Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.035066
Article

Tech Science Press

An Immutable Framework for Smart Healthcare Using Blockchain Technology

Faneela[1], Muazzam A. Khan[1], Suliman A. Alsuhibany[2,*], Walid El-Shafai[3,4], Mujeeb Ur Rehman[5] and Jawad Ahmad[6]

[1]Department of Computer Science, Quaid-i-Azam University, Islamabad, 45320, Pakistan
[2]Department of Computer Science, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia
[3]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[4]Department of Computer Science, Security Engineering Laboratory, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[5]James Watt School of Engineering, University of Glasgow, G12 8QQ, UK
[6]School of Computing, Edinburgh Napier University, Edinburgh, EH10 5DT, UK
*Corresponding Author: Suliman A. Alsuhibany. Email: salsuhibany@qu.edu.sa
Received: 06 August 2022; Accepted: 30 September 2022

Abstract: The advancements in sensing technologies, information processing, and communication schemes have revolutionized the healthcare sector. Electronic Healthcare Records (EHR) facilitate the patients, doctors, hospitals, and other stakeholders to maintain valuable data and medical records. The traditional EHRs are based on cloud-based architectures and are susceptible to multiple cyberattacks. A single attempt of a successful Denial of Service (DoS) attack can compromise the complete healthcare system. This article introduces a secure and immutable blockchain-based framework for the Internet of Medical Things (IoMT) to address the stated challenges. The proposed architecture is on the idea of a lightweight private blockchain-based network that facilitates the users and hospitals to perform multiple healthcare-related operations in a secure and trustworthy manner. The efficacy of the proposed framework is evaluated in the context of service execution time and throughput. The experimental outcomes indicate that the proposed design attained lower service execution time and higher throughput under different control parameters.

Keywords: Blockchain technology; healthcare applications; cybersecurity services; IoMT; DoS; EHR

1 Introduction

The Internet of Medical Things (IoMT) integrates the Internet of Things (IoT)-enabled smart sensors and devices that provide healthcare services. IoMT is a connected architecture of healthcare systems, including medical sensors, devices, software applications, and services. IoMT can remotely connect medical devices and healthcare professionals to provide quality medical services. IoMT has increased clinical workflow efficiency and made healthcare services more accessible. At the same time, the clinical workflow streamlines the processes performed in administrative and operational ways. The IoMT integrates the

digital and physical world to accelerate and enhance the accuracy of diagnosis of diseases and to update patient health status in real-time. The connection of medical devices will profoundly impact patients and clinicians [1]. Medical professionals employ devices in various settings, including paramedical staff, remote clinic medical staff, and healthcare professionals promoting, preventing, and screening modern medical facilities. Medical devices are essential for the diagnosis and effective treatment of the disease. Between 2020 and 2025, the IoMT market is anticipated to expand at a compound yearly growth rate of 23.4% [2]. The growing need for cost-effective pharmaceutical delivery and the increasing adoption of connected devices are two main reasons driving the IoMT market's rise. However, the IoMT market's growth is expected to be hampered by a lack of appropriate IoT technology capabilities inside healthcare systems [3].

Despite its numerous advantages, IoMT faces multiple security and privacy concerns due to its complexity and diversity, making it challenging to identify and defend against malicious attacks. Exploiting the risks of hijacking a device can lead to medical threats and loss of life. The IoMT devices are resource-constrained, which is one of the significant issues for deploying traditional and computationally expensive security algorithms. Furthermore, most IoMT systems are built with centralized approaches, making them susceptible to a single point of failure attack [4,5]. In this case, the complete healthcare system may be compromised, leading to unauthorized access to valuable healthcare records. Blockchain technology is a promising solution to address the abovementioned challenges that can add security and privacy to the existing IoMT systems.

A blockchain is viable for integrating existing Electronic Healthcare Systems (EHS) to increase access control, traceability, data unification, availability, and efficiency [6–8]. Blockchain is a decentralized database where members of the network verify their data. Blockchain is traditionally used to manage cryptographic transactional records but can also be applied to electronic medical records management. The basic working principle of blockchain is shown in Fig. 1. Blockchain verifies records using cryptographic evidence instead of trusted third-party signatories. This cryptographic authentication is done through a network of users called nodes. The cryptographic authentication adds integrity to the system by ensuring that only one 'correct' version of the events is retained in the database, which cannot be changed without the approval of the majority of nodes. These nodes are called "blocks," Each block is associated with a hash from the previous block so that when one block is changed, it replaces the hash of all subsequent blocks. Current healthcare management systems suffer from cyber-attacks as well as integrity issues. Suitable precautions must be made to secure patient data so that healthcare institutions are no longer a key target for hackers. Blockchain secures data through public-key cryptography, which generates a public key and private key for each user using a one-way encryption process called a hash. Both parties can use them for transactions: the sender signs and the recipients validate using their private key, while the public keys are used to deliver the transaction to the recipient. This enables recipients to verify the integrity of the medical blockchain. In addition, only participants can view the submitted information, eliminating tampering risk [9].

1.1 Motivations and Contributions

Numerous research projects have connected blockchain technology with electronic healthcare, and Section 2 discusses some of the most recent contributions to state-of-the-art methods. Integrating blockchain technology with IoMT is a challenging task for many reasons. First, IoT devices are networks resource-constrained. Therefore, deploying computationally extensive cryptographic algorithms and consensus mechanisms is not feasible. Because of the increasing number of medical devices and network participants, scalability has become a significant issue. This article introduces a lightweight, adaptable blockchain-based design for the IoMT to deal with these issues. The following bullets list the essential benefits of the suggested approach:

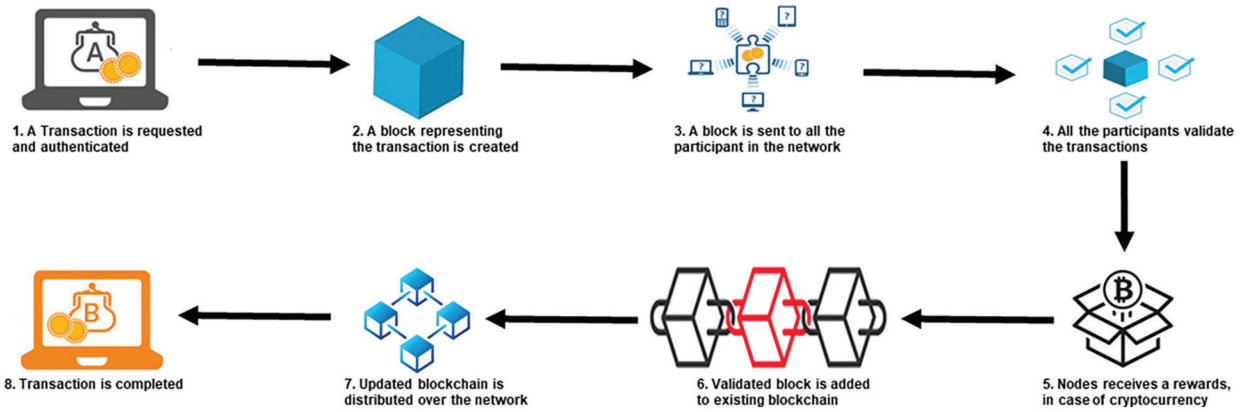

Figure 1: Working process of a blockchain

- This study realized the enormous potential of blockchain for smart healthcare applications. It introduces a fast, easily adaptable, lightweight, and private blockchain for the IoMT.
- The suggested method includes a lightweight Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure compatibility with resource-constrained IoT devices and the IoMT network. The proposed system uses the lightweight consensus technique Proof of Authentication (PoAh) to increase throughput while reducing computational complexity. The suggested framework can provide multiple healthcare-related services, including user registration, patient appointment, laboratory appointment, and patient medical history tracking.
- The efficacy of the suggested architecture is analyzed through service execution time and system throughput.

The remainder of this article is structured as follows. Section 2 summarized some latest research contributions related to blockchain implementations for IoMT applications. Section 3 discusses the proposed design's central architecture and its key components. Section 4 comprises experiments and a discussion of the results. Finally, Section 5 presents a concise conclusion and a few possible future study areas.

2 Related Work

The technological increase of IoMT-based smart healthcare systems involves authenticity, privacy, security, and high availability of health data. This section discusses several works relating to smart healthcare systems and developments in patients' EHRs. Li et al. [10] and Chen et al. [11] proposed a new method for a secure patient record exchange system based on blockchains and encryption algorithms. The architecture emphasized efficient storage and minimized the risk of irreversible data alteration. This was accomplished by sharing medical data over numerous communications channels while maintaining user privacy. Sharif et al. [12] suggested a method for managing the interoperability and synchronization of a decentralized e-Health system. This solution allows trade-offs with less calculated time as well as block verification. Pradhan et al. [13] suggested a blockchain-based Healthcare Cyber-Physical Systems (H-CPS) architecture that tracks stress monitoring in sleep patterns. Stress was forecasted for the following day based on these changes made while sleeping. Processed stress data and average physical changes were designed to transfer to the IoT Cloud for storage. Donoghue et al. [9] presented a blockchain-based infrastructure for managing electronic medical records that is both efficient and interoperable. The suggested method preserves patients' ownership while maintaining the security and privacy of valuable healthcare data. Parekh et al. [14] described a blockchain-based access control

and privacy method for enhancing data availability among healthcare professionals. The authors also used the concept of a blockchain to implement a Hyperledger-based health care record sharing system.

Pradhan et al. [4] developed a hybrid computing framework for the IoMT that incorporates a blockchain-based decentralized data storage system. The authors discussed the several challenges associated with cloud-based IoMT healthcare systems, including increased storage costs, network latency, and central point failure [15]. Presented a blockchain-based solution for IoMT that is interconnected across clusters. The authors conducted extensive experiments to determine the suggested scheme's viability and efficiency. The proposed approach effectively handles the issue of IoMT network latency. In another recent study, Raifa [16] built a scalable authentication system for IoMT devices based on smart contracts. By employing blockchain technology, the suggested scheme overcomes the drawbacks of traditional healthcare systems that are susceptible to various cyberattacks. Pratap et al. [17] demonstrated a patient-centric blockchain-enabled procedure for medical record management. The authors discussed extensive benchmarking studies using the Hyperledger Caliper tool.

2.1 Limitations in Existing Research

Privacy and security are the primary concerns of IoMT-enabled smart healthcare systems. Blockchain technology has the potential to address a wide variety of security and privacy concerns in IoMT. Numerous research initiatives have been undertaken concerning blockchain implementations in healthcare applications. However, the studies mentioned above have a few limitations. First, the scope of available research on healthcare organizations is limited. Most research focuses exclusively on the efficient capture of healthcare data, with little consideration given to the suitability of blockchain for many other critical medical processes. Second, the existing studies incorporate the computationally expensive cryptographic algorithms and consensus mechanisms that are challenges for the deployment in real-time IoMT systems. Third, a brief performance evaluation is missing for existing blockchain-based schemes for IoMT. This article suggests a private, adaptive, and lightweight blockchain-based framework for the IoMT to overcome the issues highlighted before.

3 The Proposed Architecture

Integrating blockchain with IoMT systems enhances overall system security and trustworthiness. The blockchain contains all the necessary characteristics for the protection and privacy of IoMT-driven smart healthcare. The block diagram of the proposed blockchain-based IoMT system is presented in Fig. 2. This architecture contains several modules and services, including private blockchain, patient appointments, medical history, diagnosis, and medical treatment. All of these healthcare services are interconnected. Architectural design is flexible, allowing healthcare professionals to tailor it to their needs. We assume that such a blockchain network will be maintained by health regulatory authorities and private healthcare providers, making it a private blockchain network.

All modules are designed to detect functionality in the proposed patient-centric blockchain-based healthcare framework. The patient registers for the appointment using the chain code through the client interface. The committed transaction (appointment) is distributed to all network users to prevent unauthorized access. The transaction is saved on a ledger with a timestamp and hash number, which makes it easy to verify the authenticity of the patient. This healthcare record is accessible to all authorized users, and they can make inquiries from other authorized users through the blockchain Communication Network. Patients can also book their appointments, medications, reports, medical diagnoses, and other matters with doctors.

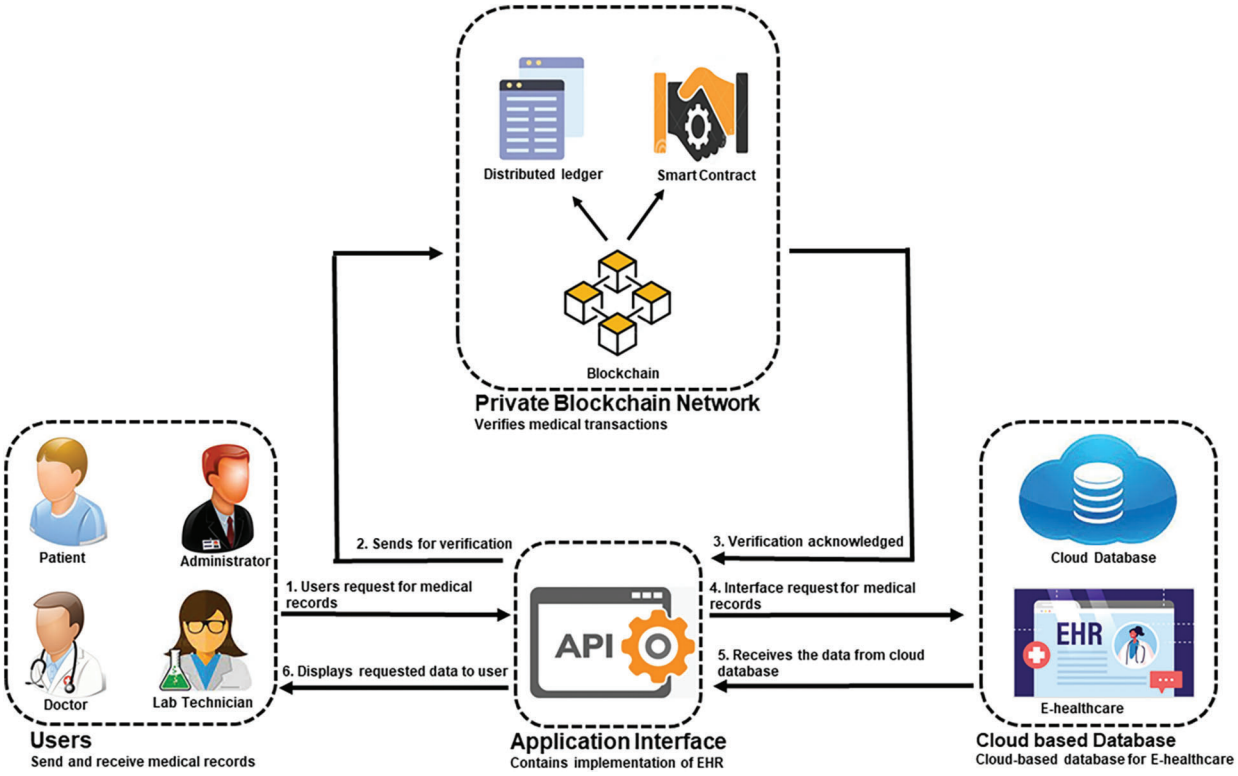

Figure 2: Block diagram of blockchain-based IoMT system

3.1 Modules and Participants

The proposed IoMT framework contains several modules and services, including data publishing, blockchain as middleware, and data seeking. The working principle of the proposed system is described through a layered architecture depicted in Fig. 3.

Following is a brief description of each module:

- **Data Publishing Module:** This module configures data publishers. For example, patients have multiple IoMT terminals, such as heartbeat, temperature, blood pressure monitoring sensors, etc., that produce large volume data sets.
- **Data Seeking Module:** This module consists of data seekers such as doctors, pharmacists, family members, and remote medical consultants. Data seekers communicate with data publishers through blockchain-based middleware.
- **Middleware Layer:** In this layer, blockchain connects data publishers with data seekers and ensures that patient data is safe and private. The proposed framework is based on a private network that restricts service access to only registered users. A chain of linked blocks makes up the distributed ledger. Each block has a timestamp, hash, hash of the previous block, and Merkel root. Authorized users can access and edit ledgers through smart contracts. These smart contracts consist of mathematical and logical functions that enable users to communicate without the involvement of any third party.

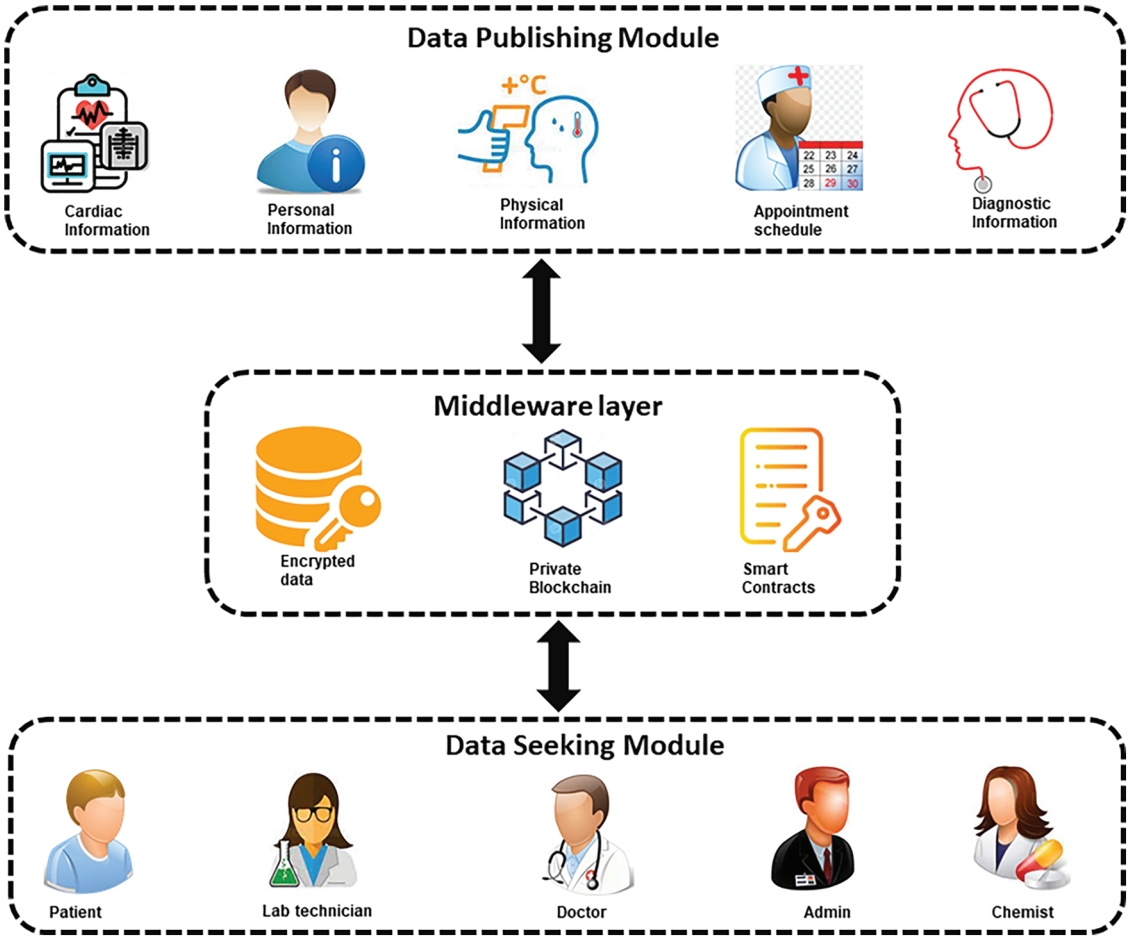

Figure 3: Layered architecture of blockchain-based IoMT system

3.2 Interaction Between Participants

All participants are integrated to create a whole healthcare network in the proposed framework.

1. **User Registration:** The user registration process within the blockchain-enabled healthcare system begins when the healthcare user wants to register for the first time. User registration involves three steps: submitting a transaction proposal, verifying the transaction, and updating the blockchain after successful verification. Fig. 4 outlines the workflow of the appointment process. The steps involved in user registration are summarized as follows:
   - Using the application interface, new healthcare user submits transactions to blockchain middleware.
   - The application interface uploads user data and transactions to blockchain middleware using smart contracts.
   - The consensus algorithm decodes transactions through blockchain middleware and extracts the user's public key and user ID.
   - Middleware calculates the hash value of a registered user and then publishes it on a private blockchain network for tracking purposes.

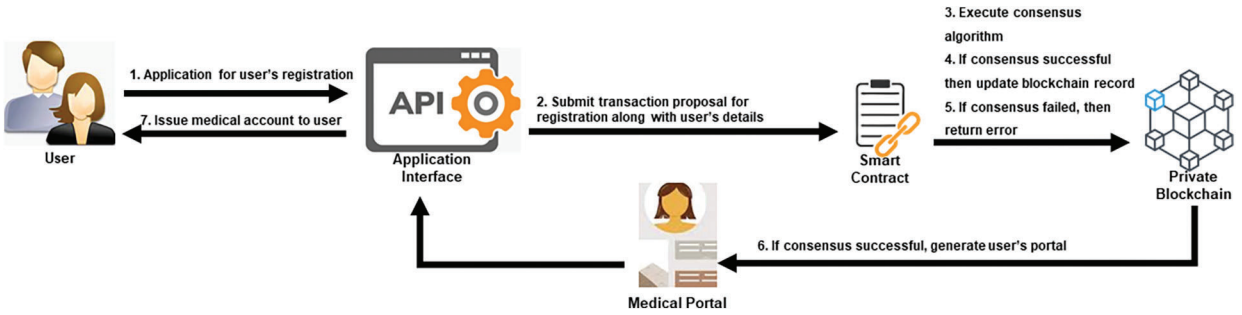

Figure 4: User registration process in the proposed system

2. **Access Control:** This process facilitates the users to access their medical records. **Access Control** is a three-step process that prompts transactions with user information, verifies users, and gives them access to medical records after completing the verification process. The flow of the access control process is presented in Fig. 5. The main steps of the access control process are highlighted as follows:
   - A healthcare user prepares an access control request involving a target user ID**.**
   - Using the application interface, each healthcare user submits transactions to blockchain middleware.
   - The application interface uploads user data and transactions to blockchain middleware using smart contracts.
   - The consensus algorithm decodes transactions through blockchain middleware and gets the user's public key and ID.
   - Middleware authenticates the private key of a registered user and then unlocks the user account on a private blockchain network.

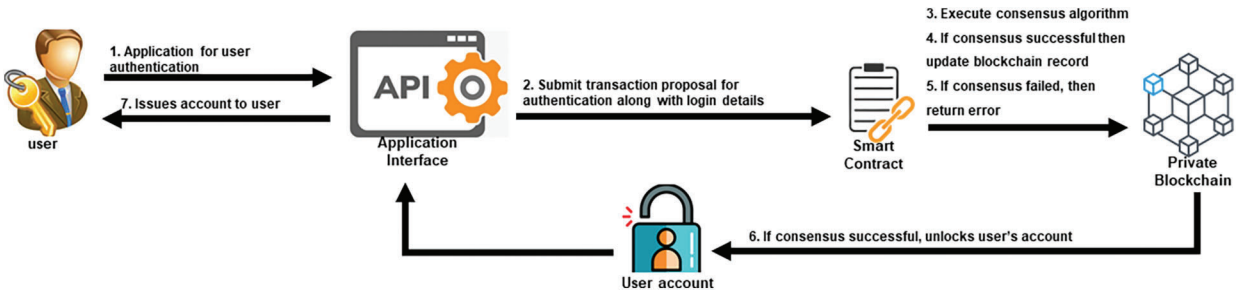

Figure 5: Access control process in the proposed system

3. **Patient Appointment Interaction:** If a patient needs to see a doctor, they will first suggest a transaction to provide their information (name, gender, identification number, age). The transaction is completed through blockchain middleware, which provides the user with a list of medical practitioners. The application is forwarded to the appropriate doctors through middleware. If the doctor confirms this, the middleware informs the patient about the available day and time. After a successful middleware operation, the blockchain prepares an appointment receipt and sends it to the patient. In addition, the receipt is encrypted, and the patient can decrypt it using their key. The appointment process is depicted in Fig. 6.

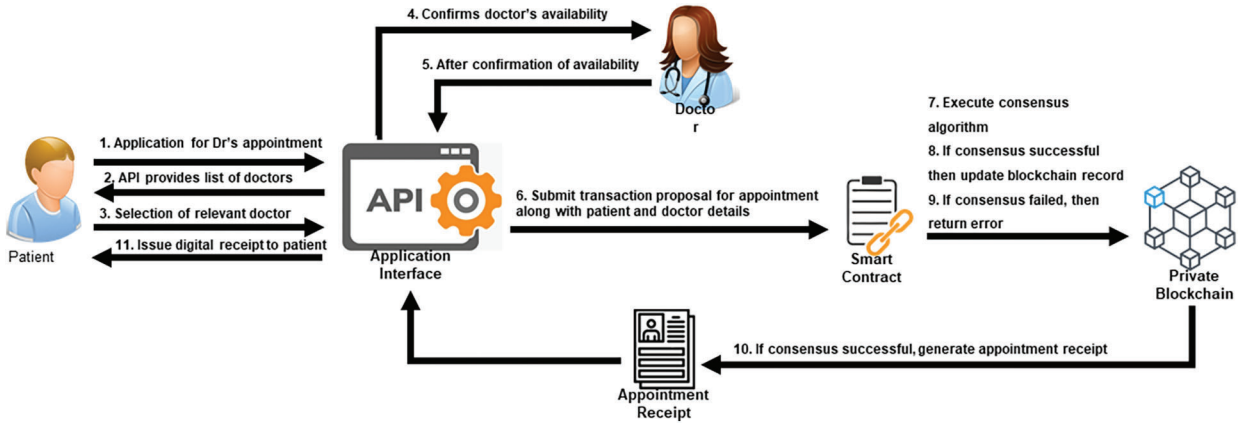

Figure 6: Patient appointment procedure in the proposed system

4. **Patient Check-up Interaction:** The patient must visit the hospital on a specific date and time in this module. First, a receptionist verifies the appointment details from blockchain middleware. After that, he/she will also confirm the payment details of the patient from his bank account or insurance balance. Once everything is approved, the middleware will update the database, and the patient will move towards a medical specialist to perform the necessary check-up. The doctor can also acquire the patient's cardiac history from blockchain middleware. Based on the check-up, the doctor can prescribe medicine or suggest some laboratory tests for further diagnosis. Once a check-up is completed, the doctor will update the record by submitting a transaction proposal to middleware. After that, the blockchain updates the history and issues an acknowledgment receipt that can only be accessed by the doctor, patient, or other authorized authorities. The flow of the cardiac check-up process is presented in Fig. 7.

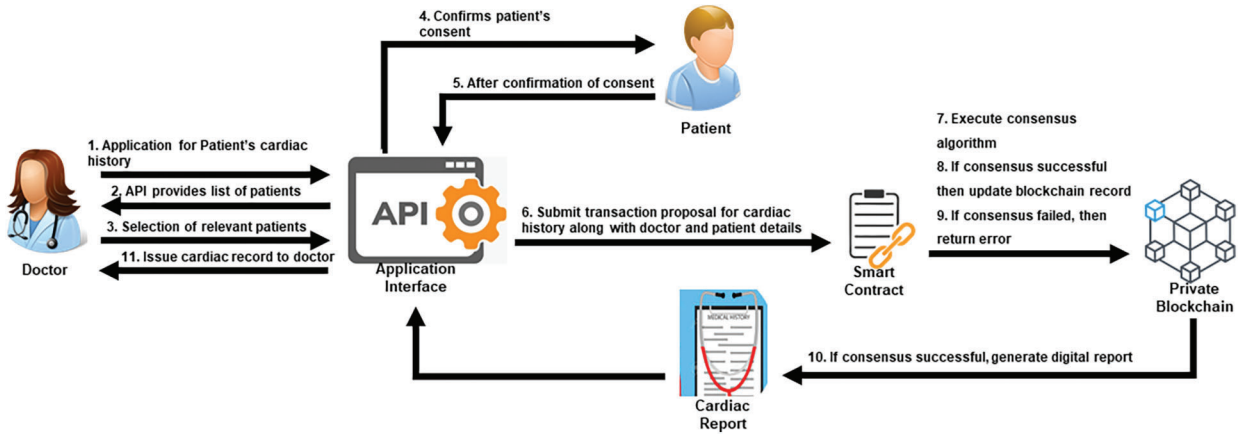

Figure 7: Patients' cardiac history access process in the proposed system

5. **Patient-Lab Interaction:** If the doctor prescribes laboratory tests such as complete blood tests, urine tests, CT scans, X-rays, etc., then the patient has to go to the diagnostic center. Using blockchain-based middleware, the diagnostic center uses patient identification to obtain details of laboratory tests. After that, payment details for the proposed tests will be confirmed. After payment is approved, the patient is taken to the laboratory. The lab staff will obtain the samples needed for testing. The patient lab interaction process is presented in Fig. 8.

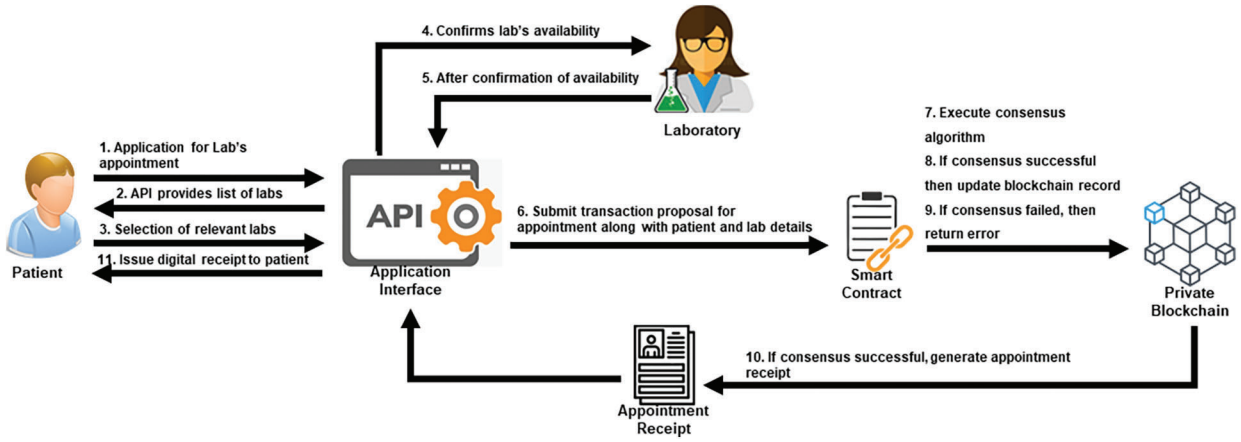

Figure 8: Patient-lab interaction process in the proposed system

4 Experiments and Performance Evaluation

This section describes the experimentation methodology and a detailed discussion of the results. All experiments are performed using an HP Elite book computer with an Intel® CoreTM i5-6300U CPU, 4 GB RAM, and Windows 10 Pro operating systems. The proposed blockchain framework is built through multiple programming languages Python, JavaScript, and HTML. The efficiency of the proposed architecture is analyzed in terms of service execution time and throughput.

4.1 Service Execution Time

The total amount of time is required to process and verify all transactions through the blockchain framework. Execution time is calculated based on the number of transactions, and the experiments and execution time evaluation are described in the following.

In the first phase of experiments, we analyze the service execution time for user registration operation through the proposed framework. Users are categorized into four groups of transactions such as 100, 200, 500, and 1000. The user registration process contains three primary operations: submission of a proposal, confirmation of the transaction, and update of blockchain after successful consensus. A comparative analysis of service execution time with varying transactions is shown in Fig. 9. For the first group, the minimum and maximum service execution times are recorded as 144.5 and 199.7 s, respectively. The average execution time is 155.6 s for the smallest group of transactions, and the average time for the biggest group of transactions was recorded as 191.2 s.

In the second phase of experiments, we analyze the service execution time for user access control operation through the proposed framework. This is also a three-step process that involves submission of a proposal with user information, user verification, and providing them access to medical records after successful authentication. Again, the size of transaction groups is maintained. The experimental outcomes of the user access control operation are presented in Fig. 10. According to the results, the maximum execution time is observed between 40.32 to 65.1 s. The average execution time varies between 32.035 and 47.52 s for the most influential and most minor groups.

In the third phase of experiments, we analyze the service execution time for lab appointment operation through the proposed framework. This process contains four stages: proposal submission, selection of the desired laboratory after successful verification, and updating the blockchain record after confirmation of the lab appointment. Again, the size of transaction groups is maintained. The experimental outcomes of

the lab appointment process are presented in Fig. 11. Results indicate that the average service execution time varies between 32.98 to 37.65 s for the biggest and smallest groups, respectively.

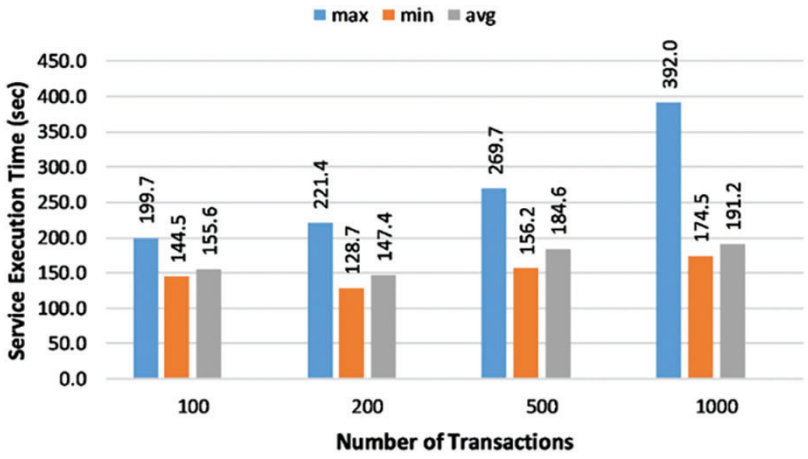

Figure 9: Service execution time for user's registration process

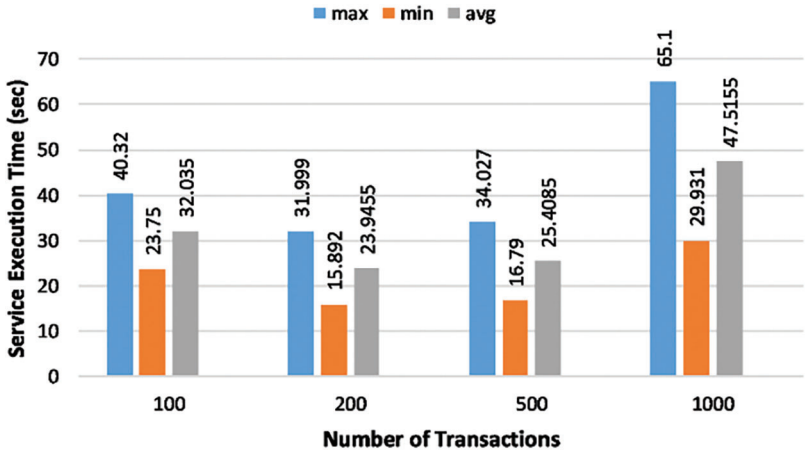

Figure 10: Service execution time for an access control process

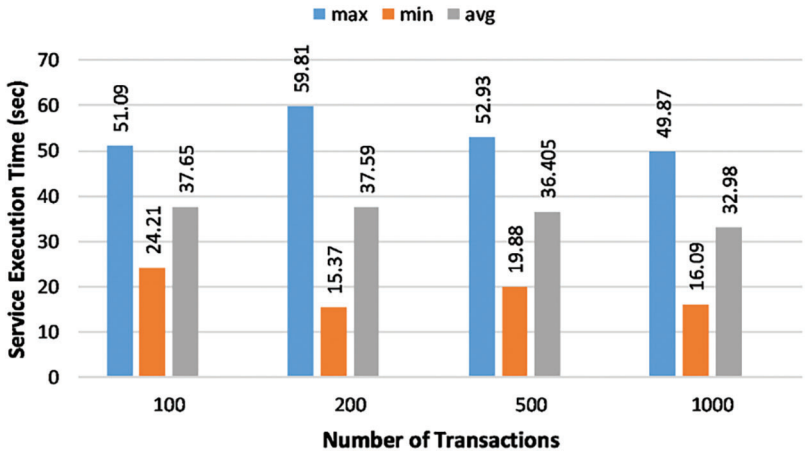

Figure 11: Service execution time for the lab appointment process

In the fourth phase of experiments, we analyze the service execution time for patient-doctor interaction through the proposed framework. Patient-doctor interaction also a four-stage process that includes proposal submission, selecting the relevant doctor after successful verification, and updating the blockchain record upon confirmation of the doctor appointment. Again, the size of transaction groups is maintained. The experimental outcomes of the patient-doctor interaction are presented in Fig. 12. Results indicate that the average service execution time varies between 29.19 to 34.96 s for the most prominent and most minor groups, respectively.

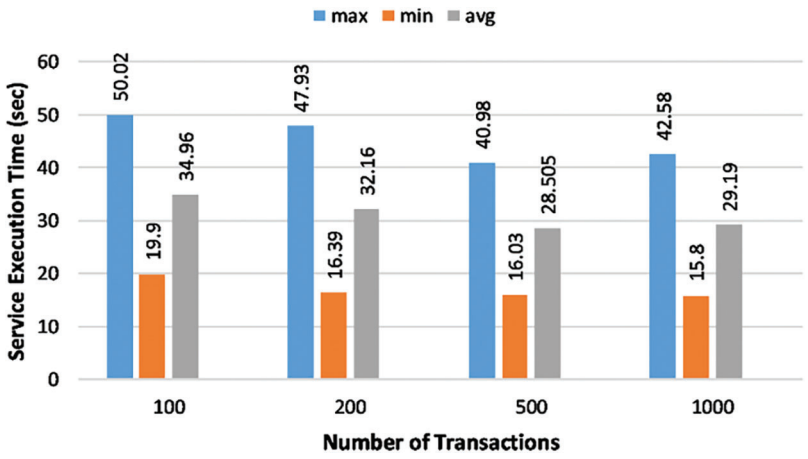

Figure 12: Service execution time for the patient-doctor interaction

In the final phase of experiments, we analyze the service execution time to access the patient's cardiac history through the proposed framework. This process contains three stages: submission of the proposal, selection of relevant patients after successful verification, and updating of the blockchain record upon completion of the task. Again, the size of transaction groups is maintained. The experimental outcomes of the cardiac history access process are presented in Fig. 13. Results indicate that the average service execution time varies between 37.57 to 79.6 s for the smallest and biggest groups, respectively.

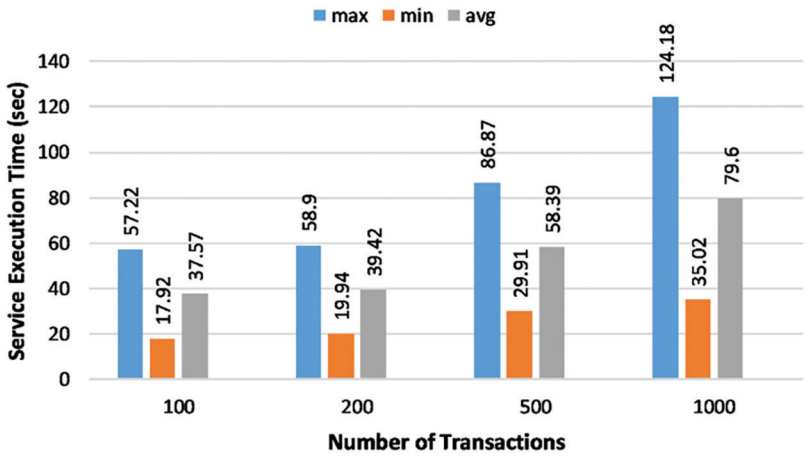

Figure 13: Service execution time for the cardiac history access operation

4.2 Transaction Throughput

The transaction throughput represents the number of transactions completed per second based on the time and place of the transaction. Transaction throughput is a cycle of processing and verifying all requests through the blockchain framework. The experiments and throughput evaluation are described in the following.

In the first phase of experiments, we analyze the throughput for user registration operation through the proposed framework. Users are categorized into four groups of transactions such as 100, 200, 500, and 1000. The experimental findings of the user registration process are presented in Fig. 14. The maximum throughputs for the smallest and biggest groups are recorded as 0.7 OPS (operations per second) and 6.9 OPS, respectively. The average throughput varies between 0.6 OPS and 6.4 OPS. The proposed framework's user registration process is the heaviest operation that contains computationally expensive operations. Therefore, this operation's throughput is minimal compared to all other operations.

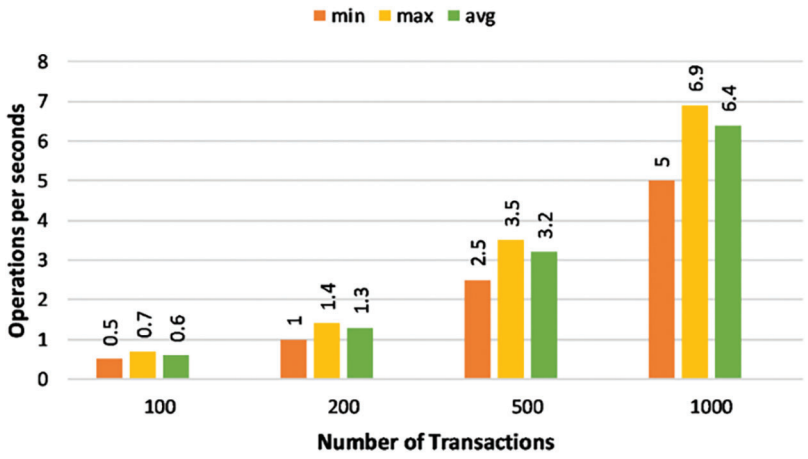

Figure 14: A comparison of transaction throughput for the user registration process

In the second phase of experiments, we analyze the throughput for access control operation through the proposed framework. The group sizes are maintained for these experiments. The experimental findings of the access control process are presented in Fig. 15. The maximum throughputs for the smallest and biggest groups are recorded as 4.2 OPS and 33.4 OPS, respectively. The average throughput varies between 3.1 OPS and 21 OPS.

In the third phase of experiments, we analyze the throughput for lab appointment operation through the proposed framework. The group sizes are maintained for these experiments. The experimental findings of the lab appointment operation are presented in Fig. 16. The maximum throughputs for the smallest and biggest groups are recorded as 4.1 OPS and 30.3 OPS, respectively. The average throughput varies between 2.7 OPS and 20.1 OPS.

In the fourth phase of experiments, we analyze the throughput for patient-doctor interaction through the proposed framework. The group sizes are maintained for these experiments. The experimental findings of the patient-doctor interaction operation are presented in Fig. 17. The maximum throughputs for the smallest and biggest groups are recorded as 5.0 OPS and 63.3 OPS, respectively. The average throughput varies between 2.9 OPS and 34.3 OPS.

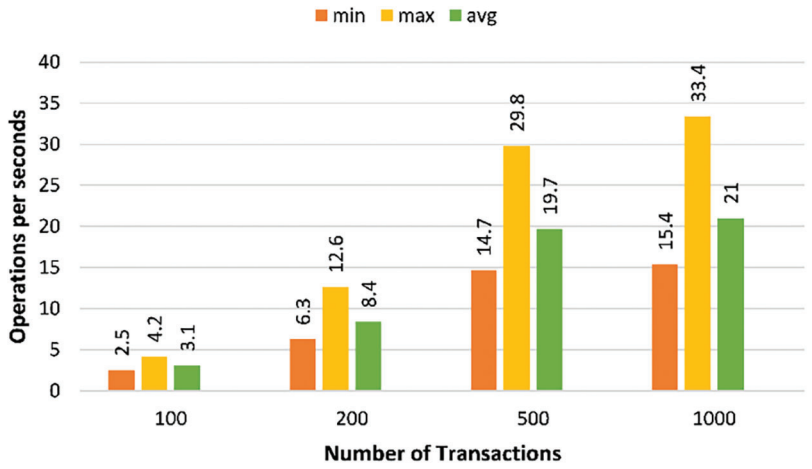

Figure 15: A comparison of transaction throughput for the access control process

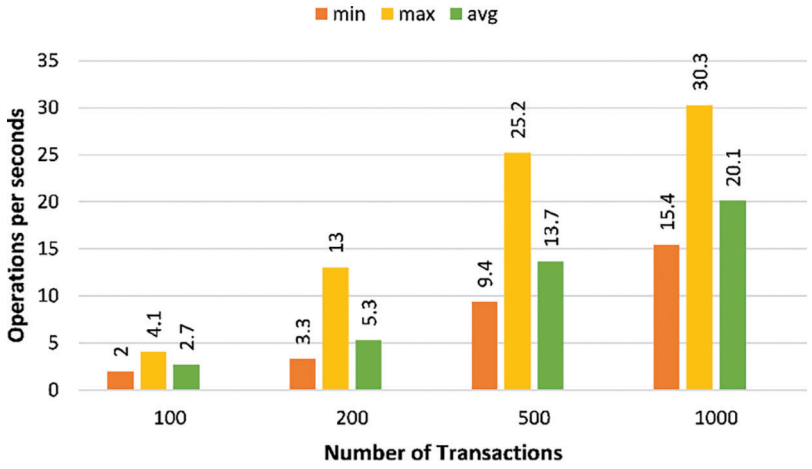

Figure 16: A comparison of transaction throughput for the lab appointment operations

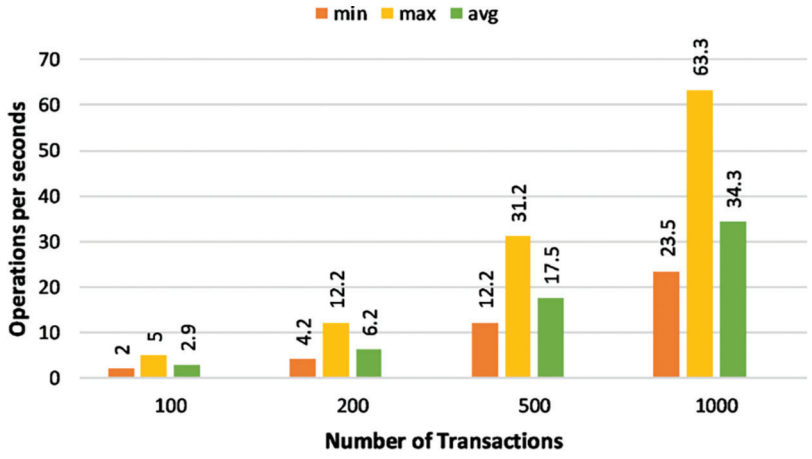

Figure 17: A comparison of transaction throughput for the patient-doctor interaction

In the final phase of experiments, we analyze the throughput for cardiac history access operation through the proposed framework. The group sizes are maintained for these experiments. The experimental findings of the cardiac history operation are presented in Fig. 18. The maximum throughputs for the smallest and biggest groups are recorded as 5.6 OPS and 28.6 OPS, respectively. The average throughput varies between 2.7 OPS and 12.6 OPS.

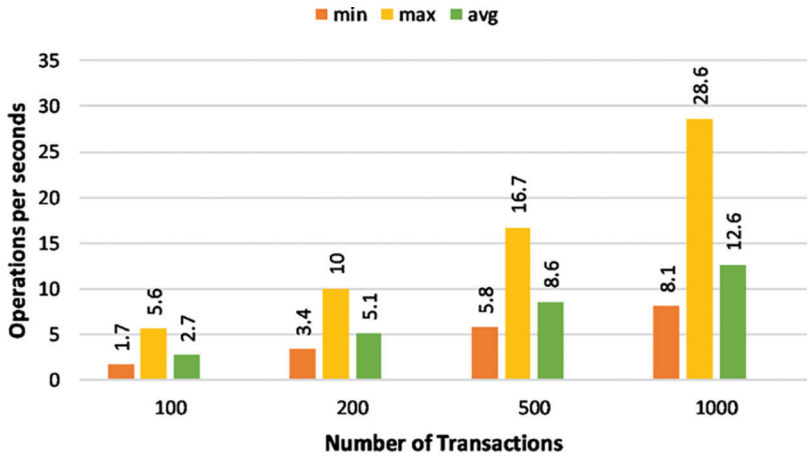

Figure 18: A comparison of transaction throughput for the cardiac history operation

The experimental outcomes indicate that the overall performance of the proposed design is satisfactory in terms of lower service execution time and higher throughput. The suggested framework can perform several healthcare-related operations and be integrated with a small-scale IoMT system.

5 Conclusion

This article proposed a blockchain-enabled healthcare system focusing on privacy protection, authentication, immutability, and performance studies. The ECDSA cryptographic algorithm underlying the proposed framework ensures the security and decentralization of IoMT. The proposed architecture facilitates the multiple participants in the healthcare sector to perform different operations, including patient appointments, medical check-ups, lab services, medical history, and medical treatments. The performance of the suggested framework is thoroughly analyzed through multi-performance indicators such as service execution time and transaction throughput. Experimental results confirmed that the proposed framework achieved lower service execution time and higher throughput for multiple operations with varying transactions. This work can be extended to the area of intrusion detection, which can be a critical problem with major societal implications.

Funding Statement: The researchers would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Jianxing, L. Xu, J. Xu, J. Zhou and X. Zhang, "The practical implementation of artificial intelligence technologies in medicine," *Nature Medicine*, vol. 25, no. 3, pp. 30–36, 2019.

[2] B. Sujit, K. Li, F. Latif, Z. Kanhere and P. Saraju, "Interoperability and synchronization management of blockchain-based decentralized e-health systems," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1363–1376, 2020.

[3] S. Rub, N. Jes, L. Gondim and R. Paulo, "IoMT platform for pervasive healthcare data aggregation, processing, and sharing based on OneM2M and OpenEHR," *Sensors*, vol. 19, no. 2, pp. 42–83, 2019.

[4] S. Pradhan, K. Badarla and P. Saraju, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 11717–11731, 2021.

[5] M. Yanambaka, V. Deepak and Y. Kumar, "Integration of internet of things and blockchain toward portability and low-energy consumption," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, pp. 10–25, 2021.

[6] B. Bo, N. Guy and S. Stefano, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 5, pp. 3796–3838, 2019.

[7] S. Zolanvari, M. Aiman and S. Mohammed, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 858–880, 2018.

[8] J. Luo, Y. Peilong and M. Jomol, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[9] V. Donoghue, O. David and M. Edward, "Blockchain vehicles for efficient medical record management," *NPJ Digital Medicine*, vol. 3, no. 4, pp. 1–5, 2020.

[10] Y. Li, T. Xizhen and W. Caifen, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45468–45476, 2020.

[11] N. Chen, L. Wang and J. Fei, "Electronic health record sharing scheme with searchable attribute-based encryption on blockchain," *IEEE Access*, vol. 8, pp. 7195–7204, 2019.

[12] B. Sharif, K. Fan, S. Saraju and W. Yu, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2343–2355, 2019.

[13] S. Pradhan, K. Badarla, V. Mohanty and P. Saraju, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 11717–11731, 2021.

[14] T. Parekh and K. Richard, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, no. 3, pp. 102–124, 2020.

[15] Y. Xiaodong, T. Pei, X. Wen and W. Caifen, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45468–45476, 2020.

[16] A. Raifa, "Blockchain for the management of internet of things devices in the medical industry," *IEEE Transactions on Engineering Management*, vol. 3, no. 5, pp. 1–22, 2021.

[17] S. Pratap, P. Ranjan, L. Agnihotri, S. Jhanjhi and D. Sinha, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 5779–5789, 2020.