Mesopotamian journal of Cybersecurity
Vol.4,No.3, **pp**. 291–317
DOI: https://doi.org/10.58496/MJCS/2024/028; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Securing Real-Time Data Transfer in Healthcare IoT Environments with Blockchain Technology

Safa Hussein Oleiwi [1,2,*], Saraswathy Shamini Gunasekaran [1], Karrar Ibrahim AbdulAmeer [3], Mazin Abed Mohammed [4], Moamin A. Mahmoud [1]

[1] *College of Computing and Informatics, University Tenaga Nasional (UNITEN), Kajang 43000, Malaysia*
[2] *College of Education for humanities, Kerbala university, Iraq*
[3] *College of Computer Science and Information Technology, Kerbala university, Iraq*
[4] *College of Computer Science and Information Technology, University of Anbar, Iraq*

ARTICLEINFO

Article history
Received 05 Oct 2024
Accepted 06 Dec 2024
Published 27 Dec 2024

Keywords
IoT
healthcare
Real-time data transfer
blockchain
DPoS
PoW
PoV
Security
COVID-19 applications

ABSTRACT

The increasing number of Internet of Things (IoT) devices in healthcare applications, particularly during emergencies, necessitates safe protocols for transmitting real-time data. Medical data are essential for healthcare applications, and reliance on IoT devices to control information flow necessitates the consideration of five critical areas. This work addresses the security challenges associated with the transmission and storage of copyrighted healthcare data, as well as the inadequacy of the present methods in facilitating real-time data transfer given the volume of data and network conditions. This research provides a theoretical framework for the secure and immediate offloading of computations in IoT healthcare systems. The objective is to implement secure communication and networking technologies to ensure the security and integrity of medical data, maintain confidentiality, and facilitate real-time transmission of information. The proposed framework is simulated in MATLAB for system model implementation. A blockchain network sandbox was established with the delegated proof-of- stake (DPoS) consensus method, supplemented by proof-of-work (PoW) and proof-of-validation (PoV) for enhanced security. To assess the efficacy of this framework, multiple test scenarios focused on the number of nodes, the volume of data, and the conditions of network connectivity. The results demonstrated the system's efficacy in facilitating the offloading of real-time data in IoT healthcare applications. The aforementioned study demonstrated that the framework exhibited rapid transaction processing, efficient resource use, and energy conservation while also enhancing secure data transmission across various network conditions. The findings confirm that the proposed architecture can effectively and securely transmit real-time data in IoT healthcare applications without jeopardizing data authenticity, privacy, or integrity. The system's ability to address security challenges and manage substantial data volumes under varying settings indicates that it can be effectively deployed in healthcare systems, particularly in critical situations.

1. INTRODUCTION

The increased deployment of IoT devices in healthcare facilities means that dependable power solutions for securing real-time data transfer of critical medical information are needed. It may be even more important in an emergent state, as per the current outbreak of COVID-19, which ensures a timely and accurate flow of accurate patient data [1]. Nevertheless, the transfer of medical data within IoT healthcare systems can be both secure and efficient, albeit with certain challenges. These limits include the safeguarding of patients' information from illegal access, challenges related to resource availability and service delivery, and potential difficulties in managing substantial volumes of data owing to network and machine constraints. Furthermore, the rise of the need for healthcare solution delivery and managing large volumes of data, especially during a pandemic such as COVID-19, has made such systems more important [2-9]

*Corresponding author. Email: safa.h@uokerbala.edu.iq

The increased deployment of IoT devices in healthcare facilities means that dependable power solutions for securing real-time data transfer of critical medical information are needed. It may be even more important in an emergent state, as per the current outbreak of COVID-19, which ensures a timely and accurate flow of accurate patient data [1]. Nevertheless, the transfer of medical data within IoT healthcare systems can be both secure and efficient, albeit with certain challenges. These limits include the safeguarding of patients' information from illegal access, challenges related to resource availability and service delivery, and potential difficulties in managing substantial volumes of data owing to network and machine constraints. Furthermore, the rise of the need for healthcare solution delivery and managing large volumes of data, especially during a pandemic such as COVID-19, has made such systems more important [2-13].

This study establishes a theoretical framework for the secure offloading of computational tasks in IoT healthcare environments. The framework proposes a blockchain system that uses the delegated proof-of- stake (DPoS) consensus mechanism in conjunction with secure multiparty computation (MPC) to safeguard patient data. This architecture enhances the reliability and speed of real-time data transmission while minimizing the data processing time, energy consumption, and low quality of service (QoS) [3-14]. The primary aim of this initiative is to improve the development of a robust and reliable framework for the transmission of real-time healthcare data in IoT applications. This document pertains to the fast and accurate dissemination of medical information while safeguarding the confidentiality, integrity, and availability of patient data. This research focuses on determining the flow rate and the system's ability to achieve QoS standards in the healthcare context, emphasizing data processing efficiency [4-17]. Therefore, the main contributions of this study are as follows:

a) Decentralized IoT Healthcare System Development

b) Integration of blockchain technology and DPoS for secure real-time medical data transmission.

c) Use of Secure Multi-Party Computation (MPC) for patient data confidentiality and regulatory compliance.

d) Optimization of real-time data transmission to address network latency and resource utilization issues.

e) Implementation of DPoS for efficient management of IoT devices in healthcare settings.

f) The application of offloading techniques minimizes processing time, energy consumption, and resource usage while maintaining high QoS.

This is highly significant for the future of the IoT, particularly for decentralized healthcare systems. Our suggested system addresses the essential issues associated with cloud data storage and processing, including data security and privacy, network quality, resource consumption, and load variability, through the integration of blockchain and intelligent offloading techniques. Research indicates that such a system can be economically created and implemented for the tele-transmission of medical data in client healthcare and overall organizational efficiency during crises such as the ongoing COVID-19 epidemic. This study enhances the security, availability, and performance of IoT healthcare systems and establishes a foundation for further research on healthcare data utilization [5-18].

This paper is organized as follows: Section 2 delineates the literature on IoT healthcare systems and the implementation of blockchain technology. Section 3 delineates the theoretical framework for the secure offloading of computing delegation, integrating DPoS and Secure MPC. Section 4 presents the specifics of the employed technique, including the simulation environment and the performance indicators for evaluating the suggested solution. Section 5 of the study presents the results and comments, whereby the authors evaluate the effectiveness of the decentralized system on the basis of multiple offloading variables. Section 7 concludes the report by summarizing the study's key findings and offering recommendations for future research.

2. LITERATURE REVIEW

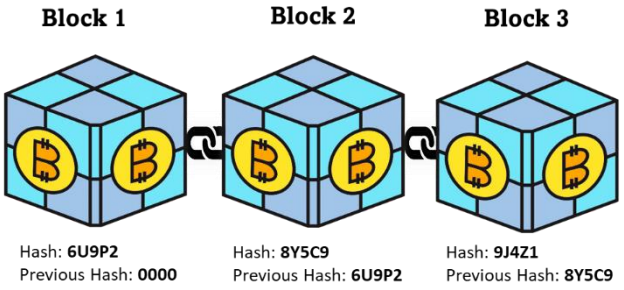
The emergence of wireless technology and sensors has initiated a novel era of digital healthcare systems, specifically inside the blockchain network, hence augmenting the efficacy of healthcare applications. This part focuses on the continuous study of endeavors aimed at enhancing the performance of healthcare applications within the network environment. Figure 1 illustrates the procedural framework for integrating blockchain technology within the IoT healthcare system.

In [6], a patient healthcare program designed to increase energy efficiency was presented. This scheme also included certificate-based security measures, which were implemented to safeguard remote healthcare services. In [7] and [8], the use of energy-efficient machine learning techniques that incorporate supervised labelling was suggested to address the problem of dynamic intrusion threats. These approaches were designed specifically for mobile Android cloud-based healthcare applications. The methodologies were developed with the objective of optimizing the application processing procedure within the blockchain-powered network. The purpose of these methodologies is to address the inherent problems with authentication and authorization that arise when dealing with patient data. These investigations effectively addressed security and energy consumption issues, particularly in relation to network-edge administering devices. Nevertheless, it is essential to highlight that the study focused mostly on the examination of security measures as well as energy consumption inside

centralized healthcare apps. When confronted with many diverse nodes in the healthcare industry, this method frequently results in excessive use of resources and increased security vulnerabilities.

Fig. 1. Process of blockchain in the IoT healthcare system.

To address these limitations, several studies [10–15] have proposed a decentralized healthcare system employing blockchain



technology in tandem with the Internet of Things (IoT). Using a decentralized method, the primary objective was to mitigate security vulnerabilities associated with centralized healthcare Internet of Things (IoT) systems. Utilizing public blockchain technologies facilitated the processing of public healthcare data, ensuring data integrity across heterogeneous groups while simultaneously reducing energy consumption relative to centralized solutions. Nonetheless, the inherent limitations of blockchain technology, specifically its capacity to manage large datasets on nodes, pose obstacles to achieving accurate governance over these healthcare systems in terms of security and energy efficiency.

In response to these issues, studies [16,19,21] have proposed blockchain-based healthcare system solutions that prioritize delay optimization and energy efficiency. The aforementioned advancements prioritized the reduction of processing delays in healthcare data transmission between fog and cloud nodes through the utilization of dynamic scheduling algorithms and machine learning techniques. Despite the implemented optimizations, the training and testing of models within consensus blocks caused delays in the final decision-making process for numerous studies.

Additional progress was made in studies [20,25,22], which included the proposal of a healthcare system propelled by federated learning, as well as the incorporation of trivial offloading as well as scheduling systems. By implementing smart agreement regulations, the primary objectives of these solutions were to reduce delays, enhance security measures, and optimize energy consumption. The use of machine learning techniques for outsourcing and adaptive scheduling is crucial to the efficient management of healthcare data within fog–cloud networks.

Recent studies have shown the emergence of innovative healthcare systems that integrate adaptive and artificial intelligence-driven mechanisms to augment security, privacy, and energy efficiency within the realm of blockchain technology [25–28]. These platforms were designed to predict security as well as energy risks in the IoT network through the use of several mining techniques, including proof of stake (PoS), proof of work (PoW), and Byzantine disappointment, to authenticate and anticipate network nodes. The previously listed blockchain frameworks, specifically Ethereum, Fabric, Corda, and IBM, have made significant advancements in the field of decentralized security. Nevertheless, scholarly studies have emphasized the importance of validating data on the client side in the context of offloading and local processing.

Table 1 provides a comprehensive list of the most important studies that have been conducted, encompassing the implemented application, the proposed methodology, the security challenges encountered, and the outstanding issues that remain unresolved. Additionally, the table outlines the objectives that were set for each study and whether they were achieved. The year in which each problem was resolved is also specified, enabling identification of the unresolved issues.

TABLE I. COMPREHENSIVE STUDY OF THE IMPLEMENTED APPLICATION, RECOMMENDED METHODS, SECURITY CHALLENGES AND OBJECTIVES.

Ref.	Implement App	Methodology	Security Challenges	Objectives	Year
[29]	System for Managing and Sharing Medical Records	Identification of unknown key exploiters	Concerning the confidentiality, integrity, availability, and privacy of data	Development of a Distributed Ledger Technology (DLT)-based Data Management Platform	2020
[30]	RPM (Remote Patient Medicine) and Telemedicine	Dedicated to bridging the gap between the blockchain platform concept and the healthcare industry	Data collecting, patient monitoring, and privacy and data security	Safe and reliable RPM using the blockchain	2021
[31]	The EHR System, or Electronic Health Record	Consider population-level data collection as an example of a work that could benefit from blockchain	Safety, distribution, accessibility, and integrity of data	E.H.R security as well as usability improved by employing blockchain technology.	2021

		automation that could be of use to healthcare practitioners.			
[32]	Data storage & Security	Dedicated to improving the technological advantages of blockchain applications, for example by coordinating Internet of Things gadgets.	Safety, Authorization, Reliability, as well as Transfer of Data	Creating Safe Methods of Data Transmission as well as Storage	2022
[33]	Data analysis, computation on the edge and in the cloud	The human body generates one-of-a-kind protocols as a transmission channel as part of its efforts to construct a blockchain-based, decentralized social network.	Problems with information safety, administration, dependability, accuracy, manipulation, communication delays, and allocation of scarce resources.	Better decisions may be made when blockchain technology is combined with other processing of data platforms, like cloud as well as edge computing.	2023

Table 2 presents a concise overview of our discussion about these six elements. First, we have blockchain's distinguishing qualities. The secondary publications provide an incomplete account of the properties of blockchain. The majority of the additional resources provide a cursory summary of blockchain characteristics. Furthermore, prior studies have examined the advantages of using blockchain technology in the healthcare sector. Nevertheless, the issue in question was examined by [34-38] across all participants in the healthcare industry. The remaining four assessments concentrated on a limited group of performers. Furthermore, the challenges and issues associated with implementing BC have been elucidated by [39, 40].

TABLE II. THE SECONDARY RESEARCH COMPARISONS INCLUDE SIX ASPECTS.

Ref.	Features of BC	BC Benefits in HC	BC Challenges & prob in implementation	Apps of BC in HC	Research Methodology	BC-based Cloud Apps & Platforms in HC
[34-36]	Relatively yes	Non	yes	Relatively yes	Non	Non
[37]	Relatively yes	Non	Non	Relatively yes	Non	Non
[38]	Relatively yes	Non	Non	Relatively yes	Non	Non
[39]	Relatively yes	Non	Non	Non	Non	Non
[40]	yes	yes	yes	yes	yes	Non

The healthcare market is currently experiencing swift advancements in technology. An analysis of the available literature reveals that only a limited number of primary studies have been incorporated into the discourse regarding the fourth aspect, namely, BC applications in HCs [35]. This study aims to expand the pool of primary studies available for analysis of blockchain applications within the healthcare sector. Moreover, extant research has employed a qualitative research methodology to elicit findings.

Despite significant advancements in the application of blockchain and IoT technology inside healthcare systems, several constraints persist that hinder the efficacy of these systems. Current solutions predominantly focus on enhancing the security and efficiency of a location-based healthcare system, as decentralization is insufficiently acknowledged. Several previous studies [6-8] addressed energy economy and security in centralized mobile Android cloud-based applications, which vary in node quantity and seldom exhibit scalability or heterogeneity. Although the application of blockchain in decentralized IoT healthcare systems, as examined in studies [10–15], appears to effectively mitigate security concerns, this technology encounters challenges regarding scalability, data management, and governance, particularly concerning heterogeneous data sources. Nonetheless, challenges persist regarding delay optimization and energy efficiency, despite the advancements in the current research on delay optimization [16] and energy efficiency [19], which indicate potential future developments in healthcare big data scheduling, as significant delays arise from the consensus mechanisms intrinsic to its complex nature. Moreover, despite the implementation of federated learning and adaptive scheduling in certain studies [20–25], blockchain technology, IoT devices, and real-time medical data transmission inside a decentralized network are lacking.

Recent advancements in artificial intelligence and other adaptive mechanisms have aimed to mitigate security and energy risks; however, they neglect the essential client-side validation of data during offloading and local processing, which remains crucial for real-time data accuracy in IoT healthcare networks. This paper addresses these issues by proposing a unique decentralized architecture that integrates the delegated proof of stake (DPoS) algorithm with safe multiparty computation (MPC). This integration enhances data protection, privacy, and the optimization of real-time healthcare data transfer, addressing the shortcomings of current centralized and decentralized systems, particularly in terms of scalability, energy consumption, and dependability.

3. METHODOLOGY

This section describes a methodology for achieving real-time dispatching in healthcare applications during the COVID-19 pandemic via the blockchain fog-cloud algorithm and the delegated proof of stake (DPoS) algorithm. The utilization of IoT technology to link sensors and equipment for real-time monitoring, data collection, and analysis is referred to as the healthcare IoT. In the long term, this interoperability will be advantageous for both patient care and malady management.

Real-time offloading is a process in which computational duties that are resource-constrained on IoT devices are transferred to edge or cloud servers that possess superior processing capabilities. By implementing this method, energy is saved, battery life is extended, and processing capabilities are improved, specifically for COVID-19 applications. The challenges posed by the pandemic require the implementation of a robust and secure Internet of Things (IoT) infrastructure. This infrastructure should encompass features such as remote patient monitoring, contact tracing, and timely symptom identification. Nevertheless, ensuring the protection of security and privacy regarding confidential healthcare information must take precedence.

The research topic is the development of a comprehensive framework for secure real-time outsourcing in healthcare applications of the Internet of Things, with a particular emphasis on addressing the difficulties brought about by the COVID-19 pandemic. The illustration of this framework in Figure 2 demonstrates its capacity to enhance the capabilities of healthcare providers through efficient surveillance and response to the ever-changing circumstances, facilitation of remote patient care, and contribution to the all-encompassing management of the pandemic.

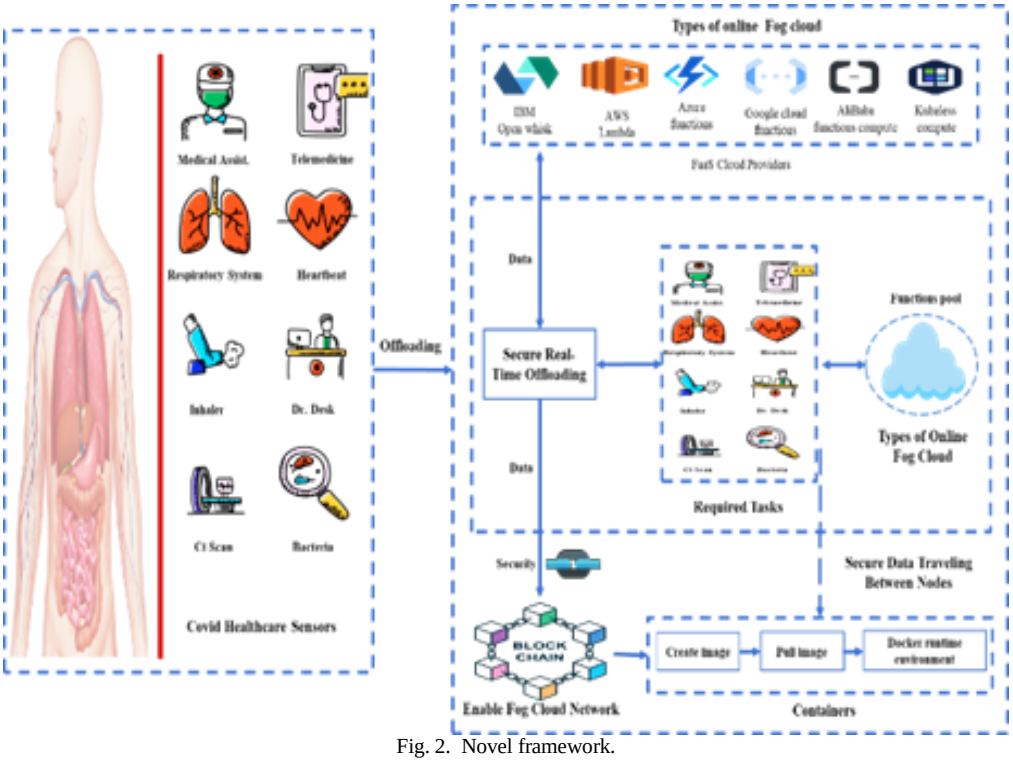


Fig. 2. Novel framework.

The principal aim of the suggested framework is to enhance the capabilities of Internet of Things (IoT) devices utilized in healthcare contexts through the efficient resolution of challenges regarding energy efficiency, security, and real-time processing. It is expected that the implementation of this enhancement will result in improved diagnostic precision, timely interventions, and improved patient outcomes.

This framework will be solved by using decentralized blockchain-enabled secure offloading that can handle secure real-time offloading for IoT healthcare applications, as well as solving the security problem by using a blockchain that consists of two cryptographic data (PoV & PoW). In addition, the approach consists of system distributed healthcare monitoring systems that assist in distributed fog–cloud networks that can process millions of queries. Hence, we design a unique blockchain-distributed healthcare monitoring system to increase the balance of QoS and resources. Figures 3 and 4 show the structure and steps used to solve the contribution.

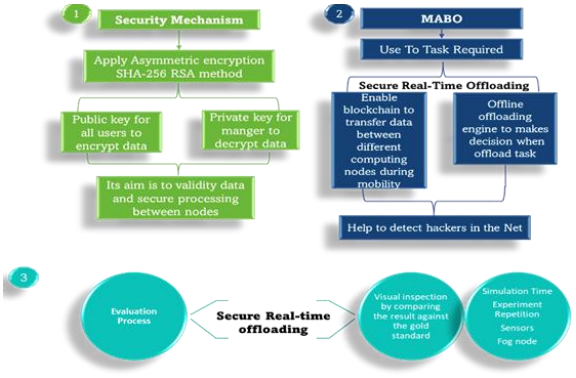


Fig.3. Structure to solve the novel approach.

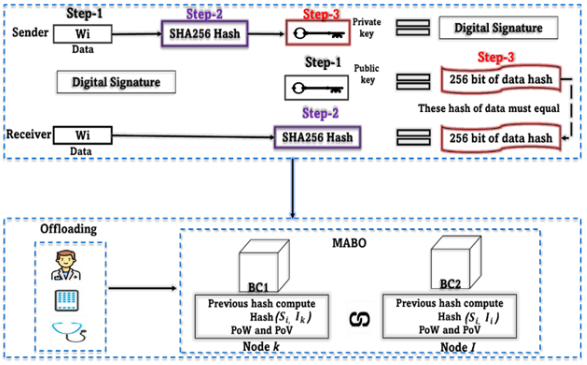


Fig. 4. Steps of RSA to solve the novel approach.

Hence, the methodology comprises distinct phases, each strategically formulated to target a particular facet of the problem at hand. These distinct phases are inserted at the following point and shown in Figure 5.

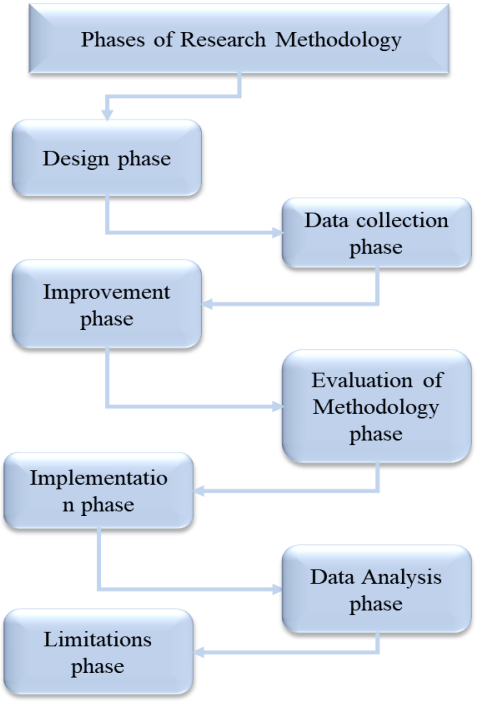


Fig. 5. Phases of research methodology.

1. Phase 1: The research design phase focuses on determining the goals, objectives, and data required for developing a secure real-time offloading system for monitoring COVID-19 healthcare. As shown in Figure 6,
2. Phase 2: Data collection phase. As shown in Figure 7
3. Phase 3 and Phase 4 involve enhancing the system architecture and framework, which includes implementing a decision-making solution and dividing the real-time offloading addresses. Figure 2 above illustrates step 4, which is the evaluation methodology step. As shown in Figure 8,
4. Phase 5: Implementation of the methodology. As shown in Figure 9,
5. Phase 6 involves the study of clinical data and
6. Phase 7 involves examining the limitations of the framework, as shown in Figure 10.

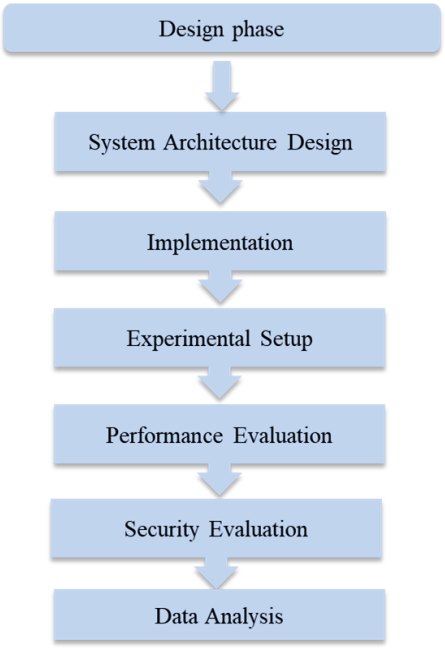


Fig. 6. Summary stages of the research design.

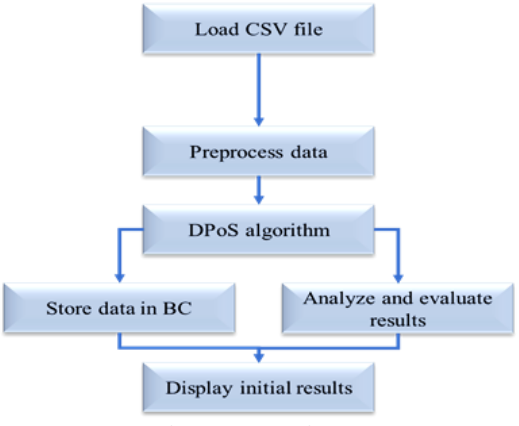


Fig. 7. Block diagram of the inclusion of the clinical data in the code.

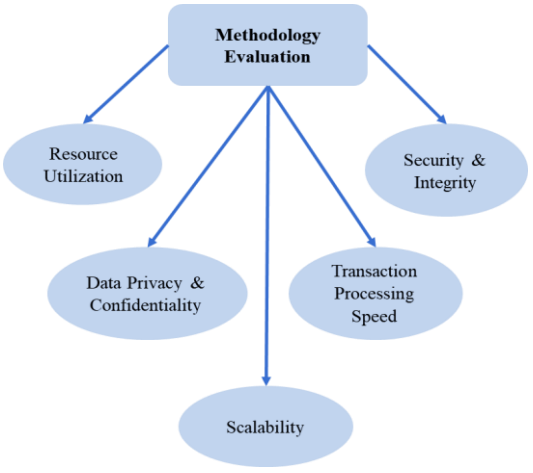


Fig. 8. Metrics used to evaluate the methodology.

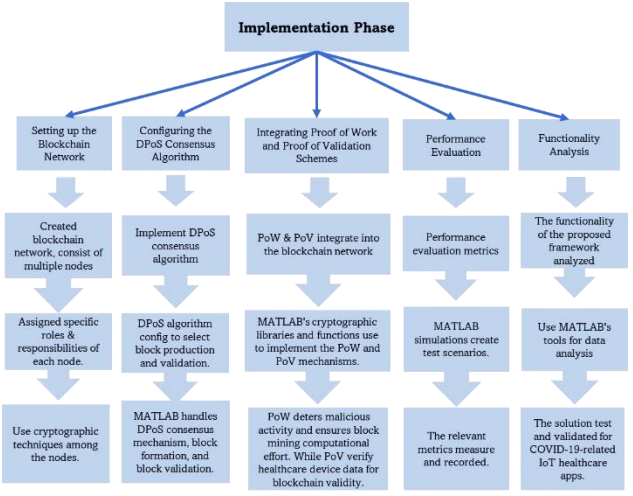


Fig. 9. These important stages of the implementation phase are presented and explained.

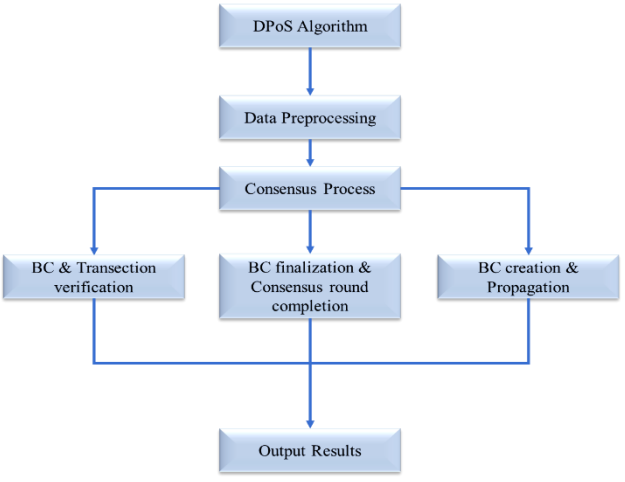


Fig. 10. Block diagram showing the analysis of the clinical data in the DPoS algorithm.

3.1 Algorithm Parameters

To ensure the accessibility and repeatability of the results, this section details the critical parameters for the DPoS and secure multiparty computation (MPC) algorithms utilized in the study. Table 3 lists the principal parameters employed in the DPoS and MPC algorithms utilized in this research. These characteristics are essential for guaranteeing the efficient functioning,

security, and scalability of the decentralized healthcare system, as well as for preserving data privacy and integrity during real-time data transmission and offloading.

TABLE III. ALGORITHM PARAMETERS

Parameter	Description	Value Used in the Study
Delegated Proof of Stake (DPoS) Algorithm		
Number of Delegates (N)	The number of elected delegates responsible for validating transactions in the blockchain.	21 delegates
Block Time (T)	The time interval required to produce a new block in the blockchain.	1 second
Transaction Per Block (M)	The maximum number of transactions allowed per block.	100 transactions per block
Voting Power (V)	The amount of power a user can delegate to a delegate based on the number of tokens held.	Proportionally assigned based on tokens held
Delegate Election Cycle (C)	The frequency with which delegates are elected.	Every 1000 blocks
Secure Multi-Party Computation (MPC) Algorithm		
Threshold (T)	The number of parties required to agree on a computation before it is accepted.	3 parties
Number of Participants (P)	The number of parties involved in the computation.	5 participants
Data Split Size (S)	The size of the data split into parts to distribute across participants.	1 MB per data split

4. IMPLEMENTATION AND RESULTS

4.1 Implementation

The implementation phase aims to create a virtual blockchain network via MATLAB to imitate real-life events in a decentralized healthcare system. The process involves establishing a simulated blockchain network, assembling the network with nodes representing different components, assigning duties and obligations to nodes, configuring the network, and initializing nodes with unique identifiers, processing capabilities, and datasets. Once these operations are completed, a functional simulated blockchain network is constructed to facilitate further research on the execution of the proposed decentralized healthcare system. This section explores specific aspects of this implementation, such as the adoption of the DPoS consensus mechanism, security measures, and performance evaluation metrics.

The DPoS consensus method is crucial for implementing a decentralized healthcare system. Delegates are responsible for creating new blocks in a predetermined order, ensuring a fair distribution of block creation responsibilities. They also validated the blocks created by other delegates, verified transactions and adhered to the network's consensus rules. Delegates play a crucial role in maintaining network security by actively participating in the consensus process and suggesting modifications to the consensus rules.

Delegates create new blocks via computational resources, verifying the integrity and authenticity of transactions. MATLAB's built-in functions and algorithms handle the consensus protocol, block creation, and validation processes in the DPoS algorithm. The consensus rounds are managed via MATLAB, ensuring the progression of block production and validation. Consensus round management is essential for maintaining integrity and efficiency. By configuring the virtual blockchain network, it is possible to assess the impact of implementing the DPoS consensus method on the proposed system's efficiency, scalability, and security.

Therefore, the implementation of PoW and PoV mechanisms in a decentralized healthcare system is discussed. It examines a blockchain network simulation in MATLAB, highlighting the integration procedures and functions of PoW and PoV. The use of cryptography libraries and functions in MATLAB helps integrate PoW and PoV schemes into the blockchain network, enhancing security and deterring bad actors. Proof of validation ensures the accuracy and reliability of medical records. The goal is to strengthen the security and data integrity of the decentralized healthcare system.

A decentralized healthcare system's performance evaluation is crucial for assessing its practical efficacy and efficiency. Measurements were taken and simulated via MATLAB, and metrics were assessed across various loads and scenarios. Table 4 provides detailed metrics for a comprehensive assessment of the system's effectiveness.

TABLE IV. DEFINED METRICS FOR PERFORMANCE ASSESSMENT

Metric	Description
Transaction Processing Speed	Measures the average time taken to process and validate a transaction within the blockchain network.
Scalability	A measure of the system's ability to handle increased load or demand.

Centralization of Power	Assesses the concentration of decision-making power within the system.
Privacy Concern	Reflects the level of concern for user data privacy within the system.
Data Storage Accesses	Measures the efficiency of data storage and access operations.
Regulatory Compliance	Evaluate the system's adherence to regulatory requirements.
Decentralization Effectiveness Efficiency	Assesses the efficiency of the decentralization strategy.
Data Integrity Security	Reflects the level of data integrity and security measures.
Data Privacy Confidentiality	Measures the system's effectiveness in preserving data privacy and confidentiality.

The MATLAB simulation process involves two main steps: scenario generation and testing. The first step generates real-life scenarios, considering variables such as data volume, network health, and node number. The second stage tests the system via MATLAB's simulation environment and develops scenarios, evaluating metrics such as transaction efficiency, scalability, and energy usage. Scalability measures measure the system's capacity to handle more transactions and nodes, transaction processing speed indicates responsiveness, and energy consumption measures evaluate the efficiency of the decentralized healthcare system. The performance evaluation metrics provide a comprehensive understanding of the system's scalability, energy efficiency, and overall performance. Comparison analysis helps identify strengths, limitations, and areas for improvement.

The proposed framework for secure real-time data transmission from healthcare applications via the Internet of Things is validated via MATLAB data analysis tools. The evaluation focuses on the punctuality, precision, and dependability of offloaded data. Reliability and accuracy evaluations verify the consistency and dependability of the offloading process. Timeliness is assessed by comparing offloaded data to expected data. The MATLAB suite of tools, including algorithms, visualization tools, and statistical analysis routines, is used for data analysis.

4.2 Results

To provide a quantitative overview of a decentralized healthcare system's performance indicators, including the mean, median, and standard deviation, the DPoS mechanism is used. It aims to enhance the understanding of the system's efficiency and stability in three scenarios with varying offloading proportions, and delegates are included in the input data for a healthcare system. These factors affect efficiency and performance, affecting data distribution and processing. Hypothesis testing uses these cases to evaluate the system's performance with different levels of data offloading. Figure 11 shows the distribution of data input for each scenario, highlighting the experimental conditions for hypothesis testing.

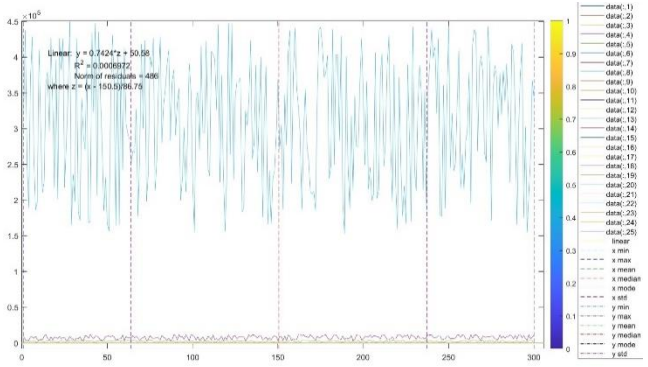


Fig 11. Execute data entry into the framework.

TABLE V. STATISTICS OF DATA 25 AND OFFLOADING RATES OF 20%, 50%, AND 80%.

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

Table 5 provides a statistical summary of x and y for three unloading percentages: 20%, 50%, and 80%. The initial observation of these data in a min–max graph promptly indicates a substantial range of variability, with the minimum value for x being 1 and the maximum being 300. The range of y is confined between 3 and 100, indicating that the values of y are less dispersed than those of x. Statistics indicate that the mean of x is 150.5, whereas the mean of y is 50.58, demonstrating that, on average, x far exceeds y. The median values for both variables approximate the central tendency, with the mean for the x variable at 150.5 and the y variable at 49, indicating that the data for both variables are balanced and devoid of notable outliers. The mode value for x is 1, as it is the smallest value that occurs most frequently; for y, the mode value is 36, as it is the value that is most likely to be sampled most often. The standard deviation of x (86.75) exceeds that of y (28.12), indicating that the variability in x is more pronounced around its mean than the y variability is. The standard deviation of x (299) significantly exceeds that of y (97), indicating a broader range of values for x than for y. These data elucidate the system's interaction with various offloading units to gain insights into how offloading influences data factors such as scalability, variability, and transmission rates, among others.

In experimental settings, normalized data are essential for consistency and comparability. The techniques are used to represent the normalized data in Figure 12 (a, b and c). The SF-style plot displays a three-dimensional surface plot. These methods complement each other to provide an alternative perspective on the distribution and attributes of the dataset. Analogous visualization methodologies can be employed to analyse normalized data in the 20%, 50% and 80% scenarios, allowing for a comprehensive comparison across varying degrees of data outsourcing.

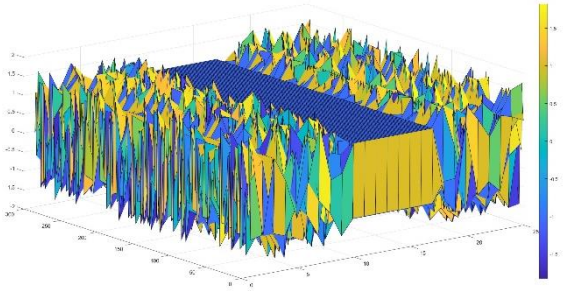


Fig. 12. (a) Normalizing result offloading 20% by Surf style plot visualization

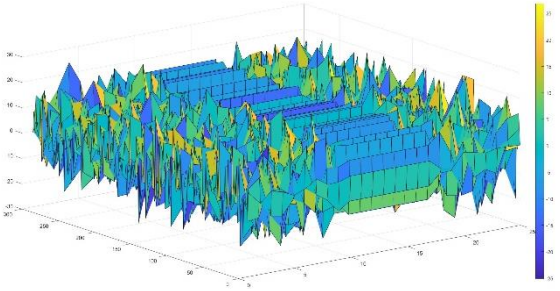


Fig. 12. (b) Normalizing result offloading 50% by Surf style plot visualization.

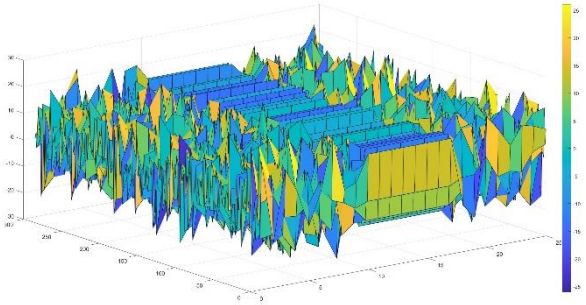


Fig. 12. (c) Normalizing result offloading 80% by Surf style plot visualization.

In addition, Table 6 displays the descriptive statistics of the normalized data for the three offloading scenarios: 20%, 50%, and 80%. The minimum and maximum values for x remain constant regardless of the offloading percentage employed, with the minimum set at 1 and the maximum set at 300. Consequently, the variability for x in all offloading situations is symmetrically distributed around the mean and median of 150.5. The mode for x is 1, indicating that the minimum value appears most frequently across all three circumstances. The standard deviation of 86.75 indicates that the x values exhibit

variability within a moderate range, whereas the range of 299 delineates the disparity between the least and maximum x values. The minimum value of y remains constant at -1.692, whereas the maximum value persists at 1.758 overall offloading situations, with y exhibiting relatively slight variance among the different scenarios. The mean of y is approximately 8.29e-17, indicating that the distribution of y is centred around zero and relatively unbiased. The median is -0.05619, indicating that half of the y values are below this threshold. The model is consequently -0.05186, representing the mean of the frequency distribution. The standard deviation for y is 1, indicating uniform variability across all distribution scenarios, whereas the range of 3.45 suggests that the variation is very small compared with the x values. Hence, examination of the three offloading rates—20%, 50%, and 80%—demonstrates that the normalized x and y values exhibit no significant alteration in statistical measurements as the percentage increases. The offloading percentage has a minimal impact on data dispersion, indicating that performance in terms of variability and the central tendency is consistently steady throughout all specified situations.

TABLE VI. DESCRIPTIVE STATISTICS OF NORMALIZED DATA FOR DIFFERENT OFFLOADING PERCENTAGES (20, 50, AND 80%).

Scenario	Statistics	x	y
Scenario 20%	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
Scenario 50%	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
Scenario 80%	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

4.3 Results of three scenarios (20%, 50%, and 80%) for the DPoS algorithm

The DPoS algorithm was implemented in three scenarios with participation rates of 20%, 50%, and 80%. The results are shown in Figures 13, 14, and 15 via Surf style plot visualization. The surf-style plot shows data points clustered near the central point, with average and middle values near zero.

Figure 14 depicts the DPoS algorithm results with an offloading percentage of 50%. Compared with the 20% offloading scenario, this visualization results in a wider spread of data points along both axes, indicating increased variability and dispersion. However, similar to the previous scenario, the mean and median values for both the x and y coordinates remain relatively close to zero. Figure 15 illustrates the outcomes of the DPoS algorithm when 80% of the workload is offloaded. The surf-style plot visualization demonstrates a greater expansion of the data distribution in comparison to the prior situations, as evidenced by data points that stretch farther away from the centre. Although the spread has expanded, the mean and median values for both the x and y coordinates remain near zero, indicating a balanced distribution despite the broader range.

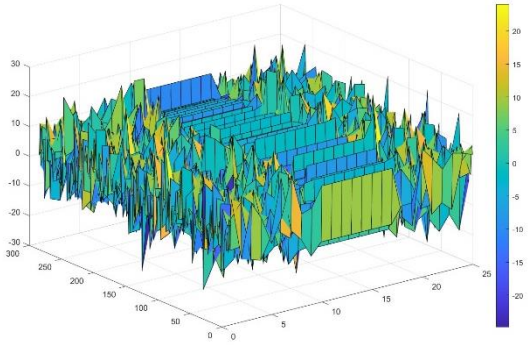


Fig. 13. Results of the DPoS algorithm offloading 20% by Surf style plot visualization.

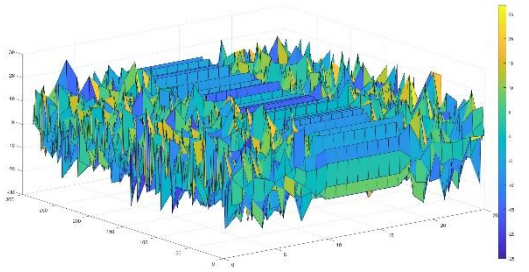


Fig. 14. Results of the DPoS algorithm offloading 50% by Surf style plot visualization.

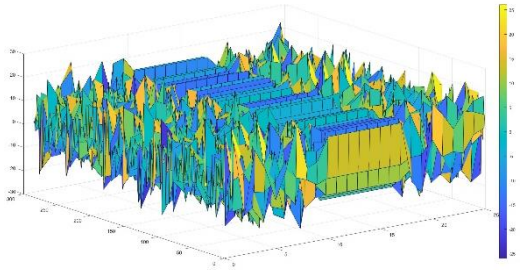


Fig. 15. Results of the DPoS algorithm offloading 80% by Surf style plot visualization.

Additionally, Table 7 shows the results of the DPoS algorithm on the basis of data offloading at the 20%, 50%, and 80% levels. The data distribution is normal and bell shaped, with a range of 1--300 and both a mean and median of 150.5. The mode of x is 1, indicating that the smallest value of x occurs with the highest frequency. The coefficient of variation is considerably significant, and absolute measures of dispersion are also notably high; additionally, the standard deviation is 299, indicating the spread from minimum to greatest values. The minimum values of y are closely aligned, whereas the maximum value of y decreases with increasing offloading ratio, as anticipated. However, at a 20% offloading rate, its value exceeds approximately 96% of the ideal value, with offloading ultimately ceasing as d increases, culminating in zero offloading at 100%. The mode for y is variable, equating to -13.95, -23.25, and -7.778 for the 20%, 50%, and 80% failure rates, respectively. This investigation allows us to ascertain the effects of different offloading rates on the data distribution and the optimized DPoS algorithm within a DEC-IoT healthcare system.

TABLE VII. DPOS ALGORITHM RESULTS AND DATA OFFLOADING RATES OF 20%, 50%, AND 80%.

Metric	Scenario 20%	Scenario 50%	Scenario 80%
Min (x)	1	1	1
Max (x)	300	300	300
Mean (x)	150.5	150.5	150.5
Median (x)	150.5	150.5	150.5
Mode (x)	1	1	1
Std (x)	86.75	86.75	86.75
Range (x)	299	299	299

Min (y)	-24.85	-23.25	-21.88
Max (y)	22.29	21.56	19.41
Mean (y)	0.04084	-0.004727	-0.0081
Median (y)	-0.1743	-0.2408	-0.2459
Mode (y)	-13.95	-23.25	-7.778
Std (y)	7.172	8.063	7.978
Range (y)	47.14	44.81	41.29

The performance of the DPoS algorithm in decentralized healthcare systems is evaluated via different outsourcing percentages (20%, 50%, and 80%). Outsourcing percentages significantly impact the data distribution, scalability, efficiency, dependability, and stability. Higher percentages indicate greater scalability, whereas 20% may indicate constraints due to precise data distribution. The mean and median values of the DPoS algorithm outputs remain near zero, indicating a well-balanced distribution. Standard deviations show increased variability in stability and dependability, indicating the system's ability to adapt to various stresses. Comparing different scenarios allows for a comprehensive understanding of the DPoS algorithm's effectiveness in decentralized healthcare systems.

5. RESULTS AND DISCUSSION

The delegated proof of stake (DPoS) algorithm is used to evaluate the performance of a decentralized healthcare system in various scenarios. The system's performance is assessed through metrics such as scalability, centralization of power, privacy concerns, data storage access, regulatory compliance, decentralization effectiveness, and data integrity security. The system's performance changes as the amount of data offload varies, providing crucial insights into its behaviour and potential consequences for practical applications. The analysis of performance metrics across different scenarios helps in evaluating the system's effectiveness and guiding potential improvements for real-world deployment. The delegated proof algorithm plays a crucial role in ensuring the security and efficiency of healthcare systems. Additionally, Tables 8 and 9 provide a detailed analysis of the statistical metrics and their explanations for a system, highlighting average and median values, standard deviations, patterns, consistent performance levels, and overall system attributes.

TABLE VIII COMPARES PERFORMANCE METRICS ACROSS DIFFERENT SCENARIOS, REVEALING DECENTRALIZED HEALTHCARE SYSTEM EFFECTIVENESS UNDER VARYING DATA OFFLOADING CONDITIONS AND GUIDING REAL-WORLD DEPLOYMENT IMPROVEMENTS.

Scenario	Metric	Mean	Median	Std
20%	Scalability	0.0060	0.0060	0.0000
	Centralization Of Power	7.0920	7.0920	0.0000
	Privacy Concern	-0.1930	-0.1930	0.0000
	Data Storage Accesses	6.8223	6.8223	0.0000
	Regulatory Compliance	-0.4954	-0.4954	0.0000
	Decentralization Effectiveness Efficiency	7.1609	7.1609	0.0000
	Data Integrity Security	-0.0707	-0.0707	0.0000
	Data Privacy Confidentiality	7.1489	7.1489	0.0000
50%	Scalability	0.0566	0.0566	0.0000
	Centralization Of Power	8.2013	8.2013	0.0000
	Privacy Concern	-0.0050	-0.0050	0.0000
	Data Storage Accesses	7.8569	7.8569	0.0000
	Regulatory Compliancy	0.4377	0.4377	0.0000
	Decentralization Effectiveness Efficiency	8.2198	8.2198	0.0000
	Data Integrity Security	-0.0790	-0.0790	0.0000
	Data Privacy Confidentiality	8.3354	8.3354	0.0000
80%	Scalability	-0.0569	-0.0569	0.0000
	Centralization Of Power	8.7759	8.7759	0.0000
	Privacy Concern	0.1165	0.1165	0.0000
	Data Storage Accesses	8.7198	8.7198	0.0000
	Regulatory Compliancy	-0.1098	-0.1098	0.0000
	Decentralization Effectiveness Efficiency	8.7645	8.7645	0.0000
	Data Integrity Security	0.1952	0.1952	0.0000
	Data Privacy Confidentiality	8.6173	8.6173	0.0000

TABLE IX. COMPARISON OF STATISTICAL MEASURES AND INTERPRETATIONS FOR SYSTEM FACTORS

Factor	Mean and Median	Standard Deviation	Additional Comments
Scalability	Negative	Zero	Potential decrease, consistent performance
Centralization of Power	High	Zero	Centralized structure, consistent distribution
Privacy Concern	Positive	Zero	Moderate concern, consistent levels
Data Storage Accesses	High	Zero	Efficient storage and access, consistent performance
Regulatory Compliance	Negative	Zero	Potential compliance issues, consistent concern
Decentralization Efficiency	High	Zero	Effective and efficient decentralization, consistent performance
Data Integrity Security	Positive	Zero	Moderate concern, consistent levels
Data Privacy Confidentiality	High	Zero	Efficient privacy and confidentiality, consistent performance

5.1 Normalization process

Figure 16 and Figure 17 detail the original data and normalization procedure, a crucial step in ensuring data standardization across various contexts and removing inherent biases and discrepancies for meaningful comparisons and analysis.

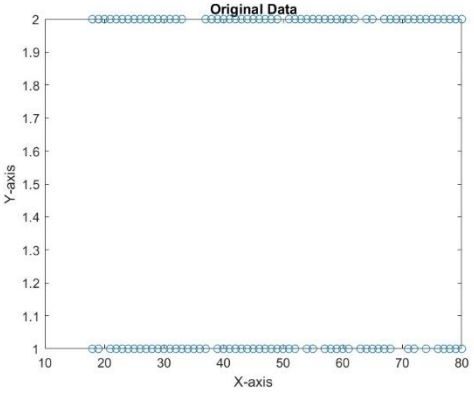


Fig. 16. Original data for the framework.

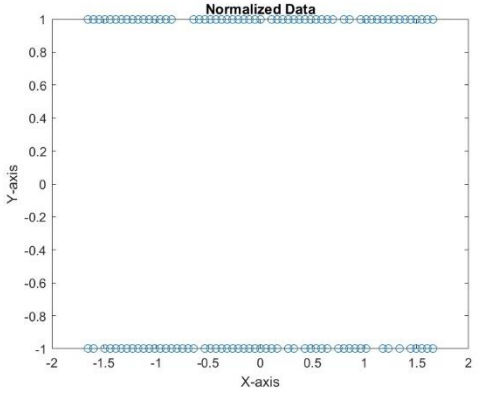
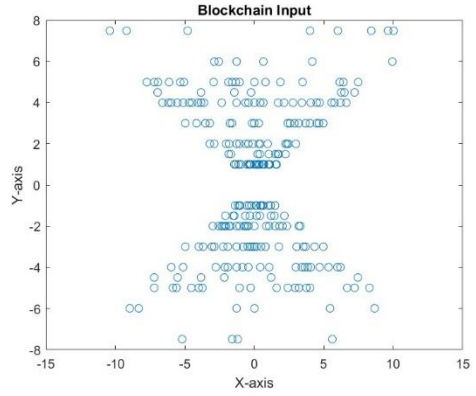


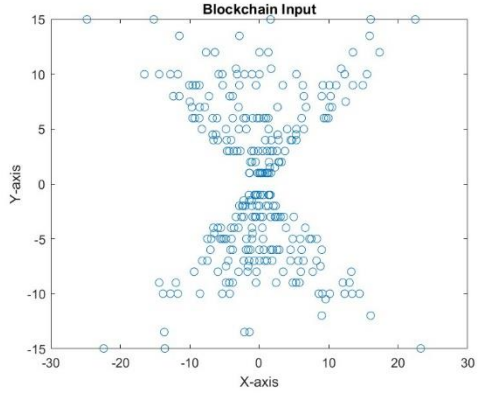
Fig. 17. Normalize the data for the framework.

The above results for the normalized data for three scenarios (20%, 50%, and 80% offloading) provide visual representations of the performance metric distributions. These results help identify trends and patterns, allowing for better interpretation and analysis of performance metrics. The normalization process ensures fair comparisons, allowing for robust conclusions about the decentralized healthcare system's effectiveness and response to different data offloading levels.
An examination is conducted on the input and output data of the centralized blockchain, alongside the results obtained from blockchain one and blockchain two under three different outsourcing scenarios (20%, 50%, and 80%). There will be a detailed look at how the centralized blockchain system handles data compared with the decentralized approach used by Blockchain One and Blockchain Two (BC1 and BC2). Three different situations are used as examples.

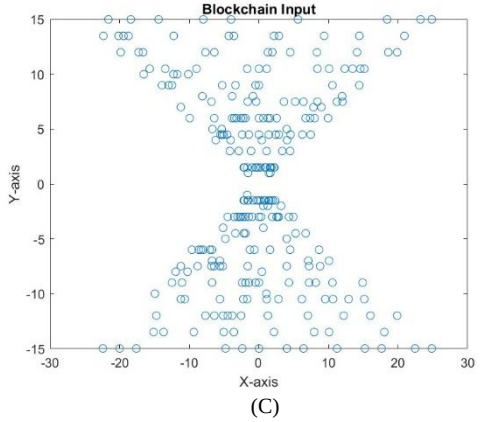
Figure 18 (A, B, and C) shows the input data for three scenarios, including decentralized healthcare system factors such as patient information, transaction details, and security measures, illustrating the centralized blockchain's initial state and specific data points.



(A)



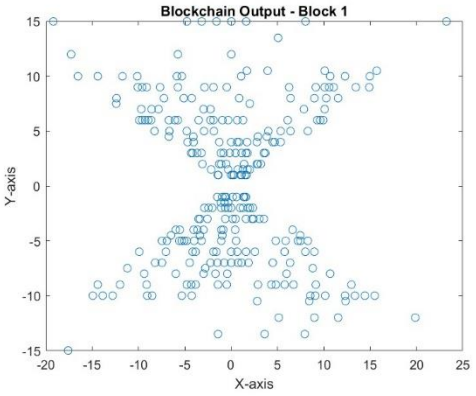
(B)



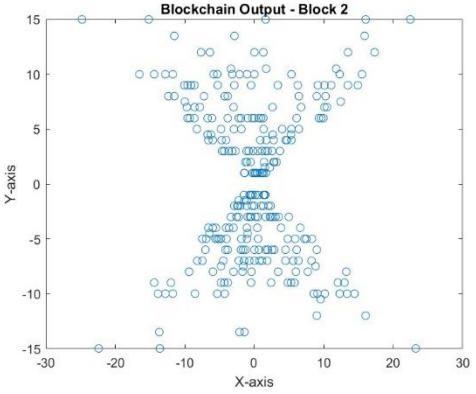
(C)

Fig. 18. (A, B, and C): Data for BC for the framework in three scenarios (20%, 50%, and 80%) for data offloading.

Figure 19 (A and B) shows data offloading for BC1 and BC2 in different scenarios (20%, 50%, and 80%). The data pertain to BC1 and BC2 in the first scenario, 50% allocation in the second scenario, and an 80% offloading rate in the third scenario. The statistics showcase the output data of the decentralized approach, highlighting any differences or improvements compared with a centralized blockchain, including transaction speed, data integrity, security measures, and system performance.



(A) Output data for BC1 in the 1st scenario when 20% of the data are offloaded

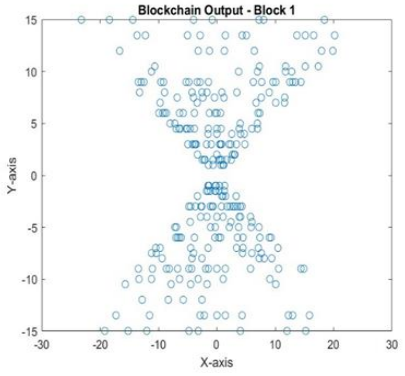


(B) Output data for BC2 in the 1st scenario when 20% of the data are offloaded

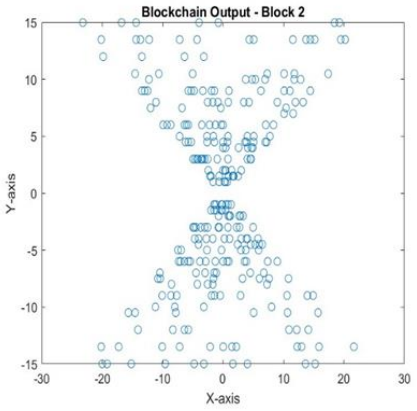
Fig. 19. (A and B). Output data for BC1 and 2 in the 1st scenario in the 20% case for the framework.

A comparative examination Through the results presented in this section, the input and output data of the centralized blockchain and the decentralized approach can be compared. By conducting a visual examination of the data generated by the decentralized blockchain in contrast to the data processed by the centralized blockchain, readers can identify any discrepancies, inefficiencies, or improvements that may arise from the decentralization process. This comparison provides critical insights into the effectiveness of the decentralized approach in addressing critical challenges and enhancing system performance.

Through an analysis of the input and output data, substantial insights can be gained concerning the impact of decentralization on the efficacy of the healthcare system, as illustrated in Figures 20 and 21. The identification of discrepancies or advancements between the input and output data of the centralized blockchain could yield significant knowledge for decision-making and guide subsequent enhancements to the decentralized framework. Moreover, this section provides significant insights into the benefits of decentralization in healthcare systems, specifically concerning scalability, efficiency, and security.

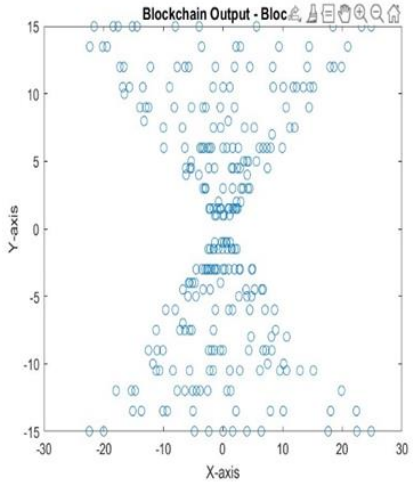


(A) Output data for BC1 in the 2nd scenario when 50% of the data are offloaded.

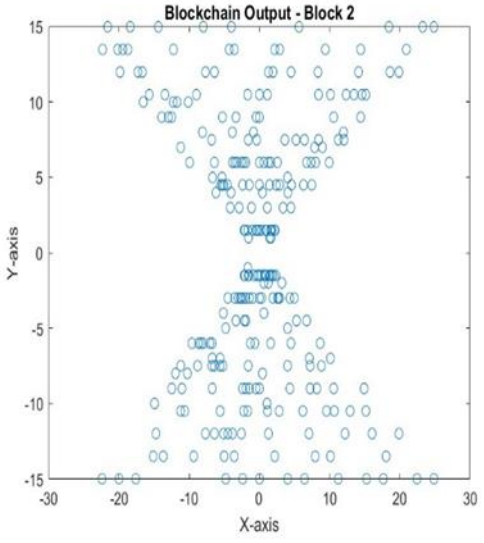


(B) Output data for BC2 in the 2nd scenario when 50% of the data are offloaded.

Fig. 20. (A and B). Output data for BC1 and 2 in the 2nd scenario in the 50% case for the framework.



(A) Output data for BC1 in the 3rd scenario when 80% of the data are offloaded.



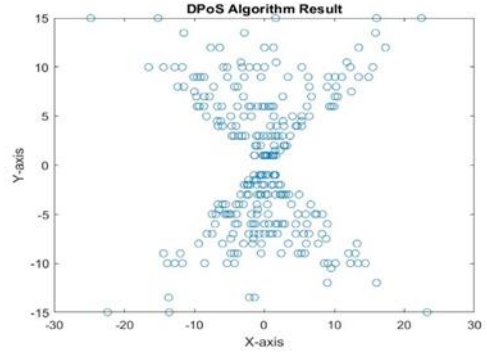
(B) Output data for BC2 in the 3rd scenario when 80% of the data are offloaded.

Fig. 21. (A and B). Output data for BC1 and 2 in the 3rd scenario in the 80% case for the framework.

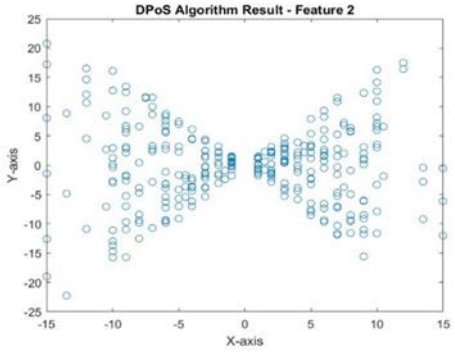
5.2 Results of the DPoS Algorithm

Within the framework of the decentralized healthcare system, we investigate the outcomes of the DPoS algorithm for three different offloading scenarios: 20%, 50%, and 80%. The purpose of this section is to analyse the performance of the DPoS algorithm in terms of supporting efficient transaction processing, building consensus among participants in the network, and maximizing resource use.

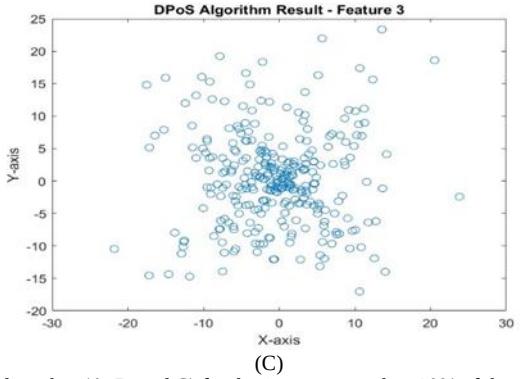
The DPoS performance evaluation results are shown in Figure 22 (A, B, and C) for the starting condition with 20% data offloading. The second situation with a 50% data offloading rate is shown in Figure 23 (A, B, and C), whereas the third scenario with an 80% rate is shown in Figure 24 (A, B, and C). The transaction processing speed, consensus mechanism, and resource utilization are measured. These statistics reveal the algorithm's decentralized consensus and network efficiency performance. Reading performance statistics can help users evaluate the DPoS algorithm's potential to scale and safeguard healthcare.



(A)

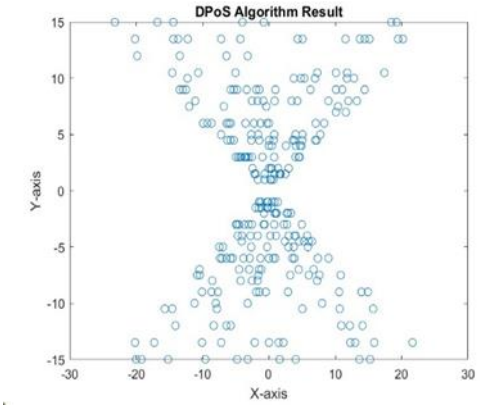


(B)

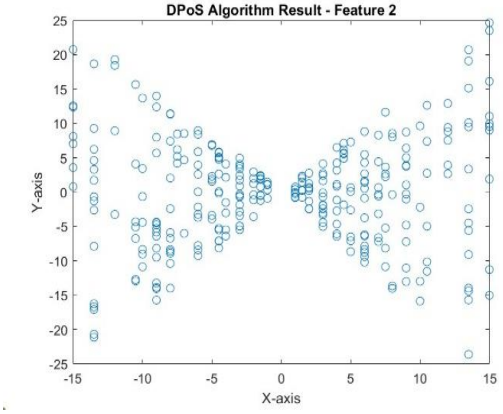


(C)

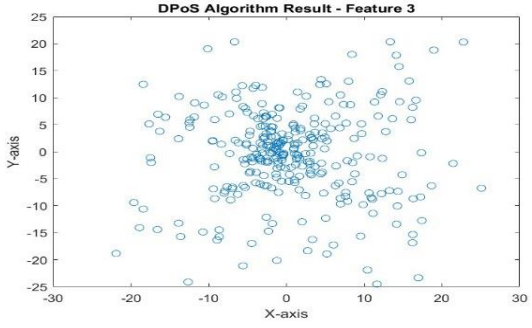
Fig. 22. DPoS algorithm (A, B, and C) for the 1st scenario when 20% of the data are offloaded



(A)

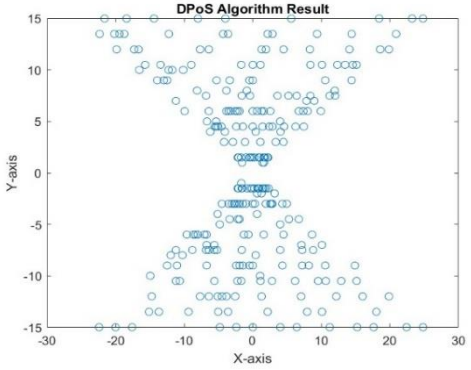


(B)

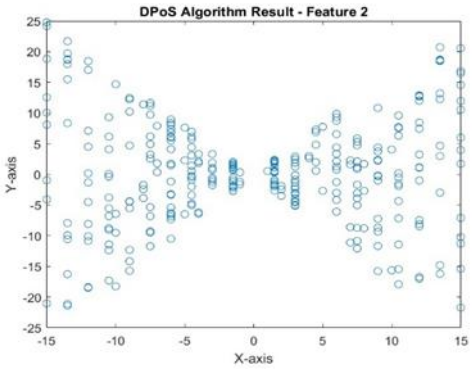


(C)

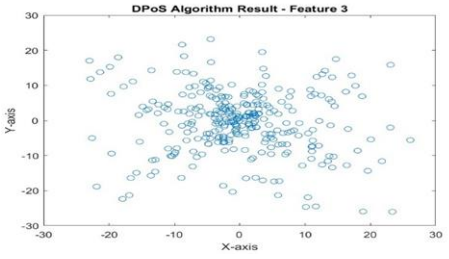
Fig. 23. DPoS algorithm (A, B, and C) for the 2nd scenario when 50% of the data are offloaded.



(A)



(B)



(C)

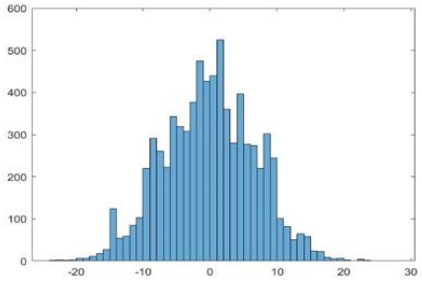
Fig. 24. DPoS algorithm (A, B, and C) for the 3rd scenario when 80% of the data are offloaded.

Decentralized healthcare applications rely significantly on the DPoS algorithm, which enhances the effectiveness of consensus procedures, transaction processing, and network security. The performance is graphically represented through infographics that highlight critical metrics, including transaction processing speed, consensus-achieving strategies, and the block generation rate. Acquiring a thorough comprehension of the advantages and disadvantages of the algorithm is critical to integrate it seamlessly into healthcare applications. By conducting an examination of patterns and trends in outcomes, stakeholders are able to assess the potential benefits and challenges of the algorithm, thereby providing guidance for decision-making regarding its implementation. In decentralized healthcare environments, the efficacy of the DPoS algorithm is of the utmost importance, as it improves network security, consensus procedures, and transaction processing.

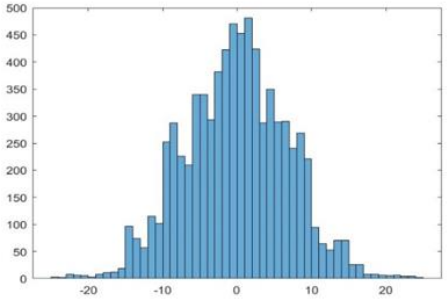
5.3 Blockchain (BC1 and BC2) Output Data Analysis

The data from two blockchain outputs are evaluated after offloading at 20%, 50%, and 80%. This approach examines the distribution and patterns of data from the decentralized offloading process in the healthcare sector. Furthermore, the assessment assesses the system's efficiency in processing and distributing data by testing different levels of offloading. The process commences by employing a data analysis methodology and providing a comprehensive explanation of the procedure for analysing blockchain output data after transferring data from the centralized system to decentralized nodes. The assessment assesses transaction volumes, processing times, data storage use, and network performance. A careful analysis may help us understand how decentralized design influences healthcare data processing and distribution.

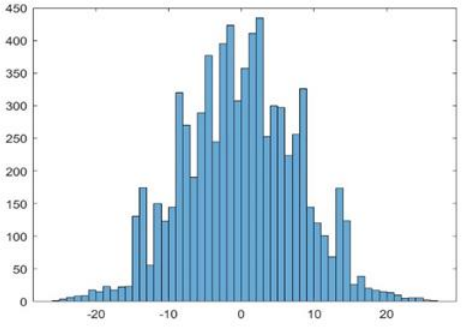
The results are employed as figures and histograms to visually illustrate the flow of output data in a blockchain. The graphs illustrate the distributions, trends, and patterns of decentralized offloading. Plot-style statistics display fluctuations in transaction volumes or processing times over some time, whereas histogram-style figures illustrate the distribution of data across different parameters. The findings for the initial 20% decline in data transmission are displayed in Figure 25 (A and B), which represent the BC1 and BC2 results. Figure 26 (A and B) displays the BC1 and BC2 results for the second situation when 50% of the data are sent. The results for BC1 and BC2 (A and B) in the third scenario, with 80% data transfer, are displayed in Figure 27 (A and B).



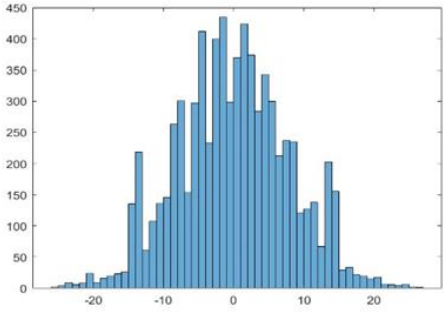
(A) Results of BC1 for the 1st scenario in the case of 20% data offloading, using histogram style.



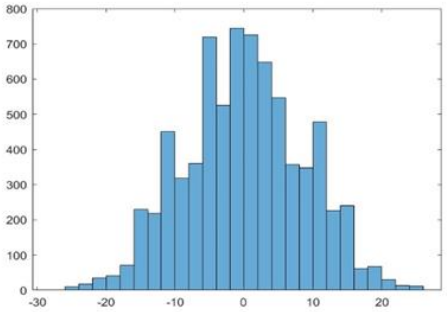
(B) Results of BC2 for the 1st scenario in the case of 20% data offloading, using histogram-style methods.
Fig. 25. (A and B) Results for BC1 and BC2 for the 1st scenario in the case of 20% data offloading.



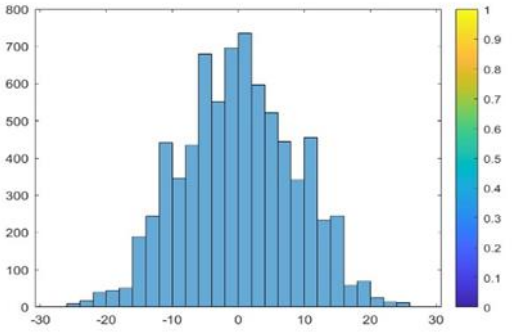
(A) Results of BC1 for the 2nd scenario when 50% of the data are offloaded, according to a histogram.



(B) Results of BC2 for the 2nd scenario in the case of 50% data offloading, using histogram style.
Fig. 26. (A and B) Results for BC1 and BC2 for the 2nd scenario in the case of 50% data offloading.



(A) Results of BC1 for the 3rd scenario when 80% of the data are offloaded, according to a histogram.



(B) Results of BC2 for the 3rd scenario in the case of 80% data offloading, using histogram style.
Fig. 27. (A and B) Results for BC1 and BC2 for the 3rd scenario in the case of 80% data offloading.

The visuals in the blockchain output data analysis are interpreted to understand the results. This interpretation examines data distribution trends, anomalies, and patterns and their effects on system performance. We can determine how decentralized offloading impacts healthcare data distribution, processing efficiency, and network performance by analysing the findings.

Thus, blockchain output data analysis illuminates the effects of decentralized offloading on healthcare system performance. Additionally, the study shows how offloading data to decentralized nodes affects the data distribution, processing efficiency, and network performance. These insights are essential for understanding healthcare application decentralized architecture benefits and drawbacks.

5.4. Limitations of study

The study explores the implementation of a decentralized healthcare system via the delegated proof of stake (DPoS) algorithm and blockchain technology. However, this study has several limitations that need to be addressed in future research, including the following:

a) The simulation of the health system conducted via MATLAB software does not fully represent the actual conditions of the health system.
b) Challenges related to extensibility persist and become increasingly evident when millions of IoT devices or extensive healthcare systems are overseeing.
c) It presents only the outcomes of synthetic and predefined scenarios, which may significantly diverge from actual healthcare data and circumstances.
d) Energy consumption modelling considers the general power parameters of devices, which are not optimal for various healthcare systems.
e) There is no comparison with certain other BFT consensus algorithms, nor is there an analysis of the advantages and disadvantages of merging this model with another.
f) The research inadequately addresses the challenges of adopting compliance with standards such as the GDPR and HIPAA across several jurisdictions within global healthcare enterprises.
g) The proposed framework design amalgamates many technologies, which may provide diverse technical, logistical, and financial challenges inside healthcare organizations throughout implementation.

6. COMPARISON WITH PREVIOUS STUDIES

Tables 10 and 11 provide a comprehensive comparison of our approach to decentralized healthcare systems, highlighting its distinctive features and advancements. The table consists of rows representing various components of the system and columns comparing our approach with prior methods. The purpose is to evaluate the unique contributions, innovations, and improvements that set our approach apart from the current literature. This comprehensive comparison demonstrates the unique value proposition of our study in promoting decentralized healthcare system progress.

TABLE X. COMPARISON OF THE NOVEL APPROACH WITH THOSE OF PREVIOUS STUDIES [34-38].

Aspect	Novel Approach	Previous Studies
Scalability	High	Moderate
Centralization of Power	Low	High
Privacy Concerns	Addressed	Partially Addressed
Data Storage Accesses	Efficient	Limited
Regulatory Compliance	Compliant	Varied
Decentralization Effectiveness	Effective	Limited Effect
Data Integrity Security	Robust	Vulnerable
Data Privacy Confidentiality	Strong	Weak
Performance Metrics	Optimal	Mixed
Technological Innovation	Advanced	Conventional
Adoption in Practice	Limited	Established

A comparative analysis of various studies on decentralized healthcare systems highlights their unique contributions, such as scalability, decentralization, security, privacy, and regulatory compliance. This table provides a comprehensive comparison tool, highlighting the methodology, security concerns, primary objectives, and year of publication. It serves as a tool to contextualize the study within the broader landscape of decentralized healthcare systems research, highlighting the unique contributions of each study.

TABLE XI. COMPARATIVE ANALYSIS OF DECENTRALIZED HEALTHCARE SYSTEMS IN OUR STUDY AND OTHER STUDIES.

Study	Applied Application	Methodology	Security Concerns	Objectives	Comparison with Our Study	Year
[41]	System for Managing and Sharing Medical Records	System for Managing and Sharing Medical Records	Confidentiality, integrity, availability, and privacy of data	Development of a Distributed Ledger Technology (DLT)-based Data Management Platform	Improvement of a Distributed Ledger Technology (DLT)-based Data Management Platform in BC and employing a decentralized healthcare system using blockchain and DPoS algorithm, focusing on scalability, Decentralization, and security aspects.	2020
[42]	RPM (Remote Patient Medicine) and Telemedicine	Bridging the gap between blockchain and the healthcare industry	Data collection, patient monitoring, privacy, and data security.	Safe and reliable remote patient monitoring (RPM) using blockchain	study explores a decentralized healthcare system, providing insights into scalability, centralization of power, privacy concerns, and regulatory compliance.	2021
[43]	Electronic Health Record (EHR) System	Blockchain automation for population-level data collection	Data security, decentralization, data accessibility, integrity	Improved EHR system security and usability with blockchain technology	study investigates the performance of a decentralized healthcare system using blockchain and DPoS algorithm, addressing scalability and security challenges.	2021
[32]	Data Storage & Security	Improving technological advantages of blockchain applications	Safety, authorization, integrity, and data transfer	Development of secure data transmission and storage systems	our study presents a decentralized healthcare system employing blockchain and DPoS algorithm, focusing on decentralization, security, and regulatory compliance.	2022
[33]	Data Analysis, Computation on Edge and Cloud	Building a blockchain-based social network	Information safety, administration, dependability, accuracy	Enhancing decision-making by combining blockchain with other platforms	Your study evaluates a decentralized healthcare system using blockchain and DPoS algorithm, emphasizing scalability, decentralization, and data integrity.	2023
Our study	Decentralized Healthcare System	Utilizing blockchain and DPoS algorithm	Privacy, decentralization, security, scalability	Advancing decentralized healthcare systems	Our study compares the performance metrics of the decentralized healthcare system under different scenarios, focusing on scalability, centralization, privacy, and regulatory compliance.	2024

7. CONCLUSION

In this study, we explore the implementation of a decentralized healthcare system that uses the DPoS algorithm and blockchain technology to address challenges associated with decentralization, privacy, and legal compliance. The decentralized system demonstrates that DPoS and blockchain technology possess superior attributes of scalability, uniqueness, and efficiency relative to a traditional centralized system. These recommendations would significantly benefit any organization intending to adopt the system, while the insights derived from this study would be crucial for evaluating the system's effectiveness. Blockchain technology and delegated proof of stake (DPoS) have been implemented across various business sectors; however, this research conceptualizes these technologies inside a decentralized Internet of Things (IoT) healthcare model for real-time applications. Medical data transfer addresses issues related to data privacy, security, and transmission. The new integration of these technologies constitutes an innovation in this field. This decentralized system improves security via secrecy, integrity, and scalability, making it feasible and sustainable for implementation. This research significantly contributes to the current understanding of blockchain applications in healthcare systems and offers guidance for the continued development of decentralized healthcare ecosystems. Nevertheless, the fundamental DPoS algorithm continues to exhibit deficiencies, particularly in terms of node and transaction scalability. Subsequent studies may explore enhancements to the DPoS algorithm or investigate alternative consensus methods that offer superior scalability without compromising security. Likewise, data-oblivious computing utilizing technologies such as zero-knowledge proofs will enhance data security. Emerging advances in blockchain technology offer opportunities for the development of additional chains and protocols that facilitate the integration of different systems into a cohesive complex, addressing issues of scalability and interoperability. Future research may explore the application of machine learning and artificial intelligence in the development of diverse prognostic models and investigate how smart contracts might enhance healthcare optimization and patient treatment.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

No funding was received.

Acknowledgement

I want to thank everyone who helped with this work.

References

[1] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, and L. Khoukhi, "IoT technologies for smart cities," *IET Networks*, vol. 7, no. 1, pp. 1–3, Jan. 2018.
[2] F. Wortmann and K. Flüchter, "Internet of things: technology and value added," *Business & Information Systems Engineering*, vol. 57, pp. 221–224, Jun. 2015.
[3] S. Shukla, M. F. Hassan, M. K. Khan, L. T. Jung, and A. Awang, "An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment," *PLoS One*, vol. 14, no. 11, p. e0224934, Nov. 2019.
[4] A. Brogi and S. Forti, "QoS-aware deployment of IoT applications through the fog," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1185–1192, May 2017.
[5] M. Alicherry and T. V. Lakshman, "Optimizing data access latencies in cloud systems by intelligent virtual machine placement," in *2013 Proceedings IEEE INFOCOM*, Apr. 2013, pp. 647–655.
[6] S. Abirami and P. Chitra, "Energy-efficient edge based real-time healthcare support system," in *Advances in Computers*, vol. 117, no. 1, Elsevier, Jan. 2020, pp. 339–368.
[7] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," *Journal of Infection and Public Health*, vol. 13, no. 10, pp. 1567–1575, Oct. 2020.
[8] N. Singh and A. K. Das, "Energy-efficient fuzzy data offloading for IoMT," *Computer Networks*, vol. 213, p. 109127, Aug. 2022.
[9] S. Y. Mohammed and M. Aljanabi, "Human-Centric IoT for Health Monitoring in the Healthcare 5.0 Framework Descriptive Analysis and Directions for Future Research", EDRAAK, vol. 2023, pp. 21–26, Mar. 2023, doi: 10.70470/EDRAAK/2023/005.
[10] A. H. Sodhro et al., "Decentralized energy efficient model for data transmission in IoT-based healthcare system," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, Apr. 2021, pp. 1–5.

[11] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology," *Future Generation Computer Systems*, vol. 129, pp. 380–388, Apr. 2022.
[12] J. J. Kang et al., "An energy-efficient and secure data inference framework for internet of health things: a pilot study," *Sensors*, vol. 21, no. 1, p. 312, Jan. 2021.
[13] Mohammad Aljanabi, “Safeguarding Connected Health: Leveraging Trustworthy AI Techniques to Harden Intrusion Detection Systems Against Data Poisoning Threats in IoMT Environments”, BJIoT, vol. 2023, pp. 31–37, May 2023.
[14] O. Albahri, A. Alamleh, T. Al-Quraishi, and R. Thakkar, “Smart Real-Time IoT mHealth-based Conceptual Framework for Healthcare Services Provision during Network Failures ”, Applied Data Science and Analysis, vol. 2023, pp. 110–117, Nov. 2023.
[15] A. Sharma, Sarishma, R. Tomar, R. Chilamkurti, and B. G. Kim, "Blockchain based smart contracts for internet of medical things in e-healthcare," *Electronics*, vol. 9, no. 10, p. 1609, Oct. 2020.
[16] H. S. Anbarasan and J. Natarajan, "Blockchain-based delay and energy harvest aware healthcare monitoring system in WBAN environment," *Sensors*, vol. 22, no. 15, p. 5763, Aug. 2022.
[17] A. M. Shanshool, “Exploring the Role of Block-chain in IoT-Driven Healthcare Solutions”, BJN, vol. 2023, pp. 82–88, Oct. 2023.
[18] I. Al Barazanchi and W. . Hashim, “Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach”, SHIFRA, vol. 2023, pp. 10–16, Feb. 2023, doi: 10.70470/SHIFRA/2023/002.
[19] L. Liu and Z. Li, "Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things," *IEEE Access*, vol. 10, pp. 53640–53651, May 2022.
[20] A. Lakhan et al., "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 664–672, Feb. 2022.
[21] A. K. Bhardwaj, P. Dutta, and P. Chintale, “AI-Powered Anomaly Detection for Kubernetes Security: A Systematic Approach to Identifying Threats”, Babylonian Journal of Machine Learning, vol. 2024, pp. 142–148, Aug. 2024.
[22] S. A. Abed, “Big Data and Artificial Intelligence on the Blockchain: A Review ”, Babylonian Journal of Artificial Intelligence, vol. 2023, pp. 1–4, Jan. 2023.
[23] A. Lakhan et al., "Hybrid workload enabled and secure healthcare monitoring sensing framework in distributed fog-cloud network," *Electronics*, vol. 10, no. 16, p. 1974, Aug. 2021.
[24] A. Lakhan et al., "Smart-contract aware ethereum and client-fog-cloud healthcare system," *Sensors*, vol. 21, no. 12, p. 4093, Jan. 2021.
[25] H. Wu et al., "EEDTO: An energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2163–2176, Oct. 2020.
[26] S. Singh and D. Kumar, "Energy-efficient secure data fusion scheme for IoT-based healthcare system," *Future Generation Computer Systems*, vol. 143, pp. 15–29, Jun. 2023.
[27] S. Jain and R. Doriya, "Security framework to healthcare robots for secure sharing of healthcare data from cloud," *International Journal of Information Technology*, vol. 14, no. 5, pp. 2429–2439, Aug. 2022.
[28] V. Pawar and S. Sachdeva, "ParallelChain: a scalable healthcare framework with low-energy consumption using blockchain," *International Transactions in Operational Research*, vol. 31, no. 6, pp. 3621–3649, Nov. 2024.
[29] M. T. Quasim, F. Algarni, A. A. Radwan, and G. M. Alshmrani, "A blockchain-based secured healthcare framework," in *2020 International Conference on Computational Performance Evaluation (ComPE)*, Jul. 2020, pp. 386–391.
[30] P. Hemalatha, "Monitoring and securing the healthcare data harnessing IoT and blockchain technology," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 2554–2561, Apr. 2021.
[31] C. Singh et al., "Medi-Block record: Secure data sharing using blockchain technology," *Informatics in Medicine Unlocked*, vol. 24, p. 100624, Jan. 2021.
[32] M. U. Chelladurai, S. Pandian, and K. Ramasamy, "A blockchain-based patient-centric electronic health record storage and integrity management for e-Health systems," *Health Policy and Technology*, vol. 10, no. 4, p. 100513, Dec. 2021.
[33] M. Verdonck and G. Poels, "Decentralized data access with IPFS and smart contract permission management for electronic health records," in *Business Process Management Workshops: BPM 2020 International Workshops*, Springer International Publishing, 2020, pp. 5–16.
[34] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, p. 164, Aug. 2017.
[35] A. R. Rajput, Q. Li, and M. T. Ahvanooey, "A blockchain-based secret-data sharing framework for personal health records in emergency condition," *Healthcare*, vol. 9, no. 2, p. 206, Feb. 2021.
[36] Q. Xia et al., "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, Apr. 2017.

[37] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: applying blockchain to securely and scalably share clinical data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, Jan. 2018.
[38] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, Jun. 2017, pp. 137–141.
[39] E. M. Adere, "Blockchain in healthcare and IoT: A systematic literature review," *Array*, vol. 14, p. 100139, Jul. 2022.
[40] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: applications in health care," *Circulation: Cardiovascular Quality and Outcomes*, vol. 10, no. 9, p. e003800, Sep. 2017.
[41] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018.
[42] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.
[43] A. Howell, T. Saber, and M. Bendechache, "Measuring node decentralisation in blockchain peer-to-peer networks," *Blockchain: Research and Applications*, vol. 4, no. 1, p. 100109, Mar. 2023.