Mantik Journal, 8 (3) (2024), ISSN 2685-4236 (Online)

Published by: Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik

The impact of end-to-end encryption on the security of digital banking transactions: an in-depth analysis

Ziqrurrahman Irsyad[1], Nurul Hidayati Indraningsih[2]
[1,2]Business Administration, University of Muhammadiyah Mataram, Indonesia

A R T I C L E I N F O

Article history:

Received Nov 11, 2024
Revised Nov 22, 2024
Accepted Nov 30, 2024

Keywords:

Data Integrity;
Digital Banking;
End-to-End Encryption;
Transaction Security.

ABSTRACT

This study aims to evaluate the impact of end-to-end encryption (E2EE) on the security of digital banking transactions through a systematic literature review method. The literature sources are from Scholar, DOAJ, and Scopus indexers in the last ten years. The analysis confirmed that E2EE plays a crucial role in enhancing the security of digital banking transactions. Data inclusion criteria included empirical studies, literature reviews, and other research articles that directly addressed the implementation, benefits, or challenges of E2EE in digital banking transactions. The research procedure began with the formulation of research questions, development of a research protocol, systematic literature search, screening of search results, and data extraction and analysis to identify key findings, trends, and research gaps. E2EE has proven to be effective in maintaining confidentiality, data integrity, and protecting information from unauthorized access and eavesdropping. The implementation of E2EE, especially in cloud storage and mobile banking, strengthens security measures and reduces the risk of fraudulent activities. The findings underscore the importance of E2EE adoption to strengthen security systems in the digital banking sector. The study further recommends further research into the integration of E2EE with blockchain technology and its implications for information security policies.

Corresponding Author:

Nurul Hidayati Indraningsih,
Business Administration,
University of Muhammadiyah Mataram,
Jl. KH. Ahmad Dahlan No.1, Mataram, NTB, 83115, Indonesia.
Email: indraningsih21@gmail.com

1. INTRODUCTION

The growth of digital banking and its popularity among consumers is a significant phenomenon in the modern banking landscape. The development of information technology has transformed the banking industry from a traditional system to a digital one, offering easy access and convenience through services such as internet banking, mobile banking, and digital payment applications (Sardana & Singhania, 2018). Consumers can now manage accounts, transfer funds, pay bills, and apply for loans without the need to visit a physical branch office. This has driven the widespread adoption of digital banking, especially among the tech-savvy younger generation, and

accelerated by the COVID-19 pandemic, which has increased the need for cashless transactions (Wasyith, 2019). Digital banking services cover a wide range of features, from balance checking to investment management and credit-based lending, enabling transactions anytime and anywhere. Innovations such as artificial intelligence (AI) and big data analytics enable personalization of services, while integration with e-commerce and fintech expands the reach and functionality of digital banking (Fang, 2023). All of these improve the user experience and operational efficiency of banks, enabling cost reductions and increased profitability.

The importance of transaction security in the context of digital banking cannot be overlooked. Transaction security refers to the protection of financial data and information exchanged during the transaction process, ensuring that it is not accessed or modified by unauthorized parties (Tkachenko *et al.*, 2019). In digital banking, common security threats include phishing, where attackers try to obtain sensitive information by posing as trusted entities; malware, malicious software that can steal data or damage systems; and data breaches, where personal and financial information is stolen by hackers (Chernyakov & Chernyakova, 2018). These threats show how vulnerable digital banking systems are to cyberattacks. Therefore, strong security measures are urgently needed to protect sensitive financial information. This includes the use of data encryption, multi-factor authentication, and real-time threat monitoring and countermeasures (Ashmarina & Vochozka, 2019).

Encryption is a cryptographic technique that secures digital communications by converting data into a code that can only be read by those who have the decryption key (Riadi *et al.*, 2022). Encryption methods include symmetric encryption, such as AES which is efficient, and asymmetric encryption, such as RSA which is secure but slower (Ali, 2019). End-to-end encryption (E2EE) is a type of asymmetric encryption that ensures data can only be accessed by the sender and intended recipient, without third-party intervention (Dahiya & Kumar, 2018). The adoption of E2EE in the banking industry is increasing, with many banks implementing it to protect customer data and online transactions. Despite its effectiveness, E2EE implementation faces challenges such as impact on system performance, high cost, and technical complexity. In addition, there are legal and ethical considerations regarding government access to encrypted data, as well as regulations that banks must comply with (Shaukat *et al.*, 2016). Overall, E2EE offers significant improvements in the security of digital transactions, but requires a strategic approach to overcome its challenges.

Bank of America, for instance, has successfully implemented E2EE in its online and mobile banking services to protect customers' sensitive data during transmission. This implementation not only enhances security but also strengthens customer trust in the digital banking services offered (Bank of America, 2024). End-to-end encryption plays a crucial role in enhancing the security of digital banking transactions. Various encryption methods such as RSA, SHA-256, and hybrid encryption techniques are applied to protect financial data (Azhari *et al.*, 2022). Blockchain technology, which combines cryptographic algorithms such as RSA and SHA-256 hashes, is utilized to secure data and reduce the risk of cyberattacks in digital banking systems (Aziz *et al.*, 2021). In addition, the use of blockchain in banking transactions ensures a high level of security by creating secure and difficult-to-modify data blocks, which provides a reliable and transparent transaction network in finance (Sanchiga & Padmapriya, 2023). The implementation of hybrid encryption methods, which combine symmetric and asymmetric encryption, further strengthens the security in digital data transmission, making it more resilient to various security threats in the digital age (Kuppuswamy *et al.*, 2023).

Beyond its technical advantages, E2EE also aligns with the principles of Islamic banking, particularly in ensuring transparency and trustworthiness. By guaranteeing data confidentiality, integrity, and authenticity, E2EE supports the ethical principles of

Sharia, which emphasize honesty, transparency, and the protection of customer rights (Mohamud, 2023 & Wahab, 2020). One prominent case study demonstrates the use of a hybrid algorithm combining least significant bits (LSB) and advanced encryption standards (AES) to protect data transmissions in mobile banking applications. This approach has proven effective against potential threats such as Man-in-the-Middle attacks, further showcasing the adaptability of E2EE to meet the specific needs of Islamic banking (Orucho *et al.*, 2023). This alignment demonstrates how E2EE can mitigate risks such as fraud and data breaches while simultaneously addressing regulatory requirements specific to Islamic finance. Its dual functionality as a security and compliance tool highlights its importance in Islamic banking contexts (Knodel *et al.*, 2021).

The digital transformation in Islamic banking offers significant challenges and opportunities. While it improves accessibility, operational efficiency, and product innovation (Naimi *et al.*, 2022 & Kamra, 2018), it also raises concerns related to cyber security, digital literacy, and Shariah compliance (H. Osman *et al.*, 2021). The implementation of blockchain technology in Islamic finance shows potential to improve transparency, risk awareness, and efficiency, but faces obstacles in standardization and regulation (Chong, 2021). To overcome these challenges, strengthening regulation is essential, especially in prudent banking principles, governance, and IT risk management for digital banks (Härle *et al.*, 2016). The adoption of fintech in Islamic banking can improve financial inclusion and expand access for MSMEs, but requires significant investment and rapid innovation (Rasheed *et al.*, 2019 & Ana, 2021). Overall, successful integration of digital technology in Islamic banking requires a balanced approach that capitalizes on opportunities while addressing regulatory and technical challenges.

Based on the research findings, there are several gaps related to the use of end-to-end encryption (E2EE) in improving the security of digital banking transactions. While many studies highlight the benefits of E2EE in protecting data confidentiality and integrity, further exploration is needed regarding the implementation of hybrid encryption technologies or integration with blockchain. In-depth studies can provide insights into the effectiveness of these technologies in overcoming complex cyberattacks. In addition, regulatory constraints and Shariah compliance need to be clarified to ensure conformity with Shariah legal and ethical principles. A comparison of regulations across different countries can provide a comprehensive understanding of the legal challenges faced. Research also needs to explore the social and economic impact of E2EE adoption, particularly in improving financial inclusion and accessibility for MSMEs. By identifying these gaps, this research aims to explore the implementation and benefits of E2EE and fill knowledge gaps to support the development of policies and best practices in digital transaction security.

2. BACKGROUND OF THE STUDY

The rapid digital transformation in the banking sector has introduced significant challenges related to cybersecurity. As digital banking services become increasingly widespread, ensuring the security of sensitive financial data has emerged as a critical issue. Cyber threats such as data breaches, phishing, and unauthorized access have highlighted the need for robust security measures to protect digital transactions. End-to-end encryption (E2EE) has been identified as a potential solution to these challenges, offering enhanced data confidentiality and integrity by securing communications between endpoints.

Despite its growing adoption, several gaps remain in the implementation of E2EE in digital banking. Current studies often focus on its technical benefits but provide limited insights into its integration with other emerging technologies, such as blockchain, or its adaptability in diverse regulatory environments. Additionally, the practical

challenges, including high costs and technical complexity, create barriers to its widespread adoption, particularly in developing countries.

This research is significant as it explores not only the technical benefits of E2EE but also its broader implications, such as its influence on digital banking policies, compliance with regulatory frameworks, and social acceptance in different contexts. By addressing these issues, this study aims to contribute to the development of a more secure and reliable digital banking ecosystem. The primary objectives include examining the effectiveness of E2EE in digital banking security, exploring its integration with other technologies, and identifying challenges and opportunities for its implementation.

3. RESEARCH METHOD

This research aims to investigate the impact of using end-to-end encryption (E2EE) in enhancing the security of digital banking transactions. The main focus is to identify the security benefits offered by E2EE, as well as to explore the challenges and constraints associated with its implementation in the modern digital banking context. A literature search was conducted by searching for related articles, journals and publications from academic databases such as Scopus, DOAJ, Google Scholar and specific databases related to information security and banking technology. The keywords used included “end-to-end encryption”, “digital banking”, “cybersecurity”, “blockchain”, and “hybrid encryption”. The search considered recent articles published within the last 10 years (2013-2024) to ensure relevance to current technologies and issues.

Inclusion criteria included empirical studies, literature reviews, and other research articles that directly addressed the implementation, benefits, or challenges of E2EE in digital banking transactions. To ensure that the criteria produce a balanced and focused dataset, additional filtering was applied during the selection process. Articles were evaluated not only for relevance to the research topic but also for their contribution to specific aspects of E2EE, such as its technical implementation, security benefits, or contextual challenges. This approach prevents the inclusion of excessively diverse data while maintaining enough breadth to explore multiple dimensions of the topic comprehensively. As a result, the final dataset is both diverse and manageable, allowing for consistent and in-depth analysis.

Exclusion criteria included news articles, editorials, and materials not directly related to the topic of this research. To ensure that the data extracted from the selected articles is not only relevant but also of high methodological quality, a standardized quality appraisal process was conducted. Each study was evaluated using the Critical Appraisal Skills Programme (CASP) checklist or equivalent tools suitable for its design. This appraisal assessed the rigor of the research methodology, clarity of findings, and validity of conclusions. Studies that failed to meet the quality threshold were excluded from the final analysis. The extracted data included information on the research methodology, key findings, and implications for the security of digital banking transactions. This systematic approach ensured that the data used in this research was both relevant and methodologically robust, supporting the credibility of the study's findings. The research procedure can be seen in Figure 1.

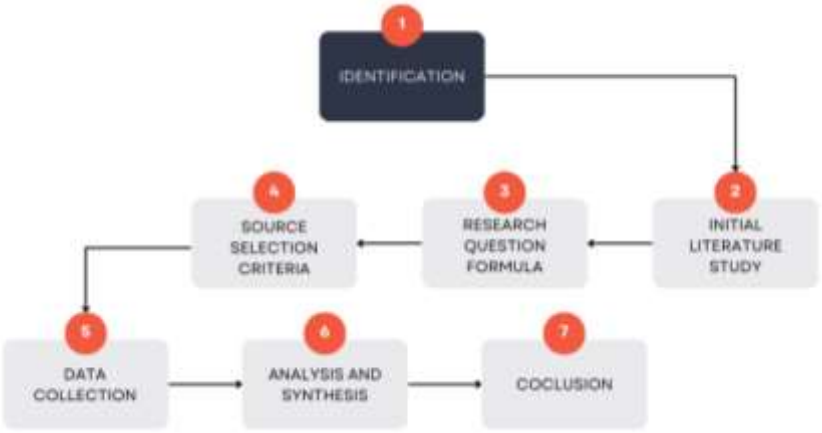

Figure 1. Research Prosedure

Figure 1 presents the research procedure, which begins with the formulation of a clear and specific research instrument related to the impact of end-to-end encryption (E2EE) on the security of digital banking transactions. The next step was the development of a research protocol that included setting inclusion and exclusion criteria and identifying relevant data sources. Then, a systematic literature search was conducted using predefined keywords on relevant academic databases such as Google Scholar, DOAJ, and Scopus. Search results were filtered by title and abstract to eliminate irrelevant articles. Articles that passed the initial screening were further evaluated through full reading to ensure they met the inclusion criteria. Data from the selected articles will then be extracted and analyzed to identify key findings, trends, and research gaps. The conclusions from this analysis will be used to develop policy recommendations and best practices for the use of E2EE in the digital banking sector.

4. RESULTS AND DISCUSSIONS

Based on the search results, several relevant research findings have been identified that can shed light on the focus and objectives of this study. We have formulated several aspects that need to be explained, including: (1) the effectiveness of end-to-end encryption (E2EE) in enhancing the security of digital banking data, (2) the integration of E2EE technology with other solutions such as blockchain in digital banking systems, (3) the influence of social and cultural factors on the adoption of E2EE technology in the banking sector, and (4) the specific technical challenges and barriers faced in the implementation of E2EE. In addition, the importance of effective regulation and governance will also be discussed as crucial factors in ensuring operational success and security in the digital transformation of the banking sector in this modern era.

Table 1. Focus and Insight into Research Results in accordance with Eligibility Criteria

No	Focus and Scope	Author	Insight
1	Data Security	Gangele (2024), Ashiqul Islam et al. (2021), Limoncelli (2023), Filchev et al. (2023), Neza et al. (2022)	The role of E2EE in ensuring the confidentiality and integrity of digital banking transaction data.
2	Cloud Storage	Sinha et al. (2023)	Data protection in cloud storage environments through E2EE.
3	Blockchain Integration	Sanchiga & Arumugam (2023)	Integration of E2EE with blockchain in mobile banking to enhance security
4	User Authentication	Karim et al. (2022), Bezhovski (2016), Filchev et	Strengthening user authentication with E2EE to protect against cyber

		al. (2023), Viswesh & Vinothiyalakshmi (2023), Nair et al. (2019)	threats.
5	Advanced Encryption Standard (AES)	Neza et al. (2022), Adhiwibowo et al. (2022), Sepdian et al. (2021), Sugawara & Nikaido (2014b)	The use of AES in smart devices and banking systems to protect data.
6	Information Security Priorities	Kumar & Gupta (2020)	Focus on data confidentiality, integrity and availability in the banking information security system.
7	Internal Control	Alina Boitan (2019)	Strengthening internal control functions to improve service quality and regulatory compliance.
8	Digital Transformation Challenges	Khalatur et al. (2022), Amiri et al. (2023), Sasea & Sakmaf (2023)	Challenges of digital transformation in banking such as high investment costs and data security risks.
9	Regulatory and Risk Management	Abubakar & Handayani (2022), Pratama (2021)	Strengthening regulations related to information technology risk management for digital banks.
10	Technical Challenges	Pramana & Suryani (2024), Widyastuti et al. (2017), Zakia & Marliyah (2023)	Specific barriers in the implementation of electronic money systems and technology integration challenges.
11	Digital Literacy	Mulyana et al. (2024)	Digital literacy issues in the implementation of digital banking technology.
12	Social and Cultural Factors	Zakia & Marliyah (2023)	Preference for traditional payment methods that hinder the adoption of new technologies.
13	Business Model Challenges	Pramana & Suryani (2024)	Lack of experience in B2C business models in financial institutions.

Table 1 shows that the implementation of end-to-end encryption (E2EE) has a significant impact in enhancing the security of digital banking transactions by ensuring data confidentiality and integrity and protecting against unauthorized access and eavesdropping. The integration of E2EE with other technologies such as blockchain and AES also strengthens security measures in digital banking systems and smart devices. However, the implementation of these technologies faces technical challenges that include the need for strengthening internal controls and improving technological skills. In addition, social and cultural factors and specific barriers in the e-money system hinder the adoption of these technologies in Indonesia. Therefore, strengthened regulation and governance in the areas of information technology and risk management are necessary to overcome these challenges and ensure the successful implementation of safe and effective digital banking technology.

4.1 End-To-End Encryption (E2EE) Implementation Enhances Digital Banking Transaction Security

End-to-end encryption (E2EE) plays an important role in enhancing the security of digital banking transactions by ensuring data confidentiality and integrity (Gangele, 2024; Ashiqul Islam *et al.*, 2021 & Limoncelli, 2023). E2EE encrypts data at the source and decrypts data only at its intended destination, preventing unauthorized access and eavesdropping, especially in cloud storage environments (Sinha *et al.*, 2023). Moreover, the integration of E2EE with technologies such as blockchain in mobile banking systems provides strong security measures, making transactions more secure and resistant to fraudulent activities (Sanchiga & Arumugam, 2023). By utilizing E2EE, banks can protect sensitive financial information, securely authenticate users, and protect against

various cyber threats, ultimately strengthening the overall security of digital banking transactions in the modern era.

End-to-end encryption (E2EE) is essential for improving the security of digital banking. Implementing the Advanced Encryption Standard (AES) on smart home devices can protect user data from unauthorized access and alteration (Neza *et al.*, 2022). In the banking sector, information security systems prioritize confidentiality, integrity and availability, with availability being paramount for Internet Banking users (Kumar & Gupta, 2020). As banks undergo digital transformation, they face challenges such as high investment costs, the need for rapid innovation, and data security risks (Khalatur *et al.*, 2022). To address these issues, it is necessary to strengthen regulations related to information technology risk management for digital banks. In addition, implementing protocols such as S/MIME in email services can enhance security by providing digital signatures and encryption, which ensure confidentiality, integrity, authentication and non-repudiation in online information transactions (Sugawara & Nikaido, 2014b).

The implementation of end-to-end encryption (E2EE) has a significant positive impact on the security of digital banking transactions. This technology not only strengthens protection against unauthorized access and data interception, but also provides a solid foundation for maintaining the confidentiality of sensitive information in digital data storage and transmission. Integration with blockchain technology provides an additional solution in the face of increasingly sophisticated security challenges, such as fraudulent activities in mobile banking. However, the successful implementation of E2EE is challenged by high investment costs and strict regulations on information technology risk management. Strong regulations are needed to ensure that additional technologies such as S/MIME in email services can enhance security with adequate digital signatures and encryption. In the face of these complexities, a comprehensive strategy is needed to maximize the security potential of E2EE by considering relevant economic and regulatory aspects. Overall, E2EE is an effective solution in strengthening the security of digital banking transactions, but its success requires an integrated approach between technology, regulation and risk management. The involvement of all relevant parties, including regulators, banking institutions, and technology providers, is key to ensuring optimal data protection and transaction security in today's digital era.

4.2 Key Benefits of Using E2EE to Protect the Confidentiality of Digital Banking Transaction Data

End-to-end encryption (E2EE) plays an important role in maintaining the confidentiality of digital banking transaction data by ensuring secure data transfer and protection from unauthorized access (Karim *et al.*, 2022; And, 2016). E2EE enhances security by encrypting information from the point of transmission to the final recipient, preventing unauthorized or malicious users from intercepting sensitive data (Filchev *et al.*, 2023). This encryption method is particularly important in online banking, where user authentication and secure data transfer are essential to prevent cybercrime and fraudulent activities (Viswesh & Vinothiyalakshmi, 2023; Nair *et al.*, 2019). By leveraging E2EE, financial institutions can offer more direct and secure movement of payment information between transacting entities, minimizing the risk of data breaches and ensuring the integrity of digital transactions (Mahalle *et al.*, 2019). Overall, E2EE provides a strong layer of protection that is essential in maintaining the confidentiality and integrity of digital banking transactions in today's advanced technology landscape (Potoglou *et al.*, 2017).

End-to-end encryption (E2EE) is essential in maintaining the confidentiality of digital banking transaction data. E2EE techniques, such as Advanced Encryption Standard (AES), can significantly improve data security on smart devices and servers (Adhiwibowo *et al.*, 2022). Combining cryptography and steganography can create a strong data security system, with methods such as the Rabin Public Key algorithm and

End of File techniques being effective in encrypting and hiding sensitive information (Sepdian *et al.*, 2021). RSA encryption algorithm has been applied successfully in e-voting applications to secure data transfer and maintain voter privacy (Juniawan, 2016). As digital technology advances, the importance of securing electronic transactions is increasing. The increasingly commonly used digital currencies and electronic payment systems emphasize the need for strong encryption methods to protect financial data in the digital era (Danuri Muhamad, 2019).

The implementation of end-to-end encryption (E2EE) in digital banking transactions effectively enhances data security by preventing unauthorized access and eavesdropping, and reduces the risk of fraudulent activities and cybercrime. The use of E2EE enables financial institutions to secure data transfer and user authentication, which are essential in online banking to protect sensitive information. While E2EE offers strong protection, challenges remain, especially in terms of high investment costs and the need for strict regulations regarding information technology risk management. Strong regulations are needed to ensure the implementation of additional technologies such as S/MIME can enhance security through digital signatures and adequate encryption. Therefore, while E2EE has demonstrated effectiveness in maintaining data confidentiality and integrity, a mature and comprehensive approach is needed to overcome these challenges and optimize the benefits provided by this technology.

4.3 Technical Challenges in E2EE Implementation Affect Its Effectiveness in the Context of Digital Banking

The implementation of end-to-end encryption (E2EE) in digital banking faces technical challenges that can impact its effectiveness. The growth of digitalization in the banking industry requires a focus on security aspects while optimizing digital technology systems to ensure customer trust and data protection (Sasea & Sakmaf, 2023). In addition, successful implementation of digital banking depends on factors such as human resources, rules and regulations, and customer satisfaction, highlighting the importance of overcoming technical challenges in E2EE implementation (Amiri *et al.*, 2023). Strengthening internal control functions such as Compliance, Risk Management, and Internal Audit with enhanced technological skills is critical to ensuring regulatory compliance and improving customer service quality in the digital banking landscape (Alina Boitan, 2019). Overcoming these technical challenges is critical to maintaining customer trust, protecting sensitive data, and ensuring smooth operation of digital banking services.

The implementation of digital banking technology in Indonesia faces various challenges. These include cybersecurity concerns, digital literacy issues, and system integration difficulties (Mulyana *et al.*, 2024). Regulatory strengthening is needed to address these challenges, especially in the areas of information technology governance and risk management for digital banks (Abubakar & Handayani, 2022). Specific barriers to the implementation of electronic money systems include limited acceptance by merchants, limited access methods and transaction channels, transaction costs, and competition with similar products (Widyastuti *et al.*, 2017). Social and cultural factors, such as preference for traditional payment methods, also hinder the adoption of this technology (Zakia & Marliyah, 2023). For financial institutions, challenges include a lack of experience in B2C business models and difficulties in acquiring new customers (Pramana & Suryani, 2024). Despite the challenges, the right implementation strategy can help overcome these barriers and capitalize on the opportunities offered by financial technology in Islamic banking (Pratama, 2021).

End-to-end encryption (E2EE) is an effective method to protect digital banking transaction data from unauthorized access and eavesdropping, but the technical challenges in its implementation cannot be ignored. These challenges include the need to strengthen internal controls such as Compliance, Risk Management, and Internal Audit,

which require better technological skills. In Indonesia, the implementation of digital banking technology also faces barriers such as cybersecurity concerns, low digital literacy, and difficulties in system integration. In addition, social and cultural factors, such as people's preference for traditional payment methods, also affect the adoption of these technologies. To optimize the impact of E2EE, a comprehensive strategy and strengthened regulations in the areas of information technology governance and risk management, as well as improved digital literacy and effective system integration are required. Thus, while E2EE has great potential in enhancing the security of digital banking transactions, its successful implementation is highly dependent on the ability to overcome the existing technical and social challenges.

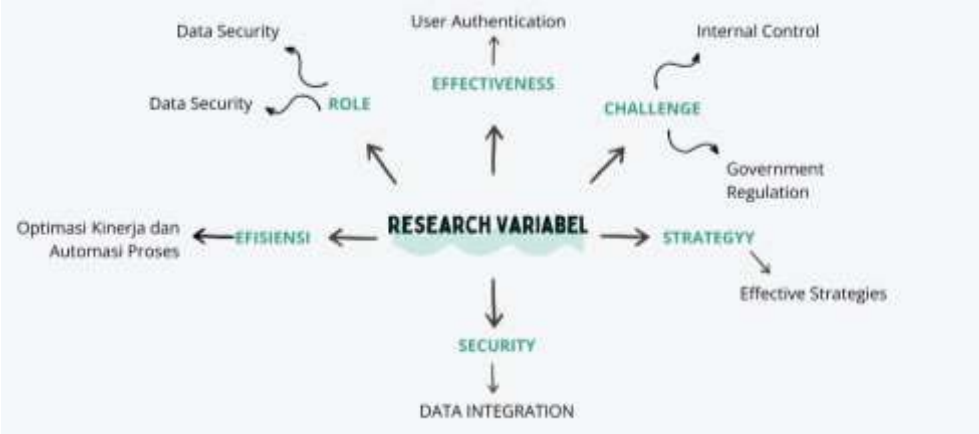

Figure 2. Development of Research Variables

Figure 2 shows that end-to-end encryption (E2EE) plays an important role in enhancing the security of digital banking transactions by ensuring data confidentiality and integrity, and protecting data in cloud storage. E2EE, which consists of Advanced Encryption Standard (AES) to maintain data security and integrity, supports secure user authentication and enhances the security of mobile banking transactions through integration with blockchain technology. The implementation of E2EE in digital banking involves strengthening internal controls and prioritizing information security, such as data confidentiality, integrity and availability. Challenges faced in implementing E2EE include government regulations, risk management, internal controls, issues, and limited transaction channels. To overcome these challenges, an effective implementation strategy is needed to capitalize on the opportunities of financial technology and ensure security and user confidence in digital banking services. By understanding the challenges and implementing the right strategies, E2EE can become a key pillar in the protection of sensitive data against evolving cyber threats.

5. CONCLUSION

This research confirms the importance of end-to-end encryption (E2EE) in enhancing the security of digital banking transactions. E2EE is proven to be effective in maintaining data confidentiality and integrity and protecting information from unauthorized access and eavesdropping. The implementation of E2EE, especially in cloud storage environments and mobile banking systems, can enhance security measures and make transactions safer from fraudulent activities. However, this study also identified some gaps that require further attention. Among them is the need for deeper research on the implementation of hybrid encryption technologies, integration with blockchain technology, as well as exploration of regulatory constraints and Shariah compliance. The

findings of this research highlight the potential of E2EE to influence digital banking policies in developing countries. In regions with significant infrastructure and regulatory challenges, E2EE can serve as a critical tool to enhance security while addressing technological limitations. Policymakers can use these insights to develop frameworks that encourage the adoption of encryption technologies, ensuring compatibility with local conditions while supporting digital banking transformation. To measure the success of E2EE implementation in digital banking transactions, banks can utilize key performance indicators (KPIs) such as the reduction in fraud incidents, increased consumer trust, improved compliance with cybersecurity regulations, and enhanced system reliability. Comparative studies between banks that have implemented E2EE and those that have not can offer benchmarks for evaluating its effectiveness and identifying areas for improvement. These metrics not only help in assessing the impact of E2EE but also provide actionable insights for continuous improvement. In addition, the social and economic impact of E2EE adoption, especially for MSMEs, also needs further research. Therefore, pressing research topics for the future include the effectiveness of hybrid encryption technology, the integration of E2EE with blockchain in Islamic banking, the impact of E2EE on financial inclusion and accessibility for MSMEs, and a comparison of international regulations on the use of E2EE. Further research in these topics is expected to fill the existing knowledge gaps and support the development of policies and best practices in digital transaction security in the future.

6. LIMITATIONS AND FUTURE WORK

This study primarily relies on a literature-based approach, which offers valuable insights into existing research but lacks empirical data or practical case studies to validate its findings. The absence of field-based evidence limits the ability to assess the real-world applicability of E2EE in diverse digital banking environments. Additionally, the focus of this study is primarily on E2EE in the context of digital banking, which may not capture its integration with emerging technologies like the Internet of Things (IoT) or quantum encryption, both of which are becoming increasingly relevant in enhancing cybersecurity measures.

Future research should address these gaps by incorporating empirical studies that involve stakeholders such as banking institutions, policymakers, and cybersecurity experts to gather practical insights into the challenges and effectiveness of E2EE implementation. Comparative studies across developed and developing countries could explore how regulatory frameworks, infrastructure limitations, and cultural factors affect E2EE adoption. Moreover, studies should investigate the economic feasibility and scalability of E2EE for small and medium-sized financial institutions, alongside its integration with blockchain and advanced encryption methods, to ensure adaptability in evolving digital ecosystems.

ACKNOWLEDGEMENTS

I sincerely express my gratitude to all parties who have supported the completion of this work. Special thanks to my family and friends for their continuous encouragement and support. Hopefully, this work can provide benefits and serve as a small contribution to the advancement of science.

REFERENCES

Abubakar, L., & Handayani, T. (2022). Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital. *Masalah-Masalah Hukum*, *51*(3), 259–270. https://doi.org/10.14710/mmh.51.3.2022.259-270

Adhiwibowo, W., Hirzan, A. M., & Suprayogi, M. S. (2022). Peningkatan Keamanan Data End-To-End Smart Door Menggunakan Advanced Encryption Standard. *Jurnal ELTIKOM*, *6*(2), 186–194. https://doi.org/10.31961/eltikom.v6i2.574

Ali, M. (2019). a Survey of the Most Current Image Encryption and Decryption Techniques. *International Journal of Advanced Research in Computer Science*, *10*(1), 9–14. https://doi.org/10.26483/ijarcs.v10i1.6350

Alina Boitan, I. (2019). *Cyber Security Challenges through the Lens of Financial Industry*. https://doi.org/10.33422/2nd.icmbf.2019.09.586

Amiri, M., Hashemi-Tabatabaei, M., Keshavarz-Ghorabaee, M., Antucheviciene, J., Šaparauskas, J., & Keramatpanah, M. (2023). Evaluation of Digital Banking Implementation Indicators and Models in the Context of Industry 4.0: A Fuzzy Group MCDM Approach. *Axioms*, *12*(6). https://doi.org/10.3390/axioms12060516

And, Z. B. (2016). The future of the mobile payment as electronic payment system. *European Journal of Business and Management*, *8*(8), 127–132. http://eprints.ugd.edu.mk/15691/

Ashiqul Islam, M., Kobita, A. A., Sagar Hossen, M., Rumi, L. S., Karim, R., & Tabassum, T. (2021). Data security system for a bank based on two different asymmetric algorithms cryptography. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 53, pp. 837–844). https://doi.org/10.1007/978-981-15-5258-8_77

Ashmarina, S., & Vochozka, M. (2019). Sustainable Growth and Development of Economic Systems Contradictions in the Era of Digitalization and Globalization. In (p. 396). http://www.springer.com/series/1262

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*. https://doi.org/10.47709/jpsk.v2i01.1390

Aziz, N., Rodiah, R., & Susanto, H. (2021). Encrypting of Digital Banking Transaction Records: An Blockchain Cryptography Security Approach. *International Journal of Computer Applications*, *174*(24), 21–26. https://doi.org/10.5120/ijca2021921147

Babu P Suresh. (2021). Digital Transformation in Banking Sector. *Happiest Minds Technologies*. issn: 0303-6286

Bank of America, B. (2024). *Online Banking uses industry-standard security protocols*. Https://Www.Bankofamerica.Com/. https://www.bankofamerica.com/online-banking/online-banking-security-faqs/?utm_source=chatgpt.com

Bitton, G., Fox, J. L., & Strickland, H. G. (1975). Removal of algae from Florida lakes by magnetic filtration. *Applied Microbiology*, *30*(6), 905–908. https://doi.org/10.1128/am.30.6.905-908.1975

Chernyakov, M., & Chernyakova, M. (2018). Technological Risks of the Digital Economy. *Journal of Corporate Finance Research / Корпоративные Финансы | ISSN: 2073-0438*, *12*(4), 99–109. https://doi.org/10.17323/j.jcfr.2073-0438.12.4.2018.99-109

Chong, F. H. L. (2021). Enhancing trust through digital Islamic finance and blockchain technology. *Qualitative Research in Financial Markets*, *13*(3), 328–341. https://doi.org/10.1108/QRFM-05-2020-0076

Dahiya, M., & Kumar, R. (2018). A Literature Survey on various Image Encryption Steganography Techniques. *ICSCCC 2018 - 1st International Conference on Secure Cyber Computing and Communications*, 310–314. https://doi.org/10.1109/ICSCCC.2018.8703368

Danuri Muhamad. (2019). Perkembangan Dan Transformasi Teknologi Digital. *Infokam*, *15*(2), 116–123.

Fang, Y. (2023). The Impact of Digital Finance on Tourism in Putuo Mountain. *Advances in Economics, Management and Political Sciences*, *55*(1), 183–189. https://doi.org/10.54254/2754-1169/55/20231005

Filchev, R., Dovramadjiev, T., Dimova, R., & Parushev, P. (2023). Protection and Transfer of Financial Digital Data Through Open Source Software. *Proceedings of the 6th International Conference on Intelligent Human Systems Integration (IHSI 2023) Integrating People and Intelligent Systems, February 22–24, 2023, Venice, Italy*, *69*. https://doi.org/10.54941/ahfe1002845

Gangele, S. (2024). Data Security System for a Bank Based on Two Different Asymmetric Algorithms Cryptography. *International Journal For Multidisciplinary Research*, *6*(1). https://doi.org/10.36948/ijfmr.2024.v06i01.11710

H. Osman, R. A., Zakariyah, L., Zakariyah, H., & Ahmad Dahlan, A. R. (2021). Cyber Security And Maqasid Al- Shariah: A Case Of Facebook Application. *International Research Journal of*

Shariah, Muamalat and Islam, *3*(6), 12–25. https://doi.org/10.35631/irjsmi.36002

Härle, P., Havas, R., Sam, H., & ari. (2016). The future of bank risk management | McKinsey & Company. *McKinsey & Company*, 1–7.

Imam Riadi, Abdul Fadlil, & Fahmi Auliya Tsani. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*. https://doi.org/10.14421/jiska.2022.7.1.33-45

Juniawan, F. P. (2016). RSA implementation for data transmission security in BEM chairman E-voting Android based application. *Proceedings - 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2016*, 93–98. https://doi.org/10.1109/ICITISEE.2016.7803054

Karim, N. K., Atikah, S., & Lenap, I. P. (2022). Faktor-Faktor Yang Memengaruhi Penggunaan Pembayaran Elektronik Non-Bank. *Jurnal Aplikasi Akuntansi*, *7*(1), 39–59. https://doi.org/10.29303/jaa.v7i1.147

Khalatur, S., Pavlova, H., Vasilieva, L., Karamushka, D., & Danilevič a, A. (2022). Innovation management as basis of digitalization trends and security of financial sector. *Entrepreneurship and Sustainability Issues*, *9*(4), 56–76. https://doi.org/10.9770/jesi.2022.9.4(3)

Knodel, M., Kolkman, O., Celi, S., & Grover, G. (2021). Definition of End-to-end Encryption. In *Internet Engineering Task Force Draft*.

Kumar, M., & Gupta, S. (2020). Security perception of e-banking users in India: An analytical hierarchy process. *Banks and Bank Systems*, *15*(1), 11–20. https://doi.org/10.21511/bbs.15(1).2020.02

Kuppuswamy, P., Al-Maliki, S. Q. Y. A. K., John, R., Haseebuddin, M., & Meeran, A. A. S. (2023). A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 1148–1158. https://doi.org/10.11591/eei.v12i2.4967

Limoncelli, T. A. (2023). Improvement on End-to-End Encryption May Lead to Silent Revolution. *Queue*, *21*(2). https://doi.org/10.1145/3590144

Mahalle, A., Yong, J., & Tao, X. (2019). Protecting Privacy in Digital Era on Cloud Architecture for Banking and Financial Services Industry. *BESC 2019 - 6th International Conference on Behavioral, Economic and Socio-Cultural Computing, Proceedings*. https://doi.org/10.1109/BESC48373.2019.8963459

Mohamud, H. A., & Farah, M. A. (2023). The Impact of E-Banking on Commercial Banks: A Literature Review. *International Journal of Membrane Science and Technology*, *10*(5), 504–512. https://doi.org/10.15379/ijmst.v10i5.2535

Mulyana, I., Hamid, A., & Syaripudin, E. I. (2024). Tantangan Dan Peluang Penggunaan Fintech Dalam Perbankan Syariah. *Jurnal Hukum Ekonomi Syariah (JHESY)*, *2*(2), 60–69. https://doi.org/10.37968/jhesy.v2i2.639

N Sanchiga Nandhini, & Padmapriya Arumugam. (2023). Digital currency banking using block chain technology. *World Journal of Advanced Engineering Technology and Sciences*, *8*(1), 053–061. https://doi.org/10.30574/wjaets.2023.8.1.0011

Naimi-Sadigh, A., Asgari, T., & Rabiei, M. (2022). Digital Transformation in the Value Chain Disruption of Banking Services. *Journal of the Knowledge Economy*, *13*(2), 1212–1242. https://doi.org/10.1007/s13132-021-00759-0

Nair, S., Khatri, S. K., & Gupta, H. (2019). A Model to Enhance Security of Digital Transaction. *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, 17–21. https://doi.org/10.1109/ISCON47742.2019.9036225

Neza, F., Joseph, A., & Joseph, M. (2022). E-Money Security Dilemma: Advanced Cybersecurity Mechanisms and Legacy Mobile Payments in Sub-Saharan Africa. *International Conference on Applied Computing 2022 and WWW/Internet 2022*, 103–114. https://doi.org/10.33965/ac_icwi2022_2022081013

Orucho, D. O., Awuor, F. M., Makiya, R., & Oduor, C. (2023). An Enhanced Data Transmission in Mobile Banking Using LSB-AES Algorithm. *Asian Journal of Research in Computer Science*, *16*(1), 43–56. https://doi.org/10.9734/ajrcos/2023/v16i1334

Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017). Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior*, *75*, 811–825. https://doi.org/10.1016/j.chb.2017.06.007

Pramana, A. M., & Suryani, E. (2024). Analisis Faktor Yang Mempengaruhi Adopsi Digital Banking

Di Indonesia Menggunakan Model Utaut2. *IDEALIS : InDonEsiA JournaL Information System*, *7*(1), 31–40. https://doi.org/10.36080/idealis.v7i1.3114

Pratama, A. P. R. (2021). Penguatan Digitalisasi Perbankan dalam Pelayanan Costumer Service Nasabah Secara Digital di Masa Covid-19. *Simbur Cahaya*, *28*(2), 312. https://doi.org/10.28946/sc.v28i2.1443

Rasheed, R., Siddiqui, S. H., Mahmood, I., & Khan, S. N. (2019). Financial Inclusion for SMEs: Role of Digital Micro-financial Services. *Review of Economics and Development Studies*, *5*(3), 429–439. https://doi.org/10.26710/reads.v5i3.686

Sardana, V., & Singhania, S. (2018). Digital technology in the realm of banking: A review of literature. *International Journal of Research in Finance and Management*, *1*(2), 28–32. https://doi.org/10.33545/26175754.2018.v1.i2a.12

Sasea, E. M., & Sakmaf, M. S. (2023). Digital Bank Legal Challenges: Security Protection and Leakage of Customer Personal Data. *Awang Long Law Review*, *6*(1), 245–250. https://doi.org/10.56301/awl.v6i1.989

Sepdian, H., Yulia Fatma, Soni, S., & Rizki, Y. (2021). Implementasi Steganografi EOF (End Of File) Pada File Gambar. *Jurnal CoSciTech (Computer Science and Information Technology)*, *2*(2), 108–112. https://doi.org/10.37859/coscitech.v2i2.2940

Shaukat, U., Ahmed, E., Anwar, Z., & Xia, F. (2016). Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges. In *Journal of Network and Computer Applications* (Vol. 62, pp. 18–40). https://doi.org/10.1016/j.jnca.2015.11.009

Sinha, S., Shankar, M., Pande, Y., Kumar, K., Sharma, S., & Virdi, K. (2023). Secure Cloud Storage using End-to-End Encryption. *International Journal for Research in Applied Science and Engineering Technology*, *11*(12), 567–574. https://doi.org/10.22214/ijraset.2023.57414

Sugawara, E., & Nikaido, H. (2014a). Properties of AdeABC and AdeIJK efflux systems of Acinetobacter baumannii compared with those of the AcrAB-TolC system of Escherichia coli. *Antimicrobial Agents and Chemotherapy*, *58*(12), 7250–7257. https://doi.org/10.1128/AAC.03728-14

Sugawara, E., & Nikaido, H. (2014b). Properties of AdeABC and AdeIJK efflux systems of Acinetobacter baumannii compared with those of the AcrAB-TolC system of Escherichia coli. In *Antimicrobial Agents and Chemotherapy* (Vol. 58, Issue 12, pp. 7250–7257). https://doi.org/10.1128/AAC.03728-14

Tkachenko, V., Kwilinski, A., Korystin, O., Svyrydiuk, N., & Tkachenko, I. (2019). Assessment of information technologies influence on financial security of economy. *Journal of Security and Sustainability Issues*, *8*(3), 375–385. https://doi.org/10.9770/jssi.2019.8.3(7)

Viswesh, G., & Vinothiyalakshmi, P. (2023). Secure Electronic Banking Transaction using Double Sanction Security Algorithm in Cyber Security. *2023 IEEE International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering, RMKMATE 2023*. https://doi.org/10.1109/RMKMATE59243.2023.10369665

Wasyith, W. (2019). Does Technology Matter?: literature Review Adopsi Teknologi Dalam Riset Ekonomi Keuangan Syariah. *Al-Urban: Jurnal Ekonomi Syariah Dan Filantropi Islam*, *3*(2), 117–136. https://doi.org/10.22236/alurban_vol3/is2pp117-136

Widyastuti, K., Handayani, P. W., & Wilarso, I. (2017). Tantangan dan Hambatan Implementasi Uang Elektronik di Indonesia: Studi Kasus PT XYZ. *Jurnal Sistem Informasi*, *13*(1), 38. https://doi.org/10.21609/jsi.v13i1.465

Zakia Rahmah Siahaan, D., & Marliyah, M. (2023). Perkembangan Perbankan Syariah Pada Era Ekonomi Digital. *Ekonom : Jurnal Ekonomi Dan Bisnis*, *3*(1), 29–36. https://doi.org/10.58432/ekonom.v3i1.765