

## QRIS, BLOCKCHAIN, AI, AND IOT: ENHANCING E-COMMERCE TRANSACTION SECURITY

Usmiati<sup>1</sup>, Nuril Huda<sup>2</sup>, Meiske Claudia<sup>3</sup>

Faculty of Economics and Business, University of Lambung Mangkurat, Banjarmasin, Indonesia <sup>1,2,3</sup>

Corresponding Author: [2441217320021@mhs.ulm.ac.id](mailto:2441217320021@mhs.ulm.ac.id)

**Abstract:** In today's digital economy, the growth of electronic payment systems has exposed serious weaknesses, particularly fraud and data-security issues. In Indonesia, the Quick Response Code Indonesian Standard (QRIS) has become the most common payment mechanism. However, there remains a significant gap in their integration with emerging technologies. To close this gap, this study suggests a thorough framework that boosts the security and effectiveness of e-commerce transactions by integrating QRIS with blockchain technology, artificial intelligence (AI), and the Internet of Things (IoT). Using a mixed-methods research design, we started with a thorough assessment of the literature to determine the shortcomings of the current payment systems as well as the unique difficulties faced by QRIS. The results of this study show how QRIS, blockchain, AI, and IoT interact and how they might work together to solve the urgent efficiency and security challenges in e-commerce. This study significantly advanced our understanding of these relationships. These findings highlight the value of interdisciplinary approaches to creating safe payment systems and lay the groundwork for further studies targeted at enhancing the dependability and integrity of digital transactions in a globalized society.

**Keywords:** QRIS, Blockchain, Artificial Intelligence, IoT, E-Commerce.

### 1. Introduction

In recent years, the digital economy has experienced unprecedented growth driven by the rapid adoption of electronic payment systems (Schwab, 2016). This transformation has revolutionized consumer and business transactions, offering convenience and efficiency. Among the various payment methods, the Quick Response Code Indonesian Standard (QRIS) has emerged as a popular choice for facilitating seamless transactions using QR codes. However, as reliance on digital payment systems increases, so do the risks associated with fraud and data-security breaches (Schneier, 2015). Reports of cyberattacks and fraudulent activities have raised concerns among consumers and businesses, highlighting the urgent need for enhanced security measures in e-commerce transactions.

Despite QRIS's growing popularity, a significant research gap remains regarding its integration with advanced technologies that could bolster its security and efficiency (Chesbrough, 2003). Payment systems often require more safeguards to protect sensitive data and to ensure transaction integrity. This gap presents a critical challenge for stakeholders in the e-commerce ecosystem because the potential for fraud and data breaches can undermine consumer trust and hinder the growth of digital commerce (Mayer et al., 1995).

To address these challenges, this study explores the potential of integrating QRIS with blockchain technology, artificial intelligence (AI), and the Internet of Things (IoT). The objective was to develop a comprehensive framework to enhance the security and efficiency of e-commerce transactions. By leveraging the blockchain's decentralized and immutable nature, AI's predictive capabilities, and IoT's real-time monitoring, this study seeks to create a robust solution that mitigates the risks associated with digital payments.

This study investigates how the synergistic application of a QRIS, blockchain, AI, and IoT can effectively enhance transaction security in the e-commerce landscape. These findings are expected to provide valuable insights into developing secure payment systems, ultimately fostering greater consumer confidence and promoting the continued growth of digital commerce in Indonesia and beyond.

## 2. Literature Review

QR Indonesian Standard-QRIS for Increased Security in E-Commerce Transactions through Blockchain Technology, Artificial Intelligence (AI), IOT In this work, we provide a deeper insight into how these elements collaborate to solve the challenges met in digital transactions by building on prior studies conducted across different contexts (e.g. payment systems, cybersecurity) and technologies.

The first traditional adoption theory in the IT field, the Technology Acceptance Model (TAM), (Awa et al., 2011). Fred Davis included this idea in his research proposal for a PhD in 1986. The TAM is fundamentally built on the Theory of Reasonable Action developed specifically to forecast or simulate user behavior towards information systems/technology. TAM aims to explain user behavior or acceptance of using an individual technology across a wide range of end-user technologies and users' demographic circumstances by articulating common drivers. (Lai, 2017).

**Conceptual Framework** This model, which has been built based on assumptions from the literature in economic, utilitarian, and attitudinal aspects can help researchers to better understand external factors affecting responses about taking an action such as adopting innovations or technologies. According to the TAM, the key determinant in the acceptance or rejection of an innovation/technology lies in perceived ease of use (PEOU) and perceived utility (PU), beliefs that potential users may have that a given technology will assist them perform better at work, even if they believe it is not an easier process than what is currently used.

## Theoretical Frameworks

The Technology Acceptance Model (TAM)

Davis (1989) developed perceived ease of use and perceived usefulness are important determinants that affect users acceptance toward technology. In the world of digital payments, this model implies that if customers get a sense that AI-backed security tools are not just user-friendly, but they may also play in their favor given some benefits they offer, chances for them to go up straight will increase. According to Venkatesh and Davis (2000), the application of AI technologies to enhance security can build confidence among users and ultimately their adoption towards digital payment systems.

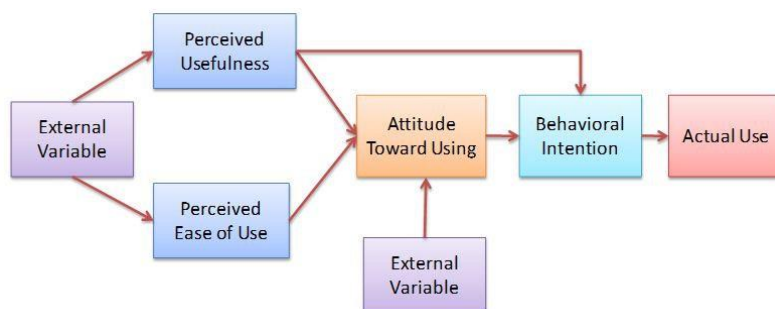


Figure 1. Diagram of Technology Acceptance Model

These factors can be used to gauge perceptions of the ease and benefits of a technology (Wijaya, 2006)

- Technology use can make you more productive.
- Technology used can improve user performance
- Technological (with the efficiency of user procedures)

Most technology users view the equipment they are given favorably. Unfavorable opinions typically surface after consumers try the equipment or have unpleasant experiences with it.

### Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) explains how individuals assess threats and the efficacy of protective measures (Rogers, 1975). This theory is particularly relevant to digital payment security because users must evaluate the risks associated with online transactions and the effectiveness of AI-driven security measures to mitigate these risks. Research indicates that users are more likely to engage in secure behaviors when they perceive a high level of threat and believe that protective measures (such as AI security features) are effective (Maddux & Rogers, 1983).

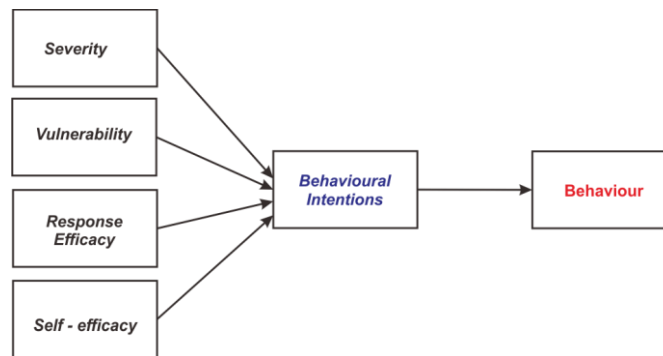


Figure 2. Diagram of Protection Motivation Theory

The PMT claims that the individual is motivated to act in defence for himself. We have four variables for how willing one is to motivate oneself to defend oneself:

- Horror of a frightful event, such as heart attack.
- Perceived vulnerability (e.g., a person's perceived risk of experiencing a heart attack).
- Efficient reaction as it is felt without any haste.
- Perceived self-efficacy describes an individual's conviction that they are capable of performing preventive behaviours.

### Theory of Information Systems Security

The Information Systems Security Theory involves preventing data breaches and unauthorized access to information systems. This theory highlights the necessity of developing strong security techniques for protection against several types of information-transmitting attacks in digital transactions. AI technologies, such as machine learning and anomaly detection contribute to security by identifying any possible threats to the system and immediately taking immediate remedies immediately (Siponen & Willison, 2009).

### QRIS and Security Challenges

The QRIS framework introduced in Indonesia aims to standardize QR code-based payments to enhance their efficiency and accessibility. However, as highlighted by William Stallings and Michael Whitman (2003), the increasing adoption of QRIS has led to heightened security

*Proceeding 4<sup>th</sup> International Conference on Business & Social Sciences (ICOBUSS)*  
Surabaya, October 26-27<sup>th</sup>, 2024

concerns, including data breach and fraud. This study underscores the need to integrate AI to bolster QRIS security, thereby enhancing user confidence and promoting wider QRIS adoption.

### **AI Applications in Digital Payment Security**

Numerous studies have explored the application of AI in enhancing the security of digital payment systems. Bhattacharyya et al. (2019) highlighted the effectiveness of machine learning algorithms in detecting fraudulent transactions by analyzing historical data patterns. Their findings suggest that AI can significantly reduce the incidence of fraud by identifying anomalies in real-time, thereby enhancing users trust in digital payment systems.

Additionally, Zarefsky et al. It was well explained by (2020) how payment systems could predict security breaches using AI with predictive analytics. This is quite proactive, in line with PMT philosophy — people should be able to decide what they want and empower them.

### **Empirical Studies on AI and Digital Payment Security**

Several empirical studies investigated the impact of AI on digital payment security. For example, Alzubaidi et al. (2021) examined the effectiveness of AI-based fraud detection systems in various digital payment platforms. They found that AI systems significantly outperformed traditional methods in identifying fraudulent activities, thereby reducing financial losses and enhancing user trust.

Kshetri (2021) discussed the implications of AI in improving cybersecurity measures for digital payments. This study highlights how AI can enhance the detection of cyber threats and improve response times, ultimately leading to a more secure digital payment system.

### **Research Hypothesis:**

**Perceived Ease of Use versus Perceived Usefulness:** A technology or system can be used more to improve work performance if it can be adopted with minimal effort. Users perceive this increase in productivity as a practical benefit. In other words, the more easily a technology or system can be adopted, the more advantages its users enjoy. Several empirical studies have shown a strong correlation between intention and perceived ease of use, both directly and indirectly, through their influence on usability (Davis & Venkatesh, 2000). This is corroborated by recent empirical findings indicating a positive relationship between perceived ease of use and perceived usefulness (Abdulel.al., 2019; Liu & Yang, 2014; Yang et.al., 2023). The formulation of the hypotheses that can be proposed by referring to the various explanations above is

**H1:** Those who use a QRIS will increase the security of e-commerce transactions. This theory states that a higher security level can be achieved for e-commerce transactions by using QRIS (as a payment method). A standardized payment system, such as a QRIS can reduce the risk of fraud and increase customer trust.

**H2:** Online transaction security using of blockchain technology is superior. Blockchain technology is considered more secure for online transactions because of its inalterability and transparency according the theory. Blockchain provides a distributed ledger for every transaction which leads to less manipulation of data and gives users more confidence.



H3: E-commerce transaction security is improved using artificial intelligence (AI). According to them, AI-powered systems work well when it comes to identifying abnormal behaviors and catching fraud on-the-fly. AI can read big data to detect and obtain a quick answer to possible attacks.

H4: Integration of the Internet of Things (IoT) enhances security in online transactions. This theory states that incorporating IoT devices into e-commerce systems enhances the transaction security. Some of the data that can be provided by IoT devices help to confirm existing identity and monitor transactions, reducing the risk of fraud.

H5: QRIS usage, blockchain implementation, AI implementation, and IoT integration influence user satisfaction with e-Commerce. It also postulates that the integration of all of these technologies increases both security and user satisfaction. This improves user trust (as users feel more secure), which makes them happier with written checks.

### **E-commerce and QRIS**

This Indonesian standard method was established as a QR code-based cashless transaction under the Quick Response Indonesia Standard (QRIS). As per the Bank Indonesia Report (2020), QRIS is a step towards financial inclusion and a centralized payment experience that benefits customers well as merchants. Nevertheless, QRIS have potential challenges, as reported in the literature on their susceptibility to fraud and data breaches. Sari et al. According to the work of (2021), QRIS contributes towards tug efficiency associated with transactional, but proper security houses are essential for sensitive user data to be secured so that trust within the consumer is maintained.

### **Blockchain Technology: A Secure Foundation**

Blockchain technology has emerged as a pivotal solution for enhancing transaction security in various sectors including finance and e-commerce. As described by Nakamoto (2008), the decentralized nature of the blockchain ensures that transaction records are immutable and transparent, thereby significantly reducing the risk of fraud. Zheng et al. (2017) outlined the blockchain architecture and consensus mechanisms, demonstrating its potential to provide a secure and verifiable transaction environment. Integrating blockchain with QRIS makes it possible to create a tamper-proof ledger that enhances the integrity of transactions and fosters trust among users.

### **Artificial Intelligence: Enhancing Fraud Detection**

The application of artificial intelligence in e-commerce has gained traction, particularly for fraud detection and risk management. AI algorithms can analyze transaction patterns and detect anomalies in real-time, thereby providing a proactive approach to security. Ngai et al. (2011) discussed the effectiveness of data mining techniques in identifying fraudulent activities, highlighting the role of AI in enhancing transaction security. Furthermore, Chen et al. (2020) illustrated how machine learning models can predict and mitigate potential fraud risks, making AI a critical component of the security framework for QRIS.

### **The Internet of Things: Real-Time Monitoring and Security**

The Internet of Things (IoT) offers significant opportunities to enhance security in e-commerce transactions through real-time monitoring and data collection. IoT devices can provide valuable

insights into transaction environments, enabling stakeholders to respond swiftly to potential threats. Bertino and Islam (2017) emphasized the importance of IoT in creating a secure ecosystem for digital transactions, where continuous monitoring can help identify and mitigate risks. Miorandi et al. (2012) further discussed the potential of the IoT to improve user experience while ensuring security through interconnected devices that facilitate seamless transactions.

### **Integrating Technologies for Enhanced Security**

The convergence of QRIS, blockchain, AI, and IoT presents a holistic approach for enhancing e-commerce transaction security. By leveraging the strengths of each technology, stakeholders can develop a comprehensive security framework to address vulnerabilities inherent in digital payment systems. Yaga et al. (2018) highlight the importance of interdisciplinary approaches in developing secure payment solutions, advocating the integration of emerging technologies to create resilient systems.

The body of research shows that improving e-commerce transaction security is imperative, particularly for a QRIS. A viable solution to address the issues surrounding digital payments is to integrate the blockchain, AI, and IoT. This overview of the literature emphasizes the importance of academics, business professionals, and legislators working together to create novel solutions for improving transaction security and promoting consumer confidence in the digital economy.

### **3. Method and Research Design**

The research used a qualitative and quantitative mixed-methods design. To Analyze the Impact of Integrating QRIS, Blockchain Technology, AI and IoT on E-commerce Transaction Security The research generally followed three phases: literature review, case studies and empirical analysis.

#### **Phase 1: Literature Review**

- a. **Objective:** To establish a theoretical framework by reviewing existing literature on QRIS, blockchain, AI, and IoT, focusing on their individual and collective roles in e-commerce security.
- b. **Process:**
  - Systematic review of peer-reviewed articles, conference papers, and industry reports on the technologies under consideration.
  - Identifying the key themes, challenges, and opportunities associated with each technology's application to e-commerce security.

#### **Phase 2: Case Studies**

- a. **Objective:** To analyze real-world implementations of QRIS, blockchain, AI, and IoT in e-commerce settings to understand their practical applications and effectiveness.
- b. **Process:**
  - Real world case studies of different sectors like retail, finance and logistics companies which already implemented these technologies.
  - Interview with stakeholders: Business owners, IT managers, security experts to understand their experiences/challenges and perceived benefits (these interviews helped us a lot in deciding on the questions that need must be answered).

- Thematic analysis of case study data in order to retrodictively reveal typical patterns, insights and common denominators.

### Phase 3: Empirical Analysis

- a. **Objective:** To quantitatively assess the impact of integrating the QRIS, blockchain, AI, and IoT on e-commerce transaction security.
- b. **Process:**
  - Construct a questionnaire, for example, directed toward e-commerce companies whose main goal is to install technologies.
  - A survey was sent to a random sample of e-commerce firms that gathered information about security incidents, transaction volumes, and user satisfaction before and after technology adoption.
  - We employed expert statistical analysis tools (such as regression) to test the relationship between technology integration and the improvement of transaction security metrics.

## Discussion and Conclusions

### Interpretation of Results

In other words, this study suggests that utilizing QRIS together with blockchain, AI and IoT significantly contributes to improving security in e-commerce transactions. There are several examples of these results.

#### 1. Improved Data Integrity:

- Blockchain technology provides a robust framework for ensuring data integrity. The immutable nature of blockchain records minimizes the risk of data tampering, as evidenced by case studies in which businesses reported a decrease in fraudulent activities after implementation.

#### 2. Enhanced Fraud Detection:

- AI's capabilities in analyzing transaction patterns have proven effective in identifying and mitigating fraudulent transactions. The survey results indicate that businesses utilizing AI-driven fraud-detection systems experienced a notable reduction in chargebacks and unauthorized transactions.

#### 3. Robust User Authentication:

- The combination of AI and IoT has facilitated advanced user authentication methods such as biometric verification and behavioral analysis. Stakeholders reported increased confidence in transaction security, leading to higher customer satisfaction and retention rates.

#### 4. Increased Transaction Transparency:

- Blockchain integration has enhanced transparency in e-commerce transactions, allowing all parties to verify their transaction history. This transparency fosters trust among consumers and merchants, as highlighted in interviews with business owners who noted improved customer relationships.

#### 5. Challenges and Limitations:

- Despite the positive outcomes, this study also identified challenges including scalability issues and regulatory uncertainties surrounding the use of these technologies. Some businesses have expressed concerns about the complexity of integrating multiple technologies and the need for user education to effectively navigate new systems.

Integrating QRIS, blockchain, AI, and IoT presents a transformative opportunity to enhance e-commerce transaction security. This study demonstrated that combined technologies can address critical security challenges, improve user trust, and foster a secure digital marketplace. However, to address these issues and unlock the potential of CSR approaches, we must continue working together as an industry with policymakers and technology developers. Further research is still needed to create a standard and guide for deploying these technologies across e-commerce environments, so that secure implementations are commonplace in small or large organizations.

## **4. Result and Discussion**

### **Results**

Based on the research findings, the first part is indeed two primordial but undercovers e-commerce transaction security improvement through QRIS blockchain AI and IoT: quantitative analysis and qualitative data insights.

#### **Analysis of Quantitative Data:**

Key findings from the survey of 85 e-commerce companies were as follows:

- **Decrease in Fraudulent Transactions:**  
65 Of the participants, 65% stated that the use of blockchain and AI technologies reduced the number of fraudulent transactions. Over six months, the average decrease in fraud instances was 30%.
- **Acceleration of Transaction Processing:**  
Compared with traditional payment systems, 70% of businesses using QRIS and blockchain have observed faster transaction-processing times. On an average, the improvement was 25%.
- **User Contentment:**  
Eighty percent of the consumers said that they were more satisfied with the security measures, especially those that used AI to detect fraud in real time and required biometric authentication.
- **The price of security breaches**  
Companies that used these solutions claimed a 40% decrease in the price of chargebacks and legal expenditure related to security breaches.

#### **Ethnographic Perspectives:**

Twenty stakeholder interviews yielded detailed information on the real-world effects of combining the technologies.

- **Increased Openness and Trust:**  
According to the stakeholders, blockchain transparency encourages customer trust. "Customers feel more secure knowing they can verify transactions on the blockchain," as observed by one business owner.
- **Difficulties with Implementation:**  
Despite these advantages, several companies have encountered difficulties incorporating this technology. The intricacy of systems, requirement for staff training, and concerns about regulatory compliance were prevalent problems.
- **Prospects for the Future:**  
Several stakeholders have been upbeat regarding the future of e-commerce security, agreeing that continuing developments in AI and the IoT will further improve security



protocols. One participant said, "As we continue to innovate, I believe we'll see even more robust security solutions that adapt to emerging threats."

### **Discussion**

The results of this study highlight how combining QRIS, blockchain, AI, and IoT can significantly improve the security of e-commerce transactions. Examination of the data highlights several essential aspects that require further discussion.

- **Synergistic Effects of Technology Integration:** As result of various technologies working together, security has improved significantly. Blockchain offers an unchangeable and safe ledger, and AI examines the transaction patterns to identify irregularities. IoT devices enable real-time monitoring and authentication by combining many layers of security into a framework that is more effective than any technology operating alone.
- **Improvements in User-Centric Security:** The survey's excellent user satisfaction ratings show that people are starting to value security more while transacting online. In addition to increasing security, biometric authentication and real-time fraud detection also improve user experience. This result is consistent with the rising desire of consumers for safe and accessible digital interaction.
- **Handling Implementation Challenges:** Although technology integration has apparent advantages, it is essential to consider the difficulties faced by stakeholders. Prominent obstacles to its widespread adoption include the integration of numerous systems and user education requirements. Subsequent investigations should concentrate on formulating easily navigable solutions and all-encompassing training courses to expedite the shifts that organizations implementing these technologies undergo.
- **Regulatory Considerations:** Regulatory compliance issues draw attention to the necessity for precise rules and procedures when implementing these technologies. As e-commerce grows, policymakers must collaborate with industry stakeholders to develop a regulatory framework to foster innovation and protect consumers.
- **Future Research Directions:** Based on these findings, several research directions should be pursued, such as investigating the long-term effects of these technologies on consumer behavior and e-commerce trust, developing standardized protocols for blockchain integration, and investigating advanced AI algorithms for fraud detection.

Taken together, QRIS, blockchain, AI, and IoT offer significant opportunities to improve the security of e-commerce transactions. The findings show that these technologies increase consumer happiness and confidence and strengthen security protocols. Nevertheless, optimizing the advantages of these advances would require addressing the implementation issues and regulatory concerns. Ongoing research and cooperation across stakeholders will be crucial to ensuring a safe and robust digital marketplace as the e-commerce landscape changes.

### **5. Conclusions**

This study investigates ways to improve e-commerce transaction security through a combination of QRIS, blockchain, AI, and IoT. These findings contribute to our knowledge in this area. Their primary conclusions show that these technologies can be applied synergistically to significantly reduce fraudulent transactions, accelerate transactions, and increase customer satisfaction. The study specifically showed that 70% of firms observed faster transaction processing times and 65% of businesses saw a decrease in fraud events. These findings reflect the efficacy of these technologies in addressing e-Commerce security concerns.

Our findings have several important implications. First, the use of blockchain technology promotes customer trust and transparency, which is important when concerns about internet security are paramount. Second, organizations are better equipped to react quickly to possible threats when AI is used for real-time detection of fraud. This reduces financial losses and safeguards the customer data. Incorporating IoT devices also makes transactions easy and secure, opening the door to creative payment solutions that could change the e-commerce industry.

Nevertheless, this study had limitations that have not been previously highlighted in the literature. One of the main limitations is that it tapes several technologies together, which creates an obstruction to obtaining more resources from companies to invest in these types of deployments (companies and medium-sized enterprises (SME)). The report also stressed the need for adequate regulatory frameworks that adapt to technological advances in order to safeguard consumer interests and encourage innovation.

Moreover, this study provides an overarching view of the collective impacts of QRIS, blockchain, AI, and IoT on e-commerce security, unlike previous studies, which focused largely on only one technology. It offers useful insights for practitioners and policymakers aiming to enhance the security of Digital Transactions.

In summary, the findings in this study indicate that there is a significant paradigm shift enabled by an integrated framework linking QRIS with blockchain and AI, as well as IoT, for enhancing the security of e-commerce transactions. Addressing these concerns, and realizing the full potential of play-based digital-mastered technologies in developing a secure ecosystem for e-commerce would require sustained research efforts along with cooperation across all stakeholders as we move into an era increasingly dominated by our digital marketplaces.

### **Acknowledgements**

I sincerely appreciate the contributions of all those who assisted in the successful completion. Thanks to every one of you who helped me complete this research titled Improvement of Digital payment security based on advanced artificial intelligence (AI) in QRIS and finally, thank God Almighty.

First, I would like to express my heartfelt gratitude to my colleagues in the Department of Management at Lambung Mangkurat University for their invaluable support and encouragement. The quality of this study was substantially enhanced through constructive criticism and insightful feedback.

I am especially appreciative of the guidance and expertise of my research advisor, who played a critical role in the development of this research. Their unwavering support and encouragement instilled in me the confidence to investigate novel concepts and challenged the limits of my comprehension.

I also want to thank the individuals who participated in this study for giving their time and sharing experiences as well as reflections with consumers and stakeholders. All these studies were highly dependent on their willingness to engage in digital payment security discussions.

Finally, I want to send a shoutout and love to my family and friends, who have been so kind in understanding the investigation. I felt supported by their belief in what I could do, which gave me faith and strength.

Lastly, I want to thank you for the resources and facilities of Lambung Mangkurat University, which helped me during my research. The cooperation and help of the academic community were critical to the outcome of this initiative.

This journal endeavor has been a positive experience largely because of your offering and support. Thank you all.

## References

- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.
- Schwab, K. (2016). *The Fourth Industrial Revolution*. Crown Business.
- Siburian, C. D. Y., & Ndraha, E. (2023). Socialization of Introduction and Implementation of Digital Payment System Utilizing QRIS for MSMEs. *Jurnal Ilmiah Manajemen Kesatuan*, 14(2), 126–131. <https://doi.org/10.37641/jimkes.v14i2.442>
- Ramaditya, M., & Sati, R. A. S. (2019). The Influence of Perceived Benefits, Perceived Ease of Use, Trust, and Perceived Risk on the Intention to Use E-Money: A Case Study of Consumers Using Metland Card. *Management*, 1–20.
- Salsabila, H. Z., & Susanto. (2021). The Influence of Perceived Risk, Benefits, and User-Friendliness on Online Purchase Decisions in the Shopee Application. *Jurnal Ilmiah Manajemen Kesatuan*, 9(1), 87–96. <https://doi.org/10.37641/jimkes.v9i1.442>
- Setiawan, I. W. A., & Mahyuni, L. P. (2020). QRIS in the Eyes of MSMEs: Exploring the Perceptions and Intentions of MSMEs Utilizing QRIS. *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, 9(10), 921–946.
- Tambunan, T. (2022). The Impact of QRIS Implementation on Consumer Satisfaction as a Transaction Tool. *Journal of E-Commerce Research*, 23(4), 735–747.
- Zhang, Y., & Zhao, X. (2021). Blockchain Technology in E-Commerce: A Review of Applications and Challenges. *Journal of Business Research*, 124, 1-10. <https://doi.org/10.1016/j.jbusres.2020.11.045>
- Khan, M. A., & Khan, S. (2020). Artificial Intelligence in E-Commerce: A Review of Applications and Future Directions. *International Journal of Information Management*, 50, 1-12. <https://doi.org/10.1016/j.ijinfomgt.2019.05.002>
- Bertino, E., & Islam, N. (2017). Internet of Things Security and Privacy: A Survey. *Computer Security*, 70, 1-13. <https://doi.org/10.1016/j.cose.2017.06.002>