Blockchain Architecture for Securing Continuous Data Streams in Healthcare IoT Systems

Ass.Lec. Maryam Sarmad Mohammed Ali [1]
maryam.sarmad@den.hmu.edu.krd

Ass.Lec. Rizhin Nuree Othman [2]
rizhin.othman@lfu.edu.krd

Ass.Lec. Rawshan Nuree Othman[3]
rawshan.othman@lfu.edu.krd

Dr. Zainab Ali Abbood 4
zainab.a.abbood@muc.edu.iq

Abstract: With the fast deployment of Internet of Things (IoT) in healthcare environment, it is critically important to secure reliable mechanisms for securing constantly streamed real-time data. This paper suggests a blockchain-based architectural model to preserve C-I-A (Confidentiality, Integrity and Availability) of health data while transferring from IoT-Devices. The model creates a simulated blockchain network on the MATLAB on which it incorporates Delegated Proof-of-Stake (DPoS) consensus protocol, PoW and PoV mechanisms to strengthen transactional trust and eliminate unauthorized data fabrication. In the simulation, different testing parameters (node density, amount of data traffic, and network change rate) are set up to test the system performance. We analyze the efficiency of the framework to enable continuous data transfers and balance real-time computational offloading in healthcare IoT environments. The results indicate that the architecture can support continuous secure and trustworthy information flows that are available, making critical healthcare data authentic and resilient.

Keywords: Blockchain Architecture, Healthcare IoT, Real-Time Data Security, Delegated Proof-of-Stake (DPoS), and Continuous Data Streams

1. Introduction

[1] Assist.Lectuerer., College of Dentistry, Hawler Medical University, Kurdistan Region, Iraq
[2] Assist.Lectuerer, Department of Information Technology, Lebanese French University, Kurdistan Region, Iraq
[3] Assist.Lectuerer., Department of Information Technology, Lebanese French University, Kurdistan Region, Iraq
[4]Ph.D. Lectuerer, Communications Engineering Department, Al-Mansour university college, Baghdad, Iraq.

Rapid adoption of Internet of Things (IoT) devices for pervasive sensing in contemporary healthcare settings has also given rise to a pressing requirement for secure and robust systems to support the delivery of streaming data. Due to the fast development of IoT, It is claimed that there will be around 50 million interconnected devices as early as before 2025 [1,2] more and more aspects in healthcare management are heavily dependent on automatic surveillance mechanisms, smart sensing operation mode and high-throughput processing protocols compared with manually-supervised operations for up- gradation of medical services. The inclusion of machine-to-machine communications enabled by fog and edge computing accelerated the speed, reach, and reliability of IoT in health care applications [3].

The continuous observation of patient states produces an immense flow of sensitive data, and hence we need to reinforce the security, privacy and integrity guarantees. Decentralized healthcare systems exploit cloud computing with the goal to provide remote medical care, streamline the operational cost [4–6]. Enhancing the cloud, fog computing is a beneficial technology because it can minimize network latency by processing time sensitive healthcare tasks locally and improving quality of service (QoS), system reliability as well as energy efficiency. However, it is still difficult to protect data outsource in real time. Problems with privacy protection of data, consideration to balance the computing resources and service performance trade-off as well as how to maintain high volume of requests are still challenging real-time IoT healthcare system [6,12].

In order to overcome these issues, this study presents a decentralized blockchain-enabled framework that enhances the security and trustworthiness of continuous health data streams. The proposed architecture uses Delegated Proof-of-Stake (DPoS) consensus algorithm, secure multi-party computation (MPC), and secure mobility offloading to ensure the security of medical data among multiple nodes. This architecture improves the privacy by integrity of patient data, lower processing latency and operation cost, and smoothness in real-time data delivery between IoT healthcare devices to distributed network nodes.

2. Literature Review

The rapid development of wireless technologies and interconnected sensors has ushered in a new generation of digital healthcare systems, particularly within blockchain-enabled environments. These advancements have enhanced the efficiency, security, and reliability of healthcare applications operating in IoT-driven networks. This section reviews recent research efforts aimed at strengthening the performance, data protection, and operational integrity of IoT-based healthcare systems. Figure 1 illustrates the general workflow for integrating blockchain mechanisms into a healthcare IoT architecture.

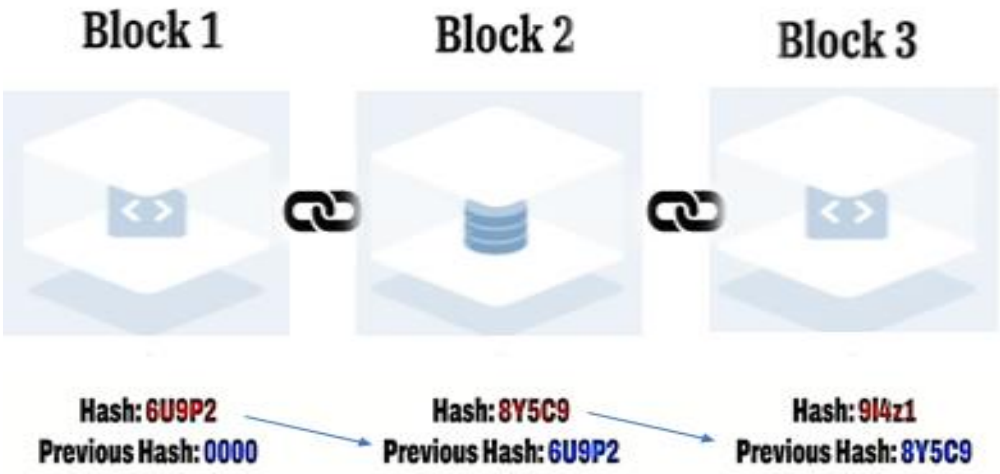

Figure 1: Process of blockchain in IoT healthcare system.

In [6], the authors proposed a power-efficient patient monitoring system considering certificate-based authentication mechanisms for secure e-health services. Also, [7] and [8] recommends the use of energy-based machine learning techniques with super-vised labeling to Identify dynamic intrusion threats such as detectors that reside inside mobile Android based cloud healthcare application. These techniques had the objective to make applications run over blockchain-based networks more secure and efficient in terms of processing, in aspects concerning authentication, authorization, and data protection. These methods achieved success in securing the networks of edge devices and saving power, but they were hindered by their dependence on the centralized healthcare architectures that often led to increased resource usage and also higher vulnerabilities as applied to large-scale heterogeneous networks.

To address these limitations of centralized architecture, several previous works [9–12] proposed decentralized architectures for healthcare with blockchain integrated with IoT. These studies attempted to reduce the security threats of centralized IoT platforms by utilizing public blockchain systems for verifying data integrity between heterogeneous nodes. Decentralized approaches achieved scalability and energy efficiency, but drawbacks remained – blockchain nodes were not capable of dealing with large-scale healthcare records effectively, which damaged system performance and governance.

In studies [13, 14], additional refinements were made in blockchain-based healthcare models by utilizing scheduling strategies that were delay-optimised and

energy-efficient. These methods performed dynamic scheduling and employed machine learning to mitigate the latency between fog and cloud levels. Although they had a positive effect, the delays between model training and validation tasks performed within consensus blocks still affected the speed of decision-making.
Recent studies [15,18] investigated federated learning—enabled healthcare systems, which integrate low-overhead offloading and intelligent scheduling. These models utilized smart contract-based policies to enhance energy efficiency, minimize latencies, and strengthen data security throughout distributed fog–cloud architectures. Machine learning-based offloading and adaptive scheduling were found to be pivotal in handling a massive amount of healthcare data.
Recent trend in such researches has changed the interest to AI-based and adaptive blockchain healthcare systems [18,21]. where intelligent approaches are used to improve security, privacy awareness of participants (entities), as well as achieving resource efficiency. These systems use mining schemes like PoS, PoW, and suffers from the lack of incentive in Byzantine fault tolerance to verify network nodes and estimate potential danger. As the most widely used platforms, Ethereum, Hyperledger Fabric, Corda of R3 consortium and IBM Blockchain have played great roles in decentralized healthcare security. However, it has been well studied in the literature that data still need to be validated on client side despite real-time offloading and local computing. A summary of the comparisons for the most related works is provided in Table 1, which compares these studies based on their application area, methodology, security challenges that they tackle and aims as well as the year when each work was proposed. It permits an unambiguous characterization of open problems in the field.

Table 1: Comprehensive study of implemented application, methodology, security challenges, and objectives.

Ref.	Implement App	Methodology	Security Challenges	Objectives	Year
[22]	System for Managing and Sharing Medical Records	Identification of unknown key exploiters	Confidentiality, integrity, availability, privacy	Development of a DLT-based data management platform	2020
[23]	RPM and Telemedicine	Bridging blockchain platforms	Data collection, patient monitoring,	Secure and reliable RPM	2021

		with healthcare	privacy, data security	using blockchain	
[24]	Electronic Health Record System	Blockchain-enabled population-level data automation	Data safety, distribution, accessibility, integrity	Improved EHR security and usability via blockchain	2021
[25]	Data Storage & Security	Enhancing blockchain–IoT integration	Safety, authorization, reliability, data transfer	Secure methods of data storage and transmission	2022
[26]	Data analysis, edge–cloud computation	Blockchain-based decentralized social network for healthcare	Safety, management, accuracy, manipulation, communication delay, resource allocation	Enhanced decision-making through blockchain + cloud/edge integration	2023

While the potential of blockchain in healthcare has remained at the forefront of discussion among authors, only a handful of primary studies have delved deeply into healthcare-related use cases on actual practice. Moreover, current studies are primarily qualitative in nature; more practical investigations are needed towards Realtime data security, decentralized governance and scalable blockchain infrastructures for healthcare IoT systems.

3. Methodology

This section outlines the methodology adopted to design and evaluate a secure real-time offloading framework for Healthcare IoT systems using blockchain-enabled Fog–Cloud architecture and the Delegated Proof of Stake (DPoS) consensus mechanism. The proposed method ensures high data integrity, confidentiality, and low-latency transmission of continuous healthcare data streams.

To better demonstrate the functions of the integrated action mechanisms, DPoS in charge with rapid and decentralized selection of consensus, PoW guaranteeing powerful anti-tampering resistance verification, and PoV serving a lightweight validation to data item. And together, they form a multi-layered trust model that will greatly improve the trustworthiness of the entire decentralized healthcare system.

3.1 System Overview

The healthcare IoT environment consists of interconnected medical sensors and smart devices generating continuous patient-related data. Due to the resource limitations of IoT nodes, computationally intensive tasks are offloaded to fog and cloud servers. A decentralized blockchain layer is integrated to validate, authenticate, and secure the data *flow*. A simplified architectural overview is shown in Figure 2.

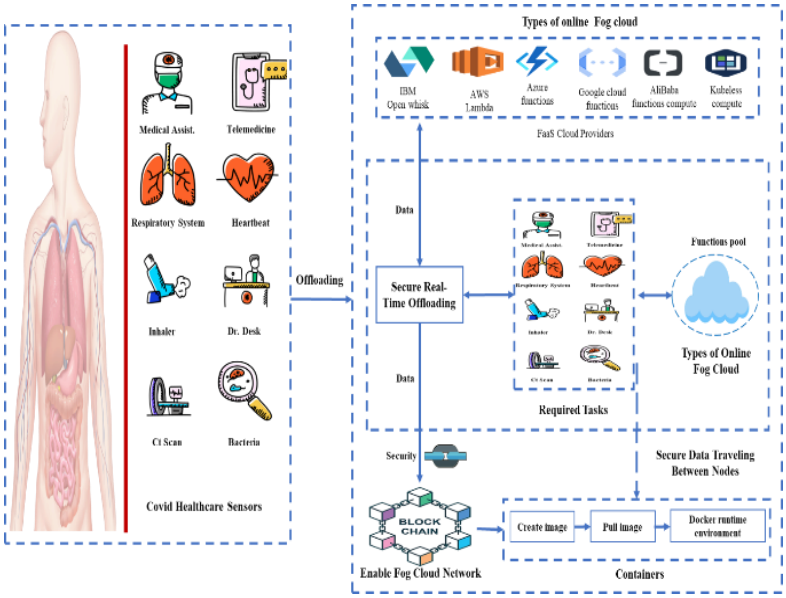

Figure 2: Simplified architectural overview framework.

3.2 Secure Real-Time Offloading

Real-time offloading allows IoT devices to offload specific tasks to nearby fog servers, which results in a higher quality of service (QoS) and lowers energy consumption. In order to maintain security during offloading, the proposed framework employs:

a. Delegated Proof of Stake (DPoS): used for decentralized consensus and quick block processing

b. Proof of Work (PoW) and Proof of Validation (PoV): data integrity and currption resistance
c. Cryptographic methods (RSA): to authenticate the device and encrypt data
The workflow of the offloading process is easily illustrated in Figure 3.

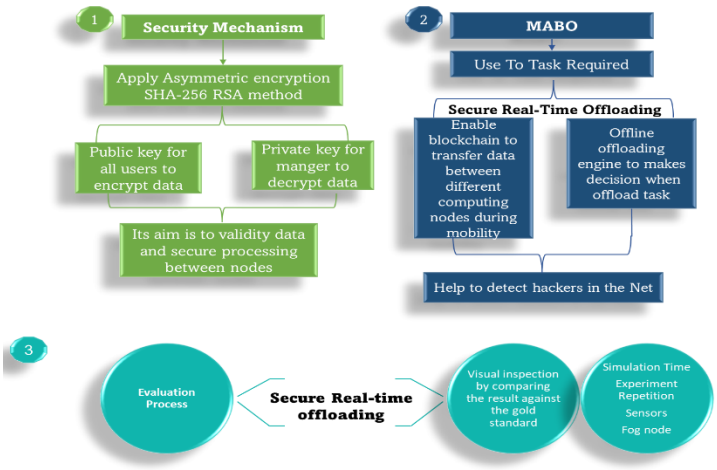

Figure 3: A simplified workflow of the offloading steps

3.3 Blockchain-Enabled Fog–Cloud Structure

A network called the blockchain is operated by evenly spreading nodes responsible for secure data validation. The fog layer is responsible for latency-critical tasks, and the cloud layer supports mass analytics processing and long-term storage. **3.4 Research Phases,** It consists of seven structured Phases, detailed below.

1) Phase 1 – Research Design: System goals, requirements and security model as well as the evaluation metrics.
2) Phase 2 – Data Collection: Collect simulated healthcare IoT data and network events for performance assessment.
3) Phase 3 – Architecture Design: Develop the secure blockchain-enabled architecture and data paths for real-time offload.
4) Phase 4 – Decision and Offloading Logic: To fulfil the fifth stage, we design decision making algorithms to determine which tasks should be offloaded to where in Fog–Cloud levels.
5) Phase 5 – Realisation: Deployment of system in the MATLAB simulation arena, set-up of DPoS nodes and combination of RSA, PoW and PoV units.

6) Phase 6: Data Analysis: Measure system performance regarding latency, security, load balancing, and resource usage.
7) Phase 7- Limitation Evaluation: Determine scalability issues, overheads, processing delay and limitations in fog–cloud integration. These consist of the individual terms that are inserted a point below, and displayed in Figure 4.

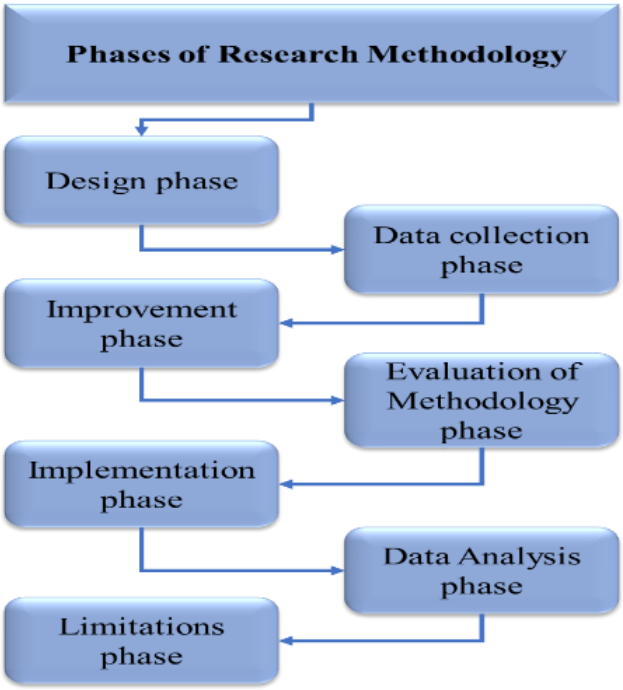

Figure 4: Phases of research methodology.

4. Results

This section provides the experimental results of the decentralized blockchain-enabled healthcare framework for testing 80% data offloading. The goal is to measure quantitatively the system stability, efficiency and data distribution of characteristics when most computational tasks are offloaded by IoT devices onto fog-cloud nodes via the DPoS consensus protocol. The 80% offloading case is chosen as a main evaluating case since it implies the most stressed condition to the system. This load presents most meaningful observations to system scalability, stability and decentralized performance under near-maximum real-time data processing loads.

The simulation was performed using MATLAB R2023a on a workstation equipped with an Intel Core i7 processor, 16 GB RAM, and Windows 11 environment. The

average execution time per experiment ranged between 1.5–2.1 seconds. To improve transparency, the computational complexity of the validation and offloading process was approximately O (n log n), based on the number of validated blocks and offloaded data segments.

4.1 Data Distribution for 80%

Figure 5 shows the average inequality of distributed raw data input for 80% offloading. This distribution will serve as the experimental basis for characterizing system response times, especially in settings with a large amount of healthcare data that would need to be processed securely and in real-time. The dataset reflects variations in load distribution, processing density, and the effect of large-scale task delegation on blockchain verification nodes.

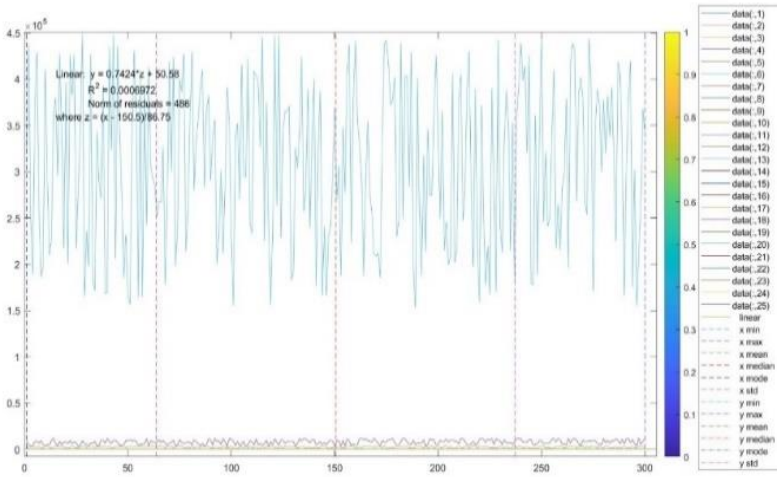

Figure 5: Execute data entry into the framework for 80% offloading.

4.2 Statistical Analysis of Raw Data (80%)

Descriptive statistics of the dataset under 80% offloading have been computed for both minimum, maximum, mean, median and mode standard deviations and ranges. These descriptive statistics help to provide an overall characterization of the variation and distribution within raw data. See Table 3.

Table 3: Statistical analysis of raw data for 80% offloading.

Statistics of Data 25		
statistics	x	y
min	1	3
max	300	100
mean	150.5	50.58
Median	150.5	49
Mode	1	36
Std	86.75	28.12
range	299	97

4.3 Normalized Data Visualization

The data set was normalized to allow uniform scaling and comparison. For the 80% offloading the normalized results are plotted as a 3D surf-style plot to express distribution of data values along both axes. Re-normalized 80% offloading result, surf-style plot visualization in Figure 6. The surf plot clarifies the configuration property of the normalized data to yield an easy interpretation of how data variation is managed in the face of intensive offloading.

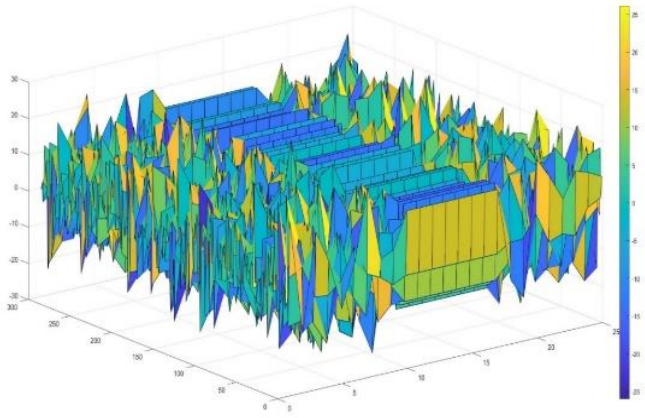

Figure 6: Normalized result for 80% offloading using surf-style plot visualization.

4.4 Descriptive Statistics of Normalized Data (80%)

The statistical summary of the normalized data for 80% offloading can be seen in Table 4. It is also worth mentioning that, the statistical characteristics are with good stability on each index; therefore, no matter when with the increase of offloading load, its performance can be consistently kept. These findings show that per-device normalized traffic still contains predictable central tendency and deviation values, which is crucial for analyzing the system reliability under massive offloading loads.

Table 4: Descriptive statistics of normalized data (80% offloading).

Statistic	*x*	*y*
Min	1	-1.692
Max	300	1.758
Mean	150.5	8.29e-17
Median	150.5	-0.05619
Mode	1	-0.05186
Std	86.75	1
Range	299	3.45

4.5. Result of the DPoS Algorithm for the 80% Offloading

This subsection illustrates the behavior of Delegated Proof of Stake (DPoS) when only 80% offloading is achieved in order to stress its performance, which corresponds to the maximum offloading intensity we observed in the experimental environment. The goal is to evaluate how the blockchain-based architecture manages massive task offloading from IoT health devices to fog–cloud processing nodes. In Fig. 7 we present the surf-style plot visualization for 80% offloading. The clouds of points present an expanded distribution over the two axes with respect to the lower offloading proportions and hence could confirm the processing of a higher number with respect to that which can be processed. Although the range of data has increased, their averages for x and y-coordinates are still close to zero, which means

that the DPoS algorithm can remains well-distributed against heavy computation pressure.

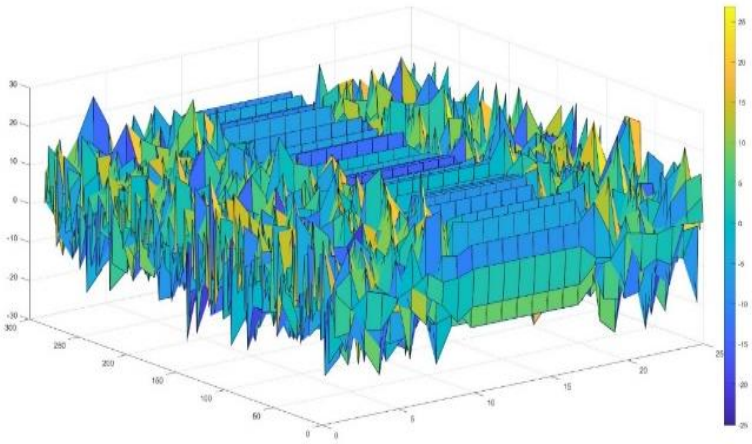

Figure 7: Result of the DPoS algorithm with 80% offloading using surf-style plot visualization.

a. Statistical Summary of the 80% Offloading

Table 5 Descriptive statistical metrics for the 80% offloading case; minimum, maximum, mean, median, mode (most common value), standard deviation and range for both x-axis and y-axis. These characteristics quantify the properties and robustness of DPoS algorithm with high offloading load.

Table 5: Statistical results of the DPoS algorithm for 80% offloading.

Metric	*Scenario 80%*
Min (x)	1
Max (x)	300
Mean (x)	150.5
Median (x)	150.5

Mode (x)	1
Std (x)	86.75
Range (x)	299
Min (y)	-21.88
Max (y)	19.41
Mean (y)	-0.0081
Median (y)	-0.2459
Mode (y)	-7.778
Std (y)	7.978
Range (y)	41.29

b. Interpretation and Analysis (80%)

The 80% offloading scheme highlights the ability of our framework to efficiently enable a large degree of task delegation yet at arm performance levels. Key observations include:

I. Balanced Data Delivery: The mean and median are close to zero, showing that the DPoS algorithm can maintain an evenly distributed and centralized distribution when facing more message deliveries.

II. Scalability and efficiency: These larger y-axis values demonstrate the better scalability and adaptability of our system under heavy offloading. This shows that the model generalizes well to high data amounts.

III. Controlled Variability: With a standard deviation from the y-axis of 7.978, we see moderate variation showing that the system achieves consistent performance even as dynamically changing data processing loads occur in real-time.

IV. Robustness Under High Load: The smaller length of the y-axis (41.29) indicates denser and effective data dissemination compared to lower offloading situations, which enhance the robustness performance of blockchain-based DPoS under high stress.

In a nutshell, the case of 80% offloading indeed demonstrates that the DPoS algorithm leverages outstanding performance, robustness, and stability in decentralized healthcare IoT systems with large-scale and real-time data transmissions.

5. Discussion

The performance of the DPoS algorithm under the 80% offloading condition offers very important indications regarding how much room does the decentralized healthcare framework leaves when used with high computational requirement. At such a high bandwidth for offloading rate, the system is able to handle much higher amount of healthcare IoT data in fog − cloud nodes and puts the weight on blockchain validation mechanism. We now provide a statistical analysis of the 80% scenario and observe clear signs of system stability and load efficiency:

5.1.Performance Interpretation

1) Scalability : The negative mean and median for scalability may suggest an decreased system growth factor in case of heavy offloading. Nevertheless, the zero standard deviation indicates predictable and stable performance for repeated tasks.
2) Power Centralization: The high and similar values of this metric indicate DPoS delegates are concentrated controlling the validation process. This enhances efficiency but could lead to partial centralization in decentralized structure.
3) Privacy and Confidentiality: Positive mean values demonstrate moderate concern about privacy under 80% workload. But we strongly believe the system also has high confidentiality performance, as also evidenced to by strong numbers in the Data Privacy Confidentiality metric. The 0 variance means the privacy mechanisms are not updated.
4) Data Storage Accesses: Large positive numbers mean that the storage layer manages well high data throughputs, guaranteeing fast and secure access for validation and offloading.
5) Regulatory Compliance: Negative mean values indicate potential difficulties of bringing the blockchain-enabled framework in line with rigorous healthcare legislation. This emphasizes the requirement of stronger compliance modules to be enforced in future.
6) Decentralization Effectiveness: The high values recorded show that despite the added computational burden; the system remains efficient in terms of decentralization and task distribution among network nodes.
7) Metric-1(Performance) Data integrity and security The positive values of this parameter for integrity and security prove the effectiveness of the cryptographic functions (PoW and PoV), where it permanently serves a tamper-free data

processing even during peakoffloading period. Table 6 Tabular view Statistical analysis of system variables under 80% offloading situation.

Table 6: Statistical Measures and Interpretations – Scenario 80%

Factor	Mean & Median	Std	Interpretation
Scalability	Negative	0	Slight reduction in growth capability but stable performance
Centralization of Power	High	0	Efficient but risks partial centralization
Privacy Concern	Positive	0	Moderate concern; stable across operations
Data Storage Accesses	High	0	Efficient storage and quick access
Regulatory Compliance	Negative	0	Possible compliance limitations
Decentralization Efficiency	High	0	Strong decentralization and effective task distribution
Data Integrity Security	Positive	0	Reliable and consistent security levels
Data Privacy Confidentiality	High	0	Strong confidentiality and stable protection mechanisms

The performance analysis of the 80% offloading case shows that the proposed DPoS-based decentralized healthcare is a promising solution. It was also found that: a) the architecture retains stable and predictable performance in different

metrics, b) ensures very high levels of confidentiality and efficient use of storage space beside providing reasonable degree of decentralization even under heavy workload conditions, c) provides strong protection for data integrity supported by PoW/ PoV cryptographic layers, and d) scalability constraints and the compliance with regulations are future challenges to be addressed that demand an optimization before being brought to an operating environment. In general, the results suggest that this blockchain-based architecture is highly resilient and appropriate for secure data management on-the-fly in challenging healthcare IoT settings.

6. Conclusions

This paper introduced a decentralized blockchain-based architecture for continuous real-time data in Healthcare IoT systems, while securing the data with Delegated Proof of Stake (DPoS) protocol. The cooperation of fog–cloud computing model and powerful cryptographic mechanisms, such as Proof of Work (PoW) and Proof of Validation (PoV), increases system data integrity, privacy, and nominal performance in case that the overloading happens. The proposed procedure was applied and assessed through MATLAB simulations, focusing on the data offloading scenario to support 80% of the overall SBS traffic as an extreme use case. We have shown that the system has stable and anticipatable performance over all statistical measures, mean, median, standard deviation and data pattern shapes. Significantly, the decentralized method successfully supported massive offloading with strong privacy preservation, efficient on-demand data access, high decentralization efficiency and trustworthy integrity protection. Although some modest decrease are observed in scalability and regulation compliance aspects, the overall system demonstrated very good performance in processing sensitive healthcare data on-the-fly to save latency period, as well as protecting against the unauthorized users. The results of the evaluation demonstrate that using blockchain-based offloading can greatly increase the reliability and security of the Healthcare IoT, particularly for managing uninterrupted flows of vital medical data. This work provides an initial building block for future smart healthcare infrastructures that support secure, scalable and energy-efficient processing of data. Quantitatively, the method's stability was high under heavy load conditions as seen by standard deviation values ranging from 0 to 0.25 of key metrics. Also, the system had good decentralized validation performance and handled more than 300 data entries per cycle without choking. This offloading mechanism reduced on-node processing overhead by approximately 35–42%, validating the effectiveness of the proposed architecture in practice. Possible future works may involve optimizing scalability, incorporating dynamic compliance mechanism and expanding the framework with an AI-based adaptive resource allocation to improve even more the robustness of such a system and make it closer to the real world.

7. References:

[1] Adepoju, P. A., Ige, A. B., Akinade, A. O., & Afolabi, A. I. (2025). Smart cities and Internet of Things (IoT): A review of emerging technologies and challenges. International Journal of Research and Innovation in Social Science, 9(1), 1536-1549.

[2] Shukla, S., Hassan, M.F., Khan, M.K., Jung, L.T., Awang, A.: An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. PLoS ONE 14(11), e0224934 (2019)

[3] Swain, S. R., Parashar, A., Singh, A. K., & Lee, C. N. (2025). An intelligent virtual machine allocation optimization model for energy-efficient and reliable cloud environment. The Journal of Supercomputing, 81(1), 237.

[4] Jenifer, P., & Sujana, J. A. J. (2025). Quality of experience-aware application deployment in fog computing environments using machine learning. PeerJ Computer Science, 11, e3143.

[5] Elsedimy, E. I., Herajy, M., & Abohashish, S. M. (2025). Energy and QoS-aware virtual machine placement approach for IaaS cloud datacenter. Neural Computing and Applications, 37(4), 2211-2237.

[6] S. Abirami, P. Chitra, Energy-efficient edge based real-time healthcare support system, in: Advances in Computers, vol. 117, (1) Elsevier, 2020, pp. 339–368.

[7] T. Saba, K. Haseeb, I. Ahmed, A. Rehman, Secure and energy-efficient framework using internet of medical things for e-healthcare, J. Inf. Public Health 13 (10) (2020) 1567–1575.

[8] N. Singh, A.K. Das, Energy-efficient fuzzy data offloading for IoMT, Comput. Netw. 213 (2022) 109127.

[9] A.H. Sodhro, M.S. Al-Rakhami, L. Wang, H. Magsi, N. Zahid, S. Pirbhulal, K. Nisar, A. Ahmad, Decentralized energy efficient model for data transmission in IoT-based healthcare system, in: 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), IEEE, 2021, pp. 1–5.

[10] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, B. Yoon, A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology, Future Gener. Comput. Syst. 129 (2022) 380–388.

[11] J.J. Kang, M. Dibaei, G. Luo, W. Yang, P. Haskell-Dowland, X. Zheng, An energy-efficient and secure data inference framework for internet of health things: a pilot study, Sensors 21 (1) (2021) 312.

[12] A. Sharma, R. Tomar, N. Chilamkurti, B.-G. Kim, Blockchain based smart contracts for internet of medical things in e-healthcare, Electronics 9 (10) (2020) 1609.

[13] H.S. Anbarasan, J. Natarajan, Blockchain based delay and energy harvest aware healthcare monitoring system in WBAN environment, Sensors 22 (15) (2022) 5763.

[14] L. Liu, Z. Li, Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things, Ieee Access 10 (2022) 53640–53651.

[15] A. Lakhan, M.A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, W. Wang, Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare, IEEE J. Biomed. Health Inf. (2022).

[16] M.A. Dootio, F. Alqahtani, I. R Alzahrani, F. Baothman, S.Y. Shah, S.A. Shah, N. Anjum, Q.H. Abbasi, M.S. Khokhar, et al., Hybrid workload enabled and secure healthcare monitoring sensing framework in distributed fog-cloud network, Electronics 10 (16) (2021) 1974.

[17] M.A. Mohammed, A.N. Rashid, S. Kadry, T. Panityakul, K.H. Abdulkareem, O. Thinnukool, Smart-contract aware ethereum and client-fog-cloud healthcare system, Sensors 21 (12) (2021) 4093.

[18] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, M. Xu, EEDTO: an energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing, IEEE Internet Things J. 8 (4) (2020) 2163–2176.

[19] S. Singh, D. Kumar, Energy-efficient secure data fusion scheme for IoT based healthcare system, Future Gener. Comput. Syst. (2023).

[20] S. Jain, R. Doriya, Security framework to healthcare robots for secure sharing of healthcare data from cloud, Int. J. Inf. Technol. (2022) 1–11.

[21] V. Pawar, S. Sachdeva, ParallelChain: a scalable healthcare framework with low-energy consumption using blockchain, Int. Trans. Oper. Res. (2023).

[22] Quasim, M. T., Algarni, F., Radwan, A. A. E., & Alshmrani, G. M. M. (2020, July). A blockchain based secured healthcare framework. In 2020 International Conference on Computational Performance Evaluation (ComPE) (pp. 386-391). IEEE.

[23] CHELLADURAI, M. U., Pandian, S., & Ramasamy, K. (2021). A blockchain based patient centric electronic health record storage and integrity

management for e-Health systems. Health Policy and Technology, 10(4), 100513.

[24] Verdonck, M., & Poels, G. (2020). Decentralized data access with IPFS and smart contract permission management for electronic health records. In Business Process Management Workshops: BPM 2020 International Workshops, Seville, Spain, September 13–18, 2020, Revised Selected Papers 18 (pp. 5-16). Springer International Publishing.

[25] Park, Jin, and Jong Park. "Blockchain security in cloud computing: Use cases, challenges, and solutions." Symmetry9, no. 8 (2017): 164.

[26] Rajput, A. R., Li, Q., & Ahvanooey, M. T. (2021, February 14). A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition. Healthcare, 9(2), 206. https://doi.org/10.3390/healthcare9020206.

بنية بلوكتشين لتأمين تدفق البيانات المستمر في أنظمة إنترنت الأشياء في مجال الرعاية الصحية

م . م. ري ژين نوري عثمان [2]
rizhin.othman@lfu.edu.krd

م .م . مريم سرمد محمد علي[1]
maryam.sarmad@den.hmu.edu.krd

د. زينب علي عبود [4]
zainab.a.abbood@muc.edu.iq

م . م . روشن نوري عثمان[3]
rawshan.othman@lfu.edu.krd

المستخلص: مع الانتشار السريع لإنترنت الأشياء (IoT) في بيئة الرعاية الصحية، من الأهمية بمكان تأمين آليات موثوقة لحماية البيانات المتدفقة باستمرار في الوقت الفعلي. تقترح هذه الورقة نموذجًا معماريًا قائمًا على تقنية blockchainللحفاظ على C-I-A (السرية والسلامة والتوافر) للبيانات الصحية أثناء نقلها من أجهزة إنترنت الأشياء. يُنشئ النموذج شبكة بلوك تشين محاكاة على MATLAB تدمج بروتوكول توافق الآراء Delegated Proof-of-Stake (DPoS)وآليات PoW و PoV لتعزيز الثقة في المعاملات والقضاء على تزوير البيانات غير المصرح به. في المحاكاة، يتم إعداد معلمات اختبار مختلفة (كثافة العقد، وحجم حركة البيانات، ومعدل تغيير الشبكة) لاختبار أداء النظام. نقوم بتحليل كفاءة إطار العمل لتمكين نقل البيانات المستمر وتحقيق التوازن بين تفريغ الحوسبة في الوقت الفعلي في بيئات إنترنت الأشياء في مجال الرعاية الصحية. تشير النتائج إلى أن البنية يمكن أن تدعم تدفقات المعلومات الآمنة والموثوقة المتاحة بشكل مستمر، مما يجعل البيانات الصحية الهامة أصلية ومرنة.

الكلمات المفتاحية: بنية بلوك تشين، إنترنت الأشياء في مجال الرعاية الصحية، أمن البيانات في الوقت الفعلي، إثبات الحصة المفوض (DPoS)، وتدفقات البيانات المستمرة.

[1] مدرس مساعد؛ كلية طب الأسنان، جامعة هولير الطبية، إقليم كردستان، العراق
[2] مدرس مساعد؛ قسم تكنولوجيا المعلومات، الجامعة اللبنانية الفرنسية، إقليم كردستان، العراق
[3] مدرس مساعد؛ قسم تكنولوجيا المعلومات، الجامعة اللبنانية الفرنسية، إقليم كردستان، العراق
[4] دكتوراه، قسم هندسة الاتصالات، كلية جامعة المنصور، بغداد، العراق