Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BLOCK CHAIN BASED SECURED EHR WITH UNIFIED SIGNATURE ENCRYPTION SCHEME

VENKATESWARAN S [1], VIJAYARAJ N [2]

[1]Assistant Professor, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Department of Computer Science and Engineering, Chennai, India
[2] Professor, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Department of Computer Science and Engineering, Chennai, India
E-mail: [1]venkates39@gmail.com, [2]vijaiphdraj@gmail.com

ABSTRACT

Electronic Health Record(EHR) manage medical information in digital form and allow the patient to view their information and distribute the same to the doctors to diagnoses. Identity-based cryptosystem, specifically Unified Signature-Encryption Scheme(US-ES) is designed to enable the efficient and secure exchange of healthcare information within a data-sharing network. Leveraging bilinear pairings, the proposed system integrates a distributed, tamper-proof database that replicates health records across peer-to-peer (P2P) network. EHRs are treated as individual events, timestamped, and assigned a cryptographic hash. To ensure transparency and data reliability, these entries are organized into transaction blocks and each node in the P2P network maintains a copy of the ledger. Additionally, the healthcare blockchain includes user permission lists, which dictate access control and serve as essential network instructions. This framework ensures secured exchange of EHR both within and between medical institutions, eliminating the need for a third-party provider. To guarantee the integrity of the EHRs, US-ES cryptographic technique is applied on the blockchain, ensuring the security of decentralized healthcare data exchanges. The US-ES mechanism combines the functionalities of both digital signatures and encryption, providing confidentiality, authenticity, and efficiency in data transmission. Ultimately, the proposed US-ES technique is combined with digital signature to present a robust and secure method for healthcare data exchange, significantly reducing vulnerabilities associated with traditional systems. By removing the necessity for a trusted third party, the proposed solution enhances both the security and integrity of EHR transactions, fostering safer data sharing in the healthcare.

Keywords: *Blockchain, Electronic Health Record(EHR), Unified Signature-Encryption (USE), Identity-Based Cryptosystem (IBC).*

1. INTRODUCTION

Blockchain technology has emerged in various sector with core properties of data integrity, transparency and immutability. A Distributed ledger systems act as core of the all transaction in the blockchain and verified by the validator are called as miners [1]. This decentralized approach eliminates the third party authority moving towards independence from the old traditional centralized mechanism. Each block in the blockchain consists of several significant components that contribute to its functionality. Merkle Root act as secured and efficient means of authenticating data by summarizing all transaction with in the block [2]. Nonce, a random number utilized in the proof-of-work consensus algorithm, assist in validating the block and maintain network integrity.

A timestamp denotes exact creation time of the block, ensuring that all entries are chronologically recorded. Finally, hash serves as a vital link to the previous block, ensuring that any alteration to prior transaction would require to complete reconfiguration of the entire blockchain, ensuring the immutability. Validators play the main role in the blockchain systems by verifying transaction within each block, therefore upholding the overall security and integrity of the network [1][3].

Their contribution is promoting through transaction fees and block rewards, which not only keep the systems operation but also encourage continuous participants from network members. Initially blockchain technology was associated with the financial sector, now its expanded in to broad range of fileds, in healthcare data management standing out as particularly promising application[4]. Secured exchange of healthcare information has been facing challenges, primarily due to privacy and data security. Due to concerns about data breaches, unauthorized access, and information misuse, patients typically hesitate to disclose their medical

information[5]. In this context transparent and secure architecture of blockchain offers a complete solution, positioning it as an ideal candidate for safeguarding sensitive data's[6]. The primary contribution of this particular research is to construct a blockchain-based healthcare network that includes sophisticated identity-based cryptosystems, such as US-ES[7]. This cryptographic framework is designed to ensure that healthcare information is exchanged in a manner that prioritizes confidentiality, data integrity, and user authentication. The US-ES enabled a very secured and efficient exchange of medical data.

The proposed system proficiently addresses the challenges associated with securing medical record while maintaining the operational efficiency by evaluating various cryptographic methods[4][8]. Research findings indicate that increasing block size and transaction arrival rate directly contribute to higher system throughput [9]. This makes it possible for blockchain to manage massive amounts of medical data without sacrificing security or functionality [10]. This approach not only enhances the protection and privacy of medical data exchange but it also improves overall efficiency of the system. Blockchain based healthcare networks provide robust solution to the longstanding issues like data breach, interoperability, and unauthorized access, especially when integrated with advanced cryptographic methods like US-ES Scheme.

This system provides more secure and reliable framework for managing healthcare information, instilling confidence in patients that their data is both protected and readily accessible to authorized entities. By introducing an architectural framework that provides robust protection against emerging threats, this innovative approach aims to revolutionize healthcare systems, ensuring the trustworthy and transparent but also resilient against the evolving landscape of cybersecurity risks. The promise of this technology lies in its ability to foster a decentralized and tamper-proof system that effectively addresses critical issues faced by traditional healthcare management systems[2][11]. Finally, by integrating blockchain technology into healthcare data management, patient data security, confidentiality, and restricted access are all ensured. This leads to better patient outcomes, increased data integrity, and a more efficient method of delivering healthcare. Figure 1 illustrates, blockchain technology has the potential to completely renovate the way healthcare information is managed by creating a transparent, safe, and effective system that will benefit both patients and healthcare professionals.

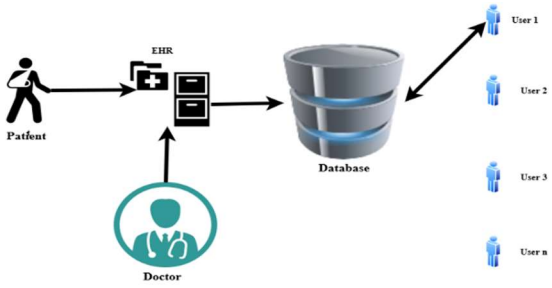

Figure 1. Accessing and Requesting the EHR

The consequent sections of the research paper are systematized to provide a comprehensive understanding of the research. Existing literature review related to healthcare data utilizing blockchain technology is discussed in Section 2, offering insights into the current landscape and foundation work. Section 3 demonstrates about the proposed methodology, highlighting its unique aspects and advantages in a detailed manner. Section 4 describes about performance analysis of the proposed approach, evaluating effectiveness and efficiency in real-world application.

2. RELATED WORK

Adoption of blockchain technology in healthcare industry has shown to be a game-changer, greatly improving data security, privacy, and productivity through a variety of applications. This innovative approach is primarily categorized into three critical areas: healthcare data sharing, health insurance claims, and personal healthcare data management, each addressing the inherent challenges of conventional centralized systems. This research has focus on importance of several parameters in healthcare data sharing, including transparency, auditability, data authenticity, user authentication, data integrity, access control, privacy, and confidentiality. Various cryptographic methods have been developed to secure data sharing process, with elliptic curve cryptography being a prominent technique[8][12]. Recent advancements have introduced identity-based encryption and Unified Signature-Encryption Scheme, which leverage bilinear pairings to further bolster the security of healthcare data transactions over blockchain networks[13]. Traditional EHR Systems have been scrutinized for their vulnerabilities, including security weakness, privacy concerns, data recovery issues, interoperability challenges and single point failures, largely due to their reliance on centralized databases that store health records in

plain text[14]. In response to these limitation, innovative solution such as blockchain based networks for health information exchange have been proposed to facilitate standardization, interoperability, and enhanced security[15]. One key development involves the creation of a Master Patient Index(MPI) that streamline the secure and interoperable data exchange of patients among medical institution[16]. Furthermore, advanced cryptographic schemes, such as ID-based Unified Signature-Encryption Scheme, have been introduced to ensure confidentiality, authenticity, non-repudiation, and forward secrecy of healthcare data, leading to significant improvements in data-sharing efficiency[17].

The advent of Multi-Party Computing (MPC) on blockchain platforms has provided a novel method for mitigating privacy risks in healthcare data sharing, enabling secure information exchange among hospitals, research entities, and patients[18]. The synergy of artificial intelligence (AI) along with blockchain technology has further strengthened the security of healthcare data sharing processes[19]. AI-driven methods, including Artificial Neural Networks (ANNs) and meta-heuristic algorithms, have been employed to optimize data-sharing efficiency and enhance the overall security of healthcare organizations[20]. Additionally, frameworks like Blockchain and AI-enabled Secure Medical Data Transmission (BAISMDT) have been proposed to facilitate secured data transmission across Internet of Things (IoT) networks in healthcare, utilizing Unified Signature-Encryption Scheme to ensure secure exchanges among multiple sources, coupled with advanced techniques for disease detection through deep learning[21].

Recent development has also introduced privacy-preserving encryption models utilizing homomorphic encryption and optimization algorithms aimed to enhancing the security of medical data exchanges[22]. Moreover, blockchain-assisted medical IoT systems have been designed to enhance patient data security, employing mechanisms such as Lamport Merkle Digital Signatures to authenticate devices and safeguard patient information through a Merkle tree model, which ensures both integrity and confidentiality during data exchanges[23]. A wide range of creative strategies aimed at enhancing healthcare data security, privacy, and efficiency by incorporating blockchain technology are presented in the substantial body of literature. These studies collectively demonstrate the enormous potential of blockchain to transform healthcare data management, presenting a future where patient information is not only secure but also more accessible and efficiently handled[24]. These breakthroughs range from improvements in cryptographic frameworks to AI-enhanced solutions[25]. Blockchain technology research and development have the potential to completely change the way that private health information is shared, stored, and safeguarded as the healthcare industry develops. This will open the door to more patient-centered and secure healthcare environment. The promise of blockchain in healthcare is its capability to deliver a decentralized, impenetrable framework that can successfully tackle the fundamental problems with traditional systems, ultimately resulting in better patient outcomes, enhanced data integrity, and a more efficient method of managing healthcare.

The proposed system US-ES combines the strengths of digital signatures, Identity Based Encryption (IBE), and Attribute Based Encryption (ABE) inorder to provide a robust and scalable security framework for EHR. In this scheme, digital signatures ensures the authenticity and integrity of the sender by allowing recipients to verify that the message truly originates from a trusted source and has not been tampered with. IBE simplifies key management by allowing user identities (email, name with Outpatient or Inpatient ID number) as registered by medical records in registration counter to function as public keys, eliminating the need for a traditional public key infrastructure (PKI). Meanwhile, ABE enforces fine-grained access control by associating encrypted EHRs with specific attributes (e.g., "Cardiologist" or "Emergency Access"), ensuring that only users with the required attributes can decrypt the data. By integrating these components into a unified scheme, US-ES with digital signature supports secure, decentralized, and policy-driven data sharing in blockchain environments, providing a reliable solution for privacy-preserving EHR management across healthcare institutions.

3. PROPOSED WORK

Sharing of health data is often met with reluctance, primarily due to the sensitivity associated with patients' healthcare information. Many individuals are hesitant to share their personal health records, fearing potential misuse or breaches of their private information. This hesitation poses a substantial challenge for research institutions and

healthcare providers who rely on comprehensive health data to improve patient care and advance scientific discoveries. Historically, both research institutes and patients have maintained extensive files of healthcare data that have been shared, but the process has often been fraught with concerns over security and privacy. The ability to share healthcare data among various health institutes is critical for enhancing collaborative efforts and focusing on the primary objective of patient safety and care. Blockchain technology came to light as a viable remedy in this regard, providing a decentralized framework that enables safe, open, and effective data sharing.

Multiple certifying authority are established within the network, which is considered as one of the major benefits of using blockchain for healthcare data sharing. These authorities play a crucial role in providing authentication and permission to access sensitive health information. By leveraging blockchain's inherent properties, such as immutability and transparency, healthcare organizations can create a secure environment for data sharing that minimizes the danger of unauthorized access or tampering. To ensure data integrity in this proposed approach, EHRs undergo a meticulous process before being stored on the blockchain. This process involves a series of cryptographic techniques designed to protect information from potential hacking attempts. Implementing these safeguards is essential to maintaining the trust of patients and healthcare providers. By protecting the integrity of EHRs, this approach not only improves data security, but also fosters a culture of trust in sharing health information. The efforts outlined in this research aim to protect the integrity of EHRs while ensuring the secure sharing of these records within different clinical institutions and organizations. A key aspect of this strategy is the removal of trusted third parties from EHR sharing transactions. Traditional models often involve intermediaries that can introduce vulnerabilities and inefficiencies into the data transfer process. By using blockchain technology, healthcare organizations can facilitate direct transactions between parties, significantly reducing the potential for data breaches and improving overall security.

Cryptographic technique like US-ES with digital signature is used on the blockchain to guarantee the secured transfer of health data. This dual capability is essential in the healthcare environment, where protecting sensitive patient information is paramount. In the proposed design approach, each step of the cryptographic process is carefully described to explain how US-ES with digital signature scheme works within the blockchain framework. Initially, health data is encrypted to prevent unauthorized access. This guarantees that no malicious actor will be able to read the data, even if it is intercepted during transit. After encryption, a digital signature is created that can be used as evidence of the data's integrity and authenticity. The intended recipient can validate this signature to make sure the data is very authentic and it comes from a reliable resource. Using a US-ES increases the safety of health data exchanges while also streamlining the process. By combining encryption and signing in a single operation, US-ES reduces the computational overhead typically associated with separate encryption and signature generation steps. This efficiency is especially useful in medical settings where prompt information availability is essential to providing quality treatment for patients. The blockchain approach used in electronic healthcare records, emphasizing its role in improving the privacy and security of patient data as illustrated in Figure 2. By leveraging a decentralized architecture, in addition to guaranteeing that private patient data is shielded from potential breaches and illegal access, this strategy allows healthcare providers to share data securely.

Integrating blockchain technology allows for the development of robust cryptography techniques, dependable authentication systems, and tamper-proof records all of which support the preservation of the privacy and integrity of EHRs. This graphic illustration in Figure 2 highlights how well blockchain works to address important issues with privacy and data security of the patients in healthcare sector.

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

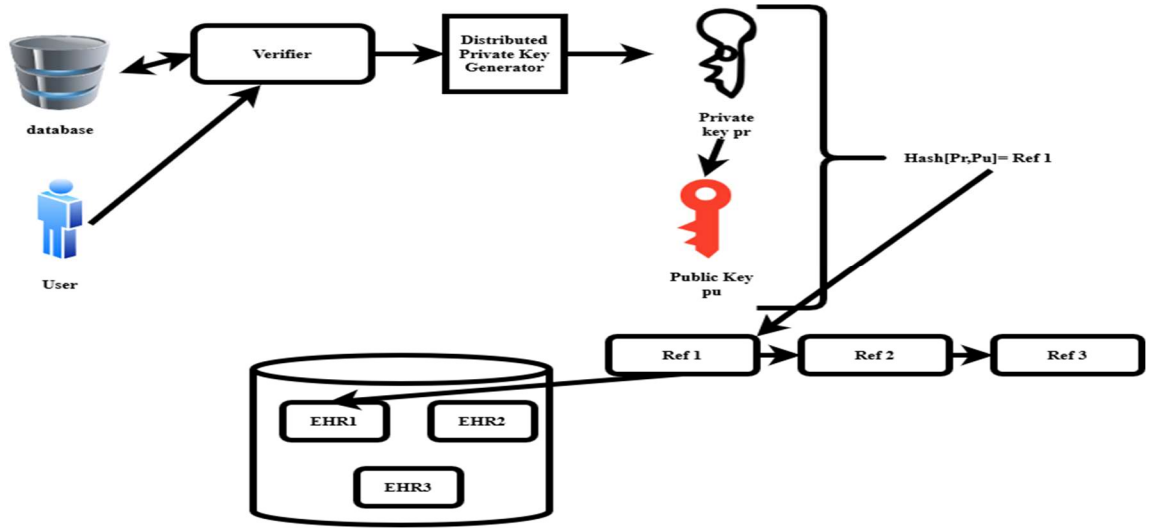

Figure 2. EHR Process Using Blockchain

3.1 Cryptographic Primitives of the Proposed System

Identity-based cryptography (IBC) provides an innovative approach to simplify public key management by eliminating the need for traditional public key infrastructure (PKI). IBC streamlines this by allowing public keys to be derived from simple public identifiers such as a user's name or email address, making it more efficient and user-friendly. In contrast to traditional PKI that relies on long public key strings, IBC uses direct public information to generate one public key per user, significantly simplifying public key generation and management, as illustrated in Figure 5. Additionally, this process eliminates the need to maintain a separate public key database because "public keys" are more intuitive and readily obtained, reducing the overhead of managing redundant or unused public keys.

The enrollAdmin asynchronous function first accesses the local wallet directory (./wallet) to check whether the admin identity already exists. If it does, the function logs a message and exits. If not, it proceeds to connect to the Certificate Authority (CA) running at http://localhost:7054 and uses the CA client to enroll the admin with the provided credentials (admin and adminpw) as shown in Figure 3. Upon successful enrollment, the function generates an identity using the X509WalletMixin by combining the certificate and private key received during enrollment. This identity is then stored in the wallet under the label 'admin'. If any error occurs during the process, it is caught and logged to the console. This script is typically part of the setup process in Hyperledger Fabric applications to ensure that an admin identity is available for performing blockchain operations such as registering and enrolling other users.

```
const { Wallets, Gateway } = require('fabric-network');
const { X509WalletMixin } = require('fabric-ca-client');
async function enrollAdmin() {
  try {
    const wallet = await Wallets.newFileSystemWallet('./wallet');
    const adminIdentity = await wallet.get('admin');
    if (adminIdentity) {
      console.log('An identity for admin already exists in the wallet');
      return;
    }
      const caURL = 'http://localhost:7054';
    const caClient = new fabric.Client();
    caClient.setCAHostName(caURL);
    const enrollment = await caClient.enroll({
      enrollmentID: 'admin',
      enrollmentSecret: 'adminpw'
    });
      const identity = X509WalletMixin.createIdentity('org1MSP', enrollment.certificate, enrollment.key.toBytes());
      await wallet.put('admin', identity);
    console.log('Successfully enrolled admin user "admin" and imported it into the wallet');
  } catch (error) {
    console.error(`Error
enrolling admin user: ${error}`);
  }}enrollAdmin();
```

Figure 3. Chain code for Enroll Admin

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
const { Wallets, Gateway } = require('fabric-network');
async function connectToPeer() {
  try {
      const wallet = await Wallets.newFileSystemWallet('./wallet');
      const adminIdentity = await wallet.get('admin');
    if (!adminIdentity) {
      console.log('An identity for admin does not exist in the wallet');
      return;
    }
    const ccpPath = './connection-profile.yaml';
    const ccp = require(ccpPath);
    const gateway = new Gateway();
    await gateway.connect(ccpPath, { wallet, identity: adminIdentity, discovery: { enabled: true, asLocalhost: true } });
    const ca = gateway.getClient().getCertificateAuthority();
    const adminIdentity = gateway.getCurrentIdentity();
    console.log('Successfully connected to peer node and retrieved CA client and admin identity');
  } catch (error) {
    console.error(`Error connecting to peer node: ${error}`);
  }
}
connectToPeer();
```

Figure 4. Creating patient in Chaincode

```
const { Context } = require('fabric-contract-api');
class PatientRegistry extends Context {
  async registerPatient(ctx, newPatient) {
    newPatient.permissionedIds = ['doctor1', 'nurse2'];
    newPatient.emergencyContacts = ['John Doe', 'Jane Smith'];
    newPatient.ehrs = ['ehr1', 'ehr2'];
    newPatient.requesters = ['doctor1', 'nurse2'];
    newPatient.bills = ['bill1', 'bill2'];
    newPatient.medicineReceipts = ['receipt1', 'receipt2'];
    newPatient.labRecords = ['labRecord1', 'labRecord2'];
    newPatient.appointments = ['appointment1', 'appointment2'];
    const patientId = newPatient.id;
    await ctx.stub.putState(patientId, Buffer.from(JSON.stringify(newPatient)));
    console.log(`Successfully registered patient with ID ${patientId}`);
  }
}
module.exports = PatientRegistry;
```

Figure 5. Register patient into the Blockchain

```
POST/readIndividualAsset 200 154.132 ms 2
OPTIONS/grantAccess 204 0.114 ms 0
POST/grantAccess 200 2977.826 ms 7
"Access has been provided to the requester with the"
{sessionkey: '6b87b157ab9ca3037239651becc4f393b84a9ad8a283fecd677ed4b51df08d88',
        requesterId: '964414396022',
        requestType: 'channeled',
        documentIds: ['dqabhl4elguol4j3ydqtx1']}
```

Figure 6. Storing the patient, EHR into the Blockchain with ID

Main cryptographic primitives in the proposed system, such as identity-based signature schemes (IBS) and identity-based encryption (IBE) are shown in Figure 4. These techniques directly use a user's identity as the key element for encryption and signature generation, simplifying the infrastructure and reducing the operational complexities tied to PKI. Since public key management is no longer a burden, the process is cost-effective and scalable for secure communications. The registerPatient function accepts a new patient's data, enriches it with various fields such as permissionedIds, emergencyContacts, ehr, requesters, bills, medicineReceipts, labRecords, and appointments, then stores this structured data on the blockchain using ctx.stub.putState(), keyed by the patient's unique id. The patient information is serialized into a buffer using JSON.stringify before storing. A

confirmation message is logged indicating successful registration as shown in figure 5. This function helps guarantee that patient data is secured and immutably stored in the blockchain ledger. The registerPatient function accepts a new patient's data, enriches it with various fields such as permissionedIds, emergencyContacts, ehr, requesters, bills, medicineReceipts, labRecords, and appointments, then stores this structured data on the blockchain using ctx.stub.putState(), keyed by the patient's unique id. The patient information is serialized into a buffer using JSON.stringify before storing. A confirmation message is logged indicating successful registration as shown in figure 5. This function helps guarantee that patient data is secured and immutably stored in the blockchain ledger. Despite the advantages of IBC, relying on a private key generator (PKG) introduces specific challenges. Figure 6 illustrates how the PKG generates private keys based on the user's identity string and master secret key. In this system, the PKG holds the master secret key and should be highly secure and reliable as it stores private keys. For all users. This centralization of authority means that the PKG must maintain a very high level of assurance and availability, exceeding the security expectations placed on a traditional Certificate Authority (CA). If the PKG is compromised, the security of the entire system can be at risk, as an attacker can access all private keys and decrypt encrypted messages or impersonate users. Also, the IPC model reduces the need for public key management and simplifies certificate distribution, but it comes with trade-offs. The concentration of trust in the PKG becomes a critical point of failure, making the strength of the PKG highly dependent. Therefore, the PKG must maintain strict security protocols and high availability to ensure that private key generation and distribution are secure and reliable. The use of IPC is particularly advantageous in systems where simplicity and efficiency are priorities in public key generation and distribution, such as identity management systems and secure data-sharing networks. However, ensuring the security and reliability of PKG remains a primary challenge that requires advanced security mechanisms and trust models to mitigate potential risks.

3.2 Unified Signature-Encryption Scheme Using IBC

Unified Signature-Encryption Scheme offers the benefits of both confidentiality and authenticity in a more efficient manner compared to separate encryption and signing processes. Unified Signature-Encryption Scheme typically involves three primary algorithms: key generation, signcrypt, and unsigncrypt.

Algorithm for Unified Signature-Encryption Scheme Using Identity-Based Cryptography (IBC)

Unified Signature-Encryption Scheme using IBC is composed of three main algorithms: Setup, Signcrypt, and Unsigncrypt.

1. Setup (Key Generation by PKG)
   - Input: Security parameter A
   - Output: System parameters params and master key MK

   step.1. PKG runs a probabilistic algorithm with the input λ (security parameter).

   step.2. It outputs:

   System Parameters: params = {G, q, P, H,...} (public key parameters where G is a cyclic group of prime order q, P is a generator, and H is a cryptographic hash function).

   Master Key: M K

   step.3. PKG makes params public and keeps MK secret.

2. Signcrypt
   - Input: Message M, sender's private key SK, receiver's public key PK,
   - Output: Ciphertext C

   step.1. Sender S selects a random value $r \in Z_q^*$.

   step.2. Compute a shared key using the receiver's public key PK, and the random value r:

   $$K_{shared} = H_1 (e (PK_r, P)^r)$$

   Where e is a bilinear pairing, and H_1 is a key derivation function.

   step.3. Encrypt the message M using a symmetric encryption function E_{nc} with the shared key:

   $C1 = Enck_{Shared} (M)$

   step.4. Compute the signature using the sender's private key SK_s:

   $$\sigma = H_2 (M) \cdot SK_s$$

   Where H_2 is a cryptographic hash function.

   step.5. The final ciphertext is:

   $$C = (C_1, \sigma, rP)$$

   Where rP is used to verify the share key.

3. Unsigncrypt

- Input: Ciphertext C = (C_1, 0, rP), sender's public key PK_s, receiver's private key SK_r,
- Output: Message M or ⊥ (if invalid)

step.1. Receiver R computes the shared key using the sender's public key PK_s, and rP:

$$K_{shared} = H_1 (e (SK_r, rP))$$

step.2. Decrypt C_1 to obtain the message M:

$$M = Dec\ K_{Shared} (C_1)$$

step.3. Verify the signature σ by checking:

$$\sigma = H_2 (M).\ PK_s,$$

If the verification succeeds, output the message M. Otherwise, output ⊥ indicating that the ciphertext is invalid.

In the above algorithm a trusted PKG issues private keys based on users' identities, eliminating the need for traditional certificate-based PKI. By unifying signature and encryption, this method allows a message to be encrypted for confidentiality and signed for authenticity in one step, reducing computational overhead. It is particularly well-suited for secure and scalable data sharing in decentralized environments like blockchain, where authentication, integrity, and privacy are crucial.

Enhanced security through distributed authentication and Unified Signature-Encryption Scheme in IBC

To enhance the security and efficiency of the system, the authority of the traditional single Private Key Generator (PKG) is distributed across four types of Certificate Authorities (CAs). These CAs are designated as follows:

Registration Authority (RA)

Encryption Certificate Authority (ECA)

Location-based Service Certificate Authority (LS-CA)

Transaction Certificate Authority (TCA)

Each CA issues certificates, denoted as CRA, CECA, CLS−CA, CTCA after verifying the user's identification credentials. The certificates are essential for the distributed authentication process in the proposed healthcare blockchain system.

User Identification: Let the user's identity be represented as IDu, and their credentials be Credu. Each CA verifies these credentials before issuing certificates.

CRA=RA (IDu, Credu)

CECA=ECA (IDu, Credu)

CLS-CA=LS-CA (IDu, Credu)

CTCA=TCA (IDu, Credu)

Certificate Distribution: After verifying IDu and Credu, the CAs issue their respective certificates, forming a set of valid certificates for the user:

{CRA, CECA , CLS-CA, CTCA }

These certificates are combined for distributed authentication.

Unified Signature-Encryption Scheme: To ensure confidentiality and integrity, a Unified Signature-Encryption Scheme operation SC is used. This operation combines encryption and digital signature in a single step, enhancing both efficiency and security. The operation can be defined as:

SC (M, S, k) = Encrypt (M, k) || Sign(S, k)

Where:

M is the message to be encrypted,

S is the signature,

k is the key (derived from identity-based cryptography).

In IBC, user identities ID act as public keys. Private keys are created and distributed by the CA using a master key msk. For user u, the private key sku is derived as:

sku= F(msk, IDu)

Where F is a cryptographic function that binds the identity to the master key.

Distributed Authentication: The authentication process is distributed across the multiple CAs, each contributing part of the certificate chain necessary for the user's authentication. The user u is authenticated only if all certificates in the set {CRA, CECA, CLS-CA, C TCA} are valid:

$$\text{Auth}(ID_u) = \begin{cases} \text{Valid}, & \text{if } C_{RA}, C_{ECA}, C_{LS-CA}, C_{TCA} \text{ are all valid} \\ \text{Invalid}, & \text{otherwise} \end{cases}$$

This use of distributed CAs and Unified Signature-Encryption Scheme IBC significantly improves the security and scalability of the healthcare blockchain's authentication system, preventing single points of failure and ensuring robust identity verification.

4. EHR BLOCKCHAIN ARCHITECTURE

The development of permissioned healthcare blockchain network aims to securely and efficiently manage the EHR data through an innovative architecture that provide multiple components to facilitate seamless communication among the healthcare participants while ensure data privacy and security. At the centre of the system architecture lies a robust framework that employs blockchain technology to store EHRs, with each record being timestamped to provide transparency and traceability of past transaction. The architecture is composed of three main modules: users, an off-chain database, and the healthcare blockchain itself. The users are various healthcare participants, including doctors, pharmacist, patients, and health insurers, or administrators, each playing a crucial role in the ecosystem. The off-chain database act as a repository for EHRs like prescription records, billing information, and any other healthcare related data that requires modification and tracking, enabling the system to handle large volume of data without overwhelming the blockchain. Meanwhile, the healthcare blockchain acts as a permissioned ledger that manages transactions related to EHRs, prescriptions and billing, providing secure access to stored data. User interactions with blockchain are different, as physicians can add new EHRs and prescriptions, pharmacists can update medication records, patients can access and modify their health profiles, and administrators can manage requests and policies. An off-chain data handling strategy effectively reduces data redundancy and optimizes storage costs by keeping EHR data off-chain while essential transactional data remains in the chain. The blockchain itself maintains a distributed ledger that ensures data consistency among all participants, with each peer having a copy of the ledger.

The system guarantees that transactions are linked in a chain of cryptographically protected blocks, preventing data tampering and making them reliable. Smart contracts, or chain code, are integrated into the system to automate specific operations based on predefined rules, facilitating efficient and transparent processing of health data by fulfilling certain conditions. When a patient register on the platform, they receive a certificate to access their health records. Creation and sharing of EHRs occurs through the blockchain using client applications that initiate transactions via the POST method; Once verified, the health records is securely recorded on the blockchain infrastructure, ensuring both accessibility and auditability. Distributed ledger storage captures the global state of data at any point in time, structures it in JSON format, and stores it in CouchDB for efficient querying and updates. This method allows transactions to be grouped into blocks and cryptographically linked, improving integrity and traceability. On a query basis, physicians and other authorized users can access patient EHRs through API endpoints, retrieving data based on patient IDs using the GET method without requiring full consensus for each query because the data is retrieved from a local ledger. The implementation of this proposed system is implemented using Hyperledger which effectively manages the registration and verification of entities such as doctors, patients and hospitals. The use of certificates and public-private key pairs ensures trusted authentication within the network, facilitating a streamlined approach to health data management while improving the overall security of the system. Through this comprehensive approach, a permissioned healthcare blockchain network not only improves the efficiency of EHR storage and sharing, but also significantly improves the privacy and security of a patient's critical health data, ultimately fostering a more collaborative and trusted healthcare environment. By integrating advanced technologies and robust architectural elements, this innovative system addresses critical challenges associated with healthcare data exchange, blockchain paves the way for safer, transparent and efficient healthcare practices. Real-time access to patient data and the potential for seamless communication between healthcare providers is revolutionary, making it easier to deliver timely and informed care while protecting patients' rights to personal health information.

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

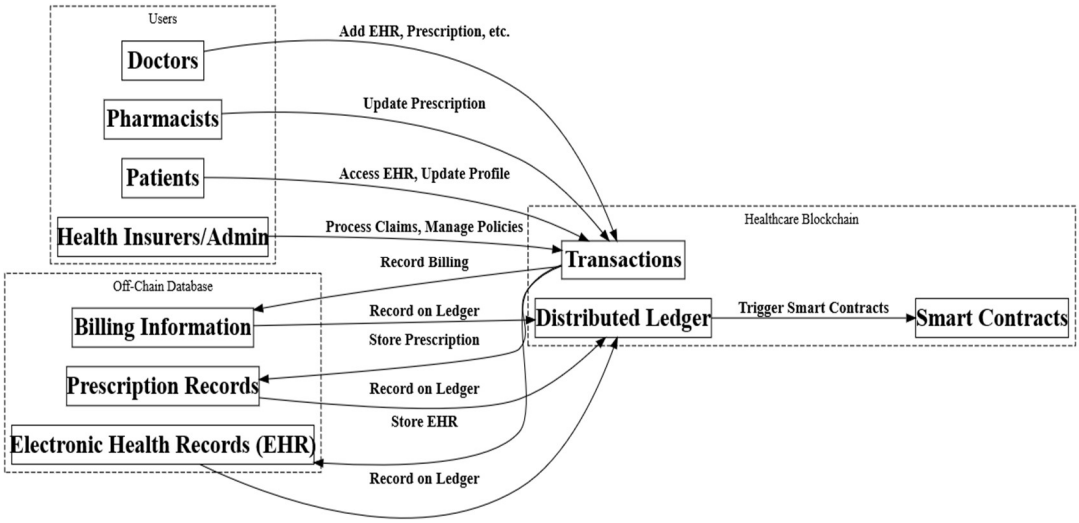

Figure 7. Blockchain-Based Healthcare System

A major step forward in the management and sharing of health data, this all-encompassing framework highlights the revolutionary power of blockchain technology in enhancing patient care and safeguarding private health data in an era of digitalization where security and privacy are critical requirements.

4.1. User Registration and Enrollment Process

The user registration process starts with a client initiating a request to the RA, which is the registration certificate authority, to register a new user. This request typically involves providing the necessary information about the user, such as their personal details, contact information, and desired username and password. The RA then processes this request, verifying the provided information and creating a new user account if everything is in order.

Registration Process:

step.1. Client sends a registration request on behalf of the user to the Registration Authority (RA).
step.2. RA provides the registration form to the client.
step.3. Client fills out the form with identity credentials and sends it to RA.
step.4. RA stores the user information U from the registration form in its local storage.
step.5. RA generates the client username U_{name} and password P_{word} (registration ID, R_{id}).
step.6. Registration ID R_{id} is created by hashing the client username:

$$R_{id}=H\ (U_{name})$$

Where H is a cryptographic hash function.

Enrollment Process:

step.1. Client sends an enrollment request to the Enrollment Certificate Authority (ECA).
step.2. ECA asks for the registration ID R_{id}
step.3. Client sends the R_{id} to ECA.
step.4. ECA checks whether R_{id} exists in the database.
step.5. If R_{id} exists, proceed to the next step. Otherwise, return an error.
step.6. ECA confirms the registration and notifies the client that the user is enrolled.
step.7. ECA generates the enrollment ID E_{id} by hashing the registration ID with a randomly
step.8. Generated one-time use ECA certificate EC A_{cert}

$$E_{id}=H(R_{id} \oplus EC\ A_{cert})$$

Where denotes concatenation or bitwise operation.

4.2. Hyperledger Fabric Transaction Flow

step.1. The client initiates the transaction process by sending a transaction proposal $T_{proposal}$ through the SDK to the endorsement peers.
step.2. Each endorsement peer P_1 executes the same chaincode C to process the transaction. Let P = {P1, P2,..., Pn} be the set of endorsement peers.

For each peer $P \in P$:

$$RW_{set}^{i} = C\ (T_{proposal})$$

Where RW_{set}^{i} is the read-write set generated by the chaincode execution on peer P_i.

step.3. Each endorsement peer sends the read-write set RW_{set}^{i} back to the client.

step.4. The client compares the results $\{RW_{set}^{1}, RW_{set}^{2}, \ldots\ldots, RW_{set}^{n}\}$ to ensure consistency:

If $RW_{set}^{1} = RW_{set}^{2} = \ldots. = RW_{set}^{n}$, proceed to step 4.

The client sends the valid transactions $\{T_{valid}\}$ to the Orderer.

step.5. The Orderer batches the transactions and organizes them into blocks:

$$B=\{T_1, T_2,..., T_k\}$$

Where B is a block containing k transactions.

step.6. The Orderer broadcasts the block B to all nodes N_i in the network.

Let $N = \{N_1, N_2,..., N_m\}$ be the set of network nodes.

step.7. Each node Ni validates the transactions in block B according to the endorsement policy EP. For each transaction $T_j \in B$, the node checks if it satisfies the endorsement policy:

step.8. If $EP(T_j)$ = True, write T_j into the distributed ledger.

step.9. The validated transactions are written into the distributed ledger L in a new block B

$$L=L \cup B$$

5. PERFORMANCE ANALYSIS

The proposed blockchain system for securely storing and managing electronic health records (EHRs) enables a comprehensive process for ledger updating and transaction invocation, focusing on network efficiency, verification and consensus mechanisms. The ledger update process is initiated by transaction calls by applications, where network overload is monitored and assessed, ensuring system stability. The blockchain system receives messages from the network, and applications confirm these messages, analysing possible network loads before processing transactions. Central to the process is the chaincode, which facilitates the writing and receiving of transaction information.

Chaincode is employed not only to ensure seamless communication between applications and the blockchain system but also to guarantee the efficient performance of applications within the system. The chaincode further allows for transaction querying and verification, providing a mechanism to validate EHRs and transactions through cryptographic hash values that ensure secure ledger updates. These hash values are vital for generating secure transactions that are subsequently added to the ledger. A consensus mechanism underpins the ledger updating process, relying on the validation of EHRs and transaction details. Transactions are successfully verified when EHRs are queried through the verifying application, which conducts the necessary tests to ensure data integrity. Chaincode querying is instrumental in this process, as it enables the network to read and retrieve transaction information that validates the operations of applications on the network. Throughout this process, the network load is continually assessed, with performance being evaluated based on how well the applications handle network load during tests, particularly during time-sensitive road trips. This continuous evaluation ensures that the network maintains optimal performance under varying conditions. To further assess the performance of the blockchain network, Hyperledger Caliper is used as the benchmarking tool. Hyperledger Caliper is a widely recognized performance evaluation framework designed to analyze blockchain systems through various metrics and tests. The proposed system is tested using Caliper to evaluate its experimental performance, specifically examining how efficiently the blockchain network handles EHR transactions.

The testing process begins with the initialization of a configuration file in Hyperledger Caliper, which sets up the genesis block and establishes the blockchain network on the admin peer. Once initialized, the chaincode for reading and writing EHRs is instantiated and installed on the network, which includes the block file associated with the newly created genesis block. This setup allows for the seamless writing and reading of EHRs during the transaction process. As data is delivered to the blockchain system through applications, it is analyzed for verification using the configuration file established in Hyperledger Caliper. Performance metrics such as block size and Transaction Arrival Rate (TAR) are closely monitored to assess the system's overall efficiency. These parameters are essential for understanding how the blockchain network handles varying transaction loads and identifying potential performance bottlenecks. Two key performance metrics used to evaluate the blockchain system are throughput and transaction latency. Throughput counts how many transactions the network processes successfully in a certain

amount of time, whereas transaction latency counts how long it takes for a transaction to be approved and added to the blockchain. By analysing these metrics, the performance of the proposed system can be accurately gauged, and any bottlenecks can be identified and addressed. During the throughput process, the system evaluates the number of transactions per second (TPS), a crucial metric for understanding how efficiently the blockchain network processes transactions. The reading and writing operations during specific periods are also monitored, with reading operations focusing on application verification and writing operations measuring the issuance of transactions on the network.

These operations are essential for understanding how effectively the blockchain network handles concurrent transaction requests. The size of the blockchain network plays a significant role in the measured TPS, as larger networks often require more time to process transactions across multiple nodes. As transactions are committed and updated on the network as shown in Figure 8, the TPS value provides insight into how efficiently the system operates under different network sizes. The system is capable of producing stable and reliable TPS results, particularly under high transaction volumes. For example, during tests, the blockchain network demonstrated stable production results for processing 1000 transactions, where the system was able to maintain a consistent queue length for pending transactions. This stability is crucial for real-world applications, where high transaction volumes must be handled without delays or timeouts. To further evaluate the performance of the blockchain system, the TPS values were varied during testing, with values of 60, 70, 80, 90, and 100 being tested under different TAR conditions. These variations were implemented during the benchmark runs to prevent timeouts and ensure that the system could handle different transaction loads effectively. The results of these tests were illustrated in Figure 7, which depicted the varying TPS values in relation to block size and throughput transactions. The figure highlighted the performance dynamics of the blockchain network, showcasing how different block sizes and transaction loads influenced the overall throughput and TPS values.

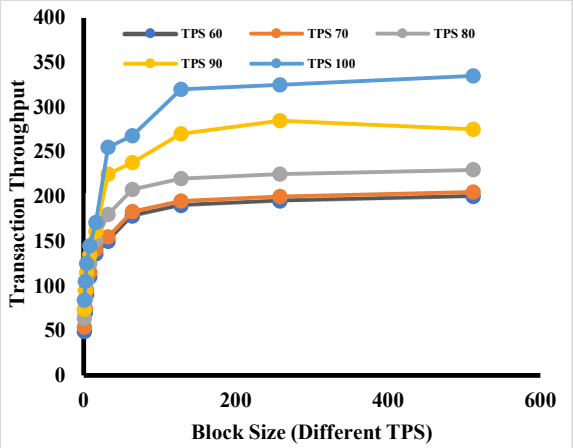

Figure 8. Invoke Transaction

This analysis provided a comprehensive understanding about the performance of the system under different conditions, allowing for the identification of optimal configurations that maximize efficiency while minimizing latency. The proposed blockchain system for managing and exchanging EHRs demonstrates robust performance under varying transaction loads, with chaincode playing a central role in transaction processing and verification. The use of Hyperledger Caliper for performance testing offers valuable insights into the system's efficiency, with metrics such as TPS, transaction latency, and throughput providing a detailed analysis of the system's capabilities. Tests results indicate that the system is well-suited for secure and efficient EHR management, with the ability to scale effectively as network size increases and transaction volumes grow. Through careful evaluation of performance metrics and network dynamics, the proposed blockchain system offers a reliable solution for the secure exchange of healthcare data.

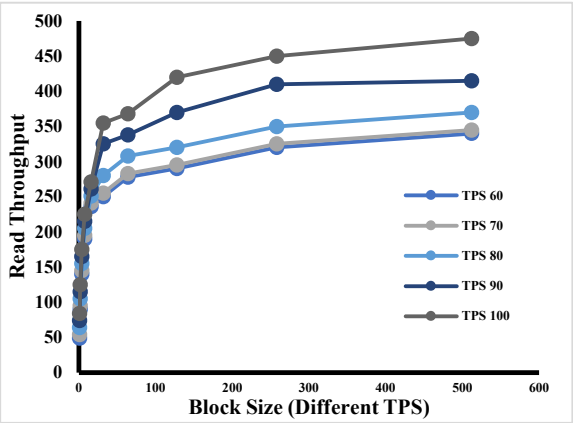

Figure 9. Query Transaction

Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The correlation between block size and throughput is a key factor in optimizing blockchain network performance, with larger block sizes generally resulting in higher throughput as shown in Figure 9. For instance, a block size of 128 TPS shows a linear increase in throughput, suggesting that network can handle a greater volume of transactions as the block size increases. One significant factor influencing throughput is the difference between read and write transactions. Read transactions tend to be faster than write transactions, meaning that the network can process read requests more efficiently, which has a positive impact on overall throughput. However, the Transaction Arrival Rate (TAR) also plays a crucial role in determining the throughput for writing transactions. For example, with a TAR of 100 TPS, the throughput for writing transactions reaches a maximum of 256 TPS, while the minimum writing throughput drops to around 43 TPS when the arrival rate is increased to 90 TPS and the block size is reduced to 1. This demonstrates that both block size and TAR significantly affect the performance of writing transactions.

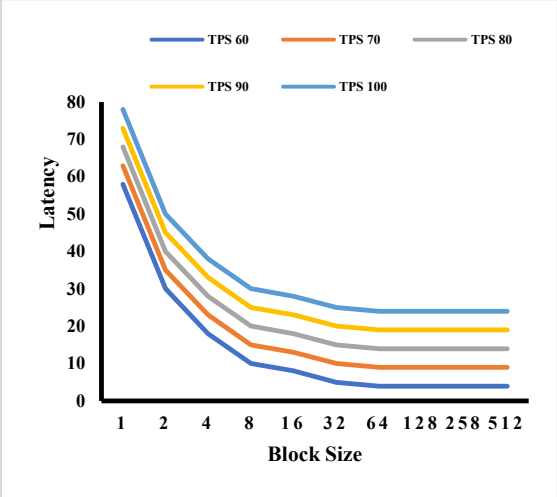

Figure 10. Read Latency

Read latency as illustrated in Figure 10 refers to the time taken to retrieve or access data from the blockchain network. In the context of blockchain-based systems, low read latency is crucial for applications requiring quick data access, such as in healthcare or financial systems. Read latency is generally much lower than write latency because reading does not require consensus or block validation. However, it can still be affected by factors such as network load, node synchronization, and the size or structure of the data. Optimizing read latency ensures faster user interactions and improves the overall efficiency of blockchain-based applications. In blockchain networks, transaction latency and read latency are essential performance metrics that significantly influence overall efficiency. Transaction latency denotes the time it takes for a transaction to be processed which is confirmed across all network peers, while read latency is the time required for a query transaction to read data from the blockchain and respond back to the issuer or verifier. These latencies are crucial for ensuring timely data retrieval and transaction completion, particularly in applications such as healthcare, where rapid access to Electronic Health Records (EHRs) is critical.

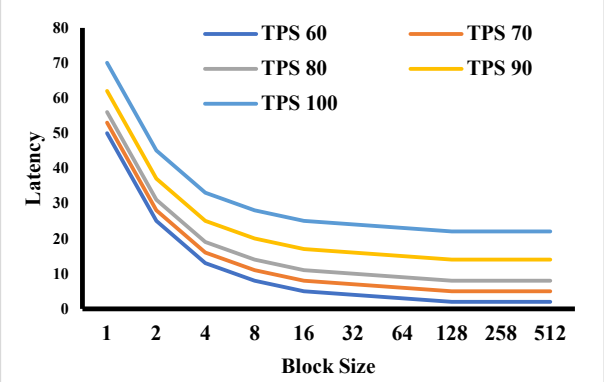

Figure 11. Transaction Latency

The delay in transaction processing is typically measured in milliseconds (ms), allowing for precise tracking of performance across varying network conditions. Figure 11 illustrate how transaction latency vary with different block sizes, providing perceptions into the system's responsiveness under various loads. One key observation from the analysis is that as the arrival rates of transactions increase, transaction latency decreases sharply, especially when using smaller block sizes such as 32 transactions per block. This indicates that the system becomes more efficient at processing higher volumes of transactions when block sizes are adjusted to handle the increased load. For example, with an arrival rate of 32 transactions per block, transaction latency is significantly reduced across all arrival rates. However, the maximum observed latencies for writing and reading transactions occur at higher arrival rates. The maximum latency for writing transactions is recorded at 85 ms, while for reading transactions, it reaches 78 ms. These peaks are observed at arrival rates of 80 TPS for writing and 100 TPS for reading, both with a block size of 1. This suggests that smaller block sizes combined with high transaction loads can lead to increased processing delays. Conversely, the minimum latency

values highlight the efficiency gains achieved with larger block sizes. The minimum latency for reading transactions is as low as 10 ms, while for writing transactions, it is 1 ms. These low latency values are observed at an arrival rate of 80 TPS with a block size of 512 TPS for reading and at 60 TPS with a block size of 32 TPS for writing. These findings indicate that under certain conditions, larger block sizes allow the network to process transactions more efficiently, reducing the time taken to confirm transactions and retrieve data. The overall trend demonstrates that larger block sizes tend to result in lower transaction latency, particularly when paired with moderate transaction arrival rates. However, at higher arrival rates, smaller block sizes can introduce processing bottlenecks, leading to increased latency.

6. CONCLUSION

The proposed system is a blockchain-based network aimed at securely exchanging medical data within the healthcare sector. It utilizes an identity-based cryptosystem, Unified Signature-Encryption Scheme, to facilitate efficient and secure information sharing. Through the evaluation of cryptographic methods, the study reveals that larger block sizes and higher transaction arrival rates increase throughput, while transaction and read latency decrease as block size grows. Widespread performance testing with Hyperledger Caliper validates the efficiency of the system under different transaction volumes and network scenarios. Throughput, transaction latency, and read latency were the key performance metrics—showing that the blockchain network maintains stable processing rates even at high transaction volumes, with throughput scaling properly with increasing block size. The system ensured a balanced transaction arrival rate (TAR) throughout, enabling smooth processing of read and write transactions. Specifically, the findings highlight the benefits of larger block sizes in minimizing transaction delay and less vulnerability to delays under high load for small block sizes. Notably, the read transactions were found to be processed with lesser latency than write transactions, which is of serious concern for applications involving quick access of medical information in time-critical healthcare situations.

Maximum latencies of 85 ms for writing and 78 ms for reading were observed at arrival rates of 80 TPS and 100 TPS, respectively. The study highlights blockchain technology's potential to enhance privacy, security and efficiency in medical data exchange. However, the model requires users to be online, as offline nodes disrupt data exchange. Future work should focus on further reducing latency and testing the system's robustness in real-world environments. The study also raises the possibility of using blockchain technology to improve the efficiency and security of sharing data in industries other than healthcare.

REFERENCES:

[1] Teutsch J, Reitwießner C. A scalable verification solution for blockchains. InAspects of Computation and Automata Theory with Applications 2024 (pp. 377-424).

[2] Li W, Feng Y, Liu N, Li Y, Fu X, Yu Y. A secure and efficient log storage and query framework based on blockchain. Computer Networks. 2024 Oct 1;252:110683.

[3] Sutradhar S, Karforma S, Bose R, Roy S, Djebali S, Bhattacharyya D. Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chain-based approach for security and scalability for healthcare industry. Internet of Things and Cyber-Physical Systems. 2024 Jan 1;4:49-67.

[4] Mourya AK, Kapil G, Idrees SM. Modernizing Healthcare Data Management: A Fusion of Mobile Agents and Blockchain Technology. InBlockchain Transformations: Navigating the Decentralized Protocols Era 2024 Feb 13 (pp. 93-106). Cham: Springer Nature Switzerland.

[5] Van der Boon RM, Camm AJ, Aguiar C, Biasin E, Breithardt G, Bueno H, Drossart I, Hoppe N, Kamenjasevic E, Ladeiras-Lopes R, McGreavy P. Risks and benefits of sharing patient information on social media: a digital dilemma. European Heart Journal-Digital Health. 2024 May;5(3):199-207.

[6] Chhabra A, Saha R, Kumar G, Kim TH. Navigating the Maze: Exploring Blockchain Privacy and Its Information Retrieval. IEEE Access. 2024 Feb 26.

[7] Ma R, Du L. Efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography. Plos one. 2024 May 9;19(5):e0300153.

[8] Ugwu JN, Mogaji SA, Akinsanya SE, Awoyemi JO, Obi JC. Comparative analysis of Different Multilevel States for Four Notable Cryptographic Schemes. Researchers Journal of Science and Technology. 2024 Apr 4;4(2):60-77.

[9] Ma R, Du L. Efficient attribute-based strong designated verifier signature scheme based on elliptic curve cryptography. Plos one. 2024 May 9;19(5):e0300153.

[10] Ranjan AK, Kumar P. Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission. Multimedia Tools and Applications. 2024 Mar 2:1-26.

[11] Tiwari A, Sikri A, Sagar V, Jameel R. Decentralized Technology and Blockchain in Healthcare Administration. InBlockchain Transformations: Navigating the Decentralized Protocols Era 2024 Feb 13 (pp. 229-237). Cham: Springer Nature Switzerland.

[12] Vaishnavi P, Sam Nithish KC, Parvathi S. Secure Data Sharing Using an Elliptic Curve Cryptography Method for Medical Mecord Transactions in Cloud Environment. InInternational Conference on Reliability, Safety, and Hazard 2024 Feb 21 (pp. 821-827). Singapore: Springer Nature Singapore.

[13] Kumar V, Ali R, Sharma PK. A secure blockchain-assisted authentication framework for electronic health records. International Journal of Information Technology. 2024 Mar;16(3):1581-93.

[14] Tyagi AK, Seranmadevi R. Blockchain for Enhancing Security and Privacy in the Smart Healthcare. Digital Twin and Blockchain for Smart Cities. 2024 Oct 15:343-70.

[15] Sahu H, Choudhari S, Chakole S. The use of blockchain technology in public health: lessons learned. Cureus. 2024 Jun;16(6).

[16] Jena SK, Kumar B, Mohanty B, Singhal A, Barik RC. An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. Decision Analytics Journal. 2024 Mar 1;10:100411.

[17] Eltayieb N, Elhabob R, Liao Y, Li F, Zhou S. A heterogeneous signcryption scheme with Cryptographic Reverse Firewalls for IoT and its application. Journal of Information Security and Applications. 2024 Jun 1;83:103763.

[18] Geng T, Liu J, Huang CT. A Privacy-Preserving Federated Learning Framework for IoT Environment Based on Secure Multi-party Computation. In2024 IEEE Annual Congress on Artificial Intelligence of Things (AIoT) 2024 Jul 24 (pp. 117-122). IEEE.

[19] Kuznetsov A, Sernani P, Romeo L, Frontoni E, Mancini A. On the integration of artificial intelligence and blockchain technology: a perspective about security. IEEE Access. 2024.

[20] Rahate KP, Sengar MS, Patel S. Artificial Intelligence in Medical Imaging by Machine Learning and Deep Learning. InApproaches to Human-Centered AI in Healthcare 2024 (pp. 121-159). IGI Global.

[21] Singh R, Gehlot A, Akram SV, Sharma R, Malik PK. Integration of Blockchain and the Internet of Things in Healthcare Sector. InSustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications 2024 Apr 3 (pp. 155-170). Singapore: Springer Nature Singapore.

[22] Ali A, Al-Rimy BA, Alsubaei FS, Almazroi AA, Almazroi AA. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors. 2023 Jul 28;23(15):6762.

[23] Farahat IS, Aladrousy W, Elhoseny M, Elmougy S, Tolba AE. Secure medical blockchain model. Information. 2023 Jan 30;14(2):80.

[24] Ali A, Ali H, Saeed A, Ahmed Khan A, Tin TT, Assam M, Ghadi YY, Mohamed HG. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Sensors. 2023 Sep 7;23(18):7740.

[25] Vignesh Saravanan K, Jothi Thilaga P, Kavipriya S, Vijayalakshmi K. Data protection and security enhancement in cyber-physical systems using AI and blockchain. InAI models for blockchain-based intelligent networks in IoT systems: Concepts, Methodologies, tools, and applications 2023 Jun 9 (pp. 285-325). Cham: Springer International Publishing.