Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

A Conic Curve Digital Signature with Blockchain Mechanism for Securing EHR Data in IOT-Fog-Cloud Environments

Dr. B. Arunapriya

Assistant Professor, Department of Computer Science, A.V.P. College of Arts and Science (Co-Education), Tirupur, Tamil Nadu, India.

Abstract

The use of Internet of Things (IoT) technology and cloud computing in healthcare, outsourcing Electronic Health Records (EHRs) created by IoT devices becomes an important issue. In a real-time scenario, since EHRs might be gathered by multiple divisions within a hospital and sent over intranet or public networks, the situation raises risks for privacy breaches. Many existing studies use cloud-based access control and encryption methods to safeguard outsourced EHRs. Nonetheless, in an IoT cloud data-sharing environment where data comes from a variety of devices and user permission status changes often, there is still a gap in achieving the complete and systematic integration of secure IoT data transmission and aggregation. Furthermore, advances in attack tactics and resources may eventually compromise any cryptographic system based on a single mathematical flaw. By designing methods that rely on a variety of challenging factors, the system is safeguarded even if one of them is compromised. Therefore, this manuscript presents a new Conic Curve Digital Signature with Blockchain (CCDSB-Chain) system for securing EHR data in IoT-Fog-Cloud environments. In this system, Conic Curve-Based Encryption with Digital Signature (CCBE-DS) is proposed, which uses blockchain and fog-cloud computing to safely manage EHR data. This system collects data from IoT devices, processes and encrypts it at fog nodes, and then securely stores it on the blockchain. Access to critical information is meticulously regulated by preset attribute sets, guaranteeing that only authorized individuals may access the data. Furthermore, the experimental results show that the proposed CCDSB-Chain enhances EHR data security, reduces computational costs, and maximizes access efficiency.

Keywords: IoT-Fog-Cloud network, E-health data, Blockchain, Conic curve encryption, Digital signature

1. Introduction

In the digital era, healthcare information systems have undergone transformative changes, with patient health data progressively stored and processed electronically. This change has improved the efficiency and quality of healthcare services while facilitating precision treatment and research through data analytics [1]. Nonetheless, it has also raised substantial issues pertaining to data security and privacy [2]. The delicate nature of patient data renders current security approaches, including data encryption and access control, unable to address the intricate requirements of medical data processing [3, 4]. This problem is especially significant in the Internet of Medical Things (IoMT) context. Consequently, guaranteeing the effective and secure protection of data within the IoMT context while preserving patient privacy has emerged as a pressing concern [5]. The rapid advancement of healthcare informatization has made the digital processing of medical data standard practice. The extensive use of IoMT devices has significantly enhanced the efficacy of data gathering, exchange, and storage [6]. The sensitivity of medical data and its widely dispersed processing environment present considerable security and privacy challenges. Despite the use of conventional encryption techniques and access control measures in current healthcare information systems, they often encounter difficulties in managing the complications posed by developing technologies such as cloud computing and the IoT [7]. In contexts characterized by extensive data dissemination, such as EHR systems, the sharing and transfer of patient data present significant privacy hazards

[8]. Conventional encryption techniques are essential for safeguarding medical data; however, they encounter several constraints. Walid et al. [9] evaluated several Attribute-Based Encryption (ABE) systems, highlighting that conventional symmetric and asymmetric encryption schemes inadequately address complex situations for data access control. These schemes often fall short in facilitating fine-grained access control based on user roles and traits. Adeniyi et al. [10] presented a blockchain-based smart healthcare system aimed at data protection, which may substantially improve privacy and security in the management of medical data.

Attribute-Based Signcryption (ABSC) is an innovative encryption method that integrates attribute-based encryption with attribute-based signing techniques. It delineates data access rights using attribute sets, facilitating precise access control [11]. ABSC facilitates access to encrypted data by providing rights via attribute sets, making it especially effective for safeguarding sensitive information, including medical data. This technique efficiently manages user authentication and data encryption concurrently in healthcare applications, while its signature process guarantees data integrity. He et al. [12] stated that ABSC can guarantee data privacy and security in cross-platform healthcare data exchange. Implementing a revocation mechanism allows for the dynamic updating of user access rights in response to changes in user privileges, hence augmenting data sharing security. While ABSC offers robust security, its substantial computing resource requirements may render it inappropriate for low-power devices in medical settings. The effective distribution and administration of several encryption keys continue to be a barrier to this method. Furthermore, its computational complexity persists as a limitation, particularly in the context of extensive medical data exchange.

Asymmetric cryptographic algorithms that balance security, computational efficiency, and attack resistance, such as Rivest-Shamir-Adleman (RSA) [13] and Elliptic Curve Cryptography (ECC) [14], were created to address this problem. The security of these algorithms is often derived from their ability to solve difficult mathematical problems such as the Discrete Logarithm Problem (DLP) and the Integer Factorization Problem (IFP) [15]. ECC uses DLP for its cryptographic strength, but RSA applies IFP for safe digital signatures. However, advancements in attack techniques and resources can ultimately hack any cryptographic system based on a single issue. By creating schemes that depend on many hard issues, the system is protected even if one of them is compromised.

Compared to ECC, Conic Curve Cryptography (CCC) is a new paradigm that offers better computing efficiency and attack resistance. It provides strong security against a range of attacks by using the characteristics of conic curves to implement issues such as IFP, as in RSA, and DLP, as in ECC. It also presents a new architecture that guarantees communication and computation efficiency, which makes it ideal for securing healthcare systems.

1.1 Motivation

The security and privacy of medical data have emerged as crucial concerns in the digital healthcare landscape, especially with the rapid proliferation of the IoMT. Although blockchain and ECC have been examined in numerous studies for the protection of healthcare data, their integration into resource-constrained IoMT contexts continues to present significant issues. This paper presents a revolutionary architecture that uniquely blends blockchain, fog-cloud computing, and CCC to meet the demands of IoMT settings. While blockchain is well-known for its capacity to assure data immutability and transparency, and CCC has been shown to offer fine-grained access control, their combination into an efficient, decentralized system for the IoMT has yet to be completely explored. Furthermore, modern blockchain-based solutions often rely on centralized cloud computing, which can lead to latency and security concerns.

1.2 Main Contributions

The primary contribution is the development of a hybrid architecture called CCDSB-Chain that combines blockchain and fog-cloud computing to provide a decentralized, secure, and scalable infrastructure for handling EHR. This proposed system considerably decreases computational cost and delay by directing encryption and decryption operations on edge nodes adjacent to data sources, which is critical for real-time medical data processing. Furthermore, the system uses CCC to guarantee that only authorized individuals who meet certain criteria may access critical medical data, making it ideal for multi-role situations in healthcare.

In contrast to prior efforts, this study focuses on the particular optimization of merging these technologies with edge computing to handle the unique problems of IoMTs, such as resource limits and the necessity for rapid, low-latency data processing. This paper provides a complete review and comparison of current solutions to highlight the benefits of our framework, such as improved security, performance, and scalability. Furthermore, a comprehensive analysis shows how edge computing boosts the overall efficiency of blockchain-based EHR systems. The contributions of this study are as follows:

1. A unique architecture i.e., CCDSB-Chain is developed that amalgamates blockchain, edge computing, and cloud computing for the secure and efficient management of EHR data, particularly tailored to fulfill the demands of IoMT settings.
2. To generate safe and effective pseudorandom sequences, a novel iterative conic curve pseudorandom number generator is presented. Also, three different cryptographic hard problems, such as the conic curve discrete logarithm problem, the Gaussian conic curve integer factorization challenge, and the conic curve integer factorization problem, are included in a proposed digital signature technique. This offers long-term security by ensuring strong authentication, data integrity, and non-repudiation.
3. Moreover, an in-depth analysis that evaluates the proposed CCBE-DS system with current blockchain-based EHR systems, highlighting its benefits regarding security, scalability, and computing efficiency.

The remaining article is prepared as follows: Section 2 discusses current related works. Section 3 explains the CCDSB-Chain system and Section 4 demonstrates its performance. Section 5 gives the conclusion and future work.

2. Literature Survey

In [16], a solution was suggested for e-health systems by integrating the Lattice-Based Access Control (LBAC) scheme with blockchain-based smart contracts to create multi-level security. LBAC provided multilayered security for access control restrictions, while smart contracts facilitated the transaction process in a decentralized system by mutual consent of the parties involved. The patient's e-health information was acquired and preserved as immutable blocks inside the blockchain network. Nonetheless, it concentrated only on enhancing multi-level security, whereas a secure distributed ledger architecture was needed for practical applications.

In [17], an effective secure 3-factor privacy-preserving authentication technique was introduced for a cloud-based digital twin environment. They included blockchain and ECC-enhanced security protocols to ensure safe interactions among authorized users and mitigate security risks. Nevertheless, it entails high costs in transmission, computing, and storage while maintaining a robust security standard. In [18], a blockchain-based authentication and key management system was developed for IoMT-enabled smart healthcare applications. However, costs associated with computation and communication were high.

In [19], blockchain technology and smart contracts were used in a cloud-based healthcare system to ensure the security and accessibility of EHRs. They proposed a blockchain-based methodology for managing EHRs and used Ciphertext-Policy ABE (CP-ABE) to establish a precise access control policy. Nonetheless, it incurs high computational overhead. In [20], a blockchain-enabled, scalable, and secure framework was designed for multidimensional data aggregation in fog-based wireless body area networks. The complex medical information was generated, encrypted, and then decoded by the Paillier cryptosystem. The batch verification approach was used to attain effective authenticity. Nonetheless, the communication overhead was high.

In [21], the RSHealth model, a methodology for ring signatures was developed that facilitates identity anonymization and transaction confidentiality in blockchain-based e-healthcare systems. This model devised a distinctive anti-tampering technique to enhance security against threats and unauthorized access. Healthcare stakeholders established a distinctive approach to safeguard data privacy, ensuring the anonymization of sensitive data during file transfer. In contrast, a significant drawback was the absence of IoT device authentication, which impacts overall security and privacy.

In [22], a blockchain-based access control mechanism was applied for outsourced IoT-enabled EHRs in fog-assisted cloud settings. Fog computing was utilized to mitigate the computational burden associated with the encryption and decryption of CP-ABE. The dynamic load-balancing strategy was implemented to facilitate the efficient distribution of workloads among the fog nodes. Moreover, blockchain was used to manage user identification and guarantee the integrity of the EHRs. However, its scalability was insufficient for extensive networks with substantial IoT traffic.

In [23], Blockchain-based Decentralized Secure Sharing (BDSS) using the Shuffled Random Starvation Link Encryption (SRSLE) method was introduced to protect sensitive EHRs. The quasi-sensitive attribute identification method was used to evaluate and categorize the sensitive instances of EHR. The essential attributes were encrypted using the novel SRSLE approach to protect the user's confidential information. The principal authentication policy was used to authenticate key node aggregation and peer-end verification for data dissemination among users. Nonetheless, it has issues with scalability and computational costs in real-time healthcare systems for safeguarding sensitive personal EHRs.

In [24], a safe trust management approach was introduced with blockchain. This methodology gathered node trust data via both time- and event-driven techniques to assess a node's trust relative to a threshold value. The trust scores of each node were securely kept in an array, and the maximum subarray (Kadane) technique was used to calculate the threshold value. The trust metrics from IoMT devices were documented in the blockchain network. Conversely, an increase in the number of devices may lead to challenges with scalability, storage, and transaction management within a network connection.

In [25], an innovative Hierarchical Blockchain Edge of Things (HBEoT) architecture was developed to enable blockchain-managed healthcare applications at the network edge. A block of healthcare data was created with Proof of Stake (PoS) consensus, with hash values recorded on the blockchain. Healthcare systems were validated with Zero-Knowledge Proof (ZKP) to enhance privacy and security. However, the costs associated with transmission and storage for this technology were high. A decentralized system was created in [26] using blockchain and cloud computing to securely access EHRs with outstanding integrity. Nevertheless, the system encounters challenges related to scalability and performance limitations while processing immense amounts of real-time data.

In [27], a method was proposed for the safe administration of mobile healthcare systems via blockchain technology. A patient-centric access control mechanism was developed via a smart contract, allowing physicians and patients to access medical test results via a decentralized web portal and mobile interface. A Proof of Concept (PoC) was conducted to automate and facilitate the safe administration and sharing of critical health information via mobile platforms. Nonetheless, it has network scalability limitations, including higher transaction costs and prolonged processing times as the user population grows.

In [28], a blockchain-based framework was developed intended to guarantee safe integration of diverse sources of IoMT data. The EHR was managed via authorized blockchain technology. Edge computing techniques were included to enhance data-processing efficiency. Nonetheless, the proliferation of IoMT devices raises computational costs, namely the delays in blockchain commitments. Table 1 summarizes the above-discussed studies in terms of techniques used, merits and demerits.

Table 1. Summary of Existing Blockchain-Based Cloud-IoT Networks in Healthcare Applications

Ref. No.	Techniques	Merits	Demerits
[16]	LBAC, smart contracts, and Keccak-256 hash function	It maintained data integrity and transparency with multi-level access control security.	It concentrated only on enhancing multi-level security, whereas a secure distributed ledger architecture was needed for practical applications.

[17]	3-factor privacy-preserving authentication and ECC	It achieved greater security and lower execution time.	It entails high costs in transmission, computing, and storage while maintaining a robust security standard.
[18]	Blockchain-based authentication, key management, and key agreement	It achieved higher transactions per second and security.	Costs associated with computation and communication were high.
[19]	CP-ABE, smart contracts	It ensured high scalability and security for health data transmission.	It incurs high computational overhead.
[20]	Blockchain-based data aggregation, Paillier cryptosystem, and batch verification	It has lower computation overhead and achieved efficient authentication.	The communication cost was high.
[21]	Ring signature, smart contracts	It increased throughput and reduced latency efficiently.	A significant drawback was the absence of IoT device authentication, which impacts overall security and privacy.
[22]	CP-ABE, pseudorandom encryption, symmetric encryption, graph-based modeling, and adaptive load distribution	It reduced encryption and decryption time significantly.	Its scalability was insufficient for extensive networks with substantial IoT traffic.
[23]	Blockchain, SRSLE, quasi-sensitive attribute detection, and key authentication policy	It ensured high reliability and security for processing EHRs.	It has issues with scalability and computational costs in real-time healthcare systems for safeguarding sensitive personal EHRs.
[24]	Blockchain, Kadane algorithm, and trust management	It ensured high dependability and lower overhead.	An increase in the number of devices may lead to challenges with scalability, storage, and transaction management within a network connection.
[25]	HBEoT	It achieved higher throughput. Also, it lowered latency, and energy usage.	The expenses associated with transmission and storage for this technology were high.
[26]	Blockchain, homomorphic encryption, smart contracts	It has high feasibility, security, efficiency, and privacy for EHR storage and access.	It encounters challenges related to scalability and performance limitations while processing immense amounts of real-time data.

[27]	Blockchain-based secure management	It reduced energy efficiency and query response time significantly.	It has network scalability limitations, including higher transaction costs and prolonged processing times as the user population grows.
[28]	Blockchain and edge computing	It enhanced interoperability, data integrity, and confidentiality.	The proliferation of IoMT devices raises computational costs, namely the delays in blockchain commitments.

The current literature on blockchain-based healthcare systems has shown significant progress in protecting EHRs; however, there are still some critical gaps. A strong emphasis on centralized, cloud-based architectures presents scalability and latency problems in resource-constrained IoMT systems. Furthermore, CP-ABE and ECC algorithms generally have high computational requirements, making them inapplicable to low-power IoT devices. Another limitation is the lack of a holistic combination of fog-cloud computing concepts and blockchain technology, a combination that would improve real-time data processing and access control systems. Moreover, most of the earlier systems do not adequately support dynamic adjustments to user permissions, limiting their practical use in healthcare environments where needs are inherently dynamic. To address these gaps, this study develops the CCDSB-Chain for securing EHRs efficiently with lower computational and communicational costs.

3. CONIC CURVE CRYPTOGRAPHY

Cryptography is increasingly using conic curves because they are easy and effective to compute. Conic curves have a simpler algebraic structure than elliptic curves, which may be useful for certain cryptographic applications. A conic curve over a finite field F_p, where p is an odd prime integer, can be defined as follows:

$$C(F_p): y^2 = ax^2 - bx \quad (1)$$

In Eq. (1), a and b are fundamentals of $\mathbb{F}_p^*$, signifying the group of non-zero elements under multiplication in the finite field. The set F_p comprises p elements, usually denoted as $F_p = \{0,1, \dots, p-1\}$ and the multiplicative group is $\mathbb{F}_p^* = F_p \backslash \{0\}$. Noticeably, if $x = 0$, the point $O(0,0)$ is the origin. For $x \neq 0$, consider $t = yx^{-1}$ and substitute $y = xt$ in Eq. (1), which provides

$$x(a - t^2) = b \text{ where } a, b \in \mathbb{F}_p^* \quad (2a)$$

When $a = t^2$, Eq. (2a) is not satisfied; when $a \neq t^2$, Eq. (2a) yields

$$x = b(a - t^2)^{-1} \text{ and } y = bt(a - t^2)^{-1}, \text{ where } a, b \in \mathbb{F}_p^* \quad (2b)$$

In Eqns. (2b), $(\cdot)^{-1}$ is the multiplicative inverse in $\mathbb{F}_p^*$. For any $t \in F_p$ such that $t^2 \neq a$, consider $P(t)$ is the point (x, y) within $C(F_p)$ calculated by Eq. (2b). As well, an idealized point O called point at infinity $P(\infty)$ is considered a point on $C(F_p)$. Consider

$$T = \{t \in F_p; t^2 \neq a\} \cup \{\infty\} \quad (2c)$$

Then $P: T \to C(F_p)$ refers to the bijective mapping. Then, consider the addition $(\oplus)$ of points in $C(F_p)$. For every point $\forall P(t) \in C(F_p)$ and $t \in T$, so that

$$P(t) \oplus P(\infty) = P(\infty) \oplus P(t) \quad (2d)$$

Consider $P(t_1), P(t_2) \in C(F_p)$, where $t_1, t_2 \in T$ and $t_1, t_2 \neq \infty$, such that

$$P(t_1) \oplus P(t_2) = P(t_3) \quad (2e)$$

$$\text{Where } t_3 = \begin{cases} (t_1, t_2 + a)(t_1 + t_2)^{-1}, & t_1 + t_2 \neq 0 \\ \infty, & t_1 + t_2 = 0 \end{cases} \quad (2f)$$

It is obvious that $t_3 \in T$ and the operation $\oplus$ is commutative. For any point $P(t) \in C(F_p)$, the negative element is provided by $-P(\infty) = P(\infty)$, $-P(t) = P(-t)$. From Eqns. (2c) to (2e), it is demonstrated that for all $\forall P(t_1), P(t_2), P(t_3) \in C(F_p)$,

$$(P(t_1) \oplus P(t_2)) \oplus P(t_3) = P(t_1) \oplus (P(t_2) \oplus P(t_3)) \quad (2g)$$

As a result, $(C(F_p), \oplus, P(\infty))$ represents a finite abelian group. Additionally, $|C(F_p)|$ is described by

$$|C(F_p)| = \begin{cases} p-1, & \left(\frac{a}{p}\right) = 1 \\ p+1, & \left(\frac{a}{p}\right) = -1 \end{cases} \quad (2h)$$

In Eq. (2h), $\left(\frac{a}{p}\right)$ refers to the Legendre symbol.

4. PROPOSED METHODOLOGY

This section explains the proposed CCDSB-Chain system, emphasizing the role of blockchain and fog-cloud computing technologies in facilitating secure data storage and transfer. The interaction procedures among the various modules and the methods used by the system to maintain data integrity and privacy at different stages are first examined.

4.1 System Model

The proposed healthcare system aggregates data from a local network channel and saves it in a public cloud, allowing access to medical information for authorized patients and healthcare providers. Medical records include patient information and identifying numbers (i.e., ID). Figure 1 illustrates the system model used for this suggested framework, based on the following assumptions.

- The information from sensing devices is confidential and held by their users, namely, patients.
- EHRs are obtained via IoT devices affixed to the patients' bodies.
- Healthcare personnel use smartphones to access cloud-based electronic health records, dependent upon their hospital identity.

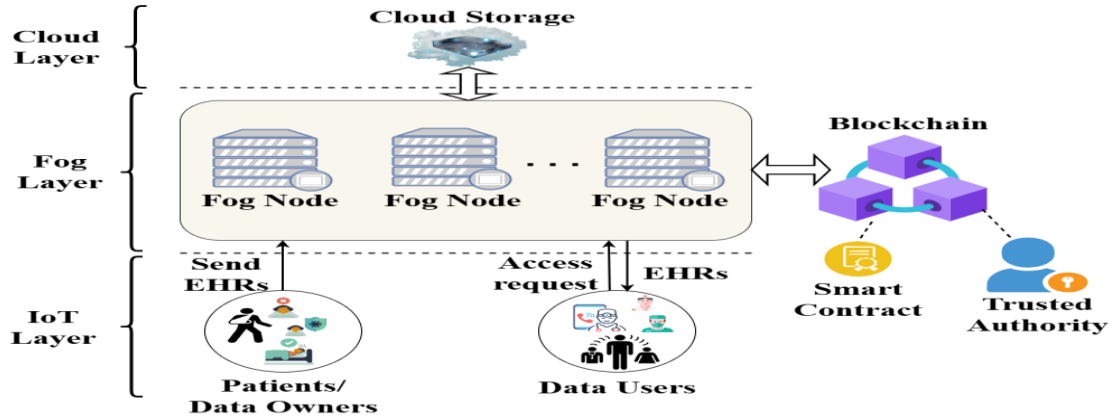

Figure 1. System Model

The suggested system architecture has three tiers: the IoT layer, the fog layer, and the cloud layer. The components inside each layer are specified below.

1. **Data Owners:** Physiological data, including temperature, blood pressure, heart rate, and electrocardiograms, are collected from the patient's body via wearable sensors or IoT devices. Every data point is linked to a corresponding user ID. Individuals whose information is collected via IoT devices are designated as

data owners. The physician who generates or modifies the patient's electronic health records on the patient's behalf is also regarded as a data owner.

2. **Data Users:** Authorized entities, including medical professionals such as doctors and nurses, are referred to as data users and may request access to cloud-stored data on the IoT.

3. **Fog Node:** The fog node serves as the intermediary among users, IoT devices, and the cloud storage system. Numerous fog-type proxy servers are intentionally situated in various places to ensure proximity between users and servers. Facilitating data interchange in response to user requests is the primary objective.

4. **Blockchain:** This research employs a consortium blockchain, an efficient method for managing and sharing healthcare information inside a network governed by a specific group of nodes consisting of healthcare consumers. It does integrity validation via smart contracts and by retaining the hash value of the data. Furthermore, it will maintain access records of people executing the validation function. Furthermore, user authentication procedures have been streamlined and secured via the use of smart contracts.

5. **Trusted Authority:** It governs all transactions and operations, including the assignment and modification of access credentials. It executes smart contracts and is the only entity capable of modifying the rules inside them.

6. **Smart Contracts:** The primary function of a smart contract is to oversee all permitted activities inside an access control system. Communication occurs via the contract address and application binary interface inside the smart contract. Additionally, they may authenticate and validate transactions, as well as provide access privileges to patients by starting transactions. Participants, validators, and administrators of the blockchain may access smart contracts and their functionalities.

7. **Cloud Storage:** A cloud database stores IoT data and access methods. This study utilizes an Interplanetary File System (IPFS). All health records are secured using the CCC approach and securely stored on IPFS. The hash values of medical data are stored and administered in Decentralized Hashing Tables (DHT), mostly by fog nodes. The amalgamation of a smart contract with IPFS augments cloud storage, optimizes data sharing, and facilitates access control.

A description of this suggested framework is as follows: The Data Owner (DO) gathers physiological data, including heart rate and blood pressure, via IoT devices. The DO encrypts the data using a lightweight encryption technique. The encrypted data is then uploaded to a proximate Fog Node (FN) for storage. Subsequently, the FN transmits the encrypted data to the blockchain, where the encrypted data is verified, guaranteeing the integrity and immutability of the data. When a Data User (DU) seeks to access the data, the DU searches the blockchain to locate the relevant encrypted message. The DU submits a request to the DO via the FN, detailing the rationale for requiring access to the data. The DO evaluates the request and determines access authorization based on the established access control regulations. Upon receiving authorization from the DO, the DU obtains the decryption key and employs it to decode the encrypted data. In this procedure, the smart contract facilitates data processing and uploads it to the blockchain, while the Trusted Authority (TA) is tasked with creating and distributing keys, verifying user identities, and maintaining data security. This process is shown in Figure 2.

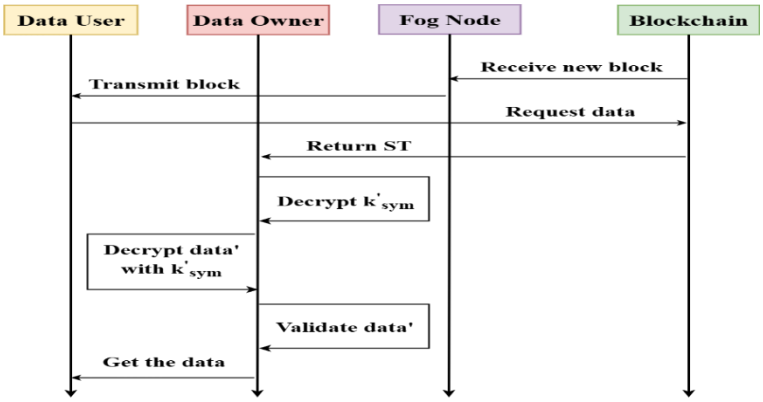

Figure 2. Roles and Functions of the Proposed Framework

4.2 Proposed Conic Curve-Based Encryption with Digital Signature Scheme

This CCBE-DS scheme includes the initialization, key generation, signature generation, and signature verification stages.

4.2.1.1 Initialization

Over the domain of conic curves, the following parameter is often needed during the CCBE-DS's initialization stage:

- Conic curve selection: Select a conic curve $C_{N_n}(a,b)$ over Z_{N_n} is represented by the solutions (x,y) of the congruence equation $y^2 = ax^2 + bx (\mathrm{mod}\, N_n)$, where $\mathrm{mod}\, N_n = pq$, and a, b are curve parameters, such that $(a, N_n) = (b, N_n) = 1$. Also, $p = x_1 + y_1 i$ and $q = x_2 + y_2 i$ are Gaussian primes.
- Calculate the norm: Determine $N_n = p \times q$, ensuring that $(a, N_n) = (b, N_n) = 1$, where N_n is the norm of n.
- Confirm curve criteria: Certify that $\frac{a}{N(p)} = \frac{a}{N(q)} = -1$, where $N(p)$ and $N(q)$ are the norms of the Gaussian primes p and q.
- Determine the curve order: Calculate $N_{N_n} = lcm\left(\#C_{N(p)}(a,b), \#C_{N(q)}(a,b)\right)$, where $\#C_{N(p)}(a,b)$ and $\#C_{N(q)}(a,b)$ are the cardinalities of the respective conic curves. Here, lcm is the function of determining the least common multiple.

4.2.1.2 Key Generation

The sender creates the individual public key as follows:

- $B = (x_B, y_B)$ is the base point of $C_{N_n}(a,b)$ and consider the order as $N_n = 2rs$.
- Select $v \in Z_{N_n}$ as the private key and determine $Y = vB$ as the public key.
- Consider $H(m)$ is the collision free one-way hash function value of the data (or message) m, the m was embedded in the conic curve using the plaintext embedding algorithm, and obtain the point $P(m) = (x_m, y_m)$, where $x_m = \frac{b}{a-m^2} (\mathrm{mod}\, n)$ and $y_m = \frac{bm}{a-m^2} (\mathrm{mod}\, n)$.
- Publish (n, a, b, B, Y), however keep (v, N_n) privately.

4.2.1.3 Signature Generation

The sender creates the signature for the data m, as follows:

- Arbitrarily choose number $r \in Z_{N_n}$.
- Determine $R = P(m) \oplus rB = (x_1, y_1)$, $u = x_1 (\mathrm{mod}\, N_n)$, and $uB = (x, y)$, where (x, y) is considered as B.
- Transform the data $P(m)$ and the value R into one integer w using hash function operation $w = H(P(m), R) \in [1, 2^t]$.
- Determine $s = (r + uwv) (\mathrm{mod}\, N_n)$.
- Transfer the signature (w, s, u, B) to the verifier.

4.2.1.4 Signature Verification

The verifier authorizes the validity of the signature for m as follows:

- Calculate Z as follows: $Z = sB \oplus (-uwY) \oplus P(m) = (x_1', y_1')$.
- Determine $x_1'B$ and calculate w as follows: $w = H(P(m), Z)$.
- When the resulting $x_1'B = (x, y)$ and $H(P(m), Z) = w$, validate the signature; or else discard it.

4.3 CCDSB-Chain Framework

This section explains the methodology of the proposed CCDSB-Chain in the healthcare system using the previously discussed CCBE-DS approach. The system design for EHR data security is categorized into four stages: system configuration, entity registration, data collection and upload, and data querying. The subsequent sections will elucidate the execution of each process and its significance in safeguarding data security.

4.3.1 System Configuration

The TAs use the setup method to generate the public parameters, denoted as pk. The TA is often engaged during the system's startup and entity registration stages. Upon completion of these procedures, the TA functions offline. Initially, given a designated service provider with a pseudonymous identity (ID), this technique produces three cyclic groups, such as G_1, G_2, and G_3, of prime order p, determined by the security parameter λ. It produces the generators g_1 for G_1 and g_2 for G_2, followed by an efficient bilinear map $e: G_1 \times G_2 \to G_3$. Subsequently, two arbitrary exponents α and β, where $\alpha, \beta \in Z_p$, are chosen. The mk is defined as $mk = (\beta, g_2^{\alpha})$. the hash functions $H_1: \{0,1\}^* \to \{0,1\}^{\lambda}$ and $H_2: \{0,1\}^* \to Z_p$ are selected. Subsequently, the TA calculates $h = g_1^{\beta}$ and $t = e(g_1, g_2)^{\alpha}$. The TA ultimately disseminates the public parameters (pk) to all relevant entities across the blockchain network, organized as follows:

$$pk = \langle p, G_1, G_2, H_2, g_1, g_2, h, t \rangle \quad (3)$$

4.3.2 Entity Registration

The TA authenticates the smart contracts, DOs, or DUs during the registration process, which is required when they join the blockchain network. The TA executes the KeyGen algorithm after a successful verification. Initially, the TA chooses the arbitrary value $r_{enc}, r_{sign} \in Z_p$, and determines $D_{enc} = g_2^{\frac{\alpha + r_{enc}}{\beta}}$, $k_{sign} = g_2^{\frac{\alpha + r_{sign}}{\beta}}$, and $k_{ver} = g_2^{r_{sign}}$. Here, k_{sign}, k_{ver}, and sk are considered the signing key, verification key, and decryption key, respectively.

Moreover, the TA determines $D_j = g_2^{r_{enc}} \times g_2^{H_2(j) \times r_j}$ and $D_j' = g_1^{r_j}$, where $r_j \in Z_p$ is the other arbitrarily chosen value for each attribute $j \in S$. After that, the TA returns the asymmetric secret key $sk = \left(D_{enc}, \forall j \in S: D_j, D_j'\right)$. Moreover, the TA securely distributes the signing key k_{sign} to the participating smart contracts via a secure communication channel, and the decryption key sk is allocated to the data owners with the attribute set S. Figure 3 illustrates the registration framework.

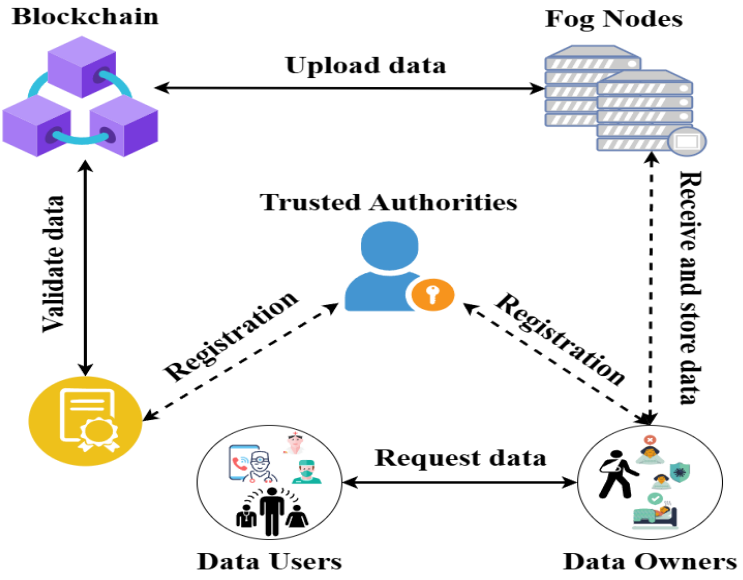

Figure 3. Processes in Entity Registration Step

4.3.3 EHR Data Acquisition and Uploading

To transmit messages to the data owners' blockchain network, the registered smart contract generates a random symmetric key, denoted as k_{sym}, and uses this key to encrypt the EHR data (m), resulting in a ciphertext referred to as C_m. The smart contract then delineates an access tree structure T, which embodies a collection of data owners that conform to the access policy. The smart contract regulates which data owners are permitted to access the encrypted data via T.

Every non-leaf node in the access tree T constitutes a threshold gate, determined by the quantity of child nodes and an associated threshold value. Leaf nodes represent attributes. For every internal node i in T, consider num_i is the number of child nodes and k_i is the threshold value, where $1 \leq k_i \leq num_i$. When $k_i = 1$, the gate does an OR operation, activating if at least one child node satisfies the criterion. When k_i equals num_i, it functions an AND operation, necessitating that all child nodes fulfill the criterion for activation.

In this study, the function $index()$ is defined to represent the order of the leaf nodes in the access tree, helping to assign unique values from 1 to num. As well, the set $attr(i)$ is defined as the attribute of the leaf node i. Once T is defined, the smart contract follows a detailed procedure to encrypt k_{sym} under the tree T. First, after the data owner collects the data from the IoT devices, the smart contract runs the encryption algorithm. This algorithm chooses a polynomial q_i for each node i, including the leaves in T. These polynomials are chosen from top to bottom, starting at the root node R. Starting from R, it randomly chooses a value $s \in Z_p$ and assigns $q_R(0) = s$. Afterwards, it randomly chooses values d_i from Z_p to fully define q_i. For any other node i, it assigns $q_i(0) = q_{par.(i)}\big(index(i)\big)$ and randomly chooses values d_i from Z_p to fully define q_i. Consider Y is the collection of leaf nodes in the access tree T. The smart contract randomly chooses a value $\zeta \in Z_p$ and calculates the following formulas: $\tilde{C} = k_{sym} \oplus t^s, C = h^s, \forall y \in Y: C_y = q_1^{q_y(0)}, C_y' = g_1^{\left(H_2(attr(y)) \times q_y(0)\right)}, \delta = e(C, g_2)^{\zeta}, \pi = H_1(m) + H_2(\delta), w = g_1^s$, and $\psi = g_2^{\zeta} \times \left(k_{sign}\right)^{\pi}$. As a result, the ciphertext with digital signature (ST) under the tree T is generated as:

$$ST = \left(T, \tilde{C}, C, \forall y \in Y: C_y, C_y'; w, \pi, \psi\right) \quad (4)$$

Moreover, given the smart contract's public key pk, pseudonymous identity ID, the block hash h_2, and the ciphertext ST (including the smart contract's signature π), the EHR is stored and transmitted to the blockchain network for verification. The format of the EHR is as follows:

$$R = (pk, ID, h_2, ST) \quad (5)$$

Figure 4 illustrates the processes in data gathering and uploading stage.

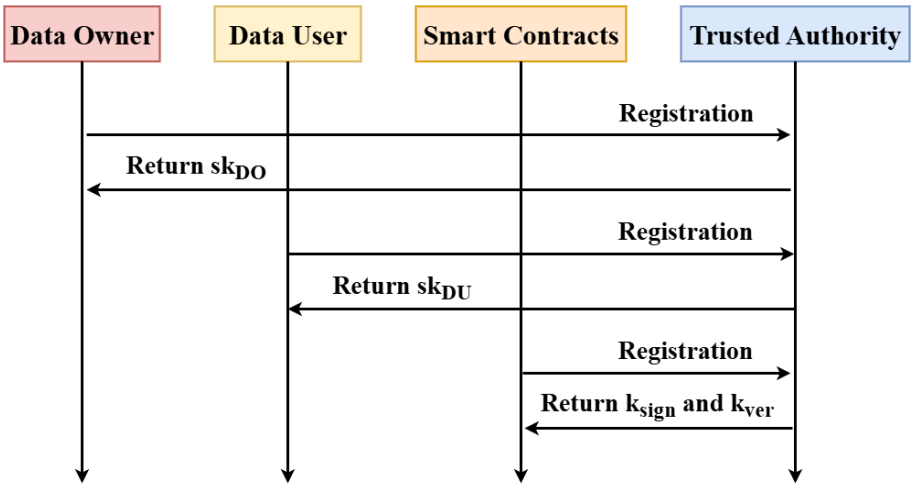

Figure 4. Processes in EHR Data Acquisition and Uploading

4.3.4 EHR Query

Upon receipt of the new block, the fog node is able to relay the blockchain header to the data owner, allowing the data owner to determine if a pull request should be initiated. If deemed essential, the data owner retrieves the signed ciphertext (ST) and the signature π from the designated block. The data user may now start a data query for the necessary information by submitting a request to the data owner. Access control is established using the tree access structure, allowing only data users who satisfy the data owner's access criteria to successfully submit a request.

Upon acquiring ST and π from the blockchain, the data owner initiates the decryption process to extract the symmetric key k_{sym}, subsequently getting the associated data m. The data owner thereafter authenticates the data integrity and advances to signature verification, as described below.

The data owner first conducts the decryption method. This recursive algorithm, $DecryptNode(ST, sk, i)$ takes pk, ST, and sk as inputs. The sk comprises a collection of attributes and a node i from the access tree T. If i is a leaf node, then let $i = attr(i)$. The algorithm yields the following result:

$$DecryptNode(ST, sk, i) = \begin{cases} e(g_1, g_2)^{r_{enc} q_i(0)}, & i \in S \\ \perp, & or\ else \end{cases} \tag{6}$$

Alternatively, when i is a non-leaf node, the algorithm initially invokes the function $DecryptNode(ST, sk, j)$ for each child node j of i, storing the results as F_j. Consider S_i is the collection of child nodes of i, with random size k_i, and comprise each child node j, where $F_j \neq \perp$. If such a set S_i exists, the algorithm determines F_j as follows:

$$F_i = \prod_{j \in S_i} F_j^{\Delta_{x_j, S_i'}(0)} = e(g_1, g_2)^{r_{enc} q_i(0)} \tag{7}$$

In Eq. (7), $x_j = index(j)$ and $S_i' = \{index(j) \| j \in S_i\}$.

The decryption algorithm then invokes the function on the root node r of the access tree T. The data owner can retrieve k_{sym} provided it holds the appropriate attribute set S. When the criteria are satisfied, the value is assigned to $DecryptNode(ST, sk, r) = A = e(g_1, g_2)^{r_{enc} q_r(0)} = e(g_1, g_2)^{r_{enc} S}$. After decryption, the decrypted symmetric key $\left(k_{sym}'\right)$ is obtained as follows:

$$\frac{\tilde{C}}{e(C, D_{enc})/_A} = \frac{k_{sym}' \times e(g_1, g_2)^{\alpha S}}{e(g_1, g_2)^{\alpha S}} = k_{sym}' \tag{8}$$

Moreover, the data owner determines $\delta' = \frac{e(C, \psi)}{(e(w, k_{ver}) \times \tilde{A})^{\pi}}$, where $\tilde{A} = e(C, D_{enc})/_A$. After retrieving k_{sym}', the data owner utilizes it to decrypt the data m'. Then, the data owner computes $H_1(m') + H_2(\delta')$. When the final result matches π, the data owner verifies that the data m has not been tampered with. Figure 5 illustrates the processes in EHR data query stage.

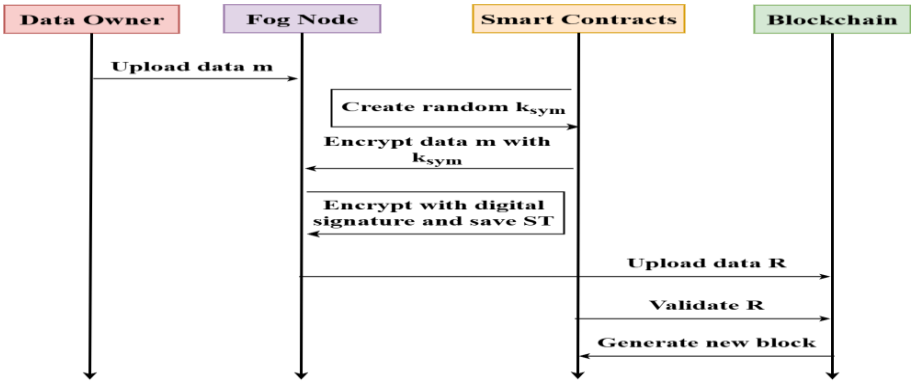

Figure 5. Processes in EHR Data Query

4. SIMULATION RESULTS

This section assesses the efficacy of the CCDSB-Chain framework in comparison to earlier frameworks, including LBAC [16], BDSS [23], RSHealth [21], and HBEoT [25]. Also, the CCBE-DS scheme is evaluated with the existing cryptographic techniques, such as CP-ABE [19], ECC [17], and SRSLE [23]. The experiments are performed on a computer with an Intel Core i7 CPU @ 3.6 GHz, 16 GB of RAM, and a 64-bit operating system. Simulations are carried out on the Ethereum blockchain. The EIP-1559 network allows the creation of a test blockchain with 100 nodes. The EIP-1559 network is developed in Python 3.6 and utilizes the SimPy module for discrete-event simulation. The simulator uses cryptographic hash functions to provide a more customized blockchain simulation compared to SimPy's stochastic model framework. SimPy simulates the Ethereum blockchain network with an object-oriented approach, eliminating the need for blockchain platform installation. The test network is designed to replicate a standard healthcare environment, featuring multiple nodes that represent service providers, data owners, and data consumers to generate network traffic and log files. The network traffic included both legitimate activities and simulated attack behaviors like identity forgery, Denial of Service (DoS), unauthorized access, etc.

4.1 Threat Model

This system's threat model eliminates a number of serious security risks that can jeopardize the availability, confidentiality, or integrity of private medical information. These consist of:

- Identity forgery: To get access to the system, an attacker can attempt to pose as a genuine user. The system depends on the TAs' authentication to stop this, making sure that only authorized users are provided access to the system and given private keys. Every access request is recorded by the blockchain, which may be used for auditing and fraud detection.
- Unauthorized access: Attackers could try to obtain medical data without authorization. However, the CCBE-DS approach, which implements fine-grained access control based on user traits, lessens this hazard. The data can only be decrypted and accessed by people who have the appropriate characteristics. Furthermore, the use of blockchain ensures prompt identification of any illegal attempts to alter or access data.
- Data integrity attacks: These attacks may attempt to alter or tamper with the stored data in the system. Since every update is documented on an immutable ledger, using blockchain guarantees that no data changes may occur undetected. Furthermore, the CCBE-DS scheme's cryptographic signatures ensure that the data is unaltered during transmission and storage.
- Availability attacks: Because the blockchain is decentralized, there is no single point of failure, reducing the possibility of Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks. Furthermore, data processing is offloaded via the edge computing architecture, which lessens the impact on any one node and increases the system's resistance to availability threats.
- Eavesdropping and data leakage: Without the right decryption keys, an attacker cannot read the data, even if they manage to intercept transmission. Data protection during transmission is ensured by the encryption provided by CCBE-DS. Additionally, blockchain technology safeguards the encryption keys, making it more difficult for hackers to obtain them.
- Replay attacks: To prevent replay attacks, the system uses time-stamped, secure communications and access control protocols that confirm the legitimacy of every transaction before executing it.

4.2 Encryption Time

It is the encryption period required to transfer a particular volume of EHR data.

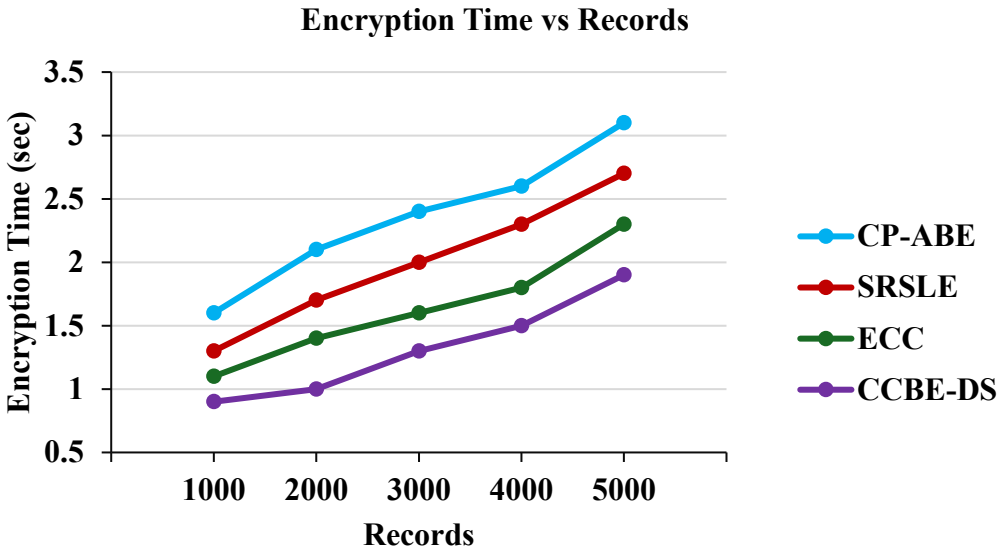

Figure 6. Encryption Time vs. No. of Records

Figure 6 illustrates the encryption time of various encryption schemes, including CP-ABE, SRSLE, ECC, and CCBE-DS for different record counts. It evidently illustrates that the CCBE-DS requires less time to encrypt EHR data compared to the CP-ABE, SRSLE, and ECC, respectively. For 5000 records, the encryption time for CCBE-DS is lowered by 38.71%, 29.63%, and 17.39% compared to the CP-ABE, SRSLE, and ECC, respectively. Thus, it provides high security against various kinds of attacks efficiently.

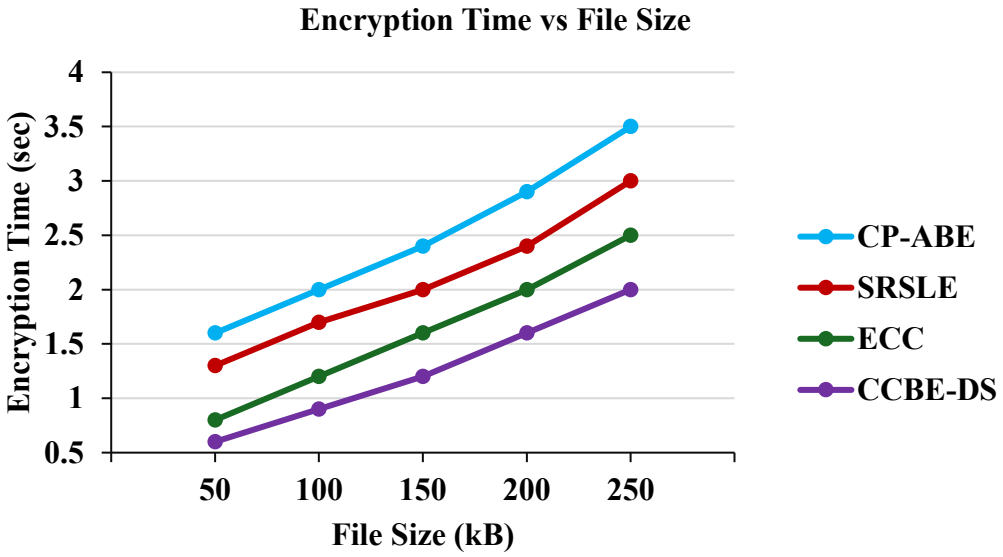

Figure 7. Encryption Time vs. File Size

Figure 7 shows the encryption time of CP-ABE, SRSLE, ECC, and CCBE-DS approaches for different file sizes in kB. It evidently illustrates that the CCBE-DS reduced encryption time by 42.86%, 33.33%, and 20% compared to the CP-ABE, SRSLE, and ECC, respectively. Thus, it provides high security against different attacks efficiently.

4.3 Decryption Time

It refers to the total time the user spends retrieving and decrypting EHR data.

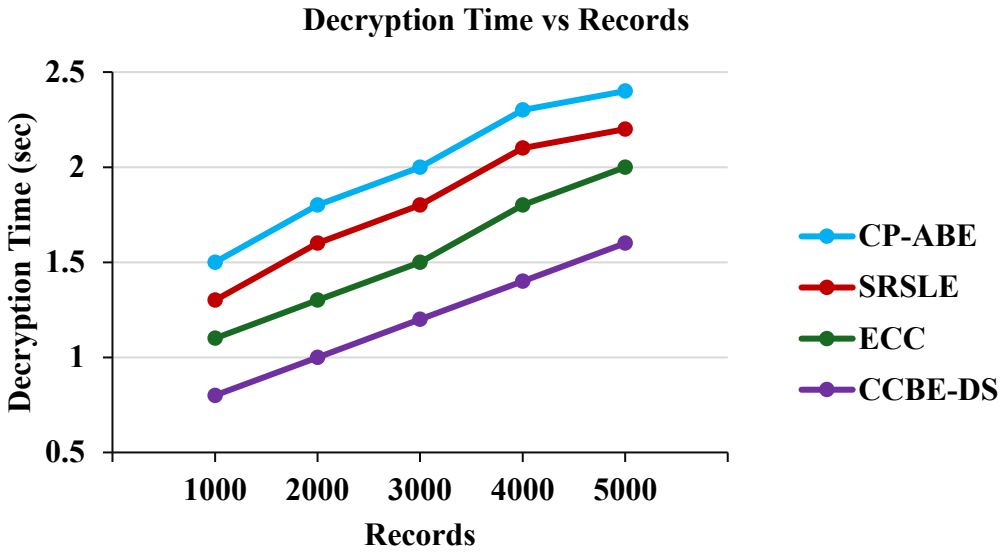

Figure 8. Decryption Time vs. Records

Figure 8 depicts the decryption time of CP-ABE, SRSLE, ECC, and CCBE-DS schemes over varying record quantities. The CCBE-DS demonstrably requires less time to decode EHR data than the other techniques. The decryption time of CCBE-DS for 5000 records is decreased by 33.33%, 27.27%, and 20% compared to the CP-ABE, SRSLE, and ECC, respectively. Thus, it offers robust protection against various attacks effectively.

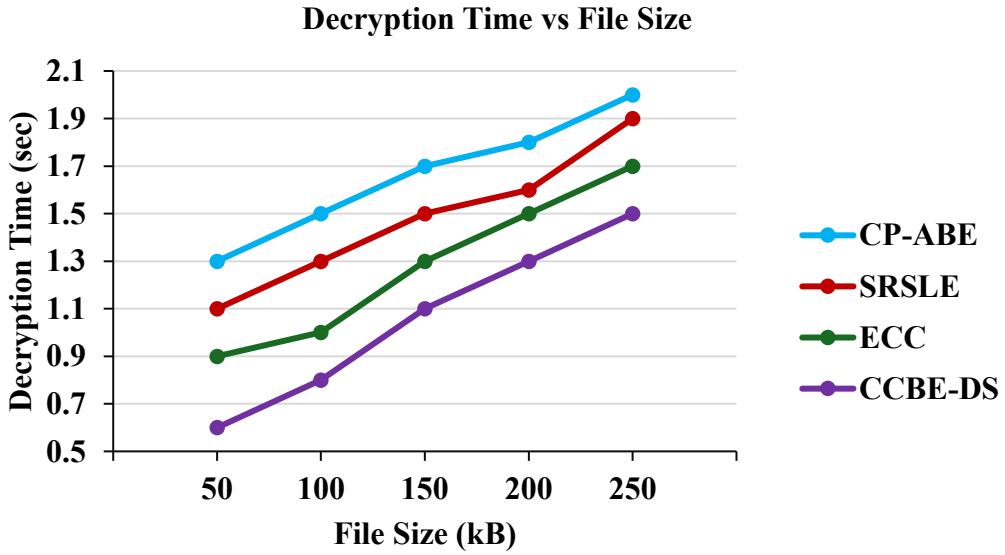

Figure 9. Decryption Time vs. File Size

Figure 9 shows the decryption time of CP-ABE, SRSLE, ECC, and CCBE-DS approaches for different file sizes in kB. It evidently illustrates that the CCBE-DS reduced decryption time by 25%, 21.05%, and 11.76% compared to the CP-ABE, SRSLE, and ECC, respectively. Thus, it efficiently provides high security against different attacks.

4.4 Latency

It is the total time delay to log a transaction on the blockchain.

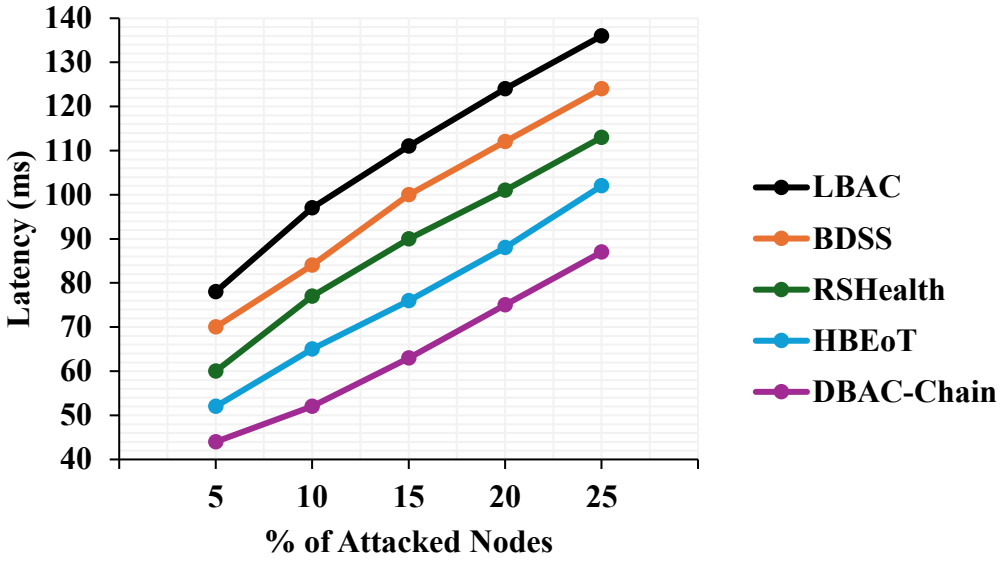

Figure 10. Network Latency vs. Percentage of Attacked Nodes

The network latency as a function of the proportion of attacked nodes is shown in Figure 10 to understand the scalability of the proposed framework. The suggested CCDSB-Chain reduces the latency when 25% of attacked nodes exist in the network by 36.03%, 29.84%, 23.01%, and 14.71% compared to the LBAC, BDSS, RSHealth, and HBEoT, respectively. Thus, the CCDSB-Chain is efficient to EHR data uploading and distribution in IoT-fog-cloud networks with higher security and lower latency.

4.5 Energy Consumption

This refers to the total energy usage of fog nodes during the processes of uploading EHR data, distributing it, and validating transactions on the blockchain.

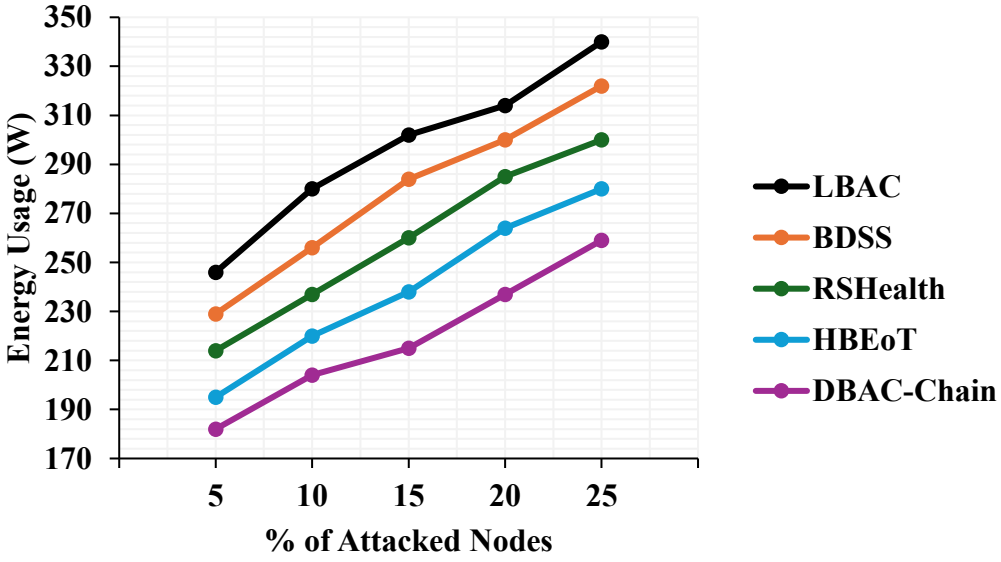

Figure 11. Energy Usage vs. Percentage of Attacked Nodes

Figure 11 displays the energy usage for varying ratios of attacked nodes (i.e., users) in the network. Energy utilization gradually increases as the number of attacked nodes increases. However, the CCDSB-Chain reduces

the energy usage when 25% of attacked nodes exist by 23.82%, 19.57%, 13.67%, and 7.5% compared to the LBAC, BDSS, RSHealth, and HBEoT, respectively. Thus, the proposed CCDSB-Chain can be effective for secure data distribution and access with less energy consumption.

4.6 Transaction Throughput

It defines the number of transactions per second on the blockchain.

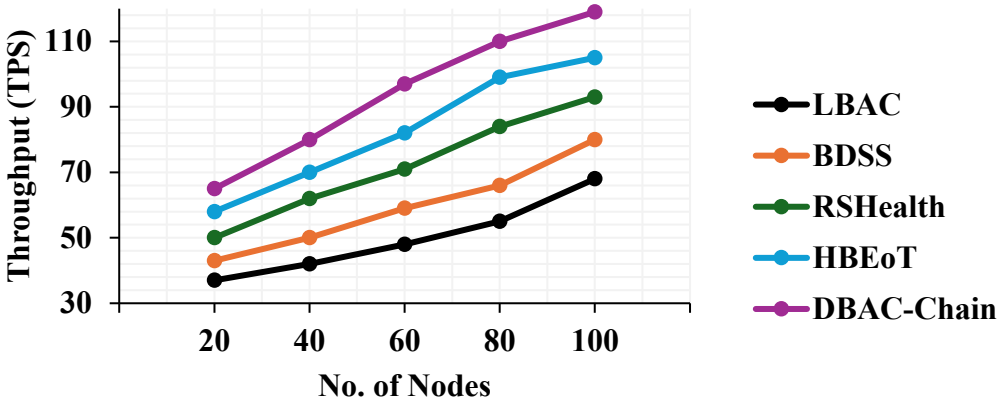

Figure 12. Throughput vs. No. of Nodes

Figure 12 shows a throughput comparison of various frameworks for secure EHR data access under a varying node counts in the network. It can be realized that the proposed CCDSB-Chain attains higher throughput compared to the LBAC, BDSS, RSHealth, and HBEoT, respectively. For instance, the CCDSB-Chain with 100 nodes increases the throughput by 75%, 48.75%, 27.96%, and 13.33% compared to the above-mentioned frameworks.

4.7 Validation Time

It represents the average time needed to evaluate user requests in the cloud.

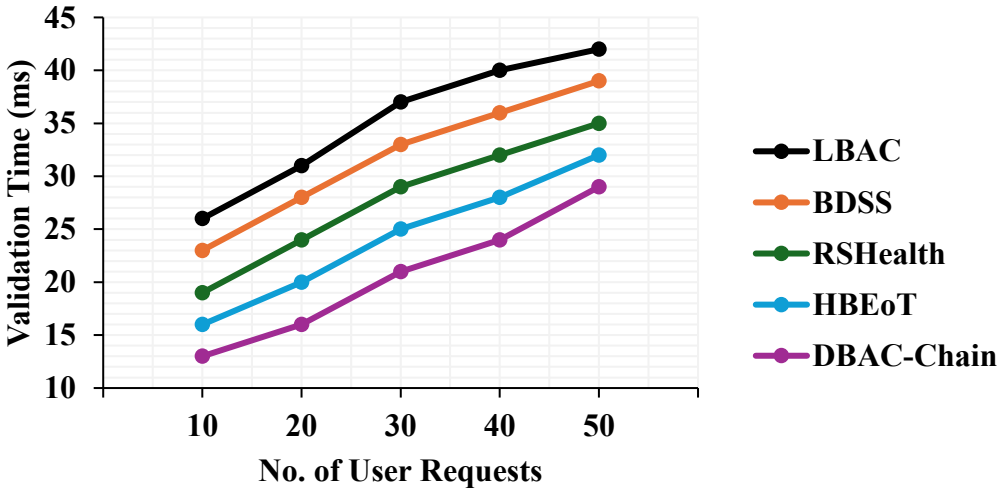

Figure 12. Validation Time vs. No. of User Requests

Figure 12 shows a validation time comparison of various frameworks under a varying quantity of user requests. It can be realized that the proposed CCDSB-Chain achieves lower validation time compared to the LBAC, BDSS, RSHealth, and HBEoT, respectively. The CCDSB-Chain reduces the validation time for 50 requests by 30.95%,

25.64%, 17.14%, and 9.38% compared to the above-mentioned frameworks. This proves that the suggested CCDSB-Chain achieves the user authentication and authorization with low validation time.

4.8 Security Analysis

To protect medical data in an IoMT setting, the proposed framework utilizes a robust security architecture based on CCBE-DS and blockchain technology. Only authorized entities, verified for certain aspects, can access the encrypted data through the CCBE-DS system. The following vital aspects are included in the security analysis:

- Data confidentiality: Only devices with the appropriate attribute sets and matching private keys can decode the data due to the CCBE-DS. This safeguards sensitive medical data from unauthorized access.
- Data integrity: The system uses cryptographic signatures to ensure that the data remains unaltered during transmission or storage. Signature verification enables the identification of any data changes.
- Authenticity of messages: The system ensures that requests for data access and transmission originate from individuals who have been validated. To execute the suggested cryptographic system, TAs issue publicly available encryption keys, which also provide an authentication framework for data consumers and the data owners they are linked with.
- Access control: By using an attribute set, the system offers fine-grained access control, guaranteeing that only authorized users may access the encrypted data. To ensure accurate data retrieval permissions, each data access request is verified according to the user's characteristics.

Table 2 provides an assessment of the CCDSB-Chain framework and current frameworks, emphasizing the essential security features. It assesses several security features using two options: Y (yes–present) and NA (not available), according to the extensive pertinent research detailed in Section 2. The evaluation results demonstrate that the proposed framework exceeds traditional frameworks, making it a viable option for improving existing e-health systems. Thus, by integrating blockchain, fog-cloud computing, and CCBE-DS, the proposed system establishes a robust defense against common and advanced security threats in IoMT settings.

Table 2. Performance Evaluation of Proposed CCDSB-Chain with Existing Frameworks

Frameworks	**Flexibility**	**Transparency**	**Data Availability**	**Access Control**	**Identity Access**	**Authentication**	**Data Privacy**	**Integrity**
LBAC [16]	NA	Y	Y	Y	Y	Y	Y	Y
BDSS [23]	NA	NA	Y	Y	Y	Y	Y	Y
RSHealth [21]	Y	NA	NA	Y	Y	NA	Y	Y
HBEoT [25]	Y	Y	NA	Y	Y	Y	Y	Y
Proposed CCDSB-Chain	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**

5. CONCLUSION

In this article, the CCDSB-Chain system was developed for safeguarding EHR data in IoT-Fog-Cloud scenarios. The CCBE-DS strategy was presented with the blockchain and fog-cloud computing for the secure management of EHR data. This system gathered data from IoT devices, processed and encrypted it at fog nodes, and then stored it securely on the blockchain. Access to essential information was rigorously controlled by predetermined attribute sets, ensuring that only authorized persons could access the data. Moreover, the experimental findings

demonstrated that this CCDSB-Chain system improves EHR data security, decreases computational expenses, and optimizes access efficiency.

REFERENCES

[1] Shen, Y., Yu, J., Zhou, J., & Hu, G. (2025). Twenty-five years of evolution and hurdles in electronic health records and interoperability in medical research: comprehensive review. *Journal of Medical Internet Research*, *27*, e59024.

[2] Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics*, *22*(1), 122.

[3] Wani, R. U. Z., Thabit, F., & Can, O. (2024). Security and privacy challenges, issues, and enhancing techniques for internet of medical things: a systematic review. *Security and Privacy*, *7*(5), e409.

[4] Li, N., Xu, M., Li, Q., Liu, J., Bao, S., Li, Y., ... & Zheng, H. (2023). A review of security issues and solutions for precision health in internet-of-medical-things systems. *Security and Safety*, *2*, 2022010.

[5] Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2023). Towards a secure and sustainable internet of medical things (IoMT): requirements, design challenges, security techniques, and future trends. *Sustainability*, *15*(7), 6177.

[6] Hireche, R., Mansouri, H., & Pathan, A. S. K. (2022). Security and privacy management in internet of medical things (IoMT): a synthesis. *Journal of Cybersecurity and Privacy*, *2*(3), 640-661.

[7] Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., ... & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, *14*(4), 448.

[8] Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: a systematic mapping study. *Journal of Public Health*, *32*(3), 435-454.

[9] Walid, R., Joshi, K. P., & Choi, S. G. (2024). Comparison of attribute-based encryption schemes in securing healthcare systems. *Scientific Reports*, *14*(1), 7147.

[10] Adeniyi, J. K., Ajagbe, S. A., Adeniyi, A. E., Adeyanju, K. I., Afolorunso, A. A., Adigun, M. O., & Ogene, I. (2025). A blockchain-based smart healthcare system for data protection. *iScience*, *28*(4), 112109.

[11] Gong, B., Guo, C., Guo, C., Sun, Y., Waqas, M., & Chen, S. (2023). SLIM: a secure and lightweight multi-authority attribute-based signcryption scheme for IoT. *IEEE Transactions on Information Forensics and Security*, *19*, 1299-1312.

[12] He, Z., Chen, Y., Luo, Y., Zhang, L., & Tang, Y. (2023). Revocable and traceable undeniable attribute-based encryption in cloud-enabled e-health systems. *Entropy*, *26*(1), 45.

[13] Liu, K., Xu, G., Cao, Q., Wang, C., Jia, J., Gao, Y., & Xu, G. (2023). A Rivest–Shamir–Adleman-based robust and effective three-factor user authentication protocol for healthcare use in wireless body area networks. *Sensors*, *23*(21), 8992.

[14] Yao, H., Yan, Q., Fu, X., Zhang, Z., & Lan, C. (2022). ECC-based lightweight authentication and access control scheme for IoT e-healthcare. *Soft Computing*, *26*(9), 4441-4461.

[15] Ivanov, A., & Stoianov, N. (2023). Implications of the arithmetic ratio of prime numbers for RSA security. *International Journal of Applied Mathematics and Computer Science*, *33*(1), 57-70.

[16] Haritha, T., & Anitha, A. (2023). Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system. *IEEE Access*, *11*, 114322-114340.

[17] Thakur, G., Kumar, P., Jangirala, S., Das, A. K., & Park, Y. (2023). An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment. *IEEE Access*, *11*, 26877-26892.

[18] Thapliyal, S., Wazid, M., Singh, D. P., Das, A. K., Shetty, S., & Alqahtani, A. (2023). Design of robust blockchain-envisioned authenticated key management mechanism for smart healthcare applications. *IEEE Access*, *11*, 93032-93047.

[19] Shahzad, A., Chen, W., Shaheen, M., Zhang, Y., & Ahmad, F. (2024). A robust algorithm for authenticated health data access via blockchain and cloud computing. *Plos One*, *19*(9), e0307039.

[20] Subramani, J., Azees, M., Rajasekaran, A. S., Aljaedi, A., Bassfar, Z., & Jamal, S. S. (2024). Blockchain-enabled secure data collection scheme for fog-based WBAN. *IEEE Access*, *12*, 38287-38297.

[21] Prabha, P., & Chatterjee, K. (2024). RSHealth: a ring signature scheme for identity anonymization and transaction privacy in blockchain based e-healthcare systems. *IEEE Access*, *12*, 117701-117720.

[22] Fugkeaw, S., Gupta, R. P., & Worapaluk, K. (2024). Secure and fine-grained access control with optimized revocation for outsourced IoT EHRs with adaptive load-sharing in fog-assisted cloud environment. *IEEE Access*, *12*, 82753-82768.

[23] Kala, M. K., & Priya, M. (2024). Smart IoT-blockchain security to secure sensitive personal medical data using shuffled random starvation link encryption. *IEEE Access*, *12*, 168182-168196.

[24] Al Qathrady, M., Saeed, M., Amin, R., Alshehri, M. S., Alshehri, A., & Alqhtani, S. M. (2024). Smart healthcare: a dynamic blockchain-based trust management model using subarray algorithm. *IEEE Access*, *12*, 49449-49463.

[25] Maheshwari, V., & Prasanna, M. (2025). Privacy-preserving authentication for 5G healthcare with HBZKP: hierarchical blockchain-based zero knowledge proof for secure edge devices. *Ain Shams Engineering Journal*, *16*(8), 103463.

[26] Alahmari, S., Alshardan, A., Al-Wesabi, F. N., Sorour, S., Alghushairy, O., Alsini, R., ... & Al Duhayyim, M. (2025). A decentralized and privacy-preserving framework for electronic health records using blockchain. *Alexandria Engineering Journal*, *126*, 196-203.

[27] Alkhalil, A., Razzaq, A., Ahmad, A., Abdelrhman, M., Altameemi, Y., Altamimi, M., & Tao, Z. (2025). A framework for blockchain-based secure management of mobile healthcare (mHealth) systems. *Journal of Web Engineering*, *24*(3), 317-354.

[28] Ali, A. S. M., Ali, S., Ziaullah, K., Joo, M. I., & Kim, H. C. (2025). IoMT and blockchain synergy: a novel approach to health data validation and storage. *IEEE Access*, *13*, 57753-57766.