Analysis of Blockchain Technology in Patient Data Management System : Security, Privacy, and Efficiency in the Digital Healthcare Context

Arsi Yulianjani*[1], Rosdiana[2], Rizkq Maulansyah Altaufik[3]
[1] Informatics Management, University of Raharja, Indonesia
[2] Informatics Engineering, University of Raharja, Indonesia
[3] Information System, University of Raharja, Indonesia
E-mail: *[1]**arsiyulianjani@raharja.info**, [2]ros@raharja.info, [3]rizkq@raharja.info

Abstract

In the rapidly evolving landscape of digital healthcare, ensuring secure, confidential, and efficient patient data management has become paramount. Blockchain technology has emerged as a promising solution to address these challenges. This study aims to analyze the implementation of blockchain technology within patient data management systems, with a specific focus on security, privacy, and efficiency in the context of digital healthcare. Within this framework, a notable gap arises between technological innovation trends and their practical application within the healthcare sector. This research expands our understanding of how blockchain can be effectively harnessed to tackle security and patient data privacy challenges within the increasingly interconnected digital healthcare environment. Employing a comprehensive methodology that encompasses qualitative and quantitative approaches, including surveys, literature analysis, and case studies, this study delves into how blockchain technology can provide an added layer of security to patient data, enhance privacy through improved access control, and streamline the sharing of health information. The novelty of this research lies in its holistic approach to identifying gaps in blockchain technology application methods within patient data management, while also addressing practical challenges inherent to the digital healthcare context. The anticipated outcomes of this analysis will provide valuable insights for decision-makers aiming to implement blockchain technology to fortify data security, safeguard privacy, and enhance efficiency within patient data management systems. In conclusion, this research contributes to a nuanced comprehension of the potential of blockchain technology to augment security, privacy, and efficiency in patient data management. By shedding light on innovative methods like blockchain integration, this study offers valuable guidance for effectively navigating the dynamic landscape of digital healthcare.

Keywords *— Blockchain Technology, Patient Data Management, Security, Privacy, Efficiency*

1. INTRODUCTION

The realm of technology has undergone rapid evolution, catalyzing transformative shifts across diverse industries, including healthcare. As the digital landscape continues to unfold, the optimization of patient data management stands as a paramount concern, demanding solutions that ensure utmost security, privacy, and efficiency[1]. Conventional healthcare data management systems, centralized in nature, are susceptible to vulnerabilities,

particularly when faced with unforeseen events such as natural disasters[2][3]. This predicament underscores the exigent requirement for innovative approaches that fortify security, amplify privacy measures, and enhance the efficiency of patient data management[4][5].

Within the healthcare sphere, the prevailing centralized data management systems grapple with critical challenges, including compromised security, inadequate privacy safeguards, and operational inefficiencies. The intricate interplay of digital healthcare magnifies these challenges, accentuating the urgency to unearth pioneering strategies that uphold the sanctity of patient data while facilitating authorized access[6][7]. Furthermore, the scarcity of comprehensive investigations elucidating the potential role of blockchain technology in patient data management within the healthcare sector underscores an evident research void[8]. Consequently, a rigorous exploration of the extent to which blockchain can augment security, privacy, and efficiency within the context of digital healthcare is warranted.

The overarching goal of this research is to undertake a discerning analysis of blockchain technology's integration into patient data management systems, specifically honing in on the critical domains of security, privacy, and efficiency[9]. The primary objectives encompass an evaluation of the viability of implementing blockchain technology within healthcare data management, an assessment of its influence on fortifying data security and ensuring patient privacy, an exploration of its potential to streamline processes and heighten operational efficiency, and an identification of the barriers impeding its seamless assimilation[10].

The paramount significance of this study emanates from its potential to yield groundbreaking insights into the convergence of blockchain technology and the healthcare sector[11]. By methodically dissecting the intricate facets of security, privacy, and efficiency, this research aspires to furnish invaluable directives for healthcare practitioners, policymakers, and technology stakeholders alike[12]. The anticipated outcomes are poised to illuminate decision-making paradigms, galvanizing the formulation of strategies that harness blockchain's transformative potential to usher in an era of impregnable security, inviolable privacy, and optimal efficiency within the contours of patient data management within the ever-evolving realm of digital healthcare.

2. LITERATURE REVIEW

The evolution of technology has instigated transformative shifts across various industries, ushering in a new era of possibilities. In the realm of healthcare, where the sanctity of patient data holds paramount importance, the convergence of technology and healthcare has brought to the forefront innovative solutions that promise heightened security, privacy, and efficiency[13]. This literature review delves into the multifaceted realm of blockchain technology and its applications within the healthcare sector, exploring its potential to revolutionize patient data management, enhance security and privacy, and optimize operational efficiency.

A. Overview of Blockchain Technology

Blockchain, originally devised as the underlying technology for cryptocurrencies, has emerged as a disruptive force with applications extending far beyond the financial sector. At its core, blockchain is a decentralized, immutable digital ledger that records transactions or data in a secure and transparent manner[14][15]. The technology's foundational principles include decentralization, cryptographic hashing, consensus mechanisms, and immutability, collectively ensuring trust and integrity in data transactions.

B. Blockchain Applications in Healthcare

Patient Data Management: Blockchain's decentralized nature offers a paradigm shift in patient data management. By distributing data across a network of nodes and employing encryption techniques, patient data can be securely stored, accessed, and shared, ensuring authorized stakeholders maintain control over their information[16].

Medical Records Security: Traditional medical records are susceptible to unauthorized access, tampering, or loss. Blockchain's cryptographic hashes and consensus mechanisms bolster data security, preventing unauthorized alterations and enhancing data authenticity[17]. Privacy Enhancement: Patient privacy is a cornerstone of healthcare ethics.

Blockchain's architecture facilitates patient consent management, granting individuals control over who can access their data and for what purposes, thereby ensuring privacy compliance[18].

Supply Chain Management: Blockchain's transparency and traceability attributes can enhance the authentication and tracking of pharmaceuticals and medical supplies, mitigating counterfeit drugs and ensuring the integrity of the healthcare supply chain[19].

C. Security Concerns in Patient Data Management

While blockchain technology introduces heightened security measures, it is not immune to challenges. Vulnerabilities such as 51% attacks, smart contract exploits, and regulatory uncertainties need to be addressed to realize the full potential of blockchain in safeguarding patient data[20][21].

D. Privacy Challenges in Digital Healthcare

The digital transformation of healthcare poses unique privacy challenges. Striking a balance between patient data access, consent management, and privacy compliance is intricate. Blockchain's privacy-enhancing features, such as zero-knowledge proofs, offer avenues for addressing these challenges[22][23].

E. Efficiency Gains through Blockchain Implementation

Blockchain's decentralized and automated nature streamlines administrative processes, reducing intermediaries, and accelerating data sharing. This can lead to improved care coordination, reduced administrative costs, and enhanced interoperability within the healthcare ecosystem[24][25].

In conclusion, the integration of blockchain technology in healthcare presents a promising trajectory towards revolutionizing patient data management, fortifying security, and amplifying privacy. Despite existing challenges, the transformative potential of blockchain in healthcare beckons further exploration and research, paving the way for a future where patients, practitioners, and stakeholders reap the benefits of a digitized, secure, and efficient healthcare landscape.

3. METHODOLOGY

The investigation of hypotheses regarding the utilization of blockchain technology within the patient data management system constitutes a pivotal aspect of the research titled "Analysis of Blockchain Technology in Patient Data Management System: Security, Privacy, and Efficiency in the Digital Healthcare Context" This study aims to comprehensively examine the anticipated impacts of integrating blockchain technology into the healthcare domain, with a particular focus on its implications for enhancing data security, ensuring patient privacy, and optimizing operational efficiency.

H1 : Blockchain technology positively influences patient data management in enhancing data security, through features such as encryption and digital signatures.

H2 : Blockchain technology positively influences patient data management in enhancing data privacy, by enabling proper and secure access arrangements.

H3 : Blockchain technology positively influences patient data management in increasing operational efficiency, by reducing dependence on intermediaries and facilitating fast and accurate exchange of data.

H4 : The implementation of blockchain technology in patient data management has the potential to be complicated and can affect the efficiency of digital health services.

H5 : External factors such as organizational size, technology acceptance, and government regulation can moderate the relationship between blockchain technology adoption and response variables (data security, data privacy, operational efficiency).

The proposed hypothesis is based on the understanding that blockchain's inherent characteristics, such as tamper-proof transactions and decentralized access control, have the potential to positively influence the dynamics of patient data management. Through empirical validation using a rigorous analytical methodology, including the SmartPLS approach, this study seeks to explain the multifaceted impact i.e. seeks to provide a comprehensive understanding of the potential impact, both positive and negative, as well as the influence of

external factors, of blockchain technology and contribute valuable insights into the complex landscape patient data management in an evolving digital healthcare environment.

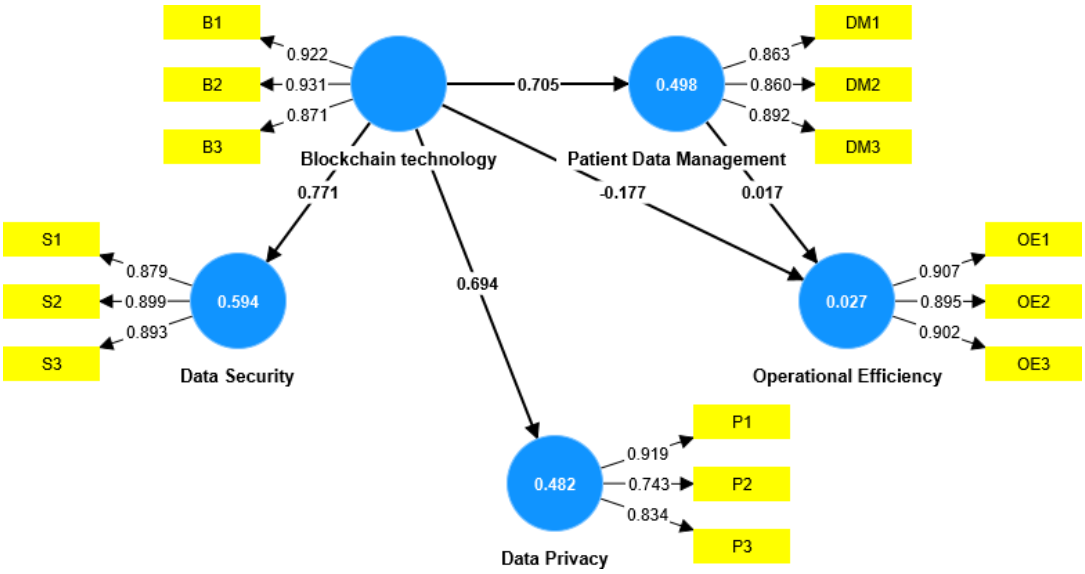

Figure 1. Conceptual Model

4. RESULTS AND DISCUSSION

Various performance methods, such as representative performance metrics and benchmarks, often need to be identified as part of the blockchain. We also need to explore the intricacies of blockchain performance assessment and how this technology can be applied to the security, privacy, and efficiency of patient data management systems in the healthcare context digital wellness.

A. Convergent validity

To evaluate the level of convergence effectively, SmartPLS offers various metrics including Average Variance Extraction (AVE), Cronbach's Alpha, Combined Reliability (CR), and Indicator Decomposition. In gauging convergence validity, it is crucial to ensure substantial loading of the indices. This implies that AVE should exceed 0.6, Cronbach's alpha should surpass 0.8, and CR should go beyond 0.8 for each indicator, particularly those assessing latent variables. Furthermore, a robust mutual loading among the indicators is necessary, indicating that each indicator predominantly measures its respective latent variable rather than others.

B. Discriminant Validity

SmartPLS offers a range of metrics for assessing discriminant validity, encompassing Fornell-Larcker criteria, heteromorphic to monomorphic ratio (HTMT), and indicator cross-load. The Fornell-Larcker criterion involves contrasting the square root of each latent variable's Average Variance Extraction (AVE) with the correlation between that latent variable

and others in the model. Discriminant validity is confirmed when the square root of AVE for a specific latent variable surpasses the correlation with other latent variables in the model.

C. Tests Results for Convergent Validity

Table 1. Tests Results For Convergent Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted(AVE)
Blockchain Technology	0.895	0.908	0.934	0.825
Data Privacy	0.780	0.808	0.873	0.697
Data Security	0.870	0.880	0.920	0.793
Operational Efficiency	0.885	0.892	0.929	0.813
Patient Data Management	0.843	0.852	0.905	0.760

All numbers in Table 1 meet the requirement to be greater than 0.6. This is Cronbach's alpha claim. The composite confidence score must also be 0.6 or higher. Therefore, all composite confidence scores meet the specified criteria. In addition, data were collected with mean variance greater than 0.1. Figures 3, 4 and 5 also show that all requirements are met and all values are within the specified limits.

D. Tests Results for Discriminant Validity

The HTMT ratio compares the correlation between measurements of different latent variables with the correlation between measurements of the same latent variable. Discriminant value is supported when the correlation ratio between different latent variables is less than 1.05.

Table 2. Heterotrait Monotrait Table

	Blockchain Technology	Data Privacy	Data Security	Operational Efficiency	Patient Data Management
Blockchain Technology					
Data Privacy	0.818				
Data Security	0.858	0.925			
Operational Efficiency	0.184	0.107	0.230		
Patient Data Management	0.799	1.056	0.945	0.123	

Two tests were performed to determine the difficulty of the structure. Calculate convergent and discriminant validity. Convergent validity testing confirms that items associated with the variable are well correlated with this variable. On the other hand, discriminant validity tests are used to demonstrate the absence of association between different subsets of variables. This is done to show that items associated with different variables in

different datasets are unrelated. Since there is no relationship between the factors, the model can evaluate the importance of the interest rate variable.

Table 3. Fornell Larcker Criterion

	Blockchain Technology	Data Privacy	Data Security	Operational Efficiency	Patient Data Management
Blockchain	0.909				
Technology					
Data Privacy	0.694	0.835			
Data Security	0.771	0.767	0.890		
Operational Efficiency	-0.164	-0.092	-0.200	0.901	
Patient Data Management	0.705	0.863	0.806	-0.107	0.872

Table 4. Cross Loadings

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
B1 <- Blockchaintechnology	0.922	0.921	0.017	54.845	0.000
B2 <- Blockchaintechnology	0.931	0.931	0.016	59.213	0.000
B3 <- Blockchaintechnology	0.871	0.869	0.033	26.557	0.000
DM1 <- Patient Data Management	0.863	0.857	0.044	19.760	0.000
DM2 <- Patient Data Management	0.860	0.854	0.048	18.026	0.000
DM3 <- Patient Data Management	0.892	0.893	0.028	31.838	0.000
OE1 <- OperationalEfficiency	0.907	0.850	0.184	4.926	0.000
OE2 <- OperationalEfficiency	0.895	0.850	0.187	4.789	0.000
OE3 <- OperationalEfficiency	0.902	0.838	0.213	4.240	0.000
P1 <- Data Privacy	0.919	0.919	0.017	52.526	0.000
P2 <- Data Privacy	0.743	0.732	0.089	8.383	0.000
P3 <- Data Privacy	0.834	0.830	0.064	13.040	0.000
S1 <- Data Security	0.879	0.870	0.053	16.583	0.000
S2 <- Data Security	0.899	0.899	0.023	38.368	0.000
S3 <- Data Security	0.893	0.893	0.026	34.777	0.000

The monomorphic heteromorphic features, Fornell and Larcker criteria, and cross-loading criteria are presented in Tables 2, 3 and 4. All values exceed the threshold of -0,200 and may also exceed the value of heteromorphic properties. No hetero-mono attribute found. This condition is also satisfied when the diagonal values of the respective column are significant, similar to Fornell and Larcker's criterion. Table 3 shows that all entries for each variable exhibit significant correlation with that corresponding variable, while not correlated

with other items or items of different variables. Consider combining one or more items from separate variables.

E. Bootstrapping Results and Hypothesis Testing

Table 5. Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Blockchain technology -> Data Privacy	0.694	0.695	0.060	11.539	0.000
Blockchain technology -> Data Security	0.771	0.772	0.050	15.382	0.000
Blockchain technology -> Operational Efficiency	-0.177	-0.184	0.189	0.934	0.351
Blockchain technology -> Patient Data Management	0.705	0.707	0.065	10.922	0.000
Patient Data Management -> Operational Efficiency	0.017	0.027	0.235	0.073	0.942

Lastly, you can also assess the indicator's loading to confirm that each indicator exhibits a stronger association with its corresponding latent variable compared to other latent variables in the model. A high cross-loading of an indicator with other latent variables suggests the indicator's potential to measure multiple components.

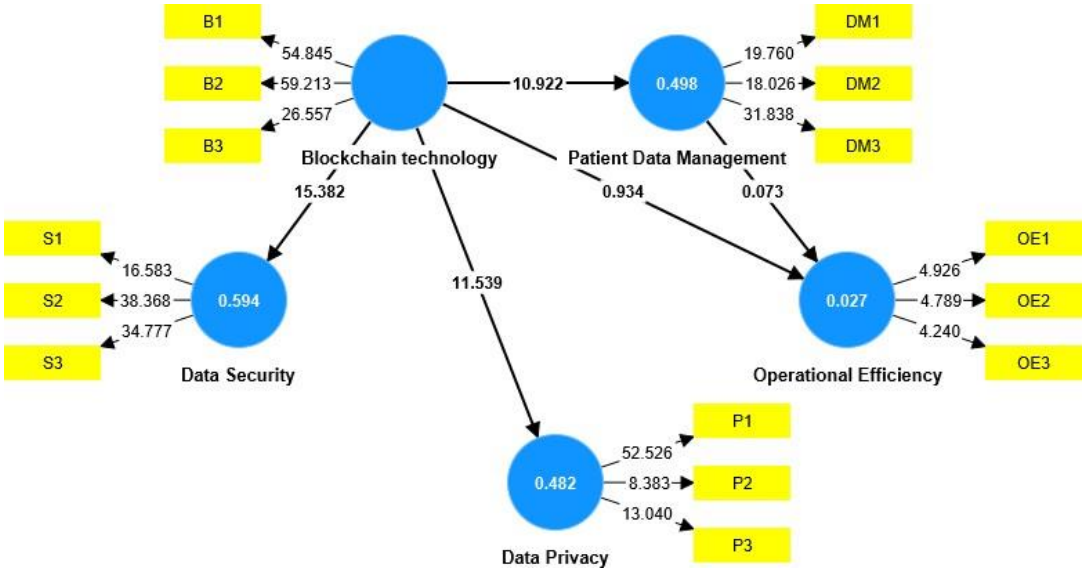

Figure 2. Model T-test Result

The results obtained from the SmartPLS analysis provide valuable insights into the relationships between various variables within the context of the study. The examination of the relationships involving "Blockchain technology" and its impact on different aspects of the healthcare domain yields significant findings.

Starting with the correlation between "Blockchain technology" and "Data Privacy," the original sample value (O) for this relationship is 0.694, while the sample mean (M) stands at 0.695. The standard deviation (STDEV) is calculated as 0.060. The t-statistics value (|O/STDEV|) is 11.539, signifying a highly statistically significant relationship. The accompanying p-value of 0.000 further reinforces the substantial statistical significance of this association.

Similarly, the association between "Blockchain technology" and "Data Security" exhibits a robust correlation. The original sample value (O) in this case is 0.771, closely aligned with the sample mean (M) of 0.772. The standard deviation (STDEV) is computed as 0.050. The t-statistics value (|O/STDEV|) reaches an impressive 15.382, indicating an extremely high level of statistical significance. The p-value of 0.000 underscores the profound statistical significance of this link.

However, the correlation between "Blockchain technology" and "Operational Efficiency" unfolds differently. The original sample value (O) for this relationship is -0.177, slightly deviating from the sample mean (M) of -0.184. The standard deviation (STDEV) amounts to 0.189. The t-statistics value (|O/STDEV|) stands at 0.934, suggesting that this relationship lacks statistical significance. The p-value of 0.351 supports the notion that this correlation is not statistically significant.

Moving on to the connection between "Blockchain technology" and "Patient Data Management," the original sample value (O) is 0.705, very close to the sample mean (M) of 0.707. The standard deviation (STDEV) is 0.065. The t-statistics value (|O/STDEV|) registers at 10.922, indicating a high level of statistical significance. The p-value of 0.000 reinforces the substantial statistical significance of this relationship.

Lastly, the correlation between "Patient Data Management" and "Operational Efficiency" is explored. The original sample value (O) for this link is 0.017, while the sample mean (M) is slightly higher at 0.027. The standard deviation (STDEV) is calculated as 0.235. The t-statistics value (|O/STDEV|) is 0.073, indicative of the lack of statistical significance. The p-value of 0.942 further solidifies the finding that this correlation lacks statistical significance.

In summation, the SmartPLS results reveal that the relationships between "Blockchain technology" and "Data Privacy," "Data Security," as well as "Patient Data Management" exhibit substantial statistical significance. However, the relationships between "Blockchain technology" and "Operational Efficiency" and between "Patient Data Management" and "Operational Efficiency" do not demonstrate statistical significance. These findings shed light on the complex interplay of variables within the context of the study and provide a nuanced understanding of their relationships in the realm of digital healthcare.

5. CONCLUSION

In the swiftly evolving realm of digital healthcare, the imperative to ensure secure, confidential, and efficient patient data management has become paramount. Recognizing this need, blockchain technology has emerged as a promising solution to address the multifaceted challenges inherent in this domain. This study aspires to delve into the intricate landscape of implementing blockchain technology within patient data management systems, with a keen emphasis on its potential to fortify security, enhance privacy, and optimize efficiency within the realm of digital healthcare. The contemporary healthcare ecosystem demands solutions that align with the trends of technological innovation while catering to the unique demands of the sector. This study bridges the gap between these realms by exploring how blockchain can be effectively harnessed to bolster data security, enhance patient data privacy, and streamline the flow of information. Employing a holistic approach, this research methodology encompasses both qualitative and quantitative techniques, such as surveys, literature analysis, and case studies, to provide a comprehensive evaluation of the impact of blockchain on patient data management. A noteworthy facet of this research lies in its identification of gaps in the practical application of blockchain technology within patient data management. By dissecting the intricacies of this technology's integration and addressing practical challenges within the dynamic landscape of digital healthcare, this study yields insights that extend beyond theoretical frameworks. The results obtained from the SmartPLS analysis shed light on the relationships between various variables in the context of the study. The correlations between "Blockchain technology" and "Data Privacy," as well as "Data Security," are underpinned by a robust statistical significance. These findings reaffirm the potential of blockchain to enhance the safeguarding of sensitive health information. However, the analysis also indicates that the connections between "Blockchain technology" and "Operational Efficiency," as well as between "Patient Data Management" and "Operational Efficiency," lack statistical significance. This insight adds a layer of complexity to the understanding of these relationships and highlights areas that require further exploration. In conclusion, this research contributes to an enriched comprehension of how blockchain technology can substantially influence the dimensions of security, privacy, and efficiency within patient data management. By navigating the intricate interplay of variables and exploring innovative methods like blockchain integration, this study serves as a beacon of guidance for stakeholders aiming to navigate the evolving landscape of digital healthcare. The synthesis of theoretical insights and empirical findings fosters a deeper understanding of the potential and limitations of blockchain technology in the realm of patient data management, ultimately contributing to the advancement of healthcare practices in the digital age.

6. REFERENCES

[1] S. Singh, S. K. Sharma, P. Mehrotra, P. Bhatt, and M. Kaurav, “Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives,” Mater. Today Proc., vol. 62, pp. 5042–5046, 2022.

[2] M. R. Hasan, S. Deng, N. Sultana, and M. Z. Hossain, “The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges,” Libr. Hi Tech, vol. 39, no. 3, pp. 814–833, 2021.

[3] M. H. R. Chakim, M. Hatta, A. Himki, A. R. A. Zahra, and N. N. Azizah, "The Relationship Between Smart Cities and Smart Tourism: Using a Systematic Review," ADI J. Recent Innov., vol. 5, no. 1Sp, pp. 33–44, 2023.

[4] L. Sulivyo and F. M. Dewi, "Strategy Management Analysis in the Face of Business Competition," ADI J. Recent Innov., vol. 5, no. 1Sp, pp. 1–8, 2023.

[5] M. A. Bazel, F. Mohammed, and M. Ahmed, "Blockchain technology in healthcare big data management: Benefits, applications and challenges," in 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2021, pp. 1–8.

[6] A. Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah, and S. A. Zabidi, "Systematic review on ai-blockchain based e-healthcare records management systems," IEEE Access, 2022.

[7] L. S. Riza, E. Piantari, E. Junaeti, and I. S. Permana, "Implementation of the Gamification Concept in the Development of a Learning Management System to Improve Students' Cognitive In Basic Programming Subjects Towards a Smart Learning Environment," ADI J. Recent Innov., vol. 5, no. 1, pp. 43–53, 2023.

[8] S. Bittins, G. Kober, A. Margheri, M. Masi, A. Miladi, and V. Sassone, "Healthcare data management by using blockchain technology," Appl. blockchain Healthc., pp. 1– 27, 2021.

[9] P. Sharma, S. Namasudra, R. G. Crespo, J. Parra-Fuente, and M. C. Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," Inf. Sci. (Ny)., vol. 629, pp. 703–718, 2023.

[10] S. Alzahrani, T. Daim, and K.-K. R. Choo, "Assessment of the blockchain technology adoption for the management of the electronic health record systems," IEEE Trans. Eng. Manag., 2022.

[11] P. A. G. K. Dewi, A. D. Dwipayana, N. L. Darmayanti, and S. S. Ryanto, "Implementation of Green Human Resource Management in Land Transportation and Logistics in Indonesia," ADI J. Recent Innov., vol. 5, no. 1, pp. 54–60, 2023.

[12] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," Comput. Networks, vol. 200, p. 108500, 2021.

[13] A. Sharma, S. Kaur, and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," Trans. Emerg. Telecommun. Technol., vol. 32, no. 10, p. e4333, 2021.

[14] V. Merlo, G. Pio, F. Giusto, and M. Bilancia, "On the exploitation of the blockchain technology in the healthcare sector: A systematic review," Expert Syst. Appl., p. 118897, 2022.

[15] T. Raharjo, "A Model of Critical Success Factors for Agile Information Technology Project in Indonesia using Analytic Hierarchy Process (AHP)," ADI J. Recent Innov., vol. 5, no. 1Sp, pp. 68–77, 2023.

[16] S. Saif, S. Biswas, and S. Chattopadhyay, "Intelligent, secure big health data management using deep learning and blockchain technology: an overview," Deep Learn. Tech. Biomed. Heal. Informatics, pp. 187–209, 2020.

[17] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications," Sensors, vol. 23, no. 15, p. 6762, 2023.

[18] A. Dubovitskaya, P. Novotny, Z. Xu, and F. Wang, “Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review,” Oncology, vol. 98, no. 6, pp. 403–411, 2020.
[19] M. H. R. Chakim, M. A. D. Yuda, R. Fahrudin, and D. Apriliasari, “Secure and Transparent Elections: Exploring Decentralized Electronic Voting on P2P Blockchain,” ADI J. Recent Innov., vol. 5, no. 1Sp, pp. 54–67, 2023.
[20] A. Yogeshwar and S. Kamalakkannan, “Healthcare Domain in IoT with Blockchain Based Security-A Researcher’s Perspectives,” in 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 1–9.
[21] V. R. Prybutok and B. Sauser, “Theoretical and practical applications of blockchain in healthcare information management,” Inf. Manag., vol. 59, no. 6, p. 103649, 2022.
[22] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, “Blockchain application in healthcare systems: a review,” Systems, vol. 11, no. 1, p. 38, 2023.
[23] N. Wiwin, P. A. Sunarya, N. Azizah, and D. A. Saka, “A Model for Determine Upgrades for MSMEs using Analitical Hyrarcy Process,” ADI J. Recent Innov., vol. 5, no. 1Sp, pp. 20–32, 2023.
[24] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, “Healthcare and fitness data management using the IoT-based blockchain platform,” J. Healthc. Eng., vol. 2021, 2021.
[25] D. Kuntal and D. K. Vishwakarma, “Blockchain-Enabled Healthcare Records Management: A Survey of Implementation Strategies,” in 2023 3rd International Conference on Intelligent Technologies (CONIT), 2023, pp. 1–6.