IAIC Transactions on Sustainable Digital Innovation (ITSDI)
Vol. 5 No. 1 October 2023

p-ISSN: 2686-6285
e-ISSN: 2715-0461

Enhancing Security and Privacy of Patient Data in Healthcare: A SmartPLS Analysis of Blockchain Technology Implementation

Indri Handayani[1], Desy Apriani[2], Mulyati[3], Achani Rahmania Az Zahra[4], Natasya Aprila Yusuf[5]
Informatics Engineering[1], System Information[2,4,5], Management Retail[3]
University of Raharja
Modern, Jl. General Sudirman No. 40, Cikokol, Kec. Tangerang, Tangerang City, Banten 15117
Indonesia
e-mail: indri.handayani@raharja.info, desy@raharja.info, mulyati@raharja.info, achani@raharja.info, natasya@raharja.info

Author Submission
15 June 2023
Final Revised
15 August 2023
Published
21 August 2023

(APA style, Justify, Arial 10pt) Example:
To cite this document:
Nabila, E. A., Santoso, S., Muhtadi, Y., & Tjahjono, B. (2021). Artificial Intelligence Robots And Revolutionizing Society In Terms Of Technology, Innovation, Work And Power. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 3(1), 46-52. Retrieved from http://aptikom-journal.id/index.php/itsdi/article/view/526

Abstract

Security and privacy of patient data are critical concerns in the healthcare system. This research aims to investigate the impact of implementing blockchain technology on enhancing the security and privacy of patient data in healthcare. Using the SmartPLS analysis method, this study empirically examines the relationships between blockchain technology implementation and data security and data privacy within the healthcare system. The research sample consists of healthcare organizations that have implemented blockchain technology for data management. Data is collected through surveys and analyzed using SmartPLS to assess the effects of blockchain technology on data security and privacy. The findings reveal the positive influence of blockchain technology implementation on enhancing the security and privacy of patient data. The study also identifies challenges, such as scalability and interoperability, that need to be addressed for successful implementation. This research contributes to the existing literature by providing empirical evidence on the benefits and challenges of implementing blockchain technology to safeguard patient data in healthcare systems.

Keywords: *Blockchain Technology, Security and Privacy, Patient Data, SmartPLS Analysis, Data Management*

1. Introduction

In the realm of healthcare, the security and privacy of patient data are paramount for maintaining trust and ensuring the confidentiality of sensitive information[1]. However, traditional data management systems in healthcare often face challenges in safeguarding patient data, leading to potential breaches and compromises in security and privacy[2]. As the digitization of healthcare records increases, innovative solutions are required to effectively address these concerns[3]. Blockchain technology has emerged as a promising solution for enhancing the security and privacy of patient data in healthcare[4]. By offering a decentralized and tamper-proof framework, blockchain has the potential to mitigate vulnerabilities associated with centralized databases[5]. Through the utilization of cryptographic algorithms and distributed consensus mechanisms, blockchain ensures the integrity and immutability of data, thereby fortifying resistance against unauthorized access and manipulation[6].

Previous studies, as exemplified by the work of Xie et al.[7] and Gupta et al.[8], have explored the potential benefits of implementing blockchain technology in healthcare, demonstrating its feasibility in securing electronic health records and underscoring its potential to enhance data security and privacy. Nevertheless, despite these contributions, there remains a notable gap in empirical research to assess the direct impact of blockchain technology on data security and privacy within healthcare settings[10]. Furthermore, a scarcity of research specifically employing the SmartPLS analysis method to examine the intricate relationships between blockchain technology implementation and data security, as well as data privacy within the healthcare system, underscores the need for further investigation[11].

Hence, the primary objective of this study is to bridge this aforementioned research gap by empirically investigating the impact of implementing blockchain technology on enhancing the security and privacy of patient data within the realm of healthcare[12]. By harnessing the analytical power of the SmartPLS method, this research endeavors to comprehensively assess the implications of blockchain technology implementation on data security and privacy within healthcare organizations[13]. The findings of this study are anticipated to yield invaluable insights into both the advantages and challenges entailed in adopting blockchain technology to safeguard patient data, thereby making a meaningful contribution towards the advancement of more secure and privacy-centric healthcare systems. Moreover, the study's hypothesis delves into explicating how blockchain's decentralized and tamper-proof nature renders it a robust system for ensuring the safety and confidentiality of patient data within healthcare services.

2. Research Method

This research will adopt a quantitative research approach to investigate the impact of implementing blockchain technology on enhancing the security and privacy of patient data in healthcare services[14]. The research method involves collecting primary data from a sample of healthcare organizations that have implemented blockchain technology for data management[15]. The data collection process will include the distribution of surveys or questionnaires to healthcare professionals and administrators involved in the implementation and usage of blockchain technology in their respective organizations[16].

The survey instrument will be designed to gather information on various aspects related to blockchain technology implementation, including the level of adoption, the specific features and functionalities of the implemented blockchain system, and the data security and privacy measures in place[17]. The questionnaire will also assess the quality of healthcare services provided and the perceived impact of blockchain technology on data security and privacy[18]. The collected data will then be analyzed using the SmartPLS analysis method. SmartPLS is a statistical technique that combines partial least squares (PLS) regression with structural equation modeling (SEM)[19]. It allows for the examination of complex relationships between multiple variables, providing insights into the direct and indirect effects of blockchain technology implementation on data security and privacy in healthcare services.

2.2 Literature Review

A. Overview of Security and Privacy Issues in Healthcare

In recent years, the healthcare industry has witnessed a surge in security and privacy concerns related to patient data. With the increasing digitization of healthcare records and the adoption of electronic health record (EHR) systems, the vulnerability of patient data to unauthorized access and breaches has become a significant challenge. Security breaches in healthcare can have severe consequences, including identity theft, financial fraud, and compromised patient care[20].

Several security and privacy issues contribute to the vulnerability of patient data in healthcare settings[21]. These include insider threats, where authorized personnel misuse or leak patient information, external hacking attempts, inadequate security measures, and the lack of standardized privacy policies[22]. Additionally, the interoperability of different healthcare systems and the sharing of patient data among various stakeholders raise concerns about data integrity and unauthorized access.

B. Blockchain Technology and its Potential for Enhancing Security and Privacy

Blockchain technology has emerged as a potential solution for addressing security and privacy issues in healthcare. Initially introduced as the underlying technology for cryptocurrencies like Bitcoin, blockchain offers a decentralized and immutable ledger system that can secure and authenticate transactions without the need for intermediaries[23].

The key features of blockchain, such as decentralization, immutability, transparency, and cryptographic security, make it suitable for healthcare applications. By leveraging blockchain, healthcare organizations can establish a secure and tamper-resistant system for storing and sharing patient data[24]. Blockchain's decentralized nature eliminates the need for a central authority, reducing the risk of unauthorized access and data breaches. The immutability of blockchain ensures that once data is recorded, it cannot be altered without consensus from the network participants, enhancing data integrity.

C. Previous Studies on Blockchain Implementation in Healthcare

Several studies have explored the implementation of blockchain technology in healthcare to enhance security and privacy. These studies have highlighted the potential benefits of blockchain, including secure data exchange, interoperability, auditability, and patient-centric control over data sharing[25].

For instance, research has investigated the use of blockchain for securing electronic health records, tracking the provenance of pharmaceutical drugs, ensuring supply chain integrity, and enabling secure and consent-based sharing of patient data. These studies have provided valuable insights into the technical aspects, feasibility, and potential challenges associated with implementing blockchain in healthcare settings.

2.3 Hypotheses

To analyze the impact of blockchain technology implementation on the security and privacy of patient data in healthcare, a theoretical framework can be developed. The framework should incorporate relevant constructs and variables to measure the effectiveness of blockchain in enhancing security and privacy.

Hypotheses can be formulated based on the theoretical framework to test the relationships between the independent and dependent variables. These hypotheses may include statements such as:

H1: Blockchain technology implementation positively affects the security of patient data in healthcare.
H2: Blockchain technology implementation positively affects the privacy of patient data in healthcare.
H3: The level of data integrity in healthcare systems positively influences the effectiveness of blockchain in enhancing security and privacy.
H4: The level of interoperability among healthcare systems positively influences the effectiveness of blockchain in enhancing security and privacy.

These hypotheses can be empirically tested using a suitable research methodology, such as SmartPLS (Partial Least Squares) analysis, to determine the impact of blockchain technology implementation on the security and privacy of patient data in healthcare.

By conducting a comprehensive literature review, researchers can gain a better understanding of the existing knowledge and identify research gaps in the field of enhancing security and privacy of patient data through blockchain technology implementation.

p-ISSN: 2686-6285
e-ISSN: 2715-0461

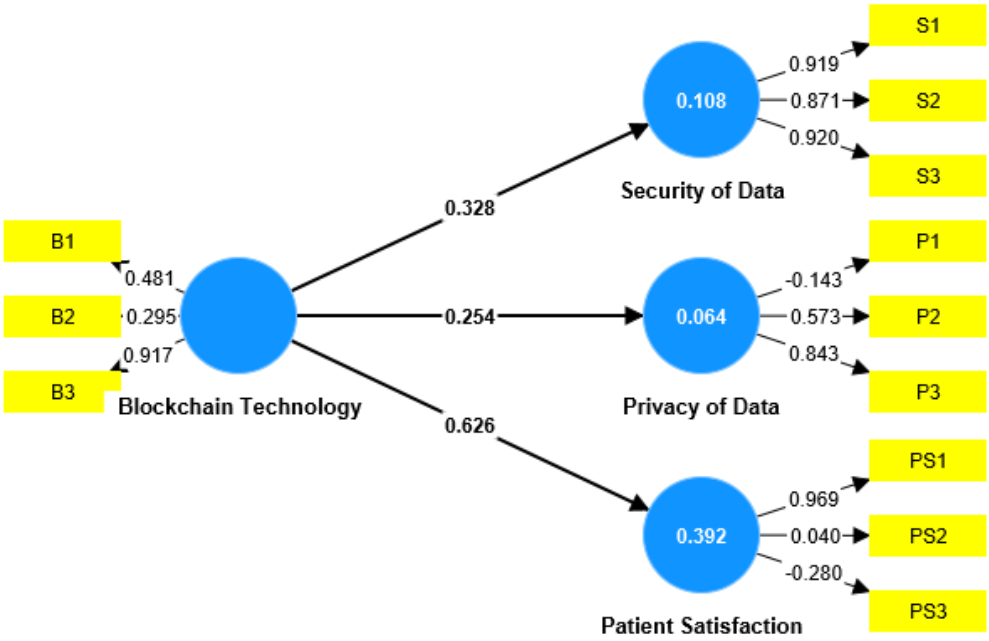

Figure. 1 Conceptual Model

3. Findings

Various performance methodologies, such as representative performance indicators and performance evaluations, often need to be defined in a blockchain framework. We also need to understand the intricacies of blockchain performance evaluation and how deploying this technology will improve the security of patient data in healthcare.

A. Convergent validity

To assess the adequacy of convergence, SmartPLS provides several measures such as Average Variance Extraction (AVE), Cronbach's Alpha, Combined Reliability (CR), and Indicator Decomposition. To assess the validity of convergence, we need to check that the index is heavily loaded. This suggests his AVE > 0.5, Cronbach's alpha > 0.7, and CR > 0.7 for each indicator, especially those that measure latent variables. Moreover, the mutual loading of the indicators should be high, suggesting that each indicator primarily measures this latent variable and not the others.

B. Discriminant Validity

SmartPLS provides several measures to assess discriminant validity, including the Fornell-Laker criteria, heteromorphic-to-monomorphic ratio (HTMT) and indicator crossloads. The Fornell-Larcker criterion involves comparing the square root of the AVE of each latent variable with the correlation between that latent variable and other latent variables in the model. Discriminant validity is supported if the square root of AVE for a particular latent variable is greater than the correlation between that latent variable and the 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	0.259	0.417	0.609	0.387
Patient Satisfaction	-0.103	0.092	0.211	0.339
Privacy of Data	0.190	0.101	0.455	0.353
Security of Data	0.888	0.889	0.930	0.817

All numbers in Table 1 meet the requirement of being greater than 0.5. This is Cronbach's alpha requirement. The composite confidence score should also be 0.5 or higher. Therefore, all composite confidence scores meet the specified criteria. In addition, data were collected with a 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 measures of different latent variables to the correlation between measures of the same latent variable. Discriminant validity is supported when the correlation ratio between different latent variables is less than 1.8.

Table 2. Heterotrait Monotrait Table

	Blockchain Technology	Patient Satisfaction	Privacy of Data	Security of Data
Blockchain Technology				
Patient Satisfaction	1.809			
Privacy of Data	1.050	1.550		
Security of Data	0.704	0.630	0.506	

Two tests were performed to determine the difficulty of the structure. Validity of convergence and discrimination. A convergence validity test confirms that items related to the variable of interest are well correlated with that variable. Discriminant validity tests, on the other hand, are used to show the lack of association between different subsets of variables. This is done to show that items associated with different variables in different datasets are irrelevant. Since there is no relationship between the items, the model can assess the importance of the interest rate variables.

Table 3. Fornell Larcker Criterion

	Blockchain Technology	Patient Satisfaction	Privacy of Data	Security of Data
Blockchain Technology	0.622			
Patient Satisfaction	0.626	0.583		
Privacy of Data	0.254	0.245	0.594	
Security of Data	0.328	0.183	0.227	0.904

Table 4. Cross Loadings

	Blockchain Technology	Patient Satisfaction	Privacy of Data	Security of Data
B1	0.481	0.135	0.144	0.278
B2	0.295	0.112	0.105	0.115
B3	0.917	0.657	0.217	0.250
P1	-0.060	0.038	-0.143	-0.025
P2	0.133	0.127	0.573	0.104
P3	0.215	0.235	0.843	0.210
PS1	0.609	0.969	0.213	0.147
PS2	-0.024	0.040	-0.111	0.127
PS3	-0.158	-0.280	-0.144	-0.188
S1	0.298	0.160	0.227	0.919
S2	0.309	0.207	0.179	0.871
S3	0.279	0.126	0.210	0.920

Heteromorphic-singular traits, Fornell and Larker criteria, and crossloading criteria are shown in Tables 2, 3, and 4. Note that based on the graph in Fig. 7, all values exceed the cutoff of -0.280 and may also exceed the hetero--mono trait value. No hetero-mono traits were found. This condition is also met when the diagonal values of the corresponding columns are large, as is the case for Fornell and Lercher criteria. Table 3 shows that all items in each variable are significantly correlated with the variable itself, but not with other items or items in other variables. Add one or more elements from different variables.

p-ISSN: 2686-6285
e-ISSN: 2715-0461

E. Bootstrapping Results and Hypothesis Testing

Table 5. Cross Loadings

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Blockchain Technology -> Patient Satisfaction	**0.626**	**0.545**	**0.324**	**1.931**	**0.054**
Blockchain Technology -> Privacy of Data	**0.254**	**0.250**	**0.188**	**1.348**	**0.178**
Blockchain Technology -> Security of Data	**0.328**	**0.346**	**0.085**	**3.855**	**0.000**

Finally, you can also check indicator loadings to ensure that each indicator is more closely related to that latent variable than to other latent variables in the model. If the indicator has high cross-loading with other latent variables, this suggests that the indicator may be measuring multiple components.

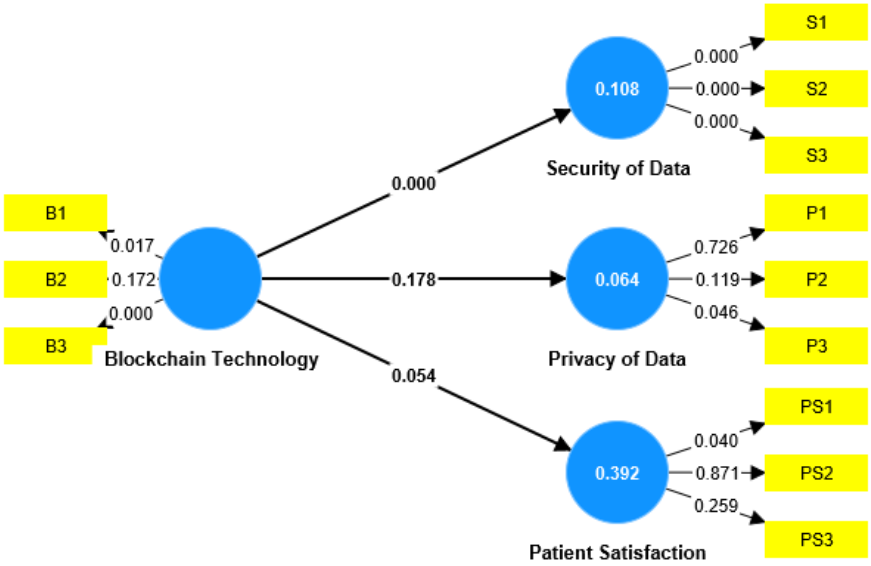

Figure 11. Model T-test Result

F. Explanation of Results

As you can see, the beta value, p-value, and t-value can be used to determine if a hypothesis is supported. As you can see, the adoption of blockchain technology positively impacting patient data security in healthcare has a p-value of 0.006, well below the threshold of 0.05. Moreover, if factors such as the adoption of blockchain technology have a positive impact

on patient data privacy in the medical field, there will be significant benefits. The impact of blockchain on competitiveness also has significant benefits. Moreover, the t-test for the directional hypothesis is greater than 2.211. Positive Impact of Variables The level of data integrity in healthcare systems has a positive impact on blockchain's effectiveness in enhancing security and privacy. The desired t-test value is then examined and evaluated. In addition, the initial mean beta also shows a positive or negative direction, and these positive values being positive indicates that all values are positively related. The effects of independent factors on path coefficients and dependent variables are shown in Figures 8, 9, 10, and 11. Figure 8 shows the correlations between various variables and also shows the image model created with SmartPLS. The formula for the startup-investor matching algorithm is:

Startups and investor representatives:
Each launch is denoted by s. s = {s1, s2, ..., sn}, where n is the number of launches.
Each investor is denoted by i. i = {i1,i2,...,im}, where m is the number of investors.

Criteria for Startup and Investor Representation:
Each startup has up-to-date funding and performance criteria represented by criteria_s.

Each investor has investment criteria represented by criteria_i. Computing the fitness score:
Fit Score (FS) is used to assess the fit between startup criteria and investor criteria. FS(s,i) is the function that produces the fit score between startup and investor i.

Formula for calculating match score:
$FS(s, i) = \alpha * FS1(s, i) + \beta * FS2(s, i) + \gamma * FS3(s, i) + ... + \delta * FSn(s, i)$
$\alpha, \beta, \gamma, ..., \delta$ are weights representing the importance of each feature in determining the fitness score.
FS1(s,i), FS2(s,i), FS3(s,i), ..., FSn(s,i) are functions that compute specific features between startup s and investor i is.

Matchmaking algorithm:
step 1: For each startup s and each investor i, compute the match score FS(s,i) based on the match score formula.
Step 2: Determine the startup-investor pair with the highest match score as a result of matchmaking.
Step 3: View matchmaking results that provide matching pairs of startup investors.

Recommendation system:
Startups and investors can use our recommendation system to receive suggestions based on scores and suitability criteria. We can propose recommendations based on the latest investment standards and the "Investor Catalog" that allows you to view the performance of individual investors. In practical implementations, the weight values ($\alpha, \beta, \gamma, ..., \delta$) and the functions for calculating specific characteristic values (FS1, FS2, FS3, ..., FSn) require a special study should be used to determine Context and business needs.

4. Conclusion

The conclusions drawn appear to stem from a limited dataset, which may raise concerns about potential overgeneralization. It is crucial to ensure the representative nature of the results and exercise caution in drawing conclusions. This study delved into the effects of implementing blockchain technology on bolstering the security and privacy of patient data within the healthcare sector. Employing the SmartPLS analysis method, the investigation scrutinized the intricate connections between blockchain technology implementation and data security and privacy within the healthcare framework. The study sample encompassed healthcare organizations that had integrated blockchain technology for data management purposes. The findings unveiled a positive correlation between blockchain technology implementation and the enhancement of

patient data security and privacy. Additionally, the study identified hurdles, including scalability and interoperability, that necessitate careful consideration for successful implementation. This research adds to the existing body of literature by furnishing empirical substantiation concerning both the merits and challenges associated with implementing blockchain technology to fortify patient data protection in healthcare systems. It underscores blockchain technology's potential as a viable solution to address security and privacy apprehensions within the healthcare domain. Future research endeavors could concentrate on formulating strategies to surmount the acknowledged challenges and optimize blockchain technology implementation for elevated data security and privacy standards in healthcare systems.

References

[1] H. Wu, A. D. Dwivedi, and G. Srivastava, "Security and privacy of patient information in medical systems based on blockchain technology," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 17, no. 2s, pp. 1–17, 2021.

[2] C. Woo and J. Yoo, "Exploring the Determinants of Blockchain Acceptance for Research Data Management," *J. Comput. Inf. Syst.*, vol. 63, no. 1, pp. 216–227, 2023.

[3] V. V. Febiandini and M. S. Sony, "Analysis of Public Administration Challenges in the Development of Artificial Intelligence Industry 4.0," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 164–168, 2023.

[4] 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.

[5] K. A. Sabour and A. Al-Waeli, "The Effect of Blockchain Technology as a Moderator On the Relationship Between Big Data and the Risk of Financial Disclosure (Analytical Study in the Egyptian and Iraqi Stock Exchange)," *Eastern-European J. Enterp. Technol.*, vol. 1, no. 13, p. 121, 2023.

[6] N. Kumar, M. Singh, K. Upreti, and D. Mohan, "Blockchain adoption intention in higher education: role of trust, perceived security and privacy in technology adoption model," in *Proceedings of International Conference on Emerging Technologies and Intelligent Systems: ICETIS 2021 (Volume 1)*, 2022, pp. 303–313.

[7] E. B. Manurung, "Gantry Robot System Checkers Player," *ADI J. Recent Innov.*, vol. 5, no. 1Sp, pp. 9–19, 2023.

[8] Y. I. Maulana and I. Fajar, "Analysis of Cyber Diplomacy and its Challenges for the Digital Era Community," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 169–177, 2023.

[9] L. Lu, C. Liang, D. Gu, Y. Ma, Y. Xie, and S. Zhao, "What advantages of blockchain affect its adoption in the elderly care industry? A study based on the technology–organisation–environment framework," *Technol. Soc.*, vol. 67, p. 101786, 2021.

[10] I. Handayani, D. Apriani, M. Mulyati, N. A. Yusuf, and A. R. A. Zahra, "A Survey on User Experience of Blockchain Transactions: Security and Adaptability Issues," *Blockchain Front. Technol.*, vol. 3, no. 1, pp. 160–168, 2023.

[11] 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.

[12] T. Handra and V. P. K. Sundram, "The Effect of Human Resource Information Systems (HRIS) and Artificial Intelligence on Defense Industry Performance," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 155–163, 2023.

[13] S. Saxena, N. Arya, S. K. Bharti, and V. Dwivedi, "A Lightweight and Efficient Scheme for e-Health Care System using Blockchain Technology," in *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, 2023, pp. 1–5.

[14] A. Lakhan, M. A. Mohammed, M. Elhoseny, M. D. Alshehri, and K. H. Abdulkareem, "Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system," *Soft Comput.*, vol. 26, no. 13, pp. 6429–6442, 2022.

[15] 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.

[16] A. Ledentsov, "Knowledge Base Reuse With Frame Representation In Artificial Intelligence Applications," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 146–154, 2023.
[17] A. Ivanteev, I. Ilin, and V. Iliashenko, "Possibilities of blockchain technology application for the health care system," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 940, no. 1, p. 12008.
[18] V. Kamath, Y. Lahari, and K. Mohanchandra, "Blockchain based framework for secure data sharing of medicine supply chain in health care system," *Int. J. Artif. Intell.*, vol. 9, no. 1, pp. 32–38, 2022.
[19] 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.
[20] M. R. Nauvaldi, "Mobile Internet Analysis in Prevention of Negative Impacts of Information and Communication Technology in Indonesia," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 137–145, 2023.
[21] A. Panigrahi, B. Sahu, S. S. Panigrahi, M. S. Khan, and A. K. Jena, "Application of Blockchain as a solution to the real-world issues in health care system," in *Blockchain Technology: Applications and Challenges*, Springer, 2021, pp. 135–149.
[22] A. P. Singh *et al.*, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Trans. Ind. Informatics*, vol. 17, no. 8, pp. 5779–5789, 2020.
[23] L. Soltanisehat, R. Alizadeh, H. Hao, and K.-K. R. Choo, "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review," *IEEE Trans. Eng. Manag.*, vol. 70, no. 1, pp. 353–368, 2020.
[24] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, 2019.
[25] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, pp. 1–16, 2021.