
Khan, H. U., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2022). Role Of Authentication Factors In Fin-Tech Mobile Transaction Security. Research Square (Research Square). Https://Doi.Org/10.21203/Rs.3.Rs-2365318/V1
Khan, H. U., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2023). Role Of Authentication Factors In Fin-Tech Mobile Transaction Security. Journal Of Big Data, 10(1). Https://Doi.Org/10.1186/S40537- 023-00807-3
Kurniawan, Y., & Kelly, V. (2024). Examining The Factors Driving Digital Banking Adoption In Indonesia: A Modified Technology Acceptance Model Approach. Journal Of Logistics Informatics And Service Science. Https://Doi.Org/10.33168/Jliss.2024.0626
Nikmah, L., Wahyuni, N. R. T., Iain, W. N., & Zunaidi, A. (2025). Optimizing Liquidity Management In Islamic Banks: A Risk And Shariah Compliance Perspective.
Nurahmasari, M., Silfiyah, S. N., & Pangaribuan, C. H. (2023). The Intention To Use Digital Banking Services Among Gen Z In Indonesia Based On The Technology Acceptance Model (Tam).
Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., & Ajayi-Nifise, A. O. (2024). Integrating Ai With Blockchain For Enhanced Financial Services
Security. Finance & Accounting Research Journal, 6(3), 271. Https://Doi.Org/10.51594/Farj.V6i3.855
Okoye, C. C., Nwankwo, E. E., Usman, F. O., Mhlongo, N. Z., Odeyemi, O., & Ike, C. U. (2024). Securing Financial Data Storage: A Review Of Cybersecurity Challenges And Solutions [Review Of Securing Financial Data Storage: A Review Of Cybersecurity Challenges And Solutions]. International
Journal Of Science And Research Archive, 11(1), 1968. Https://Doi.Org/10.30574/Ijsra.2024.11.1.0267
Oktaviani, S., & Basyariah, N. (2022). Analisis Manajemen Risiko Layanan Mobile Banking Pada Bank Syariah. Jurnal Manajemen Dan Penelitian Akuntansi, 15(1), 29. Https://Doi.Org/10.58431/Jumpa.V15i1.183
Oloyede, J. (2024). Leveraging Artificial Intelligence For Advanced Cybersecurity Threat Detection And Prevention. Ssrn Electronic Journal. Https://Doi.Org/10.2139/Ssrn.4976072
Omokanye, A. O., Ajayi, A. A., Olowu, O., Adeleye, A. O., Chianumba, E. C., & Omole, O. M. (2024). Ai-Powered Financial Crime Prevention With Cybersecurity, It, And Data Science In Modern Banking. International Journal Of Science And Research Archive, 13(2), 570. Https://Doi.Org/10.30574/Ijsra.2024.13.2.2143
Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity Risks In Online Banking: A Detailed Review And Preventive Strategies Applicatio [Review Of Cybersecurity Risks In Online Banking: A Detailed Review And Preventive Strategies Applicatio]. World Journal Of Advanced Research And Reviews, 21(3), 625. Gsc Online Press. Https://Doi.Org/10.30574/Wjarr.2024.21.3.0707
Pasandi, H. B., & Parastar, F. (2024). Location Privacy In B5g/6g: Systematization Of Knowledge. Arxiv (Cornell University). Https://Doi.Org/10.48550/Arxiv.2406.00359
Patil, D. (2025). Artificial Intelligence In Financial Services: Advancements In Fraud Detection, Risk Management, And Algorithmic Trading Optimization. Https://Doi.Org/10.2139/Ssrn.5057412
Pattnaik, D., Ray, S., & Raman, R. (2023). Applications Of Artificial Intelligence And Machine Learning In The Financial Services Industry: A Bibliometric Review [Review Of Applications Of Artificial Intelligence And Machine Learning In The Financial Services Industry: A Bibliometric Review].
Heliyon, 10(1). Elsevier Bv. Https://Doi.Org/10.1016/J.Heliyon.2023.E23492
Prabowo, I. D., & Supardal, S. (2025). Analisis Faktor-Faktor Yang Mempengaruhi Efektivitas Pengawasan Inspektorat Daerah Istimewa Yogyakarta.
Social Jurnal Inovasi Pendidikan Ips, 4(4), 731. Https://Doi.Org/10.51878/Social.V4i4.4514
Raharja, I. M. S., & Ashari, A. (2021). Enhancing Security System Of Short Message Service For Banking Transaction. International Journal Of Computing, 31. Https://Doi.Org/10.47839/Ijc.20.1.2089
Rahmayanti, P. L. D., Dharmanegara, I. B. A., Yasa, N. N. K., Sukaatmadja, I. P. G., Pramudana,

K. A. S., Rahanata, G. B., Giantari, I. G. A. K., & Martaleni, M. (2021). What Drives Millennials And Zillennials Continuously Using Instant Messaging? Perspective From Indonesia. International Journal Of Data And Network Science, 6(1), 17. Https://Doi.Org/10.5267/J.Ijdns.2021.11.001

Restika, & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan Di Era Digital.

Riasat, I., Shah, M., & Gönül, M. S. (2025). Strengthening Cybersecurity Resilience: An Investigation Of Customers' Adoption Of Emerging Security Tools In Mobile Banking Apps. Computers, 14(4), 129. Https://Doi.Org/10.3390/Computers14040129

Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024). Ai In The Financial Sector: The Line Between Innovation, Regulation And Ethical Responsibility. Information, 15(8),
432. Https://Doi.Org/10.3390/Info15080432

Salam, A., & Putri, E. L. (2023). Implementasi Teknologi Cloud Computing Pada Bidang Perbankan (Study Literature). Jurnal Kajian Teknik Elektro, 8(2), 100. Https://Doi.Org/10.52447/Jkte.V9i2.7732

Saparudin, M., Rahayu, A., Hurriyati, R., & Sultan, M. A. (2020). Exploring The Role Of Trust In Mobile- Banking Use By Indonesian Customer Using Unified Theory Of Acceptance And Usage Technology. International Journal Of Financial Research, 11(2), 51. Https://Doi.Org/10.5430/Ijfr.V11n2p51

Sudarsono, H., Kholid, M. N., Trisanty, A., & Maisaroh, M. (2022). The Intention Of Muslim Customers To Adopt Mobile Banking: The Case Of Islamic Banks In Indonesia. Cogent Business & Management,
9(1). Https://Doi.Org/10.1080/23311975.2022.2154102

Swetha, T., Kumaran, U., Meena, V. P., & Hameed, I. A. (2025). Leveraging Ai For Enhanced Cybersecurity: A Comprehensive Review [Review Of Leveraging Ai For Enhanced Cybersecurity: A Comprehensive Review]. Deleted Journal, 7(6). Https://Doi.Org/10.1007/S42452-025-06773-0

Trinh, T. T. H., Le, H. B. H., & Nguyen, N. H. (2020). Factors Affecting Private Customers In Adopting Mobile Banking In Vietnam. Management Science Letters, 2769. Https://Doi.Org/10.5267/J.Msl.2020.4.033

Vu, N. V., Nazari, M. A., Dang, T., Muralev, Y., Mohanraj, M., Tran, T., & Quoc, H. A. (2025). Type Of The Paper: Article. Https://Doi.Org/10.2139/Ssrn.5384374

Waliullah, Md., George, M. J., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. (2025). Assessing The Influence Of Cybersecurity Threats And Risks On The Adoption And Growth Of Digital Banking: A Systematic Literature
Review. 1(1), 226. Https://Doi.Org/10.63125/Fh49az18