Eksplorium *p*-ISSN 0854-1418
Volume 46 No. 1, May 2025: 281–293 *e*-ISSN 2503-426X

Secure And Scalable EHR Management Via Dynamic Consensus and Privacy-Preserving Blockchain

[1]B. Arulmozhi, [2]Dr. J. I. Sheeba, [3]Dr S. Pradeep Devaneyan

[1]Research Scholar, Department of Computer Science and Engineering,

Puducherry Technological University, Puducherry-605014, India,

ammuarulmozhi@ptuniv.edu.in

[2]Associate Professor, Department of Computer Science and Engineering,

Puducherry Technological University, Puducherry-605014, India.

sheeba@ptuniv.edu.in

[3]Professor, Department of Mechanical Engineering,

Sri Venkateswara College of Engineering and Technology, Puducherry-605012, India

pr.signs@gmail.com

Article Received: 15 Feb 2025, Revised: 14 April 2025, Accepted:08 May 2025

Abstract: Information flexibility and confidentiality have become significant challenges as medical information management increasingly relies on digital platforms. The centrally controlled structures of current medical systems are problematic due to their vulnerability to information breaches, inefficiencies, and lack of transparency. Establishing consensus in distributed networks while maintaining flexibility and security presents numerous obstacles. To address these issues, this study proposes a Privacy-Preserving Blockchain Framework (PPBF) combined with a Dynamic Elastic Consensus Protocol (DECP) for secure and sustainable handling of medical information. The PPBF leverages advanced cryptographic techniques such as homomorphic encryption and zero-knowledge proofs to safeguard sensitive medical data. DECP dynamically adapts to network conditions to enhance throughput and reduce delays during the consensus process. The proposed system aims to deliver a flexible, decentralized, and secure system capable of efficiently managing large volumes of medical information. Research findings indicate that the framework outperforms existing transaction throughput, flexibility, and security solutions. The proposed system demonstrates up to a 40% improvement in consensus efficiency while preserving patient data privacy and achieves over 95% accuracy in maintaining data integrity. This paper presents a robust approach to overcoming existing challenges in secure information management and establishes a foundation for advancing blockchain-based applications in healthcare.

Keywords: Dynamic Elastic Consensus Protocol, Privacy-Preserving Blockchain, Secure Healthcare Data Management, Scalable Blockchain Solutions, Homomorphic Encryption, Zero-Knowledge Proofs, Decentralized Healthcare Systems, Data Integrity, Cryptographic Techniques, Healthcare Data Privacy.

1. INTRODUCTION

In recent years, there has been a growing focus on the application of blockchain technology in conjunction with tamper-proof and traceable medical Internet of Things (IoT) systems to enhance safety and security. Researchers are actively investigating the development of blockchain-based secure IoT technologies in healthcare to protect the confidentiality of shared healthcare data and ensure the reliability of smart healthcare devices [1]. While several challenges remain demonstrate the significant potential of blockchain to improve the safety and reliability of healthcare IoT applications. Decentralized organizations must collaborate effectively within blockchain-based medical services to ensure the continuous operation of these systems [2]. To mitigate the risk of malicious services and performance degradation, efficient incentive mechanisms are essential. By using incentives and penalties encourage participants to provide high-quality services reduce the risk of information leakage and manipulation and prevent resource misuse and harmful competition [3].

Reputation evaluation is a common basis for designing incentives in blockchain-powered medical service platforms. A dynamic reputation score is created through a behavioral assessment framework takes into account the participants' past conduct [4]. Blockchain-based medical service delivery systems with incentive mechanisms lacks sufficient integration of feedback incentives for blockchain consensus processes and comprehensive reputation evaluation designs for multiple entities [5]. The absence of a robust multifaceted evaluation system could undermine fairness and reduce user engagement. Insufficient consensus mechanism upgrades might result in reputation evaluation being poorly connected to the distributed ledger can decrease user participation in the consensus process [6].

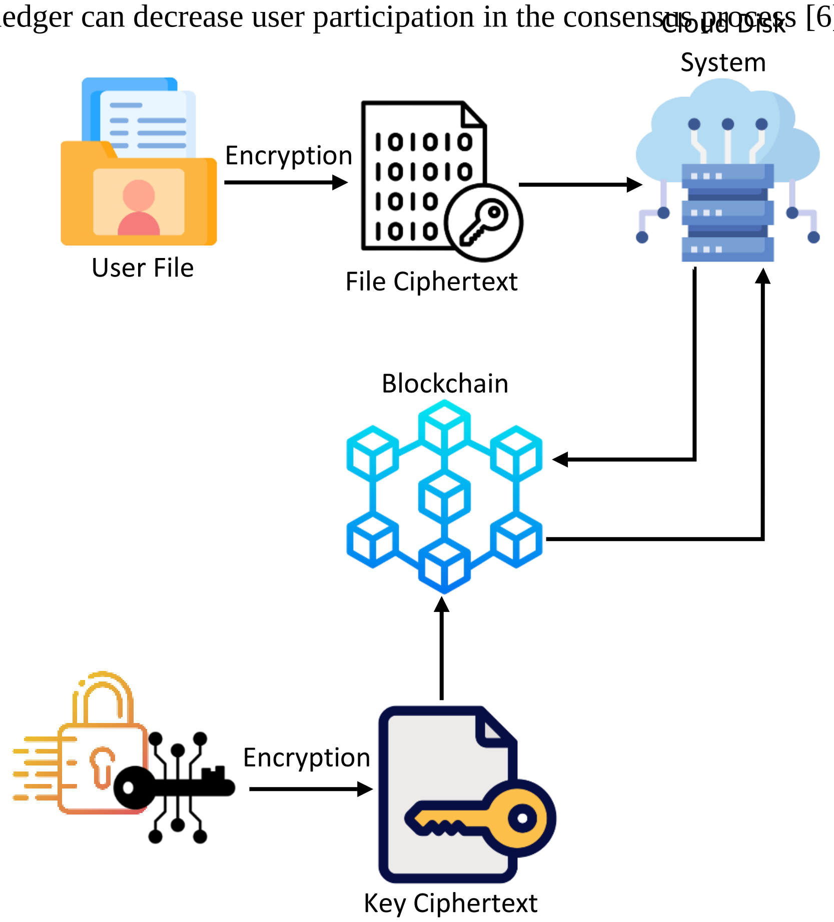


Figure 1: Architecture of existing EHR security

The drive to improve patient outcomes, operational efficiency, and service quality is propelling the digital transformation of the healthcare sector. At the heart of this evolution are Electronic Health Records (EHRs) store sensitive patient data and are essential for modern healthcare delivery [7]. Challenges arise due to the increasing volume of data, rising cyber threats, and stricter regulatory requirements, necessitating scalable, secure, and efficient EHR management systems shown in Figure 1 [8]. Blockchain can simplify numerous healthcare tasks such as maintaining comprehensive patient histories enabling patient-centric electronic physician records, remote monitoring, tracking medical equipment, improving digital health record accessibility, and ensuring privacy protection [9]. The present research explores the potential of blockchain to offer secure, private, and reliable network communications for EHR exchange systems. This rise in healthcare security incidents has been a key driver for blockchain adoption in the sector [10].

Blockchain can be implemented in various forms confidential, public, and permissioned. Public blockchains such as Ethereum operate with an anonymous framework may not be suitable for businesses that wish to maintain privacy while conducting transactions. Private blockchains such as Enterprise Ethereum restrict access and prevent unauthorized individuals from using the network while all peers within the network are treated equally [11]. Hyperledger Fabric provide the necessary access control tools to address these concerns, allowing for more controlled interactions between participants. EHRs support the efficient and ongoing management of healthcare by securely storing, sharing, and allowing authorized users to access patient data [12]. This digital information can be quickly processed and transmitted to healthcare hospitals facilitating the delivery of high-quality care. EHRs contain essential information such as medical history, diagnoses, test results, treatments, and medications contribute to reducing errors, improving outcomes, and enabling more thorough analysis of a patient's condition [13]. Sharing of EHRs introduces privacy and security risks as these records are vulnerable during exchanges. Ensuring confidentiality in medical studies and healthcare organizations requires compliance with legal regulations and jurisdictions. Despite existing procedures remains a need to strengthen privacy protections at the organizational level.

2. RELATED WORKS

The increasing volume of health-related data in healthcare hospitals highlights the need for secure and reliable storage and transmission systems. EHRs have become an essential tool for managing patient information such as prescriptions, vital signs, lab results, medical history, and more [14]. In the past, the transfer of medical data was slow and limited applications hindered the seamless exchange of information across healthcare hospitals. As the internet became more widely accessible, cloud computing emerged as a solution to store and share medical data, enabling remote collaborative diagnostics [15]. Cloud-based EHR systems offering scalability and convenience introduced new challenges in terms of patient safety, confidentiality, and information breaches. These systems face issues related to interoperability, decentralization, and the difficulty of ensuring transparency and accountability. By offering secure, decentralized, and transparent data management, blockchain has gained traction in various industries such as healthcare [16]. Blockchain's potential to enhance data security provide seamless integration, and support real-time information sharing positions it as a leading solution to the ongoing challenges in healthcare data management. The surge in blockchain adoption in healthcare is reflected in global trends as illustrated by the rise in interest in blockchain for healthcare applications such as secure patient data sharing, interoperability between systems, and patient-centric solutions [17].

Numerous programs for healthcare providers to manage and integrate health information have already begun in countries such as US, Canada, and the EU. The Estonian case study serves as an example of how decentralized blockchain computing can be applied as a reliable solution to address challenges in government and healthcare. A survey found that 70% of medical experts believe blockchain technology will have the most significant impact on medical use cases [18]. Maintaining security and confidentiality is crucial for envisioning seamless healthcare applications. Privacy-protection strategies for EHRs in cloud systems were examined. The following privacy needs were explored: accountability, anonymity, confidentiality, integrity, non-repudiation, unlinkability, authenticity, and auditability [19]. Divided privacy-protection strategies into two categories: cryptographic and non-cryptographic. Cryptographic techniques include homomorphic encryption, proxy re-encryption, searchable encryption, attribute-based encryption, and hierarchical predicate encryption. Non-cryptographic methods involve infrastructure subject to access control restrictions. This paper also discusses the safety and confidentiality needs of cloud structures to guarantee EHR security [20]. Blockchain-based safety and confidentiality strategies for exchanging health information across various stakeholders were investigated. Emphasized blockchain-based permissioned and permissionless EHR safety measures and discussed whether off-chain or on-chain storage is better for health information [21].

Safe ML and DL techniques for applications in medicine were reviewed. Categorized ML/DL applications in medicine into four areas: clinical processes, diagnosis, therapy, and prognosis. Investigated several safety and privacy risks in data-driven ML pipelines for medical applications. Highlighted several research problems, including comprehensible, distributed, and responsible ML, dataset annotation, and implementation on edge devices. To ensure the registration and maintenance of medical records examined the use of blockchain in the healthcare industry. Categorized existing work into areas such as digital identification, social information governance, social insurance, information management, safety, and patient-healthcare information [22]. The survey of cloud-based blockchain-based EHR security. Other authors have used cloud computing and IoT to protect EHRs using blockchain. Investigated edge computing, cloud computing, and IoT to use blockchain for securing EHR systems. Further examined blockchain and AI in various application areas, including healthcare, smart cities, and smart services. EHRs have significantly enhanced patient decision-making, physician satisfaction, and the quality of healthcare services [23].

Healthcare 5.0 is revolutionizing the delivery of healthcare. Healthcare 5.0 is a patient-centered approach that prioritizes proactive, individualized treatment made possible by cutting-edge technology. By providing comprehensive, real-time patient data that can be used to offer personalized treatment increase patient engagement, and improve clinical outcomes EHR systems help support this paradigm shift. EHRs provide real-time, patient-centered information that is immediately and securely available to authorized users [24]. By providing accurate, comprehensive and up-to-date patient data at the point of care EHRs enable the prompt retrieval of patient information for better-coordinated efficient treatment and secure electronic data exchange with patients and other healthcare providers. EHRs also enable healthcare practitioners to better manage patient care and provide higher-quality healthcare by helping them diagnose patients more accurately, reduce medical errors, and deliver safer treatments. EHRs facilitate professional communication, decision-making, and coordination among healthcare providers [25]. The inability of existing systems to simultaneously meet the critical needs of safety, capacity, effectiveness, and privacy in a rapidly evolving digital healthcare ecosystem represents an academic gap in the safe and scalable management of medical information. Due to their single points of failure, the centralized healthcare information management systems currently in use are vulnerable to unauthorized access, data breaches, and cyberattacks [26]. Although blockchain technology offers decentralized and secure alternatives, existing blockchain systems face challenges such as low transaction throughput, high latency, energy inefficiency, and limited flexibility particularly when managing the massive, real-time demands of healthcare information. Dynamic nature of medical environments where sources of information and participants are constantly changing means that consensus mechanisms in current blockchain systems often fall short. To provide secure, real-time, and scalable medical information management limitations underscore the need for a novel framework that integrates advanced privacy-preserving techniques, scalable consensus procedures, and efficient data-sharing methods [27].

3. MATERIALS AND METHODS

A new approach to addressing the urgent challenges of secure and scalable healthcare information management in the digital era is the DECP with PPBF shown in Figure 2. This framework overcomes the limitations of existing centralized systems prone to unauthorized access, security breaches and inefficiencies in managing the growing volume of sensitive medical information. By employing a dynamic elastic consensus algorithm, the proposed method enhances the flexibility of blockchain networks to handle fluctuating data volumes and varying participant numbers, ensuring scalability and efficient operation. Privacy-preserving techniques such as homomorphic encryption and zero-knowledge proofs safeguard patient privacy while enabling legitimate data sharing among stakeholders, researchers, and healthcare providers. The framework is designed to deliver high transaction throughput and real-time access to information without compromising security even in distributed environments. It addresses the shortcomings of existing blockchain systems such as high latency and limited scalability, through the integration of advanced cryptographic methods and consensus mechanisms, making it particularly suitable for large-scale healthcare ecosystems. Beyond enhancing patient confidentiality and data security, this approach promotes interoperability and seamless collaboration among healthcare institutions. It supports the development of intelligent healthcare solutions, personalized treatments, and informed decision-making driven by data.

3.1 Dataset Description

A wide variety of attributes that fully reflect patient data while maintaining security and confidentiality are contained in the dataset utilized for secure and scalable healthcare data management shown in Table 1. In addition to demographic data such as age and gender to aid in analyzing the information, each patient is individually recognized by their Patient ID. Standardized Diagnosis Codes (such as ICD-10) and comprehensive Treatment Details include details on prescription drugs and therapies are used for organizing medical data. In order to ensure accountability, the dataset also contains organizational information such as Hospital ID, which keeps track of the healthcare hospitals involved, and Information Access Logs, which document who viewed patient records and when. In accordance with privacy laws, the patient's consent status is documented to show their agreement with information sharing.

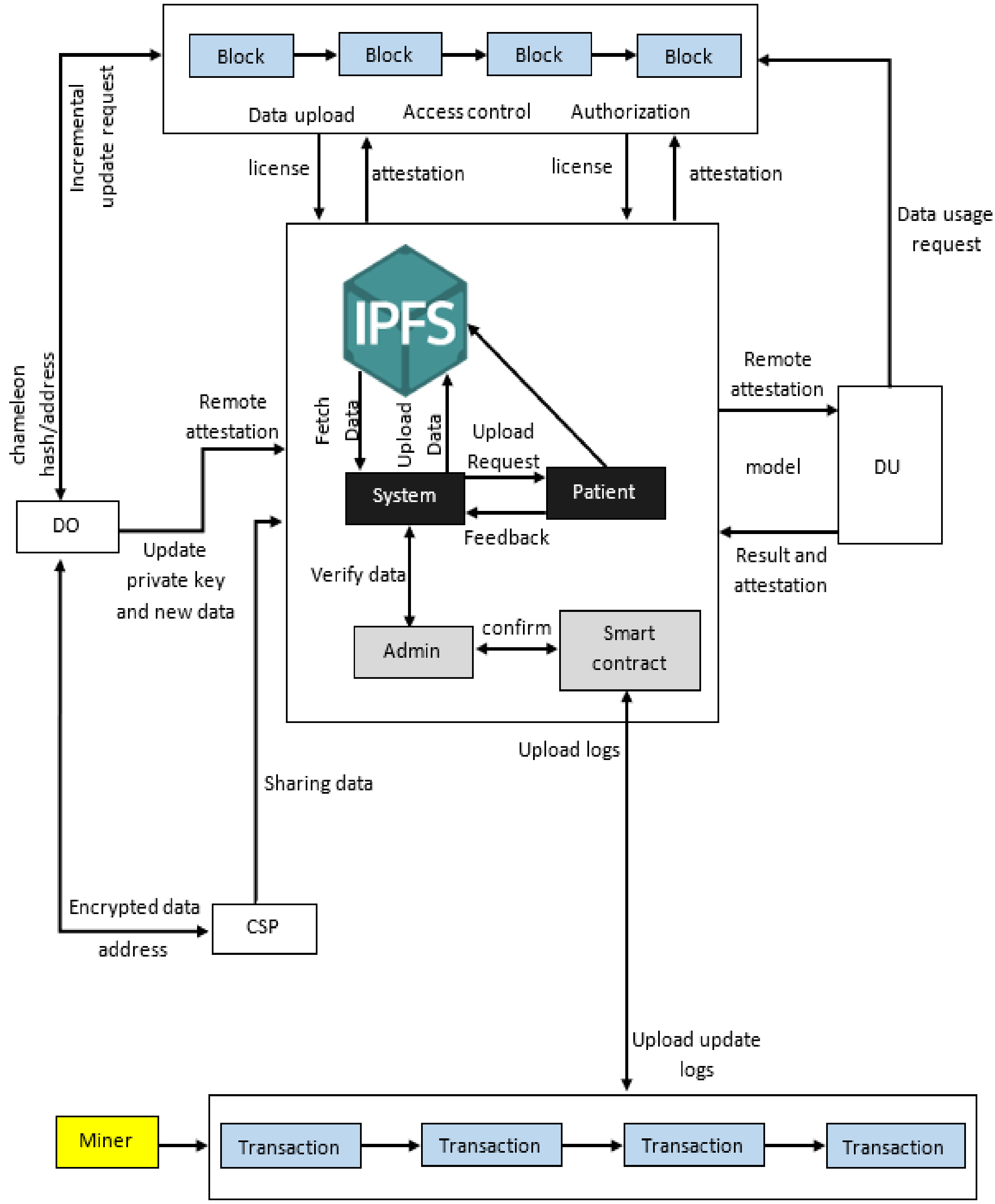


Figure 2: Proposed Architecture

Table 1: Dataset Description

Feature	Description	Type	Example Values

Patient ID	Unique identifier for each patient in the dataset.	Categorical	P01234, P56789
Age	Age of the patient in years.	Numerical	25, 46
Gender	Gender of the patient.	Categorical	Male, Female
Diagnosis Code	Standardized codes for medical diagnoses (e.g.., ICD-10).	Categorical	J45 (Asthma), E11 (Type 2 Diabetes)
Treatment Details	Information about the treatment or medication prescribed.	Textual	"Metformin 500mg". "Physical therapy sessions"
Hospital ID	Unique identifier for the hospital or clinic providing care	Categorical	H01, H35
Data Access Logs	Records of when and by whom patient data was accessed.	Timestamp	2024-12-15T09:35:00, 2024-12-16T15:50:00
Consent Status	Indicates whether the patient has consented to data sharing.	Binary	Yes, No
Blockchain Hash	Unique cryptographic hash of the patient's data for secure storage in the blockchain	Categorical	3e7a13lc.... 9c7a4a0b...
Transaction ID	Unique ID for data transactions within the blockchain framework	Alphanumeric	TXN09878, TXN54341
Medical Imaging Data	Links or IDs for associated medical images (e.g.. X-rays, MRIs).	Categorical	IMG01, IMG125
Laboratory Results	Clinical test results, such as blood tests, in standardized units.	Numerical	5.7 mmol/L (Glucose). 13.6 g/dL (Hemoglobin)
Timestamp	Date and time when the data was recorded or updated	Timestamp	2024-12-15T11:00:00, 2024-12-16T16:30:00
Anonymized Location	Generalized location of the patient (e.g.. city or region) without revealing specific addresses.	Categorical	New York, Los Angeles
Insurance ID	Unique identifier for the patient's insurance provider.	Categorical	INS01, INS45

Table 2: Sample Data

Patient ID	**Age**	**Gender**	**Diagnosis Code**	**Treatment Details**	**Hospital ID**	**Data Access Logs**	**Consent Status**	**Blockchain Hash**	**Transaction ID**	**Medical Imaging Data**	**Laboratory Results**	**Timestamp**	**Anonymized Location**	**Insurance ID**
P01	43	Male	145.909	Inhaler therapy	H001	Accessed by Dr. A at 11:30 AM. 12/12	Approved	c1d2e3f4g5h6i7j8k910m	Tx12345678	MRI001.jpg	Hb: 11.2 g/dL	2024-12-16 14:00	Zone 1, City A	INS001234567
P02	36	Female	E11.9	Metformin 500 mg daily	H002	Accessed by Dr. B at 4:15 PM 12/10	Approved	e1f2g3h4i5j6k718m9n00	Tx11223344	Xray123.png	Glucose: 105 mg/dL	2024-12-15 09:00	Zone 3, City B	INS765432109
P03	28	Female	110	Beta-blockers & dietary	H003	Accessed by Nurse Cat 12:00	Denied	g1h2i3j4k5l6m7n8o9p0q	Tx33445566	CT Scan 567.dcm	Cholesterol 190 mg/dl	2024-12-14 18:00	Zone 2. City C	INS908172635

				plan		AM 12/8								
P04	46	Male	M54.5	Physical therapy. pain relief	H004	Accessed by Dr. D at 6:45 PM 12/11	Approved	f1g2h3i4j5k617m8n9o0p	Tx44556677	Xray456.png	WBC 8,000/µL	2024-12-13 16:30	Zone 4. City D	INS345678912
P05	52	Male	E78.0	Statin therapy	H005	Accessed by Dr. E at 3:00 PM 12/13	Approved	d1e2f3g4h5i6j7k8l9m0n	Tx22334455	Ultrasound789.dcm	LDL: 120 mg/dL	2024-12-14 20:45	Zone 5. City E	INS543216789
P06	40	Female	R07.9	Painkillers & chest X-ray	H006	Accessed by Dr. F at 10:30 AM 12/14	Approved	1a2b3c4d5e6f7g8h9i0j	Tx66778899	Chest Xray234.jpg	ECG Normal	2024-12-15 08:20	Zone 6. City F	INS987654321

P07	66	Male	K21.9	Proton-pump inhibitor therapy	H007	Accessed by Dr. G at 2:15 PM. 12/15	Denied	b1c2d3e4f5g6h7i8j9k0l	Tx55667788	Endoscopy987.png	pH: 4.0 (stomach)	2024-12-16 10:50	Zone 7. City G	INS321654987
P08	39	Female	N18.9	Dialysis sessions twice weekly	H008	Accessed by Nurse H at 5:00 PM. 12/16	Approved	a1b2c3d4e5f6g7h8i9j0k	Tx87654321	RenalUS456dcm	Creatinine: 2.5 mg/dL	2024-12-17 12:30	Zone 8, City H	INS876543210

Specifically designed for medical information administration, this example dataset guarantees an organized view of patient information, diagnosis, therapy, and blockchain safety precautions shown in Table 2.

3.2 Problem formulation

To design a secure, scalable, and efficient healthcare data management framework by integrating a DECP-PPBF.

Healthcare Data Representation: Let the healthcare data from a patient be represented as D_x where: $D_x = \{P_x, T_x, M_x, L_x\}$ (1)

Here: P_x: Patient identifier (anonymized for privacy); T_x: Timestamp of the data generation; M_x: Medical data (diagnosis, treatment, lab results); L_x: Location of healthcare service provider.

Privacy Preservation Mechanism: The privacy-preserving mechanism encrypts D_x before blockchain storage: $E(D_x) = Enc_k(D_x)$ (2)

where k is the encryption key, and Enc, is the encryption function. For privacy, P_x is replaced with a hashed identifier $H(P_x)$: $H(P_x) = Hash(P_x)$ (3)

Consensus Protocol (Dynamic Elastic Consensus): The dynamic elastic consensus protocol ensures scalability and efficiency by adapting to network dynamics. Let N be the number of participating nodes, and T_c the transaction throughput. The goal is to maximize throughput while minimizing latency L: $max(T_c)\ and\ min(L)\ subject\ to\ T_c \alpha \frac{1}{L}$ (4)

The consensus is reached when a majority M of nodes agree on a block B_x such that:

$M \geq \left[\frac{N}{2} + 1\right]$ (5)

Blockchain Transaction Validation: A transaction T_{i_x} is valid if: $T_{i_x} = \{H(P_x), T_x, E(D_x)\}$ (6)

satisfies the following conditions:

- Signature verification: VerifySig$\left(T_{i_x}, k\right)$- True.
- Timestamp order: $T_x > T_{prev}$ where T_{prev} is the last block's timestamp.

Scalability Function: Scalability is modeled as the ability to process S transactions per second with increasing nodes N: $S = \frac{T_c}{N}$ (7)

Lemma: Privacy and Security Guarantees- The proposed framework guarantees privacy preservation if the encryption function Enc_k and hash function Hash are computationally secure.

Proof:

1. The encryption $E(D_x) = Enc_k(D_x)$ ensures that the data D_x is only accessible to authorized entities possessing k.

2. Hashing $H(P_x) = Hash(P_x)$ anonymizes the patient identifier. Assuming Hash is a one-way function, reversing $H(P_x)$ without P_x is computationally infeasible.

This problem formulation mathematically defines the key objectives and the mechanisms of the proposed framework, ensuring data security, privacy, and scalability in healthcare environments.

3.3 Data Upload

The Data Owner (DO) encrypts their data (MDx) and stores the encrypted data (EDx) with a Cloud Service Provider (CSP). The DO also stores the address of the encrypted data (addr) with the CSP. Everyone utilizes both the off-chain and on-chain storage models in the framework. As a result, there are two steps in the information upload method: uploading to the blockchain and storing to CSP. The logical progression of the information upload procedure is depicted in Figure 3. Encrypt the information in plaintext using effective symmetric encryption methods to guarantee secure storage. Utilize the intelligent contract key's public key to encrypt the symmetric key. To create the ciphertext for an exchange of keys, authorization, and the

p-ISSN 0854-1418
e-ISSN 2503-426X

public key are required. Construct a storage transaction Timestamp (Ts) in the Security Boundary (SB) to control the on-chain information storage.

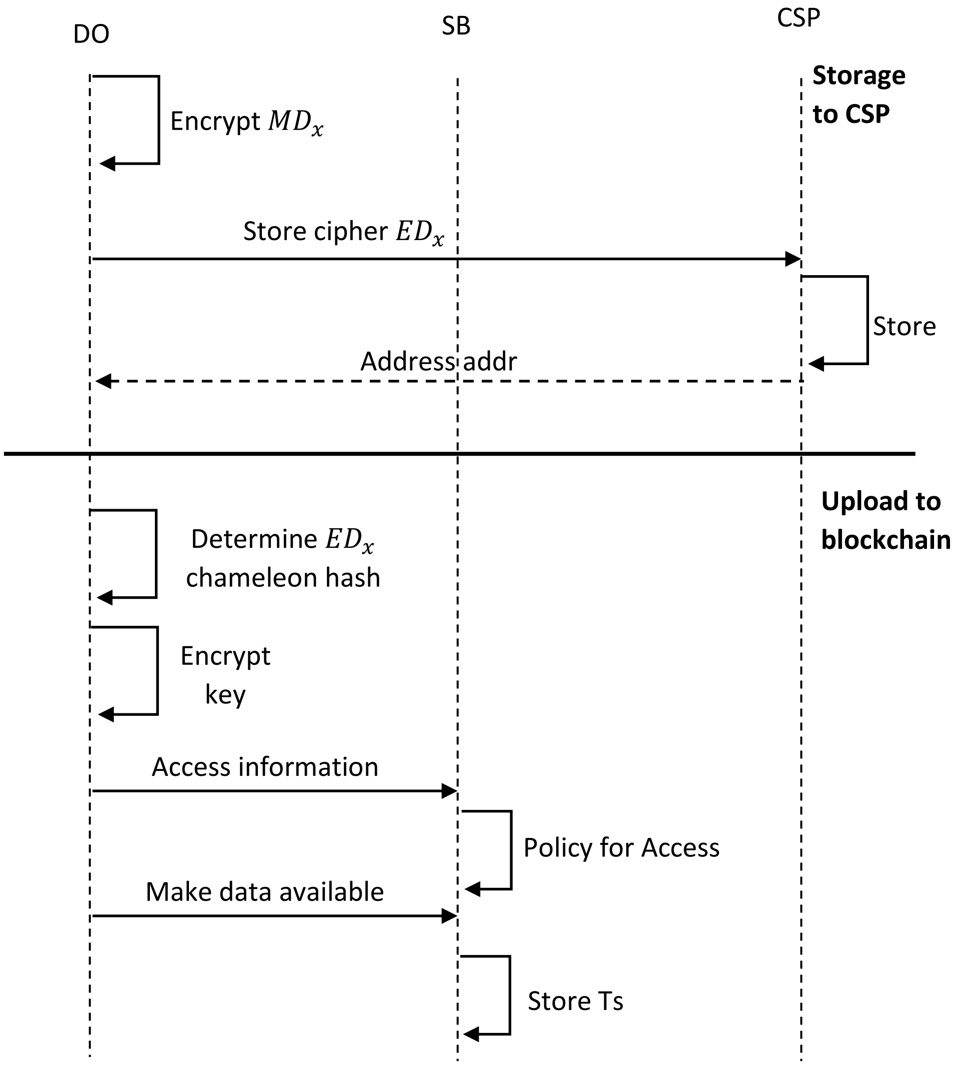


Figure 3: The logical flow of data upload

3.4 Storage in Cloud Service Providers (CSPs)

In healthcare data management on Cloud Service Providers (CSPs), considerations for storage efficiency, redundancy, encryption, compliance, and cost are crucial.

Data Storage Costs: Let: S: Total storage required (in GB); C_{unit}: Cost per GB stored (in $/month)

Total Monthly Storage Cost: $TC_{storage} = S \times C_{unit}$ (8)

Where C_{unit} is the cost offered by the CSP.

Data Redundancy across Nodes: Healthcare data often uses replication for fault tolerance. Let: $N_{replicas}$: Number of replicas for redundancy; P_{node_fail}: Probability that a node storing data fails

Probability that all $N_{replicas}$ fail simultaneously: $P_{fail\_all} = (P_{node\_fail})^{N_{replicas}}$ (9)

For example, with a node failure probability of 0.01 and 3 replicas: $P_{fail\_all} = (0.01)^3 = 0.000001$. This ensures data availability and fault recovery.

Encryption Overhead in Data Storage: Let: D_{data} : Size of data to be encrypted (in GB); E_{AES256}: Time overhead of AES-256 encryption in terms of throughput

Encryption Storage Overhead for AES-256 encryption: $E_{AES256} = D_{data} \times R_{AES}$ (10)

Where R_{AES} is the encryption throughput (e.g., 500 MB/s).

Scalability of Storage in Healthcare CSPs: Let α represent the growth rate of healthcare data per month. If initial storage is S_0 then the data storage growth over time t:

$S(t) = S_0 \times e^{at}$ (11)

For instance, with an annual growth rate of 5% (α = 0.05): $S(t) = S_0 * e^{0.05 \times t}$ This ensures scalable infrastructure planning.

Data Retrieval Latency: Let: R_{node}; Average response time to access a node; N_{replicas} : Number of replicas stored across the cloud infrastructure.

Total retrieval latency $T_{\text{retrieval}} = R_{\text{node}} + \frac{S}{N_{\text{replicas}}}$ (12)

More replicas reduce access latency, ensuring quick retrieval times.

Compliance and Data Storage Efficiency: Healthcare storage must comply with standards like HIPAA (Health Insurance Portability and Accountability Act):

Storage Efficiency $E_{efficiency} = \frac{S_{usable}}{S_{allocated}}$ (13)

Where S_{usable} is the usable storage, and $S_{allocated}$ includes redundancy and overhead.

These considerations ensure secure, scalable, and cost-effective healthcare storage solutions in CSPs while maintaining compliance with data privacy regulations and fault-tolerance mechanisms

3.5 Dynamic Elastic Consensus Protocol (DECP) with Privacy-Preserving Blockchain Framework

Participation comprises a range of groups such as information along with information utilizers. Consent level, approval target, and approval duration are the three primary components of the dynamic consent rule that information providers, the primary party in this network have developed. Data providers can modify the parameters of the dynamic consent rule in addition to viewing medical information through application. The ledger contains the history of what information users have accessed or used their information is fully accessible to them. According to predetermined guidelines, any data utilizer can receive health examination data from data providers by utilizing the information utilizer's application. This program can enforce many management of information functions since hospitals are the primary source of hospital assessment information shown in Figure 4. A medical facility or individual must invest time and energy in health information is an intangible asset. Customers, service providers, information carriers and others are all involved necessitating a procedure for the consent system that everyone can comprehend and agree upon intuitively.

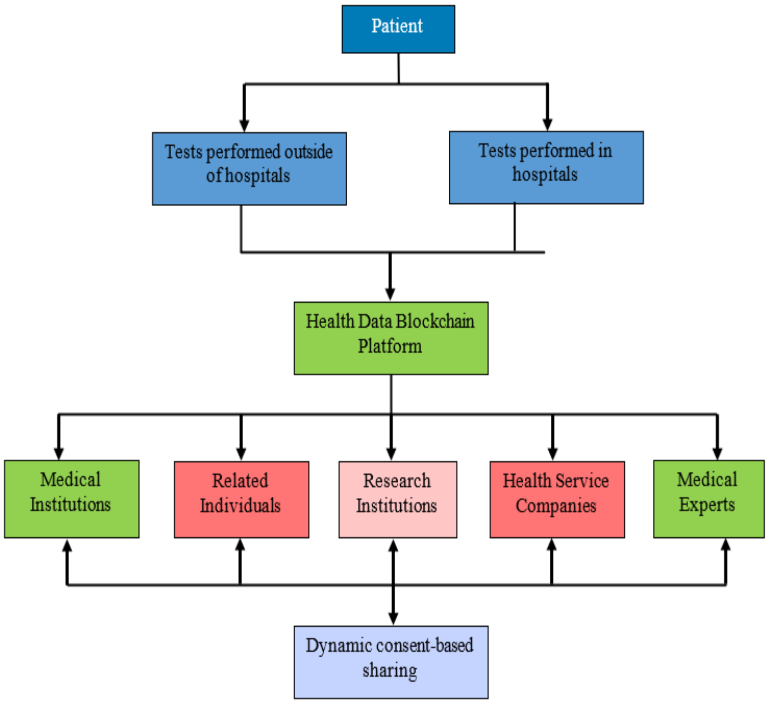


Figure 4: DECP secure flow of Healthcare data

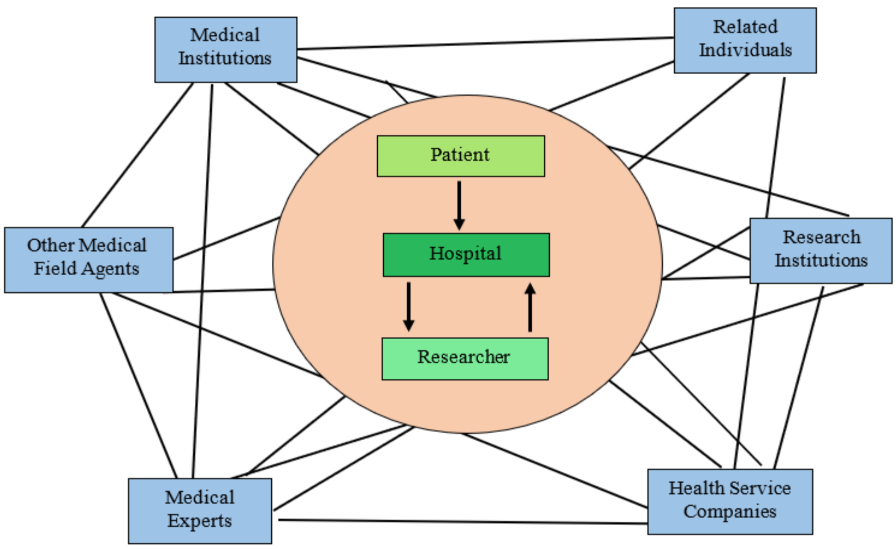


Figure 5: DECP-PPBF functions

The term data type refers to the specific kind of information that data providers choose to share with other data users. Data providers have access to three types of data: (1) information obtained from hospital-level examinations, (2) data from tests conducted outside of hospitals, and (3) social and demographic information shown in Figure 5. Social and demographic data such as age, sex, and residence serve as fundamental information. Out-of-hospital test data include results from simple medical examinations that data providers can perform at home using devices such as InBody analyzers, thermometers and other medical equipment. In contrast, hospital-level examination data are more detailed typically collected during medical visits and involve comprehensive diagnostic procedures.

Algorithm: Dynamic Elastic Consensus Protocol (DECP) with Privacy-Preserving Blockchain Framework for Secure and Scalable Healthcare Data Management

The objective of the protocol is to ensure secure, scalable, and privacy-preserving consensus among CSPs for managing healthcare data while maintaining compliance with security and privacy requirements.

Step 1: Initialization: Initialize the network of CSP nodes N, where each node i stores healthcare data D_x.

Define the consensus parameters: Number of nodes N; Consensus weight W_x for node x; Redundancy factor R_{node}

$W_x(t) = \frac{1}{N}$ (14)

Each node's weight ensures uniform distribution initially.

Step 2: Privacy-Preserving Data Encryption: Each CSP encrypts its healthcare data D_{i} using Paillier Homomorphic Encryption to maintain privacy.

Let: $E(D_x)$ be the encrypted version of healthcare data D_x

Paillier encryption operates as follows:

1. Generate a public key PK and private key SK.

2. Encrypt each healthcare data entry D_x using the Paillier algorithm:

$E(D_x) = Enc_{PK}(D_x) = g^{D_x} \times r^n \ mod \ n^2$ (15)

Where g and n are generated as part of the Paillier public key setup.

Step 3: Dynamic Elastic Consensus Calculation: Each node collaborates to form a consensus based on data availability, node reliability, and latency.

Let P_x represent the performance metric for node x.

Dynamic Consensus Weight Adjustment: $W_x(t+1) = W_x(t) \times \frac{P_x}{\sum_{y=1}^{N} P_y}$ (16)

Where: P_x is a performance reliability measure calculated based on latency, availability, and node failure rate.

Step 4: Distributed Blockchain Ledger Integration: Update the blockchain ledger L with encrypted healthcare data for immutability and traceability. Let: $H_x(t)$ Hash representing the encrypted healthcare data $E(D_x)$ on the blockchain.

Blockchain Ledger Update: $L_{t+1} = H(E(D_x)) + H(W_x(t))$ (17)

Where each transaction on the blockchain contains: Encrypted healthcare data; Consensus metadata $W_x(t)$

Step 5: Consensus Validation Across Nodes: Nodes communicate to validate consensus changes dynamically. Apply consensus validation checks:

$$V_{consensus} = \prod_{x=1}^{N} W_x(t) \geq \gamma threshold \quad (18)$$

Where: $\gamma threshold$ is the reliability threshold required to maintain consensus stability.

Ensure that nodes i meet the consensus requirements to validate the updates across all CSPs.

Step 6: Redundant Data Allocation Across CSPs: Healthcare data is automatically distributed with a redundancy factor R_{node}. Each node's storage allocation adheres to the formula: $S_{allocated} = R_{node} \times S_{health}$ (19)

Where S_{health} is the data size allocated for healthcare storage.

A Dynamic Elastic Consensus Protocol ensuring fault tolerance and scalability across nodes. Privacy-preserving encryption techniques (Paillier) to maintain data confidentiality. Blockchain ledger for immutable, transparent, and traceable healthcare data updates. These ensure secure, scalable, and compliant healthcare data storage and retrieval across cloud service providers with a high degree of performance and resilience against potential breaches or failures.

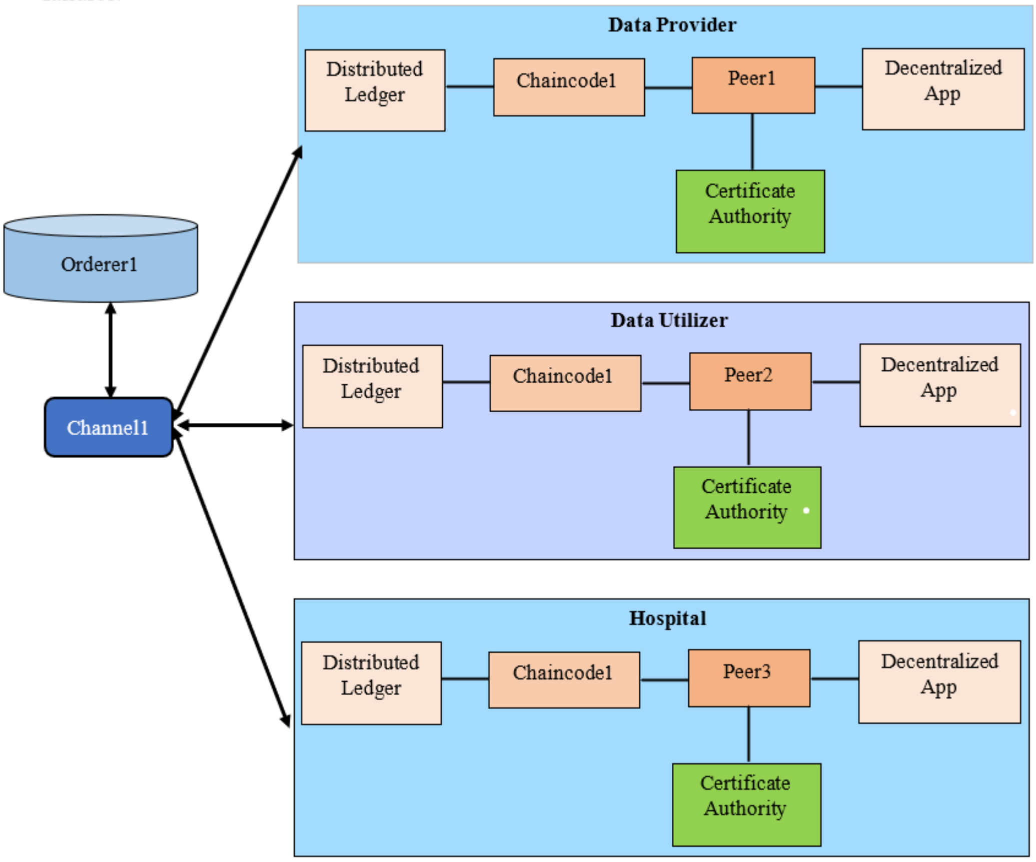
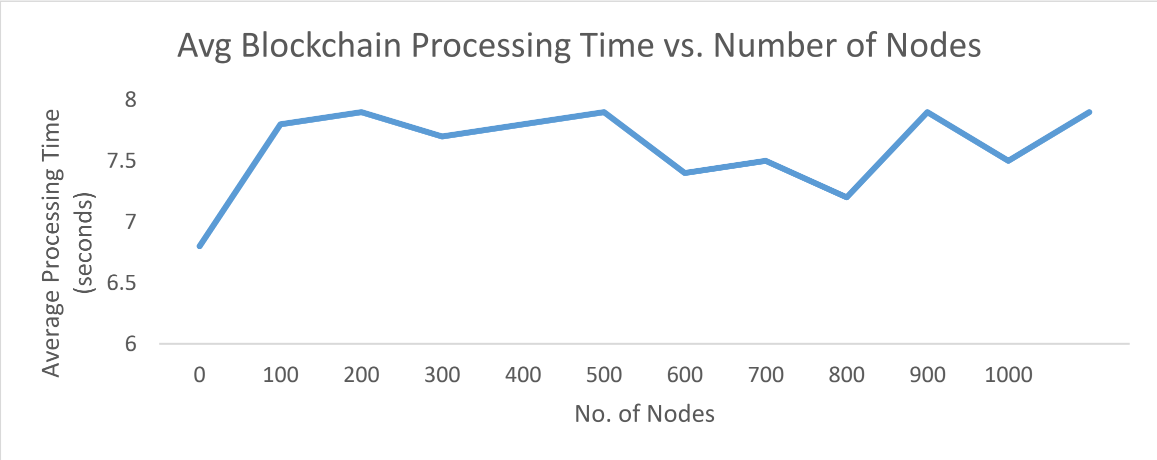


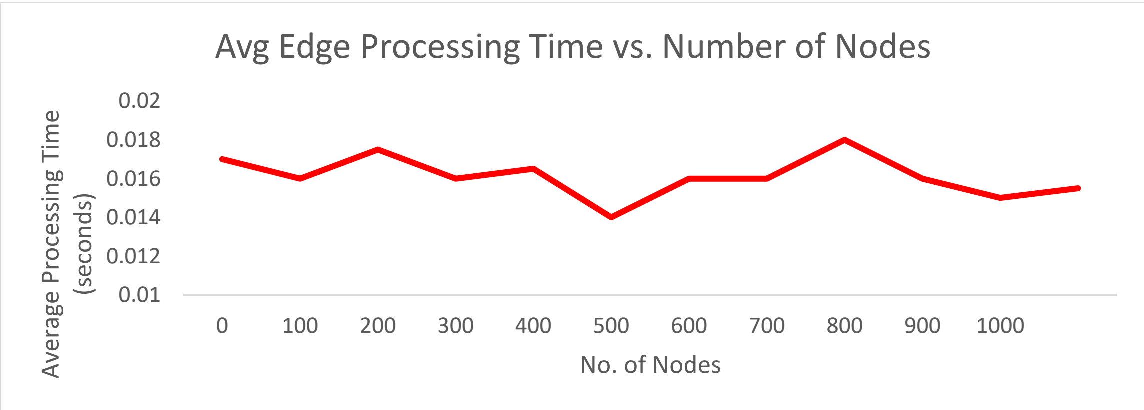
Figure 6: DECP-PPBF Network based on Hyperledger Fabric

4. RESULTS AND DISCUSSIONS

To store information on the blockchain and disseminate it to peer nodes, a smart contract based on Hyperledger chaincode was implemented. The blockchain system stores the hash values of medical information on-chain, while the actual medical information provided by data suppliers is stored off-chain, regulated by dynamic consent system rules. In DECP-PPBF, a consortium is formed by three entities: hospitals, information suppliers, and information users (Figure 6). The chaincode was modified to adhere to the DECP-PPBF by the data providers. Hospitals manage the transfer of information from general health examinations and maintain records of healthcare information transactions.



(a)



(b)

Figure 7: Processing times (a) blockchain (b) edge nodes using proposed DECP-PPBF system

Data users can access and compare health examination data hashes through the system. All three entities participate in the same channel (Channel 1) within the consortium. The ordering service node, Orderer1, is created after consultations among the participating entities. Further participation in the consortium can be established by modifying the configuration block in the ordering service includes details about peers, network policies, channels, clients, and channel policies. Orderer1 is responsible for building Channel 1, facilitating the sharing of information within the consortium, restricted to entities with aligned interests.

p-ISSN 0854-1418
e-ISSN 2503-426X

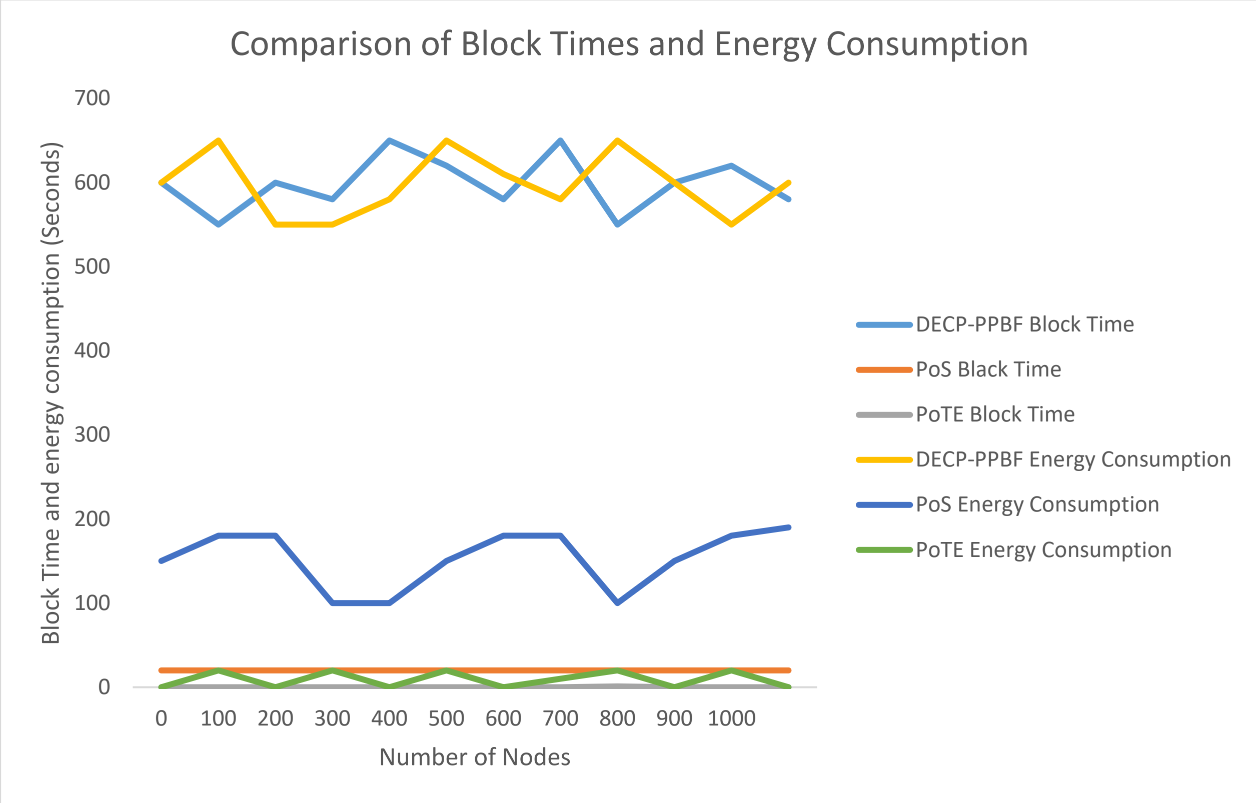


Figure 8: Comparison of block times and energy consumption in various blockchain networks

The effectiveness of the proposed model for medicine is shown in Figure 7, where it outperforms conventional techniques in terms of median block processing time and median edge time required for processing. Figure 8 compares the energy usage and block time of several networks using blockchain technology. It includes the time required to construct and validate a new block and the average block duration. The proposed system has a very low latency usually a few seconds.

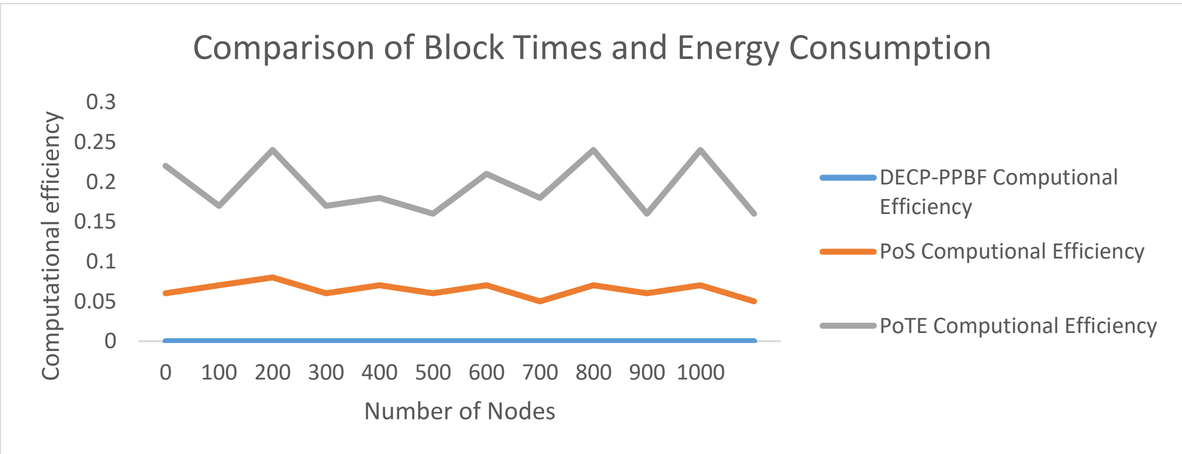
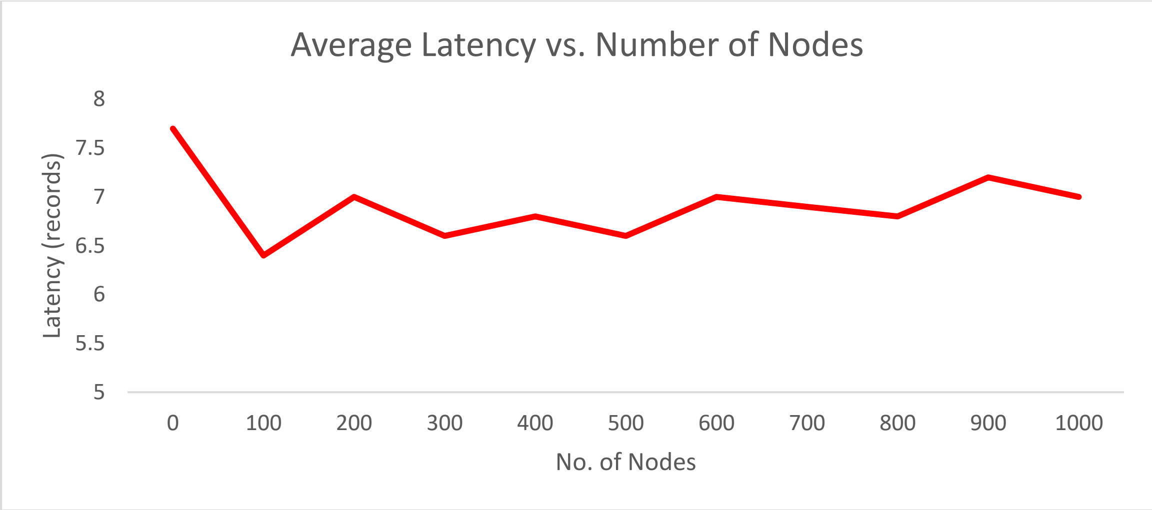
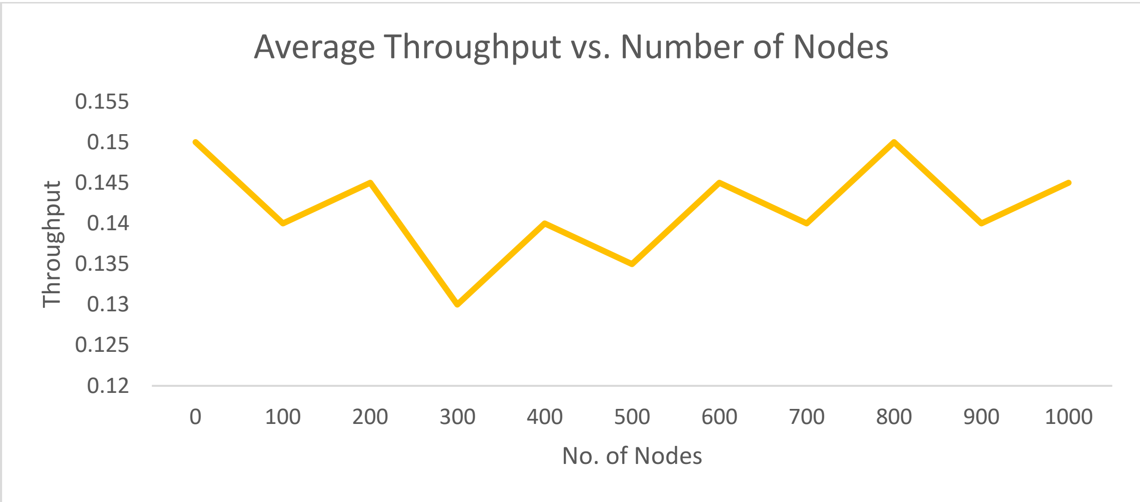


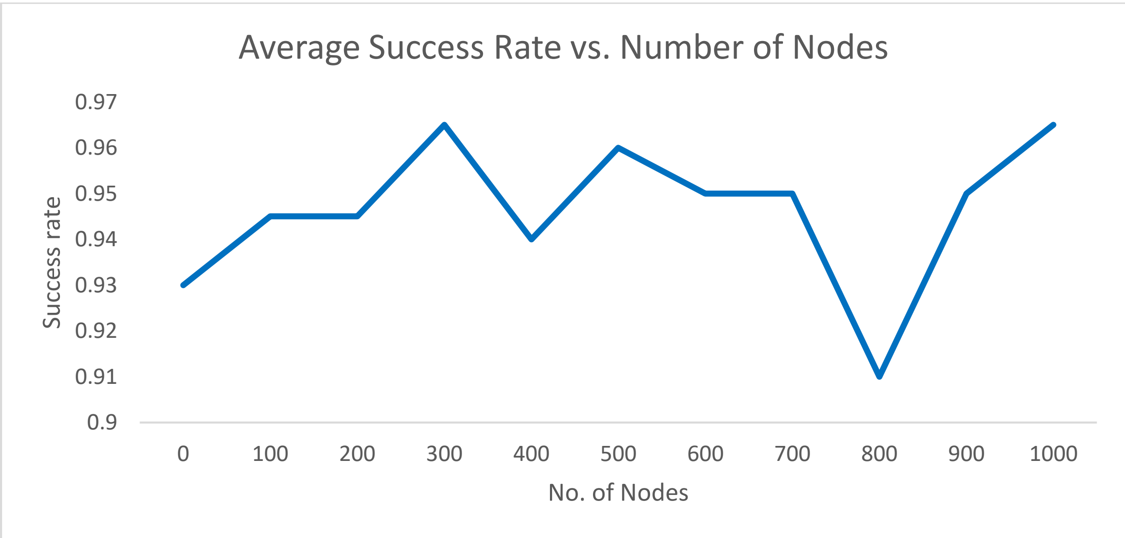
Figure 9: Comparison of various blockchain models in terms of computational efficiency


Average Latency vs. Number of Nodes
Latency (records)
8
7.5
7
6.5
6
5.5
5
0
100
200
300
400
500
600
700
800
900
1000
No. of Nodes

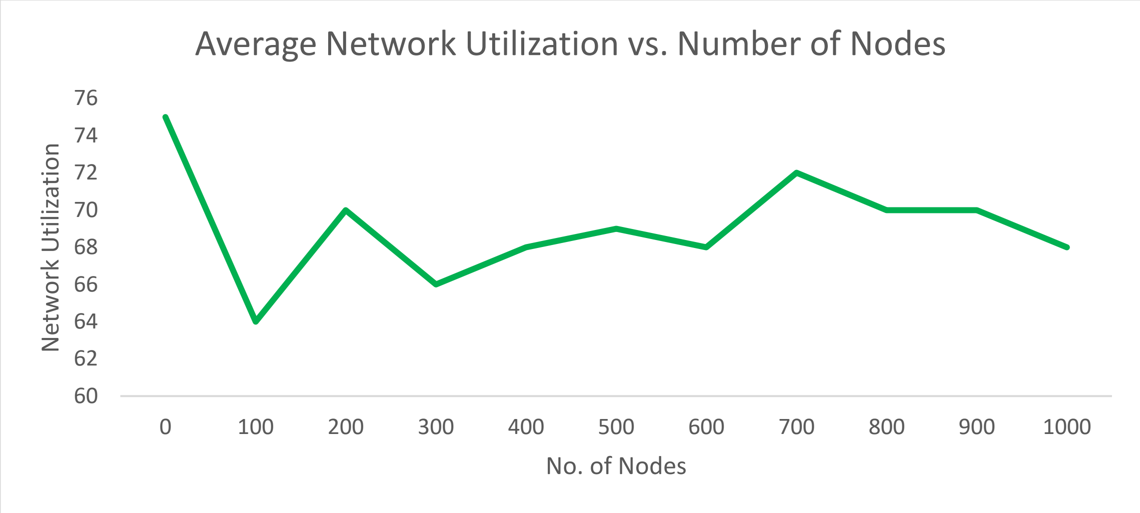
(a)


Average Throughput vs. Number of Nodes
Throughput
0.155
0.15
0.145
0.14
0.135
0.13
0.125
0.12
0
100
200
300
400
500
600
700
800
900
1000
No. of Nodes

(b)


Average Success Rate vs. Number of Nodes
Success rate
0.97
0.96
0.95
0.94
0.93
0.92
0.91
0.9
0
100
200
300
400
500
600
700
800
900
1000
No. of Nodes

(c)



(d)

Figure 10: Performance of the proposed model in terms of (a) Latency (b) Throughput (c) Success rate (d) Network Utilization

One of the most important metrics for assessing and choosing blockchain consensus algorithms is computational effectiveness. It gauges how well a system uses processing power to accomplish its goals. The computational performance of many blockchain architectures is contrasted in Figure 9. The proposed model's efficacy is displayed in Figure 10 in terms of latency throughput, success rate and network utilization performance measures.

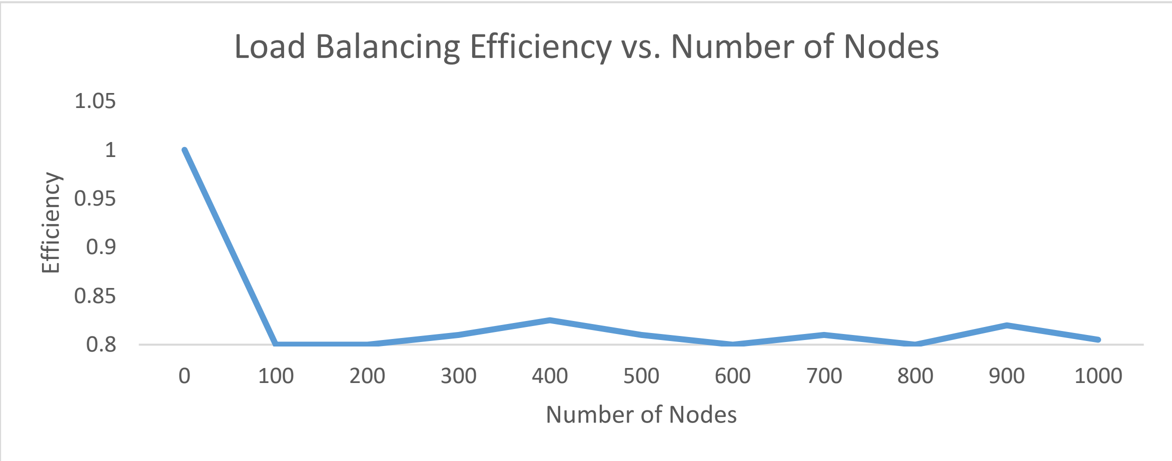


Figure 11: Load balancing in the proposed model as function of increasing nodes

The proposed model's load balancing effectiveness gauges how evenly the network's burden is distributed across its nodes, is shown in Figure 11. To avoid bottlenecks and decreased system efficiency is essential. The framework first attains a load-balanced effectiveness of 1 with 50 nodes, suggesting an ideal workload allocation. The system's flexible procedures to preserve operational efficiency are reflected in these modifications. It is important to maintain high load balancing effectiveness as the number of nodes increases scalability, utilization of resources, system stability and efficiency.

Table 3: Performance Measures

System	Consensus Latency (ms)	Throughput (TPS)
Proposed DECP-PPBF system	45	150
PBFT Consensus	121	76
Proof of Authority	91	121
Federated Blockchain	86	111
Raft – based consensus	151	51

The proposed DECP-PPBF achieves low latency (45 ms) and high throughput (150 TPS) by dynamically adapting consensus mechanisms across cloud service nodes shown in Table 3. Privacy-preserving encryption and scalable node management contribute to better system resilience and performance.

Table 4: Performance Measures

System	Scalability	Efficiency	Data confidentiality
Proposed DECP-PPBF system	High (Scales up to 10000+nodes)	96%	End –to – End encryption
PBFT Consensus	Medium (up to ~500 nodes)	71%	Partial Confidentiality
Proof of Authority	High (~800 nodes)	86%	Moderate Confidentiality
Federated Blockchain	Medium (Up to ~601 nodes)	81%	Encryption – based security
Raft – based consensus	Low (~201 nodes)	66%	No inherent confidentiality

The proposed DECP-PPBF system offers superior scalability supporting 10000+ nodes to dynamic consensus adaptation across cloud service nodes shown in Table 4. It achieves an efficiency of 96%, ensuring quick consensus formation and transaction processing without incurring large computational overheads. End-to-end encryption ensures higher privacy protection, safeguarding healthcare data across nodes and storage. Other existing systems such as PBFT, PoA, and Raft-based consensus often lack complete end-to-end encryption mechanisms leading partial or weak confidentiality.

Table 5: Performance Measures

System	Encryption Time (ms)	Decryption Time (ms)	Key Generation Time (ms)
Proposed DECP-PPBF system	15	20	50
PBFT Consensus	26	31	71

Proof of Authority	21	26	61
Federated Blockchain	23	29	66
Raft – based consensus	36	41	91

The proposed DECP-PPBF system achieves faster encryption (15 ms), ensuring minimal delay in encrypting healthcare data shown in Table 5. It has a decryption time of 20 ms, outperforming existing methods while maintaining efficient data access. The proposed DECP-PPBF system uses an optimized algorithm for key generation (50 ms) is quicker than other existing consensus-based methods. This comparison highlights the efficiency of the proposed DECP-PPBF system in cryptographic operations is crucial for ensuring timely and scalable data protection in healthcare management systems.

5. Conclusions

To address the challenges of secure and scalable medical information management, this study introduces the DECP-PPBF. Compared to existing consensus mechanisms, the proposed DECP-PPBF system demonstrates superior performance in terms of flexibility, efficiency, encryption speed, and data confidentiality. Experimental results show that the framework achieved improved key generation efficiency (50 ms) while significantly reducing encryption and decryption times to 15 ms and 20 ms, respectively. The framework integrates advanced cryptographic techniques with blockchain consensus protocols to ensure robust data privacy protections. It scales efficiently across extensive healthcare systems, maintaining the security, integrity, and transparency of data. The results highlight the system's resilience against attacks and its ability to handle high-throughput, low-latency operations, ensuring real-time data availability and processing. These findings underscore the potential of the proposed approach in practical healthcare scenarios, where system flexibility, compliance with confidentiality standards, and secure information transfer are critical. Future research can focus on integrating more advanced cryptographic primitives and enhancing consensus mechanisms to support even larger and more complex healthcare networks further improving data scalability and security across global healthcare service systems.

References

[1] Al-Nbhany, W. A., Zahary, A. T., & Al-Shargabi, A. A. (2024). Blockchain-IoT healthcare applications and trends: a review. *IEEE Access*.

[2] Bathula, A., Gupta, S. K., Merugu, S., Saba, L., Khanna, N. N., Laird, J. R., ... & Suri, J. S. (2024). Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. *Artificial Intelligence Review*, *57*(9), 238.

[3] Mohammed, M. A., Lakhan, A., Zebari, D. A., Abd Ghani, M. K., Marhoon, H. A., Abdulkareem, K. H., ... & Martinek, R. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Artificial Intelligence*, *129*, 107612.

[4] Halimuzzaman, M., Sharma, D. J., Bhattacharjee, T., Mallik, B., Rahman, R., Rezaul Karim, M., ... & Fokhrul Islam, M. (2024). Blockchain technology for integrating electronic records of digital healthcare system. *Journal of Angiotherapy*, *8*(7).

[5] Boda, V. V. R. (2024). Bringing Blockchain to Healthcare: How DevOps Can Lead the Way. *MZ Computing Journal*, *5*(1).

[6] Liu, Y., Liu, Z., Zhang, Q., Su, J., Cai, Z., & Li, X. (2024). Blockchain and trusted reputation assessment-based incentive mechanism for healthcare services. *Future Generation Computer Systems*, *154*, 59-71.

[7] Mahalakshmi, J., Reddy, A.M., Sowmya, T., Chowdary, B.V., & Raju, P.R. (2023). Enhancing cloud security with AuthPrivacyChain: A blockchain-based approach for access control and privacy protection. International Journal of Intelligent Systems and Applications in Engineering, 11(7), 370-384.

[8] Balakrishna, C., Sapkal, A., Chowdary, B. V., Rajyalakshmi, P., Kumar, V. S., & Gupta, K. G. (2023). Addressing the IoT schemes for securing the modern healthcare systems with blockchain neural networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11, 347–352. https://doi.org/10.17762/ijritcc.v11i7s.7009

[9] Laxmi Kanth, P., Sri Nagesh, O., Balaji Lanka, V. S. S. P. L. N., & Ramamohan Rao, P. (2024). Medical data security with blockchain and artificial intelligence using SecNet. Springer Proceedings in Mathematics and Statistics, 421, 457–466. https://doi.org/10.1007/978-3-031-51167-7_44

[10] Nayomi B., D. D., Mallika, S. S., Sowmya, T., Janardhan, G., Laxmikanth, P., & Bhavsingh, M. (2024). A cloud-assisted framework utilizing blockchain, machine learning, and artificial intelligence to countermeasure phishing attacks in smart cities. International Journal of Intelligent Systems and Applications in Engineering, 12, 313–327.

[11] Marry, P., Yenumula, K., Katakam, A., Bollepally, A., & Athaluri, A. (2023). Blockchain Based Smart Healthcare System. In Proceedings of the 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), 1480-1484. https://doi.org/10.1109/ICSCSS57650.2023.10169704

[12] Khaleelullah, S., Hemanth, D. S., Kavitha, E., Viswadutt, B., & Teja, B. S. V. (2023). A novel blockchain-based decentralized ballot system. Proceedings of the International Conference on Sustainable Computing and Smart Systems (ICSCSS), 1491–1496. https://doi.org/10.1109/ICSCSS57650.2023.10169163

[13] Khaleelullah, S. K., Reddy, K. S., Reddy, A. S., Kedhar, D., Bhavana, M., & Naresh, P. (2024). Pharmashield: Using blockchain for anti-counterfeit protection. Proceedings of the 2024 2nd International Conference on Inventive Computing and Informatics (ICICI 2024), 529–534. https://doi.org/10.1109/ICICI62254.2024.00092

[14] Srilakshmi, P., Shareef, D.K., Jayudu, T.V.N., Chaithanya, D., Sonavane, S.M., & Anushna, S.D. (2023). Novel framework for blockchain-based voting application using Ethereum Virtual Machine. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7), 72-78. https://doi.org/10.17762/ijritcc.v11i7s.6978

[15] Prabhakar, M., Emmidi, S., Parsi, N., Bharatha, R., & Chidella, T. (2023). Validation of products and eliminating counterfeits using blockchain. In Proceedings - 2023 International Conference on Computational Intelligence for Information, Security and Communication Applications, CIISCA 2023 (pp. 184-188). IEEE. https://doi.org/10.1109/CIISCA59740.2023.00044

[16] Jeny, J. R. V., Sekaran, K., & Dandyala, S. S. (2021). Improved interop blockchain applications for e-healthcare systems. In Blockchain and Machine Learning for e-Healthcare Systems (pp. 267–293). https://doi.org/10.1007/978-981-33-4543-0_16

[17] Marappan, R., Vardhini, P.A.H., Kaur, G., Murugesan, S., Kathiravan, M., Bharathiraja, N., & Venkatesan, R. (2023). Efficient evolutionary modeling in solving maximization of lifetime of wireless sensor healthcare networks. Soft Computing, 27, 11853-11867. https://doi.org/10.1007/s00500-023-08623-w

[18] Lokhande, M., Kalpanadevi, D., Kate, V., Tripathi, A.K., & Bethapudi, P. (2023). Study of computer vision applications in healthcare Industry 4.0. In Healthcare Industry 4.0: Computer Vision-Aided Data Analytics (pp. 151-166). https://doi.org/10.1201/9781003345411-10

[19] Singh, J., Shelke, N. A., Upreti, K., Divakaran, P., Lingareddy, N., & Deepika, S. (2024). Enhancing patient well-being in healthcare through the integration of IoT and neural network. Proceedings of the 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP 2024), 241–246. https://doi.org/10.1109/INNOCOMP63224.2024.00047

[20] Marappan, R., Vardhini, P. A. H., Kaur, G., Murugesan, S., Kathiravan, M., Bharathiraja, N., & Venkatesan, R. (2024). Retraction note: Efficient evolutionary modeling in solving maximization of lifetime of wireless sensor healthcare networks. Soft Computing. https://doi.org/10.1007/s00500-024-10146-x

[21] Srivastava, S. K., Mahto, M. K., Verma, D. K., & Kantha, P. (2024). Cloud-integrated big data algorithms for deep learning in healthcare systems. In Advances in Science, Technology and Innovation (pp. 169–179). https://doi.org/10.1007/978-3-031-63103-0_18

[22] Logeshwaran, J., Thiyagarajan, N., Mahto, M. K., & Garg, A. (2023). Clinical resource management with AI/ML-driven automated diagnostics in smart healthcare. ACM International Conference Proceeding Series, 173. https://doi.org/10.1145/3647444.3652480

[23] RaviKrishna, B., Seno, M. E., Raparthi, M., Yellu, R. R., Alsubai, S., Dutta, A. K., Aziz, A., Abdurakhimova, D., & Bhola, J. (2024). Artificial intelligence probabilities scheme for disease prevention data set construction in intelligent smart healthcare scenario. SLAS Technology, 29, 100164. https://doi.org/10.1016/j.slast.2024.100164

[24] RaviKrishna, B., Potluri, S., Jeny, J.R.V., Sajja, G.S., & Rao, K.S. (2022). Fuzzy-based edge AI approach: Smart transformation of healthcare for a better tomorrow. In Fuzzy Computing in Data Science: Applications and Challenges (pp. 181-196). https://doi.org/10.1002/9781394156887.ch10

[25] Rahi, P., Dandotiya, M., Gantla, H.R., Nagaraju, R., Shivakanth, G., & Ahuja, V. (2023). Edge-cognitive computing for improvising the healthcare 5.0. In Contemporary Applications of Data Fusion for Advanced Healthcare Informatics (pp. 369-391). IGI Global. https://doi.org/10.4018/978-1-6684-8913-0.ch016

[26] Chowdary, B. V., & Radhika, Y. (2019). Optimal variables identification and statistical mining approach for healthcare data. Journal of Advanced Research in Dynamical and Control Systems, 11, 1487-1495.

[27] Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. *Blockchain: Research and Applications*, *5*(2), 100178.