A Novel Secure and Decentralized Model for Authentication and Data Integrity in IoT-Based Cyber-Physical Healthcare System

Hijriani Hijriani[1], Muhamad Yusuf[1], Reem Abduljaleel Khaleel[2] and Banan Yousif Ahmed[3]
[1]*Department of Laws, Universitas Sulawesi Tenggara, 93121 Kendari, Indonesia*
[2]*Department of Radiology Technologies, Dijlah University College, 10021 Baghdad, Iraq*
[3]*Al-Iraqia University, Scientific Affairs Department, 10001 Baghdad, Iraq*
hijriani@un-sultra.ac.id, myusuf@un-sultra.ac.id, reem.abduljaleel@duc.edu.iq, bnan.y.ahmed@aliraqia.edu.iq

Keywords: Internet of Things (IoT), Cyber-Physical Healthcare Systems (CPHS), Authentication and Data Integrity, Blockchain Technology, Security and Privacy.

Abstract: The integration of Internet of Things (IoT) technologies in healthcare has revolutionized patient monitoring and clinical decision-making through real-time data acquisition. However, the proliferation of connected medical devices introduces significant vulnerabilities regarding the security and integrity of sensitive health information. This paper presents a novel hybrid framework for Cyber-Physical Healthcare Systems (CPHS) that addresses these critical challenges through an innovative combination of IoT and blockchain technologies. Our solution implements advanced cryptographic protocols to establish robust data authentication mechanisms while preserving patient privacy. The proposed decentralized architecture fundamentally transforms healthcare data management by eliminating single points of failure inherent in traditional centralized systems. Key advantages include enhanced system resilience, complete transaction transparency, and immutable record-keeping that prevents data tampering. Comprehensive simulation results demonstrate the framework's effectiveness in protecting sensitive patient information while simultaneously improving operational efficiency in IoT-enabled healthcare environments. The research contributes both theoretically and practically by providing a secure, scalable solution that maintains data integrity without compromising system performance - a crucial advancement for modern digital healthcare infrastructure.

1 INTRODUCTION

Health systems have been transformed by integrating IoT (Internet of Things) into patient monitoring, diagnostics, and overall care delivery systems. Patients' health can be monitored in real-time, their outcomes can be improved, and healthcare management can be improved through Cyber-Physical Healthcare Systems (CPHS) connected to the Internet of Things, featuring Internet of Things-enabled sensors and devices [1]. These systems are becoming increasingly interconnected and exchanging data, introducing significant security and integrity challenges. Patients and healthcare providers must ensure sensitive medical information is protected and the system's operations are trustworthy. The vulnerability of IoT-based CPHS to cyberattacks, data tampering, and unauthorized access is a key concern since traditional centralized models often experience single points of failure, scalability issues, and potential breaches. It is, therefore, crucial that the data exchanged within the system is authenticated using robust mechanisms [2].

As wearables and gadgets become more embedded in open environments with radio communication infrastructure, new security threats arise. During communication, patient wearable devices are at risk of security risks as well as the collected and transmitted data. Therefore, the entire ecosystem must be protected from internal and external threats. [3]. As edge devices and gateways, these networks use patient wearable devices to collect and transmit data. The threat of a network adversary, capturing or injecting malicious data into these devices, is therefore readily available [4].

A decentralized authentication and data integrity model that uses blockchains and advanced cryptography to enhance resilience, transparency, and tamper resistance. By eliminating centralized control, decentralized health systems can transmit and authenticate sensitive health information securely without relying on a single authority. The proposed

model further enhances IoT-based healthcare systems in terms of scalability, efficiency, and trustworthiness. It enables greater confidence in IoT-enabled healthcare solutions by protecting patient privacy, securing medical data, and fostering a safe and effective use of cyber-physical systems in medicine through this innovative approach. Tractia, an intelligent organization, predicts by 2025 that the blockchain technology sector will generate 19.9 billion in annual earnings [3]. Healthcare is increasingly using IoTs to provide patients and physicians with real-time services [5]. In order to achieve this, medical institutions and businesses should incorporate IoMT medical devices. In addition, there will be an increasing volume of inconsistent data as more Internet-connected medical devices (IoMT) are connected to the Internet [6]. CCS, which encapsulates all centre activities, currently faces significant challenges due to high latency (HL), network dependencies, and individual failure points.

A difficult aspect of instantaneous transactions is adjusting to them [7]. The concept of fog computing (EC) is based on the assumption that network edge services should be efficient in terms of time and resources. The Fog Layer (FL) manages edge-to-cloud operations. Figure 1 illustrates how fog IoMT works [8], [9]. In Figure 1, IOT is illustrated in a variety of contexts. In addition to transportation, industry, homes, healthcare, and education, there are many other domains where technology is used. As a result, the planner is able to establish and deliver a service more efficiently, thus reducing resource consumption and latency. With the help of the 5G network, mobile networks can connect to machines and operate [10].

Figure 1: The industrial IoT and its real-world applications.

2 LITERATURE REVIEW

The security and protection of healthcare data remain challenging despite advancements in emerging technologies such as the Internet of Things (IoT), Edge Computing, Artificial Intelligence, and Machine Learning [11], [12]. Modern attacks may pose a serious threat to the lives of patients whose sensitive and confidential information has been compromised or leaked.

The authors provide an analysis of EHR analytics using deep learning-based approaches [8]. The authors have discussed the limitations of existing frameworks, as well as models that are applied to heterogeneous data sets, patient records, and certificates. In basic image processing research, images are represented in more complicated, hierarchical ways and creatively processed using greater, more sophisticated structures [13]. Earlier this year, the author of an article [9] argued that Blockchain technologies are capable of facilitating cloud-based electronic health record sharing. Through blockchain technology, it is possible to share electronic health records (EHR) in the cloud. Blockchain and ABSC have been used to secure the sharing of EHRs [14]. The proposed model ensures the accuracy, security, and enforceability of EHRs. In addition to protecting users' privacy, cloud-based EHRs are also secured, enabling them to identify themselves. Authorized users can upload cloud-based EHRs, and signer identities remain anonymous, but they are not suitable for severe patients due to the high latency.

As outlined by the Author [15], a blockchain-enabled cloud computing approach can be used to exchange medical records. In addition to enhancing security and privacy, blockchain facilitates authorization and other functions. Consortium blockchains contain three key components: a network model, a mechanism for generating data, and a consensus mechanism. Currently, this solution has only been tested on Ethereum, so its efficiency cannot be guaranteed on other platforms due to the requirement of high bandwidth for data retrieval and storage.

These limitations can be overcome while securely exchanging information using blockchain technology [16]. The authors present modules for requesting and linking. The developed model enables patients to keep full control of their health data and ensure their privacy at all times. The current healthcare system could be made more secure, stable, and robust using blockchain technology. As a result, the developed strategy has the main weakness of

relying on the properties of a blockchain node to perform. A major disadvantage of developed strategies is that their performance is dependent on the properties of the blockchain nodes. Using MedShare, the Author [17] proposes an interoperability-focused cloud-based system for patient data exchange that can overcome existing barriers. Mediation is when independent healthcare providers do not want to share patient data with their consumers or with their competitors. Due to its reliability requirement, the proposed scheme relies on the public cloud, and the data transformer required to implement it is costly.

Attribute-based sign encryption is used in the Personal Health Record Exchange described by the author [18]. In CP-OABSC, server-aided signature verification is used in conjunction with ABE schemes and verified outsourced decryption. This paper uses attribute-based encryption techniques to demonstrate the robustness, reliability, and security of a hybrid encryption method.

3 METHODOLOGY

An edge-deployed hybrid deep-learning model will be developed using this research methodology by training it distributed. Using their local data, edge and fog devices update their pre-trained models and evaluate their models. As a consequence of the incorporation of blockchain technology, all users are considered trusted users [19] - [21]. When communicating data over the Internet of Things network, maintaining data integrity can be challenging due to the security and flexibility of the access control scheme. IoT security mechanisms also face the challenge of distinguishing between normal and attack scenarios. A medical sensor, actuator, and machine network interconnects several fog nodes [22] - [24]. For blockchain technology to be integrated into cloud-based industrial systems, a new framework for deep learning and blockchain deployment is needed. A blockchain stores and hashes meta-data, while a cloud stores backups. Due to differences in computing power across edge nodes, such frameworks are often unable to store the complete block due to their scalability issues [22], [25]. Based on our framework, the following scenarios are presented. Our aim in this chapter is to discuss how blockchain can be integrated with hybrid IOT and how it can be used in fog computing [26]. Based on our framework, the following scenarios may be considered.

Using the previous chain's hash function, a blockchain can be maintained. As a result, the system has become more verifiable. In addition, the blockchain utilizes consensus to verify the integrity of the hash chain when generating new blocks [27]. A smart healthcare application is an essential part of 5G networks. Communication through 5G networks requires smart antennas, and they are shown as essential elements of the overall 5G intelligent health network architecture. As a result of recent advancements, smart antennas are becoming more attractive for deployment in 5G [22]. Well-coordinated RF beams enable perfect transmission of signals. As attenuation increases, the location becomes less important, as the focus of interest diminishes. 5G networks (IoMT) are predicted to support intelligent healthcare through machine-to-machine (M2M) and internet-of-things (IoT) connections [28]. The strategies given have two fundamental shortcomings. First, many terminals cause dense networks. A high degree of density and scalability is needed for M2M and IoMT applications. As an additional anxiety, low-based [29] applications that use wireless sensors pose a security risk because they do not provide secure consumption methods. An overview of the proposed model's timeline and its functions is presented in the diagram. Figure 1 presents a timeline for the proposed model and its functions.

A solid approach has been developed to reduce the threat posed by attackers, addressing some of the concerns expressed about security in wireless sensors. By developing an adversarial threat model, we will be able to identify vulnerabilities that unauthorized users can exploit to gain access to authorized sessions. Our goal here is to examine three distinct protocols that employ salted hashes but have their unique architectures, methodologies, and explanatory texts. The development of a blockchain-based healthcare system capable of communicating with a cyber-physical system must be methodical. An overview of how such a system might be created is provided:

- Problem identification. To develop a cyber-physical system, one must first identify the problems that need to be addressed. It's our objective here to make healthcare data more secure, private, and interoperable.
- Requirement definition. A cyber-physical system begins with identifying the problem, followed by defining the exact requirements. System specifications include functional and performance requirements, security concerns, and scalability concerns.

- Stakeholder identification. Assign stakeholders to the system based on their use and interaction with it. The list includes healthcare providers, patients, insurers, regulators, and others who are involved in the healthcare industry.
- Use case meaning. List the specific use cases associated with the cyber-physical system according to the identified requirements and stakeholders. A stakeholder's specific actions must be identified.
- Blockchain platform selection. System requirements should be met by the blockchain platform. In addition to Ethereum and HyperLedger, there are other blockchain-based platforms [30], [31].
- Smart contract description. Defining the smart contracts for the use cases will allow for the actions to be executed. The terms of an SC are incorporated directly into the agreement, so it is self-executed.
- Data structure description. The storage of healthcare data should be based on blockchain technology. Besides defining the field and type of data to be used, we must also determine the encryption mechanism.
- Consensus mechanism description. Decide how blockchain transactions will be validated by consensus. If a proof of stake (PoS) consensus mechanism is more appropriate than a proof of work (PoW), which is computationally expensive, then a proof of stake might be more appropriate.
- System testing and deployment. A controlled environment should be used for testing and deploying the system after the design phase is complete. In addition to evaluating the scalability and security of the system, it should be tested for functionality.
- System monitoring and maintenance. Monitoring and maintaining the system is essential after deployment. Security assessments are carried out regularly, potential breaches are dealt with, and potential breaches are dealt with in order to ensure the system consistently meets stakeholder requirements.

The blockchain-based cyber-physical healthcare system we designed and deployed is secure, scalable, and interoperable.

3.1 Cyber-Physical Systems (CPSs)

Interoperability in healthcare can be enabled by combining blockchains and CPSs. A three-protocol analysis of blockchain integration with healthcare CPSs is presented in this review. This merger has both advantages and disadvantages. The healthcare industry generates a great deal of personal information, which must be preserved, transported, and updated constantly. Blockchain technology enhances data privacy as well as making it transparent, immutable, and distributed. Healthcare CPSs can maintain secure communications and control data transfers with blockchains by using the basic protocol, session protocol, and cookie protocol. CPSs use a request-response protocol model as a standard method for transferring data between participating companies. The immutability and transparency of blockchain data make this architecture possible. Blockchains record transactions securely and immutably between users. Every data transfer is audited and verified as part of the built-in system. It will enable doctors and patients to interact confidentially and have access to better data [31].

CPS components communicate through channels established and maintained by the sessions protocol model. This method is significantly enhanced by incorporating blockchain technology. Blockchain technology allows individuals and organizations to communicate securely, ensuring the confidentiality of any data they exchange. Unlike centralized ledgers, blockchain does not require a central session manager, thus removing potential vulnerabilities. In online applications, cookie protocols are commonly used to manage sessions and customize user preferences. This system is more confidential and secure with the addition of blockchain. Using blockchain technology, cookies can be stored and verified decentralized. In addition to increasing users' trust in the system, this enhancement also prevents cookies from being tampered with. Patients can also select which third parties they wish to receive their cookie data from. Blockchain can have several advantages when integrated into healthcare CPSs' fundamentals, sessions, and cookie protocols. All communication channels should use encryption, and patients should be given control over their data for improved data security, interoperability, and privacy.

3.2 Proposed Protocol

A user-specified difficulty level is used to select a reliable miner who will mine the hash under the recommended protocol. The solution we offer incorporates a method for assessing the trust value of the checker and the author, unlike previous attempts. Miners are selected randomly for block generating and validating using a trusted procedure. The

proposed blockchain-based protocol for cyber-physical health care systems comprises the following core components:

- User registration. It is necessary to register patients and healthcare providers, providing personal information and authentication methods.
- Data collection. Healthcare data can be collected using a variety of devices, including medical equipment, electronic health records, and wearables.
- Data encryption. For healthcare data acquired on the blockchain to be securely stored, it is encrypted before it is stored.
- Data storage. Blockchains provide a secure, decentralized way to store encrypted healthcare information.
- Smart contract execution. Healthcare data is securely controlled by smart contracts executed on the blockchain and is accessible only to authorised users.
- Data access. Healthcare data is stored on the blockchain, which is accessible to patients and providers by verifying their identity.
- Data sharing. It is possible to share health data among authorized parties using blockchain technology securely and transparently.
- Consensus mechanism. Proof of Stake (PoS) is one of the consensus mechanisms used in blockchains for validating transactions and maintaining data integrity.
- Audit trail. Transactions and activities related to health are secured and transparently recorded on a blockchain.
- Compliance with regulations: In accordance with HIPAA and GDPR, blockchain-based healthcare systems secure and protect patient information.

Compared to current healthcare paradigms, blockchain-based systems are more efficient, effective, and secure and offer greater privacy, transparency, and accountability. For healthcare information to be confidential, additional processes or systems may be required based on stakeholders' needs and expectations.

3.3 Proposed Neural Network

Known for its capability to classify images, the convolutional neural network (CNN) is a deep learning knowledge-based neural network. An initial layer of linear convolutions (conv) and an additional layer of fully connected (FC) are included in the model. The nonlinear function is applied over the linear function in this model. As a result, this nonlinear function impacts all layers of the input and pooling layers and minimizes their size. In many parts of images, multiple perceptrons are used to separate pixel values using learned weights and bias values. A learnable weight and bias value is used to train perceptrons. CNNs have several advantages, including using a local spatial domain for the input images, sharing parameters, and using fewer weights. There are a number of advantages to this technique, including its lower computational complexity and smaller memory requirements. Figure 2 illustrates the CNN architecture:

- Convolutional layer. It essentially resizes the input image to 224 x 224, which is CNN's standard size. Resized images undergo multiple convolutional layers with different receptive fields. Feature data are extracted from the input matrix using a convolution layer. Then, these data are mapped to successive layers through a sequence of mathematical operations over a sliding kernel matrix. A feature matrix is generated by combining the results of element-wise matrix multiplication at each coordinate. In physics, image processing, and statistics, recurrent convolutions are used as elegant linear models. Several axes are used to estimate convolution. Convoluted images are calculated by multiplying input images by kernel filter coefficients and dividing by input images.

$$S(i,j) = \sum_{m} \sum_{n} I(-m,n)k(i-m,j-n). \quad (1)$$

- Pooling layer. Following the convolutional layer comes the pooling layer, which reduces the spatial domain representation, thereby reducing network computations. Typically, CNN uses a long and wide pooling kernel with a long and wide stride.
- Fully connected layer. As a result of convolution, CNN replicates this FC layer. There are normally two tensors in the tensor space, n1 and n2, where n1 is the input tensor size, and n2 is the output tensor size.
- Dropout. In deep learning, this layer is known as Drop. It is usually used to eliminate input overfits; the primary purpose is to improve conjecture and prediction. A weight is normally assigned to each node in a network.
- Softmax. Convolutional layers are followed by ReLU layers, which determine the nonlinearity of CNN and improve it accordingly.

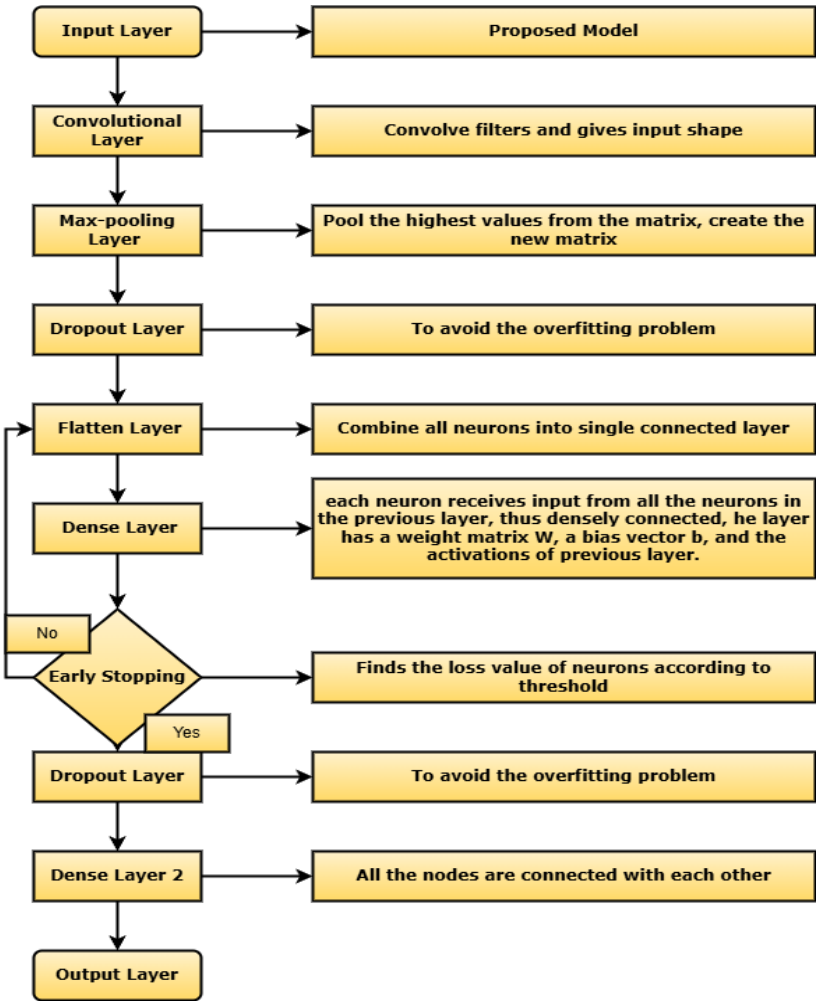

Figure 2: An overview of the convolutional neural network architecture.

4 RESULTS AND DISCUSSION

Models that are currently available were compared with the proposed framework. Compared to the benchmark models, the new framework performs better than the old framework (Fig. 3).

Using the benchmark model as a benchmark, the simulation included varying the percentage of malicious nodes to compare the proposed framework with its performance. A total of 150 malicious nodes were detected. When there are more than 50% of malicious nodes, accuracy declines significantly. In comparison with the other frameworks, the proposed one outperforms them due to its use of positive values to select honest miners. This performance advantage is further reflected in the cache efficiency, as shown in Figure 4, which illustrates the cache hit rate versus the number of blocks. Real blockchain scenarios typically do not have more than 50% malicious nodes. Therefore, the proposed framework would be more reliable.

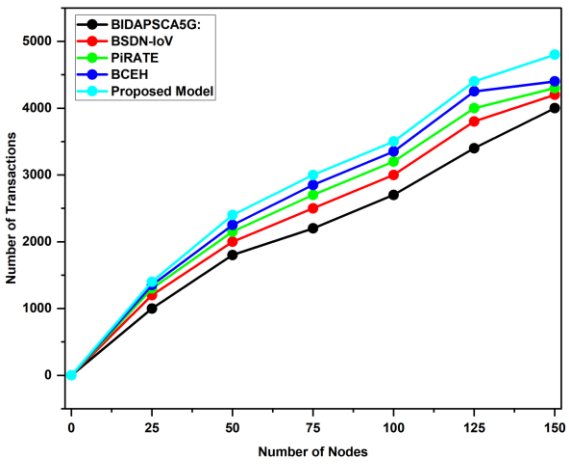

Figure 3: The number of transactions based on node count.

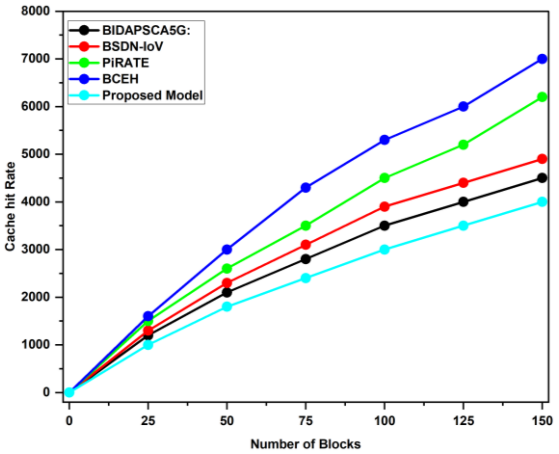

Figure 4: Cache hit rate versus number of blocks.

Figure 5 illustrates how the proposed framework enhanced security while reducing risks significantly. To assess how efficient single block creation can be, a second simulation was conducted using different numbers of nodes. A simulation based on the average time it takes to generate 80 (or 50) rounds of blocks was used to make sure the results were generalizable. A high level of safety and security can be maintained with less computational resources using this framework.

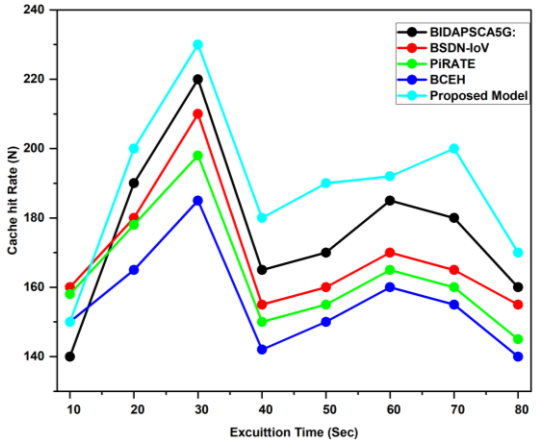

Figure 5: Cache hit rate versus execution time (sec).

Using Figure 6, we can see the time and number of records involved in the simulation. The number of records found ranged from 500 to 12,500. A comparison of the proposed framework with the benchmark model reveals that the proposed framework takes significantly less time to run for the same number of rounds as the benchmark model, as illustrated in Figure 6.

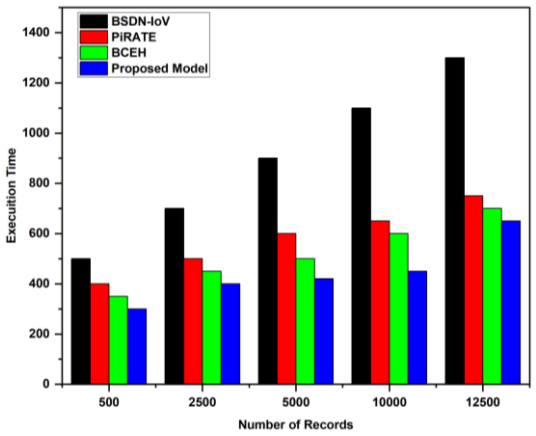

Figure 6: Execution time and record count simulation results.

Based on the simulation results, it is evident that the number of blocks and processing time are correlated significantly (Fig. 7). Our framework outperformed benchmark models based on a comparison we conducted with benchmark models.

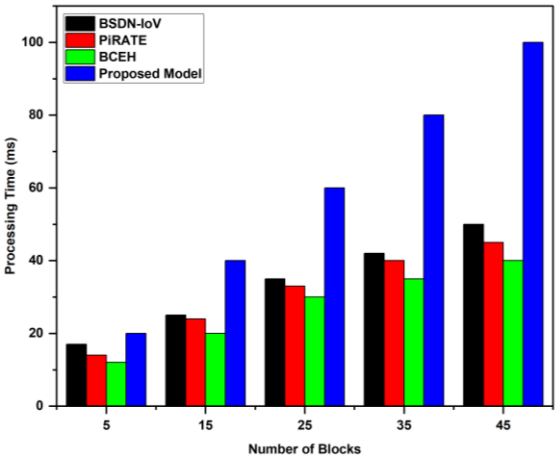

Figure 7: Process time and block count simulation results.

5 CONCLUSIONS

Cyber-Physical Healthcare Systems (CPHS) based on IoT are presented in this paper, leveraging blockchain technology and cryptography to ensure data integrity and security. In addition to effectively addressing critical security challenges, the proposed model offers robust protection for sensitive healthcare data against risks such as unauthorized access, data breaches, and information tampering. Simulation results demonstrate that the designed framework outperforms current methodologies by significantly

enhancing data management capabilities, system efficiency, and security safeguards, which collectively improve patient trust and operational reliability. Moving forward, researchers and practitioners should focus on expanding the framework's scalability, ensuring adaptability to diverse healthcare settings - including remote clinics and large hospitals - and thoroughly assessing practical deployment barriers. Further investigation is recommended into integrating emerging technologies, such as 5G connectivity, wearable healthcare devices, and intelligent analytics solutions, to optimize patient care delivery, enhance real-time monitoring capabilities, and maintain rigorous standards of patient privacy and data protection.

REFERENCES

[1] P. Rani and M. H. Falaah, "Real-Time Congestion Control and Load Optimization in Cloud-MANETs Using Predictive Algorithms," NJF Intell. Eng. J., vol. 1, no. 1, pp. 66–76, 2024.

[2] A. Singh et al., "Smart Traffic Monitoring Through Real-Time Moving Vehicle Detection Using Deep Learning via Aerial Images for Consumer Application," IEEE Trans. Consum. Electron., vol. 70, no. 4, pp. 7302–7309, Nov. 2024, doi: 10.1109/TCE.2024.3445728.

[3] A. Ali et al., "Performance analysis of AF, DF and DtF relaying techniques for enhanced cooperative communication," in Proc. 6th Int. Conf. Innovative Computing Technology (INTECH), Dublin, Ireland: IEEE, Aug. 2016, pp. 594–599, doi: 10.1109/INTECH.2016.7845056.

[4] P. Rani et al., "Federated Learning-Based Misbehavior Detection for the 5G-Enabled Internet of Vehicles," IEEE Trans. Consum. Electron., vol. 70, no. 2, pp. 4656–4664, May 2024, doi: 10.1109/TCE.2023.3328020.

[5] Z. Mushtaq et al., "Automatic Agricultural Land Irrigation System by Fuzzy Logic," in Proc. 3rd Int. Conf. Information Science and Control Engineering (ICISCE), Beijing, China: IEEE, Jul. 2016, pp. 871–875, doi: 10.1109/ICISCE.2016.190.

[6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in Proc. 2nd Int. Conf. Open and Big Data (OBD), Vienna, Austria: IEEE, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[7] M. Hasnain, M. F. Pasha, I. Ghani, B. Mehboob, M. Imran, and A. Ali, "Benchmark Dataset Selection of Web Services Technologies: A Factor Analysis," IEEE Access, vol. 8, pp. 53649–53665, 2020, doi: 10.1109/ACCESS.2020.2979253.

[8] A. Ali et al., "Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain," Electronics, vol. 10, no. 16, p. 2034, Aug. 2021, doi: 10.3390/electronics10162034.

[9] P. Rani, P. N. Singh, S. Verma, N. Ali, P. K. Shukla, and M. Alhassan, "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment," Wirel. Commun. Mob. Comput., vol. 2022, pp. 1–14, 2022.

[10] A. Ali, M. Naveed, M. Mehboob, H. Irshad, and P. Anwar, "An interference aware multi-channel MAC protocol for WASN," in Proc. Int. Conf. Innovations in Electrical Engineering and Computational Technologies (ICIEECT), Karachi, Pakistan: IEEE, Apr. 2017, pp. 1–9, doi: 10.1109/ICIEECT.2017.7916523.

[11] S. S. Gill et al., "Transformative effects of ChatGPT on modern education: Emerging Era of AI Chatbots," Internet Things Cyber-Phys. Syst., vol. 4, pp. 19–23, 2024, doi: 10.1016/j.iotcps.2023.06.002.

[12] P. Rani and R. Sharma, "Intelligent transportation system for internet of vehicles based vehicular networks for smart cities," Comput. Electr. Eng., vol. 105, p. 108543, 2023.

[13] N. Kumar, P. Rani, V. Kumar, S. V. Athawale, and D. Koundal, "THWSN: Enhanced energy-efficient clustering approach for three-tier heterogeneous wireless sensor networks," IEEE Sens. J., vol. 22, no. 20, pp. 20053–20062, 2022.

[14] A. Singh et al., "Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication," IEEE Trans. Consum. Electron., vol. 70, no. 2, pp. 4898–4907, May 2024, doi: 10.1109/TCE.2024.3351221.

[15] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain," IEEE Access, vol. 7, pp. 136704–136719, 2019, doi: 10.1109/ACCESS.2019.2943153.

[16] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," IEEE J. Biomed. Health Inform., vol. 24, no. 8, pp. 2169–2176, Aug. 2020, doi: 10.1109/JBHI.2020.2993072.

[17] Y. Yang et al., "Medshare: A Novel Hybrid Cloud for Medical Resource Sharing Among Autonomous Healthcare Providers," IEEE Access, vol. 6, pp. 46949–46961, 2018, doi: 10.1109/ACCESS.2018.2865535.

[18] F. Deng, Y. Wang, L. Peng, H. Xiong, J. Geng, and Z. Qin, "Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records," IEEE Access, vol. 6, pp. 39473–39486, 2018, doi: 10.1109/ACCESS.2018.2843778.

[19] A. A. Shah, G. Piro, L. A. Grieco, and G. Boggia, "A qualitative cross-comparison of emerging technologies for software-defined systems," in Proc. 6th Int. Conf. Software Defined Systems (SDS), IEEE, 2019, pp. 138–145. Accessed: Apr. 03, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8768566/.

[20] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A Blockchain-Based Location Privacy Protection Incentive Mechanism in Crowd Sensing Networks," Sensors, vol. 18, no. 11, p. 3894, Nov. 2018, doi: 10.3390/s18113894.

[21] A. Shah, G. Piro, L. Grieco, and G. Boggia, "A review of forwarding strategies in transport software-defined networks," in Proc. 22nd Int. Conf. Transparent Optical Networks (ICTON), 2020, pp. 1–4, doi: 10.1109/ICTON51198.2020.9203103.

[22] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, "Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring System for Diabetes Mellitus Research and Care," Sensors, vol. 19, no. 15, p. 3319, Jul. 2019, doi: 10.3390/s19153319.

[23] A. Beebeejaun, "VAT on foreign digital services in Mauritius; a comparative study with South Africa," Int. J. Law Manag., vol. 63, no. 2, pp. 239–250, Feb. 2021, doi: 10.1108/IJLMA-09-2020-0244.

[24] A. Cirstea, F. M. Enescu, N. Bizon, C. Stirbu, and V. M. Ionescu, "Blockchain Technology Applied in Health: The Study of Blockchain Application in the Health System (II)," in Proc. 10th Int. Conf. Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania: IEEE, Jun. 2018, pp. 1–4, doi: 10.1109/ECAI.2018.8679029.

[25] R. R. Bruce, J. P. Cunard, and M. D. Director, From Telecommunications to Electronic Services: A Global Spectrum of Definitions, Boundary Lines, and Structures. Oxford, UK: Butterworth-Heinemann, 2014. Accessed: Apr. 03, 2025. [Online]. Available: https://books.google.com/books?id=AEeeBQAAQBAJ.

[26] P. Rani, U. C. Garjola, and H. Abbas, "A Predictive IoT and Cloud Framework for Smart Healthcare Monitoring Using Integrated Deep Learning Model," NJF Intell. Eng. J., vol. 1, no. 1, pp. 53–65, 2024.

[27] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain," IEEE J. Biomed. Health Inform., vol. 24, no. 8, pp. 2146–2156, Aug. 2020, doi: 10.1109/JBHI.2020.2969648.

[28] A. Singh et al., "Resilient wireless sensor networks in industrial contexts via energy-efficient optimization and trust-based secure routing," Peer–Peer Netw. Appl., vol. 18, no. 3, p. 132, Jun. 2025, doi: 10.1007/s12083-025-01946-5.

[29] A. Ali, M. Naveed, M. Mehboob, H. Irshad, and P. Anwar, "An interference aware multi-channel MAC protocol for WASN," in Proc. Int. Conf. Innovations in Electrical Engineering and Computational Technologies (ICIEECT), IEEE, 2017, pp. 1–9. Accessed: Apr. 03, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7916523/.

[30] M. M. Nair, A. K. Tyagi, and R. Goyal, "Medical Cyber Physical Systems and Its Issues," Procedia Comput. Sci., vol. 165, pp. 647–655, 2019, doi: 10.1016/j.procs.2020.01.059.

[31] X. Liu, B. Xu, X. Wang, K. Zheng, K. Chi, and X. Tian, "Impacts of Sensing Energy and Data Availability on Throughput of Energy Harvesting Cognitive Radio Networks," IEEE Trans. Veh. Technol., vol. 72, no. 1, pp. 747–759, Jan. 2023, doi: 10.1109/TVT.2022.3204310.