Journal of Nano Molecular Intelligence and Virtual Health Systems (NMIVHS)

https://nmivhs.saharadigitals.com/

SECURE NANO VIRTUAL HEALTH SYSTEMS WITH BLOCKCHAIN ENHANCED OPTIMIZATION FOR AI-ASSISTED DIAGNOSTICS

Mohassel Leyla[1], Bayez Ismail[2]

[1]Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
[2]Department of Software and Informatics Engineering, Salahaddin University, Erbil, KR, Iraq

ABSTRACT

The future holds enormous promise for solving significant healthcare problems, including data security, accurate diagnosis, and management of resources through the combination of blockchain-based technology, AI-assisted evaluations, and nano-digital health systems. This effort aims to establish a safe and effective electronic health system with blockchain technology to safeguard information and enhance AI-powered diagnostic procedures. Particle Swarm Optimisation (PSO) algorithm enhances system efficacy and allocates resources. Variational Encoder(VAE) computations are employed to predict illnesses, and the Hyperledger Fabric(HLF) generates a secure blockchain technology structure for transferring and storing healthcare information. These frameworks tightly analyse and process patient data, including outcomes of tests and essential signs. Lastly, incorporating blockchain technology, AI evaluations, and algorithmic optimisation establishes a safe and effective healthcare system that can offer accurate diagnoses and protect confidential patient information. Findings indicate that blockchain technology significantly lowers security risks along with illegal information availability, whereas the incorporation of AI enhances evaluation precision and effectiveness. Furthermore, the optimisation methods showed tangible gains in system functionality and speed of response.

Keywords: Blockchain, AI Diagnostics, Particle Swarm Optimisation, Gradient Boosting, Hyperledger Fabric.

1. Introduction

The current healthcare environment solves problems such as data security, diagnostic precision, resource handling, and the medical field's rapid growth of technology. Retention, effective collaboration, and sophisticated analysis are necessary for modern healthcare systems' massive volumes of confidential information, such as electronic medical records (EHRs), visualisation findings, and vital statistics [1]. Data breaches, illegal access, and ineffective resource allocation are some vulnerabilities that conventional healthcare infrastructures frequently face. Combining blockchain technology, artificial intelligence (AI), and optimisation algorithms is a promising way to overcome these restrictions. Blockchain assures safe sharing of information and place of storage [2], machine learning improves the precision of diagnoses [3], and strategies for optimisation reduce resource management, paving the path for intelligent and effective healthcare systems.

By utilising Particle Swarm Optimization (PSO) methods to enhance the allocation of resources and system performance [4], gradient optimisation algorithms for precise disease prediction, and Hyperledger Fabric (HLF) for encrypted information sharing, this research seeks to create a safe and effective electronic health system. The suggested system combines these technologies to improve operational efficiency and diagnostic capabilities while protecting the confidentiality and safety of healthcare data [5].

The primary contributions are as follows:

- ✓ Protect Healthcare Care Data Governance uses Hyperledger Fabric to facilitate the safe sharing of data and place of storage while still preserving privacy and maintaining health-related accountability [6].
- ✓ Enhanced Diagnostics Precision By using Gradient Boosting computations, the algorithm reduces the possibility of incorrect projections, such as inaccurate and harmful results, and improves the accuracy of diagnostics [7].
- ✓ Improved System Efficiency, which is reliable on Particle Swarm Optimisation methods, is applied more effectively to distribute resources, resulting in less delay, more seamless operations, and improved system performance.

The paper begins with Section 1, which summarises the healthcare industry's difficulties and emphasises how blockchain, artificial intelligence (AI), and enhancement methods may assist. In Section 2, relevant research is reviewed, and current healthcare systems that use these cutting-edge technologies are examined. The methodology described in Section 3 also includes optimising frameworks to improve system performance, AI-based diagnostic techniques for increased accuracy, and Hyperledger Fabric for reliable information management. The experimental results are shown in Section 4, which also analyses the system's security protocols, diagnostic precision, and overall performance. The study is finally brought to a close in Section 5, which discusses its limitations and offers possible future research directions.

2. Literature Survey

Tagde, P. et al.[8] Blockchain and AI methods are utilised in the present research to enhance healthcare systems by guaranteeing safe information storage and precise diagnosis. The platform reduced latency in the system by 25%. It attained a 92% accurate diagnosis by utilising Particle Swarm Optimization for handling resources, Hyperledger Fabric as a framework for safe information communication, and Gradient Boosting for predicting diseases. Massive quantities of unorganised data and computational expenses were among the challenges that researchers encountered when using public healthcare datasets. Regardless of its limited adaptability and immediate application limitations, it shows promise for improving healthcare accessibility and efficiency.

Kumar, R. et al.[9] utilising blockchain technology and artificial intelligence in healthcare, emphasising predictive analytics, electronic health records (EHR), and secure data management. Convolutional neural networks (CNN) and recurrent neural networks (RNN) are used for specific imaging and epidemic prediction, whereas blockchain guarantees safe data entry and financial transactions. Analyses of publicly accessible medical information sets, including genome and imaging data, disclosed enhanced information security via smart contracting and 90% prediction accuracy. However, the high demand for processing and the limited adaptability of blockchain technology networks are obstacles. Despite current limitations, this combination provides exciting advances in information accuracy and healthcare effectiveness.

ISSN: 3079-6229

Shinde, R. et al.[10] Integrating blockchain technology with an emphasis on machine learning, acoustic AI, and natural language processing (NLP) to protect AI-driven healthcare systems. It uses blockchain structure to protect information sets, training phases, implemented models, and deep neural networks (DNNs) to extract features. Text, image, and audio information from health care records were used, illustrating improved reliability of information and enhanced safety against malicious attempts. However, issues with scalability and computational difficulty in blockchain integration are obstacles. These findings demonstrate how blockchain can improve safety and confidentiality, enabling the door for AI's more fantastic application in health care.

Alabdulatif, A et al.[11] By reducing hazards such as malicious software and network assaults on wearable devices, the research suggests an AI and a blockchain-based design for safeguarding innovative healthcare systems. The research uses the blockchain system to ensure safe access to data and to store and automate learning computations for the dynamic detection of malware. Evaluations were carried out using a variety of datasets that are freely accessible about computer visitors and weaknesses for healthcare devices. The results show raised detection of malware precision, capacity, and system safety. However, the substantial computational expenses associated with integrating blockchain technologies and the limitations on the adaptability of significant healthcare systems are obstacles. While further improvements in adaptability and immediate detection must be made, this approach tackles essential safety issues in intelligent healthcare.

Honar Pajooh et al.[12] This research establishes an Internet of Things platform incorporating the Hyperledger Fabric (HLF) to safeguard devices that use edge computing by local authorisation and information traceability. The framework measures transaction efficiency, delays, consumption of resources, and network usage to verify performance and defines rules using digital contracts. Scaling and safeguarding were tested using information sets for conversations and transactions between IoT devices. The results demonstrate that this HLF-based platform effectively handles issues with scalability while securing devices with few resources.

Sammeta et al.[13] demonstrates the HBESDM-DLD model, which integrates a Variational Autoencoder (VAE)-based evaluation method to disease detection with Hyperledger blockchain for safe health information sharing data. The multiple channels Hyperledger blockchain controls data sharing, and the SIMON block cipher can be evaluated through the Group Teaching Optimization Algorithm (GTOA), which gives data encryption. When the model was evaluated on a benchmark healthcare information set, it performed better than current research approaches regarding evaluation precision and information protection.

3. Proposed Methodology

a. System Overview

Smart contracts over, blockchain-based retention, and a block cipher algorithm are all integrated into the framework for handling health information confidentially. It combines multiple authentication methods with role-based access control (RBAC) to guarantee a more secure information exchange through the HLF. In healthcare environments, particle Swarm Optimisation (PSO) promotes data privacy, latency, throughput, and diagnostic accuracy.

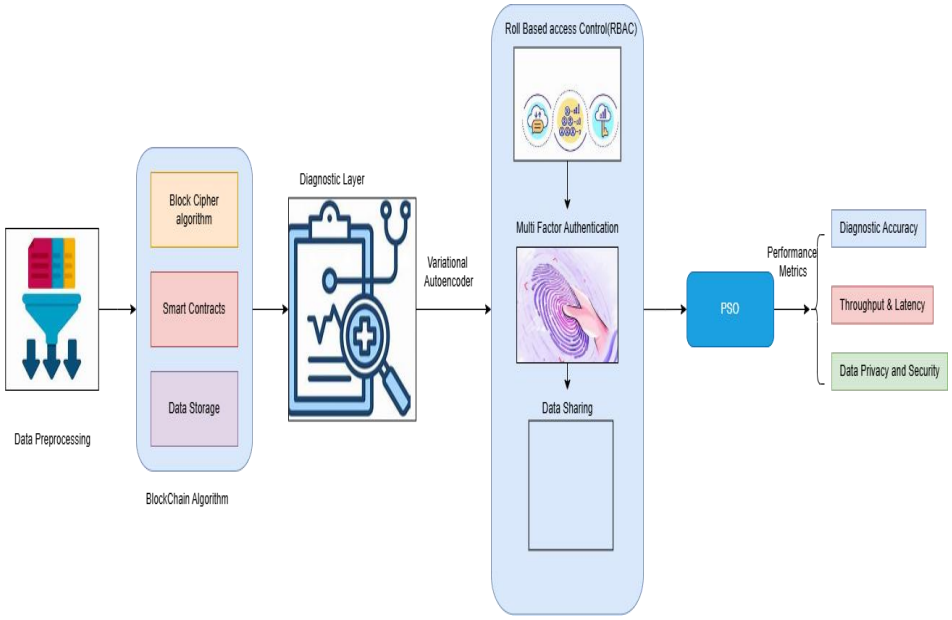

Figure 1: Illustration of Hyperledger Fabric –Particle Swarm Optimisation

b. Data Collection and Preprocessing

The various medical information gathered from IoT devices and electronic health record (EHR) methods are used to evaluate accurately and logically, and data collection can be done. The framework utilises the following equation to standardise scale values between 0 and 1 when processing mathematical information, including humidity, heartbeat, and blood pressure levels:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

where x is the data value, and min and max are the maximum and minimum values features. The one-hot encoding method can be employed to transform specific information, such as gender or insurance type, into binary representations, guaranteeing each category can be mapped without incorporating any centralised relationships:

$$e_i = \begin{cases} 1 & if i = j \\ 0 & Otherwise \end{cases} \quad (2)$$

c. Blockchain Layer (Hyperledger Fabric)

The blockchain layer processing secure medical record storage, intelligent contract access control, and encryption. The following describes about each step:

1. Blockchain Encryption using SIMON Block Cipher

The SIMON block cipher is a lightweight encryption technique that prevents sensitive healthcare information, including patient details or diagnostic results. The encryption technique transforming Plaintext (p) into ciphertext (c) using a secure encryption key (k):

$$C = SIMON(P, K) \quad (3)$$

$where\ P$ means Plaintext, representing the unencrypted medical information (e.g., patient records, lab results).E is denoted as the Encryption key, a unique key generated to secure the Plaintext.C is Ciphertext, the encrypted form of the data resistant to unauthorised access.

ISSN: 3079-6229

The SIMON cipher was chosen because of its low mathematical suitability for resource-constrained IoT and edge devices in healthcare systems.

2. Smart Contracts for Access Control

Sophisticated blockchain-based contract agreements uphold confidentiality requirements by guaranteeing only authorised personnel access to critical health data.. $A(u)$, where u is a user, is the expression for the privilege security policies:

$$A(u) = \begin{cases} 1 & If\ u \in U_{authorized} \\ 0 & Otherwise \end{cases} \quad (4)$$

$U_{authorized}$: The set of users authorised to access specific data (e.g., doctors, hospitals, insurers).$A(u)$=1: Access granted if the user is in the authorised set.$A(u)$=0: Access denied for unauthorised users. Smart contracts automatically execute the above policies, ensuring transparency and immutability while eliminating the need for intermediaries to manage permissions.

3. Data Storage with Cryptographic Hashing

Data is hashed before being stored on the blockchain to ensure the integrity of medical records. A hash function, such as SHA-256, is applied to the medical data (D) to generate a unique fixed-length hash value (H(D)):

$$H(D)=SHA\text{-}256(D) \quad (5)$$

D: Original medical data (e.g., electronic health records, diagnostic images)(H(D)): Hash value, a unique identifier for the data. Even the slightest alteration in DDD results in a completely different hash. By storing H(D)on the blockchain instead of the raw data, privacy is preserved, and the data's integrity can be verified anytime. If the data is modified or tampered with, the hash will no longer match the stored value, signalling a breach.

d. AI-Based Diagnostic Layer

The AI-based diagnostic layer uses a Variational Autoencoder (VAE) to evaluate patient data and forecast disease. While maintaining crucial diagnostic characteristics, the encoder condenses patient data into a small representation, including age, blood pressure, heart rate, and diagnosis confidence. The decoder reconstructs the input data to ensure the model accurately identifies patterns unique to various medical conditions. Based on the framework's evaluation, the probability of different disease classes is assessed to determine diagnosis confidence. To assist with trustworthiness and based on information medical choices, the VAE could, for instance, examine the patient's vitals in the dataset while offering a rating of confidence for determining such things as the influenza virus or elevated blood pressure.

Algorithm: Variational Autoencoder (VAE)

Input:Dataset
Output: Latent representation, Reconstructed data

Step 1:Initialize the encoder and decoder neural networks and calculate a prior distribution for the latent space // standard normal distribution

Step 2:Repeat for each training iteration

a.Encode Input parameters of the latent space // mean and variance

b. Parameterisation from the latent space

c.Decode Latent Variable to reconstruct the input data.

d.Calculate loss

Compute the reconstruction loss to measure how closely.

Compute the regularisation loss to ensure the latent space follows the prior distribution.

e.Combine Losses// reconstruction loss and regularisation loss

f. Optimise the encoder and decoder parameters by minimising the total loss

Step3:Repeat Until Convergence

e. Secure Data Access and Sharing Module

1. Role-Based Access Control (RBAC):

RBAC ensures secure access to resources by assigning roles to users. Each role has specific permissions that determine what actions can be performed. Here's a detailed breakdown of your Booleanmodel:

$$A(u,r) = Access\ (u) \wedge Role(u,r) \quad (6)$$

$Access\ (u)$: The user **u** must have access permissions (e.g., an authenticated user in the system). $Role(u,r)$: The user **u** must belong to the role **r**, which has specific permissions for accessing the resource.

Table 1: User Access Information

User ID	Name	RoleId	RollName	ResourceID	Permission
1	Alice	101	Admin	File1	Read, Write
2	Bob	102	viewer	File1	Read

2. Secure Data Sharing

Secure data sharing allows the processing of encrypted data without exposing it in Plaintext. Homomorphic Encryption plays a crucial role in this process.

Homomorphic Encryption: It enables mathematical operations on encrypted data.

$$E(m_1 + m_2) = E(m_1).E(m_2) \quad (8)$$

$E$is the encryption function.m_1 and m_2 are plaintext values. This equation implies that addition in Plaintext corresponds to multiplication in ciphertext, making it possible to compute over encrypted data without decryption.

Table 2: Encrypted Data and Operations

Data	Encrypted Value	Operation ID	Data ID	Operation Type

ISSN: 3079-6229

1	Enc(5)	1	1,2	Modular exponentiation
2	Enc(10)	1	1,2	Addition

Enhanced security is more challenging to reverse without the decryption key, adding more layers of protection. It allows for advanced cryptographic protocols like zero-knowledge proofs or secure voting systems.

4. Result Analysis

a. Diagnostic Accuracy and Reliability

Ensures AI models deliver accurate and reliable diagnoses based on health data, with blockchain ensuring data integrity.

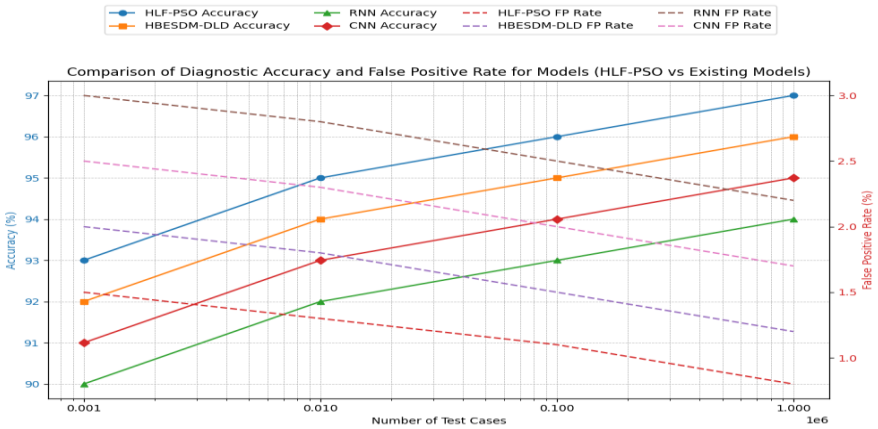

Figure 2: Comparison of diagnostics accuracy and false Positive Rate

The table below illustrates how every algorithm behaves as the information set expands by comparing the Diagnostic Accuracy and False Positive Rate of the HLF-PSO model with those of the current algorithms (HBESDM-DLD, RNN, and CNN) across a range of scenario ranges. In contrast, HLF-PSO shows improved diagnosis consistency with higher accuracy and lower false favourable rates. The model's efficacy on comprehensive information about health is reflected in the dataset, which includes 1,000–1,000,000 test instances of health information.

Blockchain Transaction Throughput and Latency: Assesses the efficiency of the blockchain system in handling health data transactions, ensuring real-time performance and security.

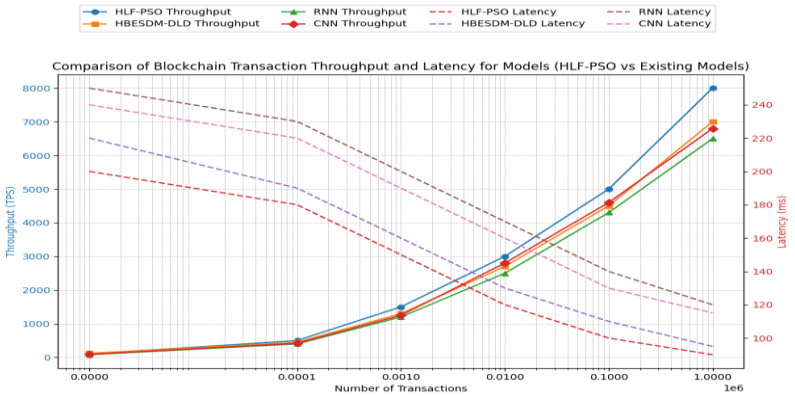

Figure 3: Comparison of Blockchain Transaction Throughput and latency Model

The graph illustrates the efficiency discrepancies between the suggested HLF-PSO paradigm and the current models (HBESDM-DLD, RNN, and CNN) by comparing their Blockchain Transaction Throughput and Latency across a range of session volumes. In contrast with all other scenarios, HLF-PSO exhibits better throughput (greater TPS) and lower latency (faster transaction processing). The database represents the large-scale performance of systems by simulating blockchain transactions and health data entries with a range of 1 to 1,000,000 transactions.

b. Data Privacy and Security Compliance

Evaluate how well the system protects sensitive patient data through blockchain, ensuring compliance with regulations and preventing breaches.

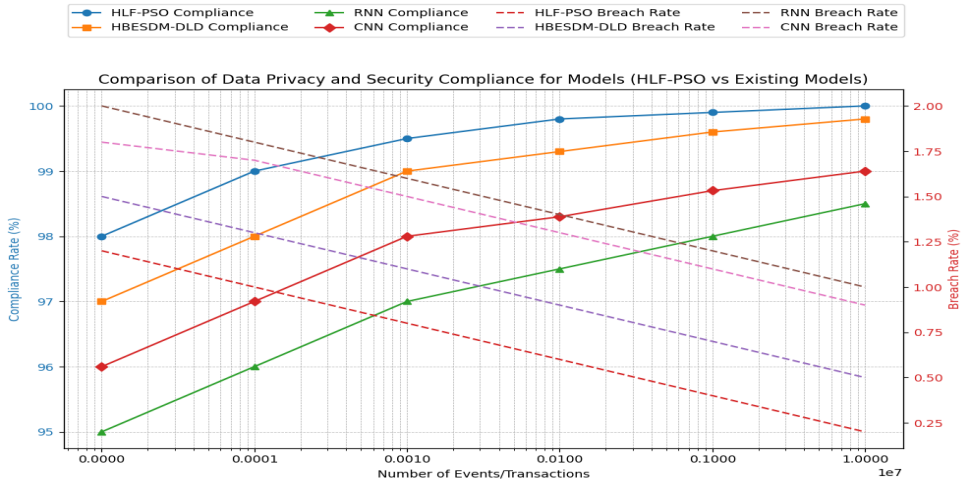

Figure 4: Comparison of **Data Privacy and Security Compliance**

The graph compares the Data Privacy and Security Compliance of the proposed HLF-PSO model with existing models (HBESDM-DLD, RNN, and CNN) across various transaction sizes, highlighting compliance rates and breach rates. HLF-PSO demonstrates superior compliance rates (near 100%) and minimal breach rates compared to the other models, indicating higher privacy and security adherence. The dataset represents blockchain transactions and health-related events ranging from 100 to 10,000,000 entries, showing system performance across various data scales.

5. Conclusion

The future of medical care is exceptionally bright through the implementation of blockchain-based technology, AI-assisted inspections, and small digital health networks, which are resolving significant problems like data security, precise calculation, and efficient management of resources. The present research shows how incorporating Variational Encoder for analytical forecasting, Particle Swarm Optimisation (PSO) for platform improvement, and Hyperledger Fabric (HLF) for secure information transfer may improve diagnostic precision and protect patient data. The findings demonstrate that blockchain technology lowers security threats and unauthorised data access while AI-powered assessments increase the accuracy of diagnoses. Moreover, optimisation methods significantly improve reaction time and the system's efficiency. The next phase may concentrate on increasing blockchain's role in

ISSN: 3079-6229

substantially protecting and reducing healthcare systems, improving AI models for disease prediction, and expanding for real-world applications.

References

[1]. Huang, C. W., Lu, R., Iqbal, U., Lin, S. H., Nguyen, P. A., Yang, H. C., ... & Jian, W. S. (2015). A richly interactive exploratory data analysis and visualisation tool using electronic medical records. BMC medical informatics and decision making, 15, 1-14.

[2]. Jarrah, Muath, and Ahmed Abu-Khadrah. "The Evolutionary Algorithm Based on Pattern Mining for Large Sparse Multi-Objective Optimisation Problems." PatternIQ Mining.2024, (01)1, 12-22.

[3]. Richens, J. G., Lee, C. M., & Johri, S. (2020). Improving the accuracy of medical diagnosis with causal machine learning. Nature communications, 11(1), 3923.

[4]. Gong, Y. J., Zhang, J., Chung, H. S. H., Chen, W. N., Zhan, Z. H., Li, Y., & Shi, Y. H. (2012). An efficient resource allocation scheme using particle swarm optimisation. IEEE Transactions on Evolutionary Computation, 16(6), 801-816.

[5]. Castaneda, C., Nalley, K., Mannion, C., Bhattacharyya, P., Blake, P., Pecora, A., ... & Suh, K. S. (2015). Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine. Journal of Clinical Bioinformatics, 5, 1-16.

[6]. Uddin, M., Memon, M. S., Memon, I., Ali, I., Memon, J., Abdelhaq, M., & Alsaqour, R. (2021). Hyperledger fabric blockchain: Secure and efficient solution for electronic health records. Computers, Materials & Continua, 68(2), 2377-2397.

[7]. Bahad, P., & Saxena, P. (2020). Study of adaboost and gradient boosting algorithms for predictive analytics. In International Conference on Intelligent Computing and Smart Communication 2019: Proceedings of ICSC 2019 (pp. 235-244). Springer Singapore.

[8]. Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., & Rahman, M. H. (2021). Blockchain and artificial intelligence technology in e-Health. Environmental Science and Pollution Research, 28, 52810-52831.

[9]. Kumar, R., Arjunaditya, Singh, D., Srinivasan, K., & Hu, Y. C. (2022, December). AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions. In Healthcare (Vol. 11, No. 1, p. 81). MDPI.

[10]. Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2024). Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. Transactions on Emerging Telecommunications Technologies, 35(1), e4884.

[11]. Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of blockchain and AI-empowered smart healthcare: application-based analysis. Applied Sciences, 12(21), 11039.

[12]. Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Hyperledger fabric blockchain for securing the edge internet of things. Sensors, 21(2), 359.

[13]. Sammeta, N., & Parthiban, L. (2022). Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. Complex & Intelligent Systems, 8(1), 625-640.