**West Science Information System and Technology**
Vol. 1, No. 01, August 2023, pp. 35~43

# Enhancing Security and Reliability of Information Systems through Blockchain Technology: A Case Study on Impacts and Potential

**Adi Nugroho Susanto Putro[1], Sabil Mokodenseho[2], Nur Alim Hunawa[3], Muhatir Mokoginta[4], Evelin Ragil Marjoni[5]**
[1]STAB Negeri Raden Wijaya, Wonogiri, Jawa Tengah
[2,3,4,5]Institut Agama Islam Muhammadiyah Kotamobagu

**Article Info**

***Article history:***

Received August 2023
Revised August 2023
Accepted August 2023

***Keywords:***

Security
Reliability
Information Systems
Blockchain Technology

## ABSTRACT

In the digital age, ensuring the security and reliability of information systems is a paramount concern for organizations. This research investigates the potential of blockchain technology to enhance information system security and reliability within the dynamic landscape of Indonesian start-up companies. By employing a mixed-methods approach, combining qualitative interviews and quantitative surveys, this study explores the current state of information system security practices, assesses the challenges faced by start-ups, and evaluates perceptions regarding the adoption of blockchain technology. The qualitative findings highlight the existing security measures, challenges, and potential benefits associated with blockchain. The quantitative results provide insights into security practices and willingness to adopt blockchain. Through the integration of these findings, the study offers practical recommendations for enhancing information system security and reliability in the context of start-ups, while considering the challenges of blockchain adoption. This research contributes to the understanding of the symbiotic relationship between technology adoption and information security, offering guidance for start-ups, policymakers, and researchers.

***Corresponding Author:***

Name: Adi Nugroho Susanto Putro
Institution: STAB Negeri Raden Wijaya, Wonogiri, Jawa Tengah
Email: adinug@radenwijaya.ac.id

## 1. INTRODUCTION

In the contemporary business landscape, where digitization and data-driven operations are prevalent, ensuring the security and reliability of information systems is of paramount importance. Organizations face numerous cyber threats, including ransomware, data breaches, and vulnerabilities in their digital infrastructure [1]. Some common cybersecurity threats that web developers should be aware of include unauthorized access to networks and online services, data leakage, and privacy breaches [2]. To protect against these threats, organizations should implement robust security measures, such as data encryption, intrusion detection systems, and regular security audits [3]. Preventing data breaches is essential to protect sensitive information and maintain the integrity of an organization's information systems. Some strategies to prevent data breaches include:

Implementing strong access controls and authentication mechanisms [4]. Regularly updating software and hardware to address known vulnerabilities [4]. Employing intrusion detection systems to monitor and analyze network traffic for signs of malicious activity [3]. Conducting regular security audits and assessments to identify potential weaknesses and areas for improvement [5]. Developing and enforcing a comprehensive information security policy that covers all aspects of the organization's digital infrastructure [6]. Ensuring that employees are trained in cybersecurity best practices and are aware of the potential risks associated with their actions [7].

Integrating information security into an organization's strategic planning process is crucial for ensuring the effective use of information systems in a secure manner [6]. This involves embedding information security policies within the organization's strategic information systems planning, which can help increase the security capability of the organization and make the deliverables from the planning process more effective and efficient [6]. Additionally, organizations should consider implementing business continuity management plans to prepare for and respond to potential disruptions, such as cyberattacks or natural disasters [2]. In conclusion, ensuring the security and reliability of information systems is of paramount importance in today's digital business landscape. Organizations must be proactive in addressing cyber threats, implementing data breach prevention strategies, and integrating information security into their strategic planning processes to protect sensitive data and maintain the uninterrupted flow of information.

Blockchain technology has gained significant attention due to its potential to improve the security and reliability of information systems. Its unique attributes, such as decentralization, transparency, and immutability, make it an ideal solution for various applications beyond digital currencies [8]. Blockchain uses cryptographic techniques and consensus algorithms to create a tamper-resistant, distributed ledger that can authenticate transactions and secure data in untrustworthy environments [8]. Some of the key components of blockchain technology include its architecture, consensus algorithms, and cryptographic techniques [8]. Consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), are used to achieve agreement among network participants on the validity of transactions [8]. Cryptographic techniques, such as hash functions and digital signatures, ensure data transmission and access security [9].

Blockchain technology has been applied in various fields, including financial services, reputation systems, Internet of Things (IoT), and supply chain management [8], [10]. In the healthcare industry, blockchain can address issues such as lack of comprehensive peer-to-peer records and difficulty in accessing patients' medical histories [11]. In supply chain management, blockchain can improve transparency, traceability, and security, making it easier to manage and control global supply chains [10]. However, there are still challenges to overcome, such as scalability and security issues [8]. For instance, the trade-off between decentralization, privacy, and lower transaction costs is a concern in blockchain-based transactions [12]. Additionally, the adoption of blockchain technology faces barriers in inter-organizational, intra-organizational, technical, and external aspects [10]. Recent advances in blockchain technology have focused on improving consensus algorithms and cryptographic techniques [12]. For example, the modified Merkle hash tree (MMHT) consensus algorithm has been proposed to improve data integrity check performance in smart homes while ensuring network stability [13]. Furthermore, research on blockchain security has expanded to include business, organizational, and operational issues [9].

In conclusion, blockchain technology has the potential to significantly improve the security and reliability of information systems through its unique attributes, such as decentralization, transparency, and immutability. However, there are still challenges to overcome, such as scalability, security, and adoption barriers. As research and development in this field continue, we can expect further advancements and applications of blockchain technology in various industries.

Indonesia's startup ecosystem has experienced significant growth in recent years, with startups increasingly relying on digital infrastructure to operate efficiently and deliver value to customers [14]. This rapid digitization, however, also increases the risks associated with cyberattacks and data breaches [15]. The Indonesian software startup ecosystem is influenced by various factors, including socio-cultural, institutional, technological, methodological, educational, and ecosystem aspects [14]. The government plays an indirect role in the development of startups through ecosystem support, marketing, and regulations [15]. However, taxation does not have a significant impact on startups, as the majority of them do not have income above IDR 4.8 billion [15]. Venture capital plays an active role in the development of startups in Indonesia, providing financial support, mentoring, and networking opportunities [15]. The country's digital infrastructure development is also supported by collaborative governance, which helps provide information to stakeholders and improve regulations and policies for state agencies and practitioners [16].

Despite the growth and support, Indonesia's digital landscape is not without challenges. Cyberattacks and data breaches, such as the case of Hacker Bjorka, have raised concerns about the country's cybersecurity readiness [17]. The National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Information Technology are responsible for addressing these issues [17]. To mitigate the risks associated with cyberattacks and data breaches, it is essential for startups to adopt a risk-based approach to cybersecurity [18]. This includes incorporating governance mechanisms into their risk management processes, focusing on security control, data retention, and continuous monitoring [18]. Audit committees with IT expertise can also play a crucial role in reducing the likelihood of data breaches and enhancing the monitoring and oversight of cybersecurity risks [19].

In conclusion, Indonesia's growing startup ecosystem relies heavily on digital infrastructure, which brings both opportunities and challenges. To ensure the continued growth and success of startups in the country, it is crucial to address cybersecurity risks and strengthen the digital infrastructure through collaborative governance, regulatory support, and the involvement of key stakeholders such as venture capital firms and government agencies.

Blockchain technology has the potential to improve information security and reliability in various sectors, including startups in Indonesia. The decentralized and zero-trust architecture of blockchain can enhance privacy, security, versatility, and reliability in various applications [20]. Here are some examples of blockchain integration in different contexts, A study developed an IoT information management system for smart labs based on blockchain technology, which showed higher speed, efficiency, and better performance in processing information and data compared to the traditional IoT laboratory information management system [20]. Blockchain technology can help build smart islands by integrating various resources from stakeholders, improving accessibility and connectivity, and ensuring the achievement of sustainability. A case study in the Seribu Islands in Jakarta, Indonesia, showed that good digital literacy and blue economy management significantly influenced blockchain technology adoption and impacted smart islands [21]. A Blockchain-based Online Information Sharing (BOIS) platform can improve the resilience of Industrial Symbiosis-based Multi Energy Systems by enabling firm-to-firm (F2F) IS relationship establishment through blockchain-based smart contracts [22]. Blockchain technology can enhance data security and reliability for web applications, such as online course platforms, by protecting against common web application attacks targeting user authorization processes [23].

Blockchain technology can be adopted by Micro, Small, and Medium Enterprises (MSMEs) in Indonesia to improve access to capital, information, technology, organization, and management. The TRAM model, which integrates the Technology Readiness Index (TRI) and Technology Acceptance Model (TAM), can be used to measure and analyze MSMEs' readiness in using blockchain technology [24]. Electricity Information Collection: A secure electricity information collection model based on blockchain technology can effectively improve the reliability of electricity information data and collection equipment, ensuring the safety of the power grid [25]. In conclusion, blockchain technology can improve the resilience of information systems in various sectors, including startups in Indonesia. By exploring blockchain integration in different contexts, it is possible to understand the feasibility and implications of this technology in enhancing information security and reliability.

This study aims to investigate the effect of improving the security and reliability of information systems through the utilization of blockchain technology, specifically focusing on start-up companies in Indonesia. Start-up companies, as innovative and agile entities, play an important role in driving economic growth and technological advancement in the country. However, limited resources and rapidly evolving operational environments often expose them to vulnerabilities that threaten the integrity of their information systems.

## 2. LITERATURE REVIEW

### *2.1 Information System Security and Reliability*

Information system security is a critical issue for organizations, as breaches can lead to financial losses, reputational damage and legal consequences. Ensuring the confidentiality, integrity, and availability of data is critical to protecting digital assets [26]–[29]. Techniques such as encryption, access control, and intrusion detection systems have been used to mitigate cyber threats and vulnerabilities. However, the evolving nature of cyberattacks and the interconnectedness of modern systems continue to challenge traditional security measures.

Reliability, a closely interrelated concept, refers to the ability of information systems to consistently deliver accurate and timely data. Unreliable systems can result in operational disruptions, loss of credibility, and compromised decision-making. Achieving reliability involves addressing issues such as system downtime, data corruption, and data consistency [30], [31].

### *2.2 Blockchain Technology*

Blockchain technology, which was originally designed as the underlying infrastructure for digital currencies, has gained significant attention for its potential to address information security and reliability challenges. At its core, blockchain is a decentralized, distributed ledger that records transactions across a network of participants in a tamper-resistant manner. Its cryptographic techniques and consensus mechanisms ensure data integrity and prevent unauthorized modifications [32]–[34].

Blockchain's decentralized nature eliminates reliance on a single point of control, reducing vulnerability to single points of failure and attacks. Immutability, achieved through cryptographic hashing, makes it extremely difficult to alter historical transaction records. This makes blockchain attractive for applications beyond finance, including supply chain management, healthcare, and digital identity.

### *2.3 Start-up Ecosystem and Information Security*

Start-ups, characterized by their innovative nature and limited resources, face unique challenges in maintaining strong information security practices. These challenges stem from factors such as limited budgets, lack of skilled personnel, and the need to develop and deploy products quickly.

Startups often prioritize functionality over security, potentially exposing them to cyber risk [35]s.

The impact of security breaches on startups can be severe, leading to reputational damage and loss of customer trust. The interconnectedness of today's digital landscape means that a breach in one aspect of a start-up's systems can quickly cascade into wider vulnerabilities.

### *2.4 Blockchain Adoption in Startups*

Research on the adoption of blockchain technology in start-ups has gained attention in recent years. While the potential advantages of blockchain in terms of security and reliability have been recognized, its implementation has many challenges. These challenges include technical aspects, such as scalability and interoperability, as well as operational considerations such as cost and integration with existing systems [32], [36], [37].

The study highlights the need for new enterprises to carefully assess the suitability of blockchain for their specific use cases. Decisions regarding public vs. private blockchains, consensus mechanisms, and data privacy considerations are critical. Understanding the potential trade-offs between security, efficiency, and flexibility is critical for informed decision-making.

### *2.5 Research Gaps and Contributions*

While the existing literature provides insights into information system security, blockchain technology, and startup dynamics, there is still a research gap regarding the effect of blockchain in improving information security and reliability specifically in the context of startups in Indonesia. The challenges and opportunities faced by these startups, operating within the country's economic and technological landscape, require thorough investigation.

This research seeks to bridge this gap by conducting a comprehensive analysis of the impact of blockchain technology on the security and reliability of information systems in the Indonesian start-up ecosystem. By synthesizing findings from various domains and tailoring them to the specific context, this research aims to contribute valuable insights and practical recommendations for start-ups considering the adoption of blockchain technology to enhance their information security and reliability measures.

## 3. METHODS

A mixed methods approach, which combines qualitative and quantitative research methods, will be used to provide a comprehensive understanding of the research topic [38]-[41]. This approach allows for a deeper exploration of the complexities involved in the integration of blockchain technology in start-up information systems, while allowing for the measurement and analysis of relevant variables.

### *3.1 Data Collection*

Semi-structured interviews were conducted with key stakeholders from various start-up companies in Indonesia. Interviewees will include founders, IT managers, and other relevant personnel who have insight into information system security practices, challenges, and potential blockchain adoption. The interviews were designed to obtain detailed narratives about current security measures, experiences with data breaches, and perceptions about blockchain technology.

An online survey was administered to a larger sample of 150 start-up companies representing various industries, sizes, and geographic locations in Indonesia. The survey was designed to collect quantitative data relating to information system security, reliability, perceived challenges, and willingness to adopt blockchain technology. The survey utilized Likert-scale questions and structured response options to facilitate data quantification.

### *3.2 Sampling Strategy*

A purposive sampling strategy was used to select diverse start-up companies for qualitative interviews. The initial selection was based on factors such as industry representation, company size, and geographic location. As the interviews progressed, snowball sampling would be used, which allowed interviewees to recommend other potential participants who could provide valuable insights.

For the quantitative survey, a convenient sampling method will be used to collect responses from a broad spectrum of emerging companies. Survey links were disseminated through relevant industry associations, startup networks, social media platforms, and professional networks.

### *3.3 Data Analysis*

Qualitative data from the interviews underwent thematic analysis. Transcribed interviews will be systematically coded to identify recurring themes, patterns, and variations in responses. This analysis will enable the extraction of insights related to the current state of information system security, challenges faced, and perceptions of blockchain technology among start-up companies. The quantitative survey data was analyzed using SPSS statistical techniques. Descriptive statistics were used to summarize the survey responses.

## 4. RESULTS AND DISCUSSION

The results obtained from the qualitative interviews and quantitative survey are followed by a comprehensive discussion that contextualizes these findings with the research objectives, existing literature, and the specific dynamics of the startup ecosystem in Indonesia.

### *4.1 Qualitative Findings*

#### 4.1.1 Information System Security Practices

The qualitative interviews revealed insights into the prevailing information system security practices among Indonesian startups. Encryption, firewalls, and access control are commonly mentioned security measures. However, due to limited resources and prioritization challenges, cybersecurity education and incident response plans are often overlooked, leaving startups vulnerable to potential breaches.

#### 4.1.2 Challenges and Threats

The speakers explained the challenges that startups face in the area of information security. Limited budgets for cybersecurity investments, lack of skilled cybersecurity professionals, and a rapidly evolving cyber threat landscape were frequently mentioned challenges. The interconnected nature of start-up systems was highlighted as a risk factor, making them vulnerable to internal and external threats.

#### 4.1.3 Perceptions of Blockchain Adoption

Conversations about blockchain adoption revealed a generally positive outlook, with many participants recognizing the technology's potential to improve the security and reliability of information systems. The transparency, immutability, and decentralized nature of blockchain were perceived as attributes that could increase trust in data transactions. However, concerns regarding scalability, integration complexity, and technical knowledge required for blockchain implementation were also articulated.

### *4.2 Quantitative Findings*

#### 4.2.1 Information System Security Measures

The quantitative survey provided insights into the security measures implemented by start-ups. While basics such as firewalls and password protection are widely used, more advanced practices such as regular security audits and ongoing employee training are less common. This underscores the need for greater emphasis on a comprehensive security strategy.

#### 4.2.2 Willingness to Adopt Blockchain

Survey responses (85%) indicate a moderate interest among emerging companies in adopting blockchain technology to improve the security and reliability of information systems. Respondents recognized the potential benefits, such as higher data integrity and reduced vulnerability to data tampering. However, reservations centered on the complexity of blockchain implementation and the lack of in-house expertise.

## DISCUSSION

### *Integration of Qualitative and Quantitative Findings*

The integration of qualitative and quantitative findings offers a nuanced perspective on the challenges and opportunities associated with information system security and blockchain adoption in Indonesian start-up companies. Resource constraints and evolving threats identified in the qualitative interviews find validation in the quantitative survey results.

### *Leveraging Blockchain for Security Enhancement*

The discussion underscored the alignment between the benefits of blockchain adoption and the security challenges faced by start-ups. The decentralized nature of blockchain has the potential to mitigate risks associated with single points of failure and unauthorized access. Immutability and data integrity mechanisms hold promise in building trust, especially in industries where data accuracy is critical.

### *Overcoming Challenges in Blockchain Adoption*

While blockchain adoption provides potential benefits, this discussion recognizes the complexity of this process. Scalability issues, integration challenges, and the need for specialized expertise are significant hurdles that resonate with the operational realities of start-ups.

### *Practical Implications and Recommendations*

Based on the research findings, the discussion section offers practical implications and recommendations for academia and the start-up industry. These recommendations include technological considerations, such as conducting a thorough feasibility assessment before blockchain implementation, as well as organizational aspects such as developing a cybersecurity-aware culture within start-ups.

## CONCLUSION

In an era marked by technological advancements and data-driven operations, the importance of information system security and reliability cannot be overstated. This research explored the potential of blockchain technology to address these concerns within the realm of Indonesian start-up companies. The synthesis of qualitative and quantitative findings revealed the complexities of information security in start-ups, driven by limited resources, evolving threats, and interconnected systems. The willingness to adopt blockchain underscores its perceived advantages in data integrity and transparency. However, challenges like scalability and integration complexities cannot be ignored. The implications of this research are far-reaching. For academia, the study adds to the growing body of knowledge on blockchain adoption in the context of start-ups, contributing to the literature on technology-driven security enhancement. Practically, the findings offer actionable recommendations for start-ups, emphasizing the need for comprehensive security strategies and careful evaluation of blockchain feasibility. Policymakers can draw insights from this research to create an environment conducive to blockchain adoption. As blockchain continues to evolve and gain traction, its potential to revolutionize information system security remains promising. Future research can delve deeper into specific industries, explore innovative blockchain use cases, and examine the long-term effects of blockchain adoption on start-up performance. By bridging the gap between theory and practice, this research contributes to the ongoing dialogue on harnessing technology to fortify the security and reliability of information systems in the ever-changing landscape of start-up entrepreneurship.

## REFERENCES

[1] J. Lee and J.-W. Jeong, "A Study on the Serious Issues in the Practice of Information Security in IT: With a Focus on Ransomware," in *Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2017 11*, 2017, pp. 31–36.

[2] R. M. Ndege, “Relationship between Strategic Planning and Business Continuity Management of Private Security Firms in Kenya,” *Int. J. Innov. Res. Dev.*, vol. 6, no. 3, 2017.

[3] J. Cunha, “Cybersecurity Threats for a Web Development,” *ARIS2-Advanced Res. Inf. Syst. Secur.*, vol. 2, no. 2, pp. 73–82, 2022.

[4] B. V. Tulus and A. R. Tanaamah, “Design of Information Technology Governance in Educational Institutions Using COBIT 2019 Framework,” *J. Inf. Syst. Informatics*, vol. 5, no. 1, pp. 31–43, 2023.

[5] C. Adharsh and S. Vijayalakshmi, “Prevention of Data Breach by Machine Learning Techniques,” in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2022, pp. 1819–1823.

[6] A. Issa-Salwe and K. Mustafa, “Security Assurance through Strategic Information Systems Planning”.

[7] S. Varshney, D. Munjal, O. Bhattacharya, S. Saboo, and N. Aggarwal, “Big data privacy breach prevention strategies,” in *2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, 2020, pp. 1–6.

[8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *2017 IEEE international congress on big data (BigData congress)*, 2017, pp. 557–564.

[9] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, “Blockchain security: A survey of techniques and research directions,” *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2490–2510, 2020.

[10] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,” *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, 2019.

[11] C. Murugumani, B. R. N. Singh, K. Pravalika, P. R. Sri, C. S. Sowmya, and M. S. Reddy, “Block Chain and Distributed Computing Aided with Cloud Technology-A Specific Reference to Security Issues of Healthcare Industry,” in *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 2023, pp. 1–6.

[12] S. J. Kim, “An impossible trinity in blockchain-based transactions: decentralization, privacy, and lower transaction costs,” 2021.

[13] A. R. Kairaldeen, N. F. Abdullah, A. Abu-Samah, and R. Nordin, “Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash algorithms,” *Wirel. Commun. Mob. Comput.*, vol. 2021, pp. 1–23, 2021.

[14] A. Asmoro and L. E. Nugroho, “Software Startup Ecosystem in Indonesia: A Conceptual Framework,” in *2018 4th International Conference on Science and Technology (ICST)*, 2018, pp. 1–6.

[15] R. N. Suwarni, M. Fahlevi, and M. N. Abdi, “Startup valuation by venture capitalists: An empirical study Indonesia firms,” *Int. J. Control Autom.*, vol. 13, no. 2, pp. 785–796, 2020.

[16] M. Rozikin, A. B. Sulistyo, C. Saleh, and B. S. Riyadi, “The Collaborative Governance in Digital Infrastructure Development in Indonesia: A Public Policy Perspective,” *Int. J. Membr. Sci. Technol.*, vol. 10, no. 3, pp. 449–459, 2023.

[17] T. Sutikno and D. Stiawan, “Cyberattacks and data breaches in Indonesia by Bjorka: hacker or data collector?,” *Bull. Electr. Eng. Informatics*, vol. 11, no. 6, pp. 2989–2994, 2022.

[18] X. M. Liu, “A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches,” *Coast. Bus. J.*, vol. 18, no. 1, p. 2, 2021.

[19] C. Chen, C. Hartmann, and A. Gottfried, “The Impact of Audit Committee IT Expertise on Data Breaches,” *J. Inf. Syst.*, vol. 36, no. 3, pp. 61–81, 2022.

[20] J. Zhong, H. Chen, Q. Zhang, and W. He, “Discussion and application of blockchain technology in information management of internet of things in smart lab,” *Mob. Inf. Syst.*, vol. 2022, 2022.

[21] D. Pranita, S. Sarjana, B. M. Musthofa, H. Kusumastuti, and M. S. Rasul, “Blockchain Technology to Enhance Integrated Blue Economy: A Case Study in Strengthening Sustainable Tourism on Smart Islands,” *Sustainability*, vol. 15, no. 6, p. 5342, 2023.

[22] M. K. Nallapaneni and S. S. Chopra, “Blockchain-based Online Information Sharing Platform for Improving the Resilience of Industrial Symbiosis-based Multi Energy Systems,” 2020.

[23] B. Aliya, U. Olga, B. Yenlik, and I. Sogukpinar, “Ensuring Information Security of Web Resources Based on Blockchain Technologies,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, 2023.

[24] A. E. Wahyuni, A. Juraida, and A. Anwar, “Readiness factor identification Bandung city MSMEs use blockchain technology,” *J. Sist. dan Manaj. Ind.*, vol. 5, no. 2, pp. 53–62, 2021.

[25] J. Lu *et al.*, “Application Research of Blockchain Technology in Electricity Information Collection,” in *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 2020, pp. 171–176.

[26] J. Luo, Q. Meng, and Y. Cai, "Analysis of the impact of artificial intelligence application on the development of accounting industry," *Open Journal of Business and Management*. scirp.org, 2018.

[27] P. Petratos and A. Faccia, "Accounting information systems and system of systems: Assessing security with attack surface methodology," *Proc. 2019 3rd Int. …*, 2019, doi: 10.1145/3358505.3358513.

[28] A. Wicaksono, M. Kartikasary, and N. Salma, "Analyze cloud accounting software implementation and security system for accounting in MSMEs and cloud accounting software developer," in *2020 International Conference on Information Management and Technology (ICIMTech)*, 2020, pp. 538–543.

[29] Q. A. Al-Fatlawi, D. S. Al Farttoosi, and A. H. Almagtome, "Accounting information security and it governance under cobit 5 framework: A case study," *Webology*. webology.org, 2021.

[30] J. McCallig, A. Robb, and F. Rohde, "Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain," *… J. Account. Inf. Syst.*, 2019.

[31] A. Yarali, R. Joyce, and B. Dixon, "Ethics of Big Data: Privacy, Security and Trust," in *2020 Wireless Telecommunications Symposium (WTS)*, 2020, pp. 1–7.

[32] A. Saini and V. Garg, *Transformation for Sustainable Business and Management Practices: Exploring the Spectrum of Industry 5.0*. emerald.com, 2023. doi: 10.1108/978-1-80262-277-520231023.

[33] O. P. Brunila, V. Kunnaala-Hyrkki, and T. Inkinen, "Hindrances in port digitalization? Identifying problems in adoption and implementation," *European Transport Research …*. Springer, 2021. doi: 10.1186/s12544-021-00523-0.

[34] N. Karnik, U. Bora, K. Bhadri, P. Kadambi, and ..., "A comprehensive study on current and future trends towards the characteristics and enablers of industry 4.0," *J. Ind. …*, 2022.

[35] U. Shrivastava, J. Song, B. T. Han, and D. Dietzman, "Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation," *Int. J. Med. Inform.*, vol. 148, p. 104401, 2021.

[36] R. Joseph *et al.*, "Triple-Entry Accounting (TEA) and Blockchain Implementation in Accounting and Finance-A Survey," in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, 2023, pp. 1–7.

[37] A. French, J. P. Shim, M. Risius, K. R. Larsen, and ..., "The 4th Industrial Revolution powered by the integration of AI, blockchain, and 5G," *Commun. …*, 2021.

[38] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: CV. Alfabeta, 2017.

[39] Sugiyono, "Metode Penelitian," *Sugiyono*, 2016.

[40] S. Naim and S. Mokodenseho, "Implementation of the virtual learning models during the covid-19 pandemic: Students' perspectives and its lessons," *J. Kependidikan J. Has. Penelit. Dan Kaji. Kepustakaan Di Bid. Pendidikan, Pengajaran Dan Pembelajaran*, vol. 8, no. 3, pp. 617–628, 2022.

[41] M. Idris, E. Willya, I. Wekke, and S. Mokodenseho, "Peace resolution in education and application on information and communication technologhy," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 6, 2021.