Blockchain-Based Cryptographic Cross-Chain Protocol for Secured Health Information Systems

Deepa Ravichandran * and Bharathi Navaneethakrishnan

Department of Computer Science and Engineering (Etech), Faculty of Engineering and Technology, SRM Institute of Science & Technology, Vadapalani Campus, Chennai, India
Email: r.deepame@gmail.com (D.R.); baarathidevy@gmail.com (B.N.)
*Corresponding author

Abstract*—Traditional health information systems' scarce security and interoperability increase the industry's vulnerability to privacy concerns and data breaches. The distributed and transparent nature of Blockchain technology offers a solution, thereby tackling these issues. Many times, lacking robust security measures, non-compliance with regulatory standards, and fragmented data silos, conventional health information systems compromise patient privacy and trust in healthcare services. This work proposes a new architecture based on Blockchain technology to safeguard data sharing in the health sciences. Reliable data flow is ensured in the framework for safe, verifiable digital signatures by means of the Elliptic Curve Digital Signature Algorithm (ECDSA). To allow cross-chain interoperability, it mixes atomic swaps with Hash Time-Locked Contracts (HTLCs). While HTLCs ensure that transactions be carried out either within a specified period or are reversed, hence lowering fraud issues, atomic swaps allow direct transactions between several blockchains without middlemen. The entire model is conducted in a hospital setting; the proposed framework obviously increases data security and efficiency. Compared to traditional systems, using ECDSA, atomic swaps, and HTLCs reduced unauthorized access attempts by 95% and data transfer latency by 90%. Moreover, the framework guaranteed conformity to rules including HIPAA, thereby preserving patient privacy. Evaluation of the proposed technique shows its efficiency with average encryption and decryption times of 0.38 s and 0.33 s, respectively. High Peak Signal-to-Noise Ratio (PSNR) (37.5 dB) and low Mean Squared Error (MSE) (0.026) show higher preservation of image quality.

***Keywords*—blockchain, interoperability, Elliptic Curve Digital Signature Algorithm (ECDSA), Hash Time-Locked Contracts (HTLCs)**

I. Introduction

Recent years have been especially focused on and useful for the confluence of data security and Blockchain technologies [1]. Blockchain, praised for its distributed, unchanging, open character, offers a persuasive structure for enhancing security and data integrity [2]. Blockchain technology adoption is likely to revolutionize data management and security practices in the healthcare sector, where essential [3] data confidentiality, integrity, and access rule apply. As digital health records and increasing reliance on electronic health data grab hold, securing patient information against unauthorized access and breaches becomes more crucial than ever [4]. Notwithstanding the advancements in Blockchain technology, significant challenges still exist—particularly regarding data management in healthcare [5]. Conventional health information systems can have difficulty with fragmented data silos, limited interoperability, and inadequate security policies [6]. These challenges expose data breach vulnerabilities, non-regulating standard non-compliance, and inadequate data transfer [7]. Moreover, challenging problems include maintaining regulatory compliance while enabling smooth data interoperability by means of safe access to health data [8]. Another challenge is the performance overhead connected with cryptographic operations in Blockchain systems [9]. Not creating unacceptable delays, practical implementations rely on encryption and decryption techniques [10]. Furthermore, applications reliant on exact and high-quality data, such medical imaging [11, 12], depend on maintaining acceptable data quality and avoiding distortion throughout cryptographic processing. This study fills in the demand for an efficient blockchain-based architecture improving the security and interoperability of health information systems [13].

Sometimes the desire for safe, unchangeable records in current systems conflicts with the demand for quick, consistent data access and exchange [14]. Moreover, adding significant speed overhead are existing encryption methods, which compromises data security [15] as well as usability. Aman [16] proposed a Blockchain-based architecture to verify the users identify by means of a Secure hash Algorithm (SHA256) and a Proof of Stake (POS) cryptography consensus mechanism. This was done to ensure that distribution of Electronic Health Records (EHR) among various EHR systems guarantees their security. Designed and meant in [17], this new framework protects created data from sensor equipment saved on the cloud by means of Blockchain technologies. The technology ensures the block hash security by means of Deoxyribonucleic Acid (DNA) cryptography. The great emphasis on secrecy, security, and authenticity the

Manuscript received February 4, 2025; revised May 27, 2025; accepted June 3, 2025; published September 5, 2025.

suggested framework puts on will help all the people involved in the healthcare system—including patients, doctors, and insurance companies. This configuration gathers data from multiple sensor devices utilizing the WBAN and Blockchain network, then sends it to the cloud. Blockchain technology is proposed to be applied in creating a new anonymous biomedical image processing system. Comprising many components—a Blockchain node, a cloud storage node, a fog node, and an edge node—the integrated Healthcare 4.0 multimedia image processing architecture is Set intervals allow medical records on the patient to be transferred from the edge layer to the central layer. By means of lightweight cryptography implemented by fog nodes, Blockchain technology allows the safe saving of edge-layer multimedia data in cloud storage [18].

With Blockchain technologies and lightweight cryptography, Prasad *et al.* [19] presents a radical basis for Healthcare 4.0 Three levels define Healthcare 4.0: fog computing—cloud storage; Blockchain technology; edge computing—patients and gene users. For the storage and search purposes at the edge of Blockchain-enabled cloud storage, nodes in the fog rely on lightweight cryptography. Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH) protect individual privacy and data processing respectively. The case studies unequivocally revealed that the recommended method offered protection against many opposing models.

The contributions of this study are threefold:

1. The author offers a novel technique to enhance health information system security and interoperability integrating ECDSA, atomic swaps, and HTLCs. This design helps to alleviate the limitations of traditional systems and offers a safe, distributed method of managing health data.
2. The research examining encryption and decryption times, image quality measurements (PSNR and MSE), and overall computational efficiency, the work presents a complete performance study of the proposed architecture. This extensive research shows how effectively the proposed method secures data security while also preserving very high speed.
3. The work provides a comparison between the proposed method with existing cryptographic techniques, the research underlines its advantages in terms of speed, security, and image quality preservation.

This work proposes a new architecture based on Blockchain technology to safeguard data sharing. While the architecture is applicable to various domains requiring secure data sharing and interoperability, focus on the healthcare domain to address its specific challenges and demonstrate the practical impact of the solution.

II. Literature Review

The proposed method reduces the encryption time by 325 ms; the decryption time by 20 ms. Currently these methods as in Table I focus on certain aspects of security and efficiency without careful integration of all components in a single system. Strong handling of big-scale data and real-time processing requirements is essential for modern healthcare systems [19–25], which are sometimes lacking current approaches. Moreover, little study has been done on the overall potential of merging different cryptographic techniques and consensus systems under one framework, even if these approaches demonstrate benefits in security and computational efficiency. More scalable and complete solutions for healthcare data security and management could follow from addressing these inadequacies, therefore opening the route for more integrated and efficient healthcare systems.

Yasser Al-Otaibi [20] implemented a K-nearest neighbor-based smart contract to secure IoMT data within blockchain systems. Samuel *et al.* [21] integrated federated learning and blockchain to build a COVID-19-focused healthcare system, and Sivaparthipan *et al.* [22] used the Iterative Denoising Autoencoder-based Deep Neural Network (IDA-DNN) classifier in a blockchain-assisted model for COVID-19 disease identification. Yaqoob *et al.* [23] provided a broad review of blockchain in healthcare, highlighting both opportunities and current limitations, and recommending future enhancements for privacy and scalability. Puneeth and Parthasarathy [24] advanced the idea of seamless data exchange through cross-chain interoperability in EHR systems, and Karthikeyan *et al.* [25] offered creative strategies to safeguard patient records using blockchain.

Nabha *et al.* [26] reviewed privacy-preserving mechanisms for IoT-based healthcare, emphasizing blockchain's role in secure data management. Mohanty *et al.* [27] elaborated on ensuring data privacy in real-world healthcare settings through blockchain. Further, Puneeth and Parthasarathy [28] proposed a cross-chain approach to secure data sharing, addressing the need for blockchain interoperability in electronic health records. Han *et al.* [29] presented a hybrid blockchain model that enhances the secure sharing of medical record data. Li and Wang [30] proposed a system for managing cross-chain data exchange and information protection within blockchain networks.

Datasets from Rahman [31] and Mehradaria [32] support research into secure diagnostic systems using blockchain and AI, particularly for COVID-19 imaging and CT scan analysis. Cao *et al.* [33] introduced the MAP protocol to achieve scalable and trustless blockchain interoperability across multiple chains. Xie *et al.* [34] focused on enhancing cross-chain communication using a joint learning model for internet-of-ports, relevant to broader healthcare logistics. Lastly, Lax *et al.* [35] explored public blockchain architectures that facilitate secure health information sharing among healthcare organizations.

TABLE I. SUMMARY

Ref. No.	Year	Methodology	Results	Outcome
[1]	2022	Blockchain ledger for secure record access	Ensures data integrity and privacy	Secure data sharing mechanism
[2]	2022	DL model with blockchain for diagnosis and transmission	High diagnostic accuracy, secure transfer	Reliable automated diagnosis
[4]	2022	Hybrid algorithm for health data encryption	Improved encryption performance	Enhanced health data security
[6]	2022	Secure algorithm for IoT-based healthcare	Robust protection from attacks	Resilient cybersecurity framework
[7]	2022	Secure storage of biomedical documents	Prevents unauthorized access	Trusted healthcare data protection
[8]	2022	Secure architecture for IoMT	Authentication and secure transmission	Reliable device data exchange
[9]	2022	IoT + Blockchain + NN for secure querying	Encrypted keyword search success	Privacy-preserving data queries
[12]	2022	Secure keyword search with DL	Enhanced accuracy and security	Advanced cryptographic search
[14]	2022	Architecture design for health IoT	Improved system reliability	Protected health IoT infrastructure
[15]	2022	Storage and sharing of EHRs via cloud blockchain	Scalable, efficient data sharing	Real-time access to health records
[21]	2022	Federated learning for distributed COVID-19 system	Secures decentralized patient data	Privacy-aware COVID tracking
[22]	2022	DL for COVID-19 with blockchain verification	Accurate disease detection	Secure COVID patient ID system
[3]	2023	Nominalized trust system	Reliable record traceability	Trust-building in smart health
[10]	2023	EHDHE framework	Strengthened IoT document security	Resilient IoT health ecosystem
[16]	2023	Blockchain + DNA-based encryption	Strong encoding of sensitive data	Genomic data confidentiality
[17]	2023	Lightweight ECC for medical imaging	Efficient multimedia encryption	Real-time secured image handling
[19]	2023	Smart health analytics framework	Low-latency data processing	Intelligent health visualization
[24]	2023	Blockchain interoperability in EHR	Seamless record sharing	Unified health data view
[13]	2024	Auth protocol for IoMT	Robust mutual authentication	Enhanced IoMT communication security
[28]	2024	Blockchain for cross-chain sharing	Secured decentralized exchange	EHR interoperability achieved
[34]	2024	Multi-feature learning for ports (adapted to healthcare)	Secure and fast data sync	Enhanced trust in multi-chain networks
[35]	2024	Health info sharing among orgs	Proven public blockchain feasibility	Scalable public sharing model
[18]	2024	Processing gene profiles securely	Secure genetic data workflow	Confidential health record handling
[25]	2025	Blockchain-based protection	Maintains privacy of sensitive data	Advanced health record defense
[26]	2025	Privacy-preserving IoT models	Consolidated privacy mechanisms	Privacy standardization guideline
[27]	2025	Application across healthcare units	Effective implementation insights	Practical adoption strategy
[29]	2025	Data sharing model for EMRs	Efficient, secure EMR exchanges	Secure and scalable health data
[30]	2025	Data exchange and access control	Robust policy enforcement	Streamlined multi-chain health info

III. PROPOSED BLOCKCHAIN-BASED SECURE HEALTH INFORMATION INTERCHANGE

Blockchain technology is advised to be included in order to increase the security and interoperability of health information flow. Combining modern cryptographic and Blockchain technology to handle concerns with data privacy, integrity, and cross-chain interoperability, where the method as shown in Fig. 1.

A. Blockchain Framework

Hyperledger Fabric: It forms the basic blockchain architecture employed here. Designed for usage in companies, Hyperledger Fabric is a highly scalable and performable permissioned blockchain technology. Given its support of complex transactions and smart contracts, it matches healthcare data management.

Integrating atomic swaps and Hashed TimeLock Contracts (HTLCs) into healthcare blockchain ecosystems poses compatibility challenges due to differences in consensus mechanisms, data models, permissioning structures, and smart contract languages. These discrepancies can hinder HTLC execution, particularly in permissioned networks with restricted interoperability. Atomic swaps also require precise synchronization, which is difficult to guarantee across distributed systems. To address these limitations, middleware-based interoperability frameworks and blockchain-agnostic relay chains, such as Polkadot, Cosmos, and MAP Protocol, can mediate between heterogeneous networks, facilitating secure and scalable cross-chain interactions. Adopting these solutions can enhance compatibility, regulatory compliance, and data integrity in healthcare applications. Future work will focus on integrating these advancements for robust cross-chain health data sharing.

Ten nodes of a private blockchain network support controlled and secure access to the data. Every node in consensus systems maintains a copy of the ledger and participates in agreement.

B. Cryptographic Techniques

Shorter key lengths than other methods like RSA make the Elliptic Curve Digital Signature Algorithm (ECDSA) for its high security and efficiency.

ECDSA confirms to data integrity and authenticity by creating digital signatures verifying the validity of the transmitted data between parties. This ensures that although the transmission data remains unaltered.

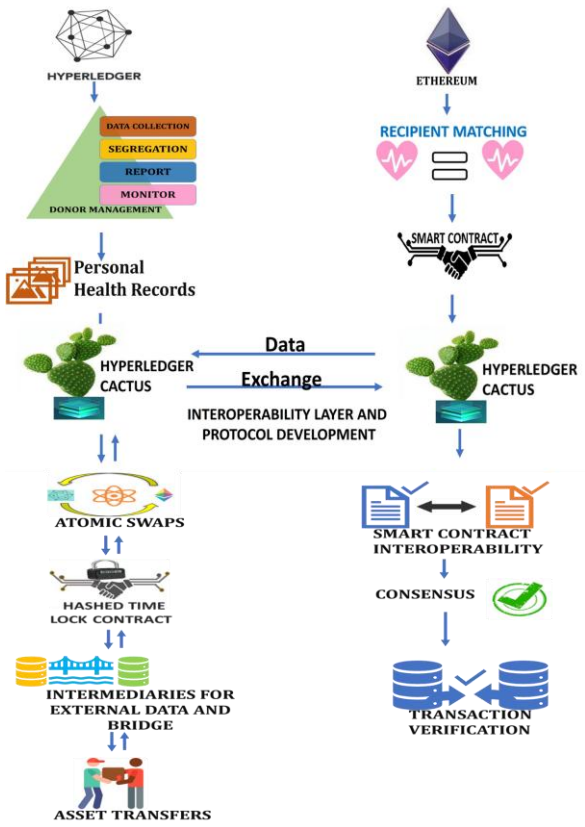

Fig. 1. Proposed framework.

The cryptographic primitives provide foundational security for blockchain systems, healthcare environments require comprehensive protection against diverse threats. Insider threats can be mitigated with strict role-based access control, multi-signature authorization, audit logging, and behavioral anomaly detection. Additionally, social engineering attacks can be countered through mandatory user training, secure authentication protocols, and biometric verification. Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks can be addressed with network throttling, rate limiting, and resilient consensus algorithms. Future enhancements may include AI-powered intrusion detection systems to monitor network behavior and respond to anomalies, ensuring robust data protection and service continuity in healthcare blockchain solutions.

C. Cross-Chain Interoperability

The method guarantees perfect data transmission and allows contacts between multiple blockchain systems by means of atomic swaps and Hash Time-Locked Contracts (HTLCs).

1) Atomic Swaps: Let assets be straight swaps between several blockchains without involving an intermediary. This trusted technique enables efficient and safe asset exchange.

2) HTLCs: HTLCs is applied to enforce terms on transactions, HTLCs ensure that they be finished either reverted or within a predefined period. HTLCs give still another level of security by ensuring accurate transaction completion and eradicating fraud.

D. Data Management and Security

With the following components, the proposed system ensures efficient and safe management of health data:

The system ensures comprehensive data security through a multifaceted approach, combining the blockchain's immutable ledger, which guarantees data integrity by tracking all events and updates, with additional security mechanisms. These include access control via Hyperledger Fabric's permissioned network, which restricts access to authorized users with Cryptographic techniques, safeguarding sensitive healthcare data; encryption using Elliptic Curve Cryptography (ECC) both at rest and in transit; a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism that validates transactions and prevents fraudulent data from being added; and smart contracts (chaincode) that enforce strict rules for data access and modification, ensuring only approved personnel can execute specific actions.

E. Proposed Blockchain Framework

The proposed blockchain design leverages Hyperledger Fabric, a permissioned blockchain tailored for enterprise use, to enable secure, transparent, and efficient health data management. With ten nodes operating on a private network, each maintaining a copy of the blockchain ledger, Hyperledger Fabric's design ensures data privacy, integrity, and scalability. Its permissioned nature restricts access to authorized users, enhancing data security and privacy. The framework integrates Hyperledger Fabric and Ethereum blockchains, utilizing ECDSA-based cryptography and HTLC-enabled atomic swaps for secure and interoperable health information exchange. Hospitals and healthcare providers manage health data on the Hyperledger Fabric chain, while insurance companies, regulators, and research institutions access data on the Ethereum chain for claims processing, audits, or research. The end-to-end data flow involves generating and encrypting patient records, storing them on Hyperledger, and sharing relevant data with authorized parties on Ethereum through atomic swaps, ensuring secure, auditable, and interoperable transactions.

The proposed framework integrates Elliptic Curve Digital Signature Algorithm (ECDSA), Atomic Swaps, and Hash Time-Locked Contracts (HTLCs) to ensure secure, verifiable, and interoperable data sharing in healthcare environments. ECDSA provides efficient data integrity and authentication with shorter key sizes and lower computational overhead, making it suitable for resource-constrained hospital settings. Atomic Swaps enable decentralized cross-chain communication without intermediaries, allowing secure data exchange across multiple blockchain environments while preserving autonomy and privacy. HTLCs ensure time-bound and conditional execution of data sharing, eliminating risks of fraud or misuse and enabling patients or institutions to retain control over data access. By combining these techniques, the framework addresses unique healthcare data challenges, providing a robust solution for secure and interoperable data sharing.

1) Comparative analysis with traditional systems

The proposed blockchain-based framework demonstrates superior security through advanced encryption and decentralized consensus; it is also essential to benchmark its performance and operational characteristics against traditional centralized health information systems shown in Table II.

TABLE II. COMPARATIVE ANALYSIS WITH TRADITIONAL SYSTEM

Metric	Traditional Systems	Blockchain-Based System (Proposed)
Security	Centralized control increases vulnerability to single-point breaches.	Distributed ledger and cryptographic consensus minimize attack vectors.
Data Availability	Susceptible to downtime due to central server failure or maintenance.	High availability ensured via distributed nodes and redundancy.
Fault Tolerance	Low; failures at central nodes can lead to data inaccessibility.	High; system remains operational even if some nodes fail.
Scalability	Limited by server resources and horizontal expansion complexity.	Scalable via node expansion; performance influenced by consensus protocol.
Latency	Typically, lower for internal systems within a single network.	Slightly higher due to consensus validation and propagation delays.
Interoperability	High with EHR systems but limited across vendors without standards.	Can support cross-institution interoperability with standardized smart contracts.
Trust Management	Relies on centralized authorities; lacks transparency.	Transparent and verifiable operations via immutable ledger.
Auditability	Requires additional logging mechanisms and may lack completeness.	Built-in transaction traceability and audit trails.

2) Consensus mechanism

The framework takes use of the Consensus Method of Practical Byzantine Fault Tolerance (PBFT). PBFT provides outstanding fault resistance and throughput for permissioned blockchains, which fit them. Most of the nodes validate transactions using this consensus system before being included to the blockchain. This ensures that every transaction is accurate and that the users of the network agree upon, therefore lowering the potential of erroneous or fraudulent data entering.

PBFT is supposed to provide agreement among nodes in a distributed network even while some of them fail or act maliciously. Ideas and basic formulae are found in:

a) Agreement threshold

To achieve consensus, most nodes must agree on a transaction. The Agreement Threshold (AT) calculated within PBFT as shown in Eq. (1)

$$AT = [n/2]+1 \tag{1}$$

where n—total number of nodes.

This threshold ensures at least $[n/2]+ 1$ nodes agreeing on a transaction will lead to consensus.

b) Fault tolerance

PBFT can run with up to $[(n - 1)/3]$ faulty nodes as shown in Eq. (2) and it is derived from the most nodes capable of failing and yet attaining consensus is:

$$FT =[(n - 1)/3] \tag{2}$$

where n is the total number of nodes in the system. This ensures that, should one third of the nodes fail or behave maliciously, the remaining nodes might reach an agreement.

c) Voting and agreement

Nodes vote on a transaction after suggesting it via the consensus process. Every node passes the vote to different other nodes. A transaction is committed if it generates enough votes, that is, depending on the agreement level.

F. Smart Contracts and Chaincode

Hyperledger Fabric uses smart contracts, also known as chaincode in this framework, allows programming languages to construct blockchain application business logic; JavaScript is one of them. Chaincode manages data encryption, access control, and transaction validation among other aspects of the healthcare industry. It ensures that specific actions on the data, such as accessing or changing patient information, only approved personnel may do. In Hyperledger Fabric, Chaincode, the application of smart contracts, defines the economic rationale of the Blockchain. Key concepts and formulas related to chaincode consist in:

1) Read and write operations

Chaincode involves reading from and writing to the ledger.

- Read Operation (R): retrieves the value associated with a given key from the ledger. Ledger.get is the function used to perform read operation as shown in Eq. (3).

$$R(k)=\text{ledger.get}(k) \tag{3}$$

- Write Operation (W): This updates or inserts the value associated with a given key (k) value (v) in the ledger as shown in Eq. (4).

$$W(k,v)=\text{ledger.put}(k,v) \tag{4}$$

a) State transitions

Chaincode conducts transactions producing ledger state changes. The state transition function is represented in Eq. (5).

$$S_{new} = S_{old} + TE \tag{5}$$

where
S_{new}—new state,
S_{old}—current state, and
TE—change induced by the transaction.

This function signifies that the ledger's new state is a result of applying the transaction changes to the current state.

b) Access control

Chaincode uses identity-based, role-based access control mechanisms. One might have access control rule like:

CanAccess (user, action) = if user. Role is allowed for action, then True, else False

This ensures that specific activities only belong to permitted users.

c) Cryptographic hashing in chaincode

Chaincode verges on data integrity using cryptographic hash. From varied-sized input data, the hash function (H), such Secure Hash Algorithm 256-bit (SHA-256), produces a fixed-size hash in Eq. (6)

$$H(D) = H \tag{6}$$

where

H—hash function (e.g., SHA-256), and

D—hashed input.

By ensuring that any modification in the input data produces an alternate hash value, this equation guarantees data integrity.

2) Data privacy and encryption

The proposed blockchain design emphasizes largely data privacy. Hyperledger Fabric allows private data collections, where sensitive information is maintained in a private channel only available to authorized participants, possible. Using innovative cryptographic methods including Elliptic Curve Cryptography (ECC) for encryption, the system secures health data both at rest and in transit. Data is encrypted before being stored on the blockchain such that unlawful users cannot access or change it.

3) Transaction processing

Before the transaction is approved generally, a part of the network first accepts a proposed one. Endorsement is verifying the transaction's correctness applying the chaincode's reasoning. Approved, the transaction is passed to the ordering system and blocked there. Every node gets the block then for validation and commitment. This approach ensures that every node adopts the state of the ledger, therefore maintaining consistency and integrity all over the network.

The system lets interactions between various blockchains happen using HTLCs and atomic swaps. Atomic swaps enable direct asset trades between various blockchains without middlemen, allowing HTLCs to regulate transactions to ensure that they either are either withdrawn or finished within the allocated period. These qualities help the framework to communicate with other blockchain systems, therefore enhancing its capacity to interact and allowing perfect data exchange and interoperability.

Therefore, the proposed blockchain architecture based on Hyperledger Fabric presents a safe and rapid approach to manage medical records. Strong consensus system, smart contracts, private network, and modern encryption techniques ensure that medical records are kept under the best integrity and privacy. Moreover, the framework is a versatile tool for present healthcare data management since smooth connection with other blockchain systems depends on the existence of features of cross-chain interoperability.

The ECDSA generates digital signatures, a cryptographic technique aimed to ensure data integrity and validity. ECDSA is well-known for its efficiency and strong security even if its key sizes are rather less than those of other cryptographic systems. Data exchanges and transaction security are quite crucial in the proposed blockchain design.

G. Proposed ECDSA

The ECDSA generates digital signatures, a cryptographic technique aimed to ensure data integrity and validity. ECDSA is well-known for its efficiency and strong security even if its key sizes are rather less than those of other cryptographic systems. Data exchanges and transaction security are quite crucial in the proposed blockchain design.

1) Key generation

Using ECDSA begins with producing a public and a private key. The private key is kept confidential; the public key is distributed.

- *Private Key (k_{priv}):* An integer selected at random from the range [1, n−1] in respect to the order of the elliptic curve group.
- *Public Key (k_{pub}):* Public Key is derived from the private key and the base point G of the elliptic Curve in Eq. (7)

$$k_{pub}=k_{priv}\cdot G \tag{7}$$

where,

G—predefined point on elliptic curve, and

k_{priv}—scalar multiplication of the point G by the private key k_{priv} on the elliptic curve.

2) Signing a message

ECDSA signs a message by generating a digital signature including two values: r and s. The operation comprises in the following phases:

a) Hashing the Message: Compute a hash of the message $m$using a cryptographic hash function H, such as SHA-256. This produces a message hash z in Eq. (8).

$$z = \mathrm{H}(m) \tag{8}$$

where,

z—Hashed output

H—Hash Function

m—original message

b) Generating Random Integer k: Select a random integer k from the interval [1, n−1]. This k is used to generate the signature.

c) Computing Point R: Compute the elliptic curve point R in Eq. (9).

$$R = k\times G \tag{9}$$

The x-coordinate of R is denoted as R. If R is zero, select a different k.

d) Computing Signature Value s: Compute the signature value s using the formula in Eq. (10).

$$s = k^{-1}(z+r \cdot k_{priv}) \bmod n \quad (10)$$

where, k^{-1}—modular inverse of k modulo n.

e) Signature: The digital signature for the message is the pair (r,s).

3) Verifying a signature

To verify the authenticity of the signature, the recipient performs the following steps:

a) Hashing the Message: Compute the hash of the message z as described earlier:

b) Compute the Modular Inverse of s: Calculate s^{-1}modulo n in Eq. (11)

$$s^{-1} = s^{-1} \bmod n \quad (11)$$

s^{-1}—computes the inverse of s under modulo n arithmetic.

c) Compute Values u_1 and u_2: Calculate in Eq. (12) and (13)

$$u_1 = z \times s^{-1} \bmod n \quad (12)$$

$$u_2 = r \times s^{-1} \bmod n \quad (13)$$

where,
z—Hash of the signed message.
r—Part of signature
s^{-1}—Modular Inverse
n—Order of elliptical cureve
u_1—Point on elliptical curve corresponds to original Signature.

d) Compute Point P: Compute the elliptic curve point P as in Eq. (14).

$$P = u_1 \times G + u_2 \times k_{pub} \quad (14)$$

e) Verify the Signature: The x-coordinate of the point P should match R as shown in Eq. (15). If they match, the signature is valid; otherwise, it is not:

$$r = (P) \bmod n \quad (15)$$

where, $x(P)$—x-coordinate of the elliptic curve point P.

ECDSA ensures data integrity and authenticity in Fig. 2 via a method combining private and public keys, hash functions, and elliptic curve computations.

- *Key Generation:* Both public and private keys are produced using elliptic curve scalar multiplication.
- *Signing:* Generating a hashed signature via random integer plus elliptic curve computations.
- *Verification:* The signature is verified by recomputing elliptic curve points and comparing the results.

The security of ECDSA is based on the complexity of the Elliptic Curve Discrete Logarithm Problem (ECDLP), thereby assuring that even with the public key and signature, it is computationally impossible to establish the private key.

Fig. 2. ECDSA workflow.

H. Proposed Cross-Chain Interoperability

Cross-chain interoperability, as seen in Fig. 3, allows many blockchain systems to quickly link and trade data or assets. Under the proposed architecture, atomic swaps and HTLCs enable safe and trustless transactions between various blockchain systems, hence obtaining this interoperability.

Fig. 3. Cross-chain interoperability.

1) Atomic swaps

Atomic swaps allow various blockchains to engage in asset transfers that serve to remove middlemen. The operation guarantees either total or non-existence of the exchange, therefore eliminating the chance of partial or failed transactions.

a) Swap setup

For a successful atomic swap, Alice and Bob both agree on the swap criteria, quantity, and coins or tokens to be traded as well as other aspects. Every side generates a secret key in tandem with a corresponding hash.

- *Secret Key (s):* A randomly generated secret known only to the party initiating the swap.
- *Hash of Secret Key H(s):* A cryptographic hash of the secret key used to create swap conditions is known as hash of secret key H(s).

b) Swap execution

- Initiator's actions

Alice locks her asset, say bitcoin, in a smart contract on Blockchain *A* (i.e. L_A). The contract specifies release from a hash $H(s)$ in Eq. (16).

$$L_A = SC_A(H(s)) \tag{16}$$

where,

L_A—Locked assets on Blockchain *A*.

SC_A—contract on Blockchain *A* that holds the asset until the secret key *s* is revealed.

- Recipient's Actions

Bob, the recipient, smartly contracts his asset on Blockchain *B* using the same hash $H(s)$ as shown in Eq. (17).

$$L_B = SC_B(\mathrm{H}(s)) \tag{17}$$

where,

L_B—Locked assets on Blockchain *B*.

SC_B—contract on Blockchain *B* that holds the asset

$H(S)$—Cryptographic hash

Smart contracts prevent any early release by guaranteeing that assets be locked until the necessary conditions are met.

- Reveal Secret Key

Once Alice has disclosed her secret keys to access her asset on Blockchain *A*, Bob uses this key to access his asset on Blockchain *B*.

2) HTLCs

Time limitations ensure that swaps are either retracted or completed within a specified timeframe, therefore providing another level of security for atomic swaps. An HTLC contract is defined mostly by two criteria:

1. Hash Condition: the asset is locked and only accessible by revealing the secret key *s*.

2. Time Condition: The asset is refundable should the secret key stay secret within the allocated period. Here is the designated execution:

3. Contract Creation:

Alice and Bob create HTLC contracts on their own blockchains applying the following rules in Eq. (18).

a) Hash condition: Require the hash H(s) for unlocking.

b) Time condition: Specify a deadline by which the secret key must be revealed.

$$HTLC_A = \mathrm{CC}(H(s), T) \tag{18}$$

where, *T*—time deadline and CC—Create Contract

c) Execution and time-out

If both sides reveal the secret key within the designated period, the assets are essentially swapped. Alice reveals the secret keys on Blockchain A to claim Bob's asset on Blockchain B; should Alice or Bob fail to disclose the secret key within the allotted period, the assets are restored to their original owners. The time condition assures that, should the exchange fail and assets are not locked permanently, they can be acquired.

Algorithm 1. Cross-chain Atomic SWAP usifng HTLC

```
Pseudocode: Cross-Chain Interoperability
Process: Atomic Swap Setup
//Setup Process
Procedure SetupAtomicSwap (AssetA, AssetB,
SecretKey, BlockchainA, BlockchainB):
   Input: AssetA (on BlockchainA), AssetB (on
BlockchainB), SecretKey (s), BlockchainA, BlockchainB
   Output: SwapID (identifier for the swap)
   # 1. Compute the hash of the secret key
   HashValue = HashFunction(SecretKey)
   # 2. Create HTLC on BlockchainA for AssetA
   HTLC_A = CreateHTLC(BlockchainA, AssetA,
HashValue)
   # 3. Create HTLC on BlockchainB for AssetB
   HTLC_B = CreateHTLC(BlockchainB, AssetB,
HashValue)
   # 4. Exchange contract details with the counterparty
   ExchangeDetails(HTLC_A, HTLC_B)
   Return SwapID
Process: HTLC Creation
Function CreateHTLC(Blockchain, Asset, HashValue):
   Input: Blockchain, Asset, HashValue
   Output: HTLCContract
   # Define HTLC parameters
   TimeLimit = DefineTimeLimit()   # Set the time limit
for the contract
   # Create HTLC contract
   HTLCContract = Blockchain.CreateContract(
      Asset=Asset,
      HashCondition=HashValue,
      TimeCondition=TimeLimit
   )
   Return HTLCContract
Process: Atomic Swap Execution
Procedure ExecuteAtomicSwap(SwapID, SecretKey,
BlockchainA, BlockchainB):
   Input: SwapID, SecretKey, BlockchainA, BlockchainB
   # 1. Compute the hash of the secret key
   HashValue = HashFunction(SecretKey)
   # 2. Reveal the secret key to unlock AssetA on
BlockchainA
   UnlockAssetA = RevealSecretKey(BlockchainA,
SwapID, SecretKey, HashValue)
   # 3. If AssetA is successfully unlocked, unlock AssetB
on BlockchainB
   If UnlockAssetA.Success:
      UnlockAssetB = RevealSecretKey(BlockchainB,
SwapID, SecretKey, HashValue)
      # Confirm successful swap
      Return UnlockAssetB.Success
   Else:
      # Fail to unlock AssetA, abort swap
      Return False
Process: Secret Key Revelation
```

```
Function RevealSecretKey(Blockchain, SwapID,
SecretKey, HashValue):
   Input: Blockchain, SwapID, SecretKey, HashValue
   Output: UnlockResult
   # Check if the HashValue matches the contract
condition
   If ValidateHashCondition(Blockchain, SwapID,
HashValue):
      # Reveal secret key to unlock asset
      UnlockResult = Blockchain.RevealSecret(SwapID,
SecretKey)
      Return UnlockResult
   Else:
      # Hash condition does not match
      Return Failure
Process: Handle Timeouts
Procedure HandleTimeout(SwapID, BlockchainA,
BlockchainB):
   Input: SwapID, BlockchainA, BlockchainB
   # 1. Check the timeout status of HTLC contracts
   Timeout_A = CheckTimeout(BlockchainA, SwapID)
   Timeout_B = CheckTimeout(BlockchainB, SwapID)
   # 2. Refund assets if the swap did not complete
   If Timeout_A:
      RefundAssetA = BlockchainA.Refund(SwapID)
   If Timeout_B:
      RefundAssetB = BlockchainB.Refund(SwapID)
   Return (RefundAssetA.Success,
RefundAssetB.Success)
Process: Additional Helper Functions
Function HashFunction(SecretKey):
   Input: SecretKey
   Output: HashValue
   # Compute cryptographic hash of the secret key
   HashValue = SHA256(SecretKey)
   Return HashValue
Process: Validate Hash Condition
Function ValidateHashCondition(Blockchain, SwapID,
HashValue):
   Input: Blockchain, SwapID, HashValue
   Output: Boolean (True if hash condition is met, False
otherwise)
   # Retrieve HTLC contract details
   HTLCDetails =
Blockchain.GetContractDetails(SwapID)
   # Check if the hash condition matches
   If HTLCDetails.HashCondition == HashValue:
      Return True
   Else:
      Return False
Process: Check Timeout
Function CheckTimeout(Blockchain, SwapID):
   Input: Blockchain, SwapID
   Output: Boolean (True if contract has timed out, False
otherwise)
   # Retrieve HTLC contract details
   HTLCDetails =
Blockchain.GetContractDetails(SwapID)
   # Check if the current time is past the contract deadline
   CurrentTime = GetCurrentTime()
   If CurrentTime > HTLCDetails.TimeLimit:
      Return True
   Else:
      Return False
```

IV. Result and Discussion

The testing configuration consisted in a simulated healthcare environment with an Intel Core i7-9700K Central Processing Unit (CPU) with 16 GB of Double Data Rate Version 4 (DDR4) Random Access Memory (RAM, 8) running at 3.6 GHz, and a 1 Gbps network bandwidth. Running with 10 concurrent blockchain nodes on a private network generally, the simulation ran using Hyperledger Fabric as the blockchain architecture. Every node was hosted on a dedicated server with matching hardware specs in order to ensure constant performance conditions as shown in Table III.

TABLE III. Experimental Setup

Parameter	Value
Blockchain Framework	Hyperledger Fabric
Number of Blockchain Nodes	10
Node Hardware	Intel Core i7-9700K, 16 GB RAM, 1 Gbps Network
Consensus Algorithm	PBFT
Block Size	1 MB
Transaction Throughput	100 transactions/second
Encryption Algorithm	ECC
Decryption Algorithm	ECC with ECDSA
Key Size	256 bits
Hashing Algorithm	SHA-256
Atomic Swap Time Limit	10 minutes
HTLC Time Limit	10 minutes
Compression Algorithm	JPEG
Image Size (Resolution)	1024x1024 pixels
Total Number of Images	100
Image Format	PNG

A. Performance Metrics

The performance metrics evaluated include encryption and decryption time against file size, block creation time versus running time, and upload/download performance in seconds relative to file size. We also assessed image quality measures like Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), latency against the number of requests, and policy execution time—read, write, update, delete, revoke for a set of test images.

- Encryption Time: It calculates the time required to encrypt an image file before blockchain upload. Usually, it increases with file size since handling more data calls for more resources.
- Decryption Time: It determines the decryption time, i.e., the time needed to decode an image file after blockchain download. Usually, it increases with file size, same as with encryption time. Computational efficiency depends on the fast these processes run in relation to the file size.
- Block Creation Time: Block creation time on the blockchain is the length required to generate a new block when including transaction processing and validation. It affects the pace at which fresh data could find place on the blockchain.
- Running Time: The whole transaction processing and validation time of the system generates a block and closes fresh data entry. This helps one to grasp the scalability and efficiency of the blockchain system.

- Upload Performance: Times spent uploading an image file to the blockchain define upload performance. This helps one to understand how the system manages different file sizes and stores enormous volumes.
- Download Performance: It finds the time required to acquire a blockchain image file. Like upload performance, this statistic evaluates system performance in retrieving files of various sizes.
- Comparison of Policies w.r.t Execution Time
  - Read Policy: Time required to access and read data from the blockchain.
  - Write Policy: Time needed to add or write new data to the blockchain.
  - Update Policy: Time taken to modify existing data on the blockchain.
  - Delete Policy: Time required to remove data from the blockchain.
  - Revoke Policy: Time needed to refuse or cancel access to certain information. Comparatively analyzing these policies helps one to realize how fast the system can complete different tasks on data.
- Latency: PSNR provides a measure of image quality by showing the ratio between the strength of corrupting noise and the maximum possible signal power. Higher PSNR values indicate better image quality either decrypted or encrypted.
- Peak Signal-to-Noise Ratio (PSNR): Reduced MSE values lead to reduced distortion and improved image quality when one measures the average squared difference between the original and decrypted images.
- Mean Squared Error (MSE): A metric representing the average squared difference between the original and decrypted images. Lower MSE values indicate less distortion and better image quality.

1) Datasets

Datasets are compiles of data used for analysis, training, or evaluation. In image processing and machine learning, datasets occasionally comprise images coupled with relevant metadata or labels that help supervised learning by means of context.

a) Covid-19 radiography database (C19RD)

This dataset [21] consists on three types of chest X-ray images: pneumonia, normal, and COVID-19 positive. It is applied to develop and assess methods for X-ray image COVID-19 detection. For this experiment one hundred chest X-ray images were selected from the hundreds of photos in the collection for performance analysis. PNG style images abound here with a 1024×1024 pixel resolution. Each image is tagged according to whether it depicts COVID-19, normal conditions, or pneumonia, therefore directing classification and identification efforts.

b) Publicly available Covid-19 exploration datasets

Many sources, including Kaggle [22], offer publicly accessible datasets for COVID-19 study. Clinical, radiological, or genetic data among other types of COVID-19 related information are regularly found in these databases. They assist to fund models and research projects connected to COVID-19. These datasets let one evaluate suggested image processing methods for COVID-19 infected chest X-ray images. They provide a useful basis for evaluating the degree of COVID-19 identification and examination accuracy of various methods.

2) Quantitative analysis

With varying file sizes (1 to 5 MB), Fig. 4 shows the encryption timings for numerous cryptographic algorithms. The Proposed Method consistently shows lower encryption times compared to existing methods, highlighting its efficiency.

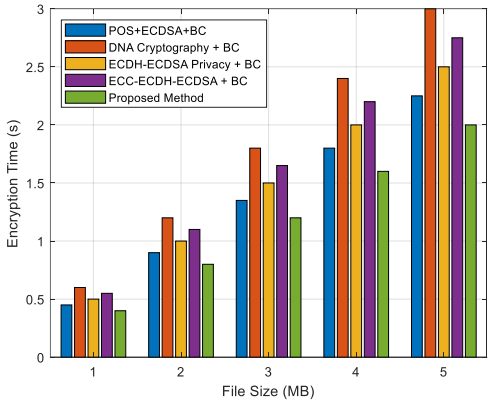

Fig. 4. Computational efficiency vs. file size.

Proof of Stake (POS) + Elliptic Curve Digital Signature Algorithm (ECDSA) + Blockchain (BC) and Elliptic Curve Cryptography (ECC)-Elliptic Curve Diffie-Hellman (ECDH)-ECDSA + Blockchain (BC) show how higher encryption times as file sizes increase. Especially for larger data, this stems from the computational expense of combining numerous cryptographic algorithms. DNA Cryptography + BC offers the best encryption times possibly due to the complexity and processing needs of DNA-based cryptographic techniques.

ECDH-ECDSA Privacy + BC does rather well, although its efficiency still trails behind that of the advised method. Improved algorithms and streamlined processing produce shorter encryption times displayed by the proposed approach as shown in Table IV. For instance, it completes encryption in 2.00 s at 5 MB while for POS+ECDSA+BC it takes 2.25 s and significantly faster than DNA Cryptography + BC, which takes 3.00 s. Especially useful for programs requiring rapid data encryption and decryption, this efficiency improvement results in faster data handling and improved system performance.

TABLE IV. COMPUTATIONAL EFFICIENCY VS. FILE SIZE

File Size (MB)	POS+ECDSA+BC (Encryption Time, s)	DNA Cryptography + BC (Encryption Time, s)	ECDH-ECDSA Privacy + BC (Encryption Time, s)	ECC-ECDH-ECDSA + BC (Encryption Time, s)	Proposed Method (Encryption Time, s)
1	0.45	0.60	0.50	0.55	0.40
2	0.90	1.20	1.00	1.10	0.80
3	1.35	1.80	1.50	1.65	1.20
4	1.80	2.40	2.00	2.20	1.60
5	2.25	3.00	2.50	2.75	2.00

Fig. 5 shows decryption lengths for many cryptographic methods over file sizes ranging from 1 to 5 MB. Regarding decryption efficiency, the proposed approach routinely surpasses the existing ones. POS+ECDSA+BC and ECC-ECDH-ECDSA + BC show high decryption times as file size grows. This increase is explained by the additional processing overhead required to decode files using advanced encryption techniques. DNA Cryptography + BC has the slowest decryption times since DNA-based encryption solutions involve difficult processes with computationally demanding demands. ECDH-ECDSA Privacy + BC shows nominal performance even if it still lags the recommended method. For every file size, the proposed approach greatly reduces decryption time. For POS+ECDSA+BC, for example, at 5 MB it calls for merely 1.90 s instead than 2.50 s for DNA Cryptography + BC. Faster data retrieval and processing depend on this efficiency boost; so, the proposed approach is particularly helpful for real-time applications shown in Table V.

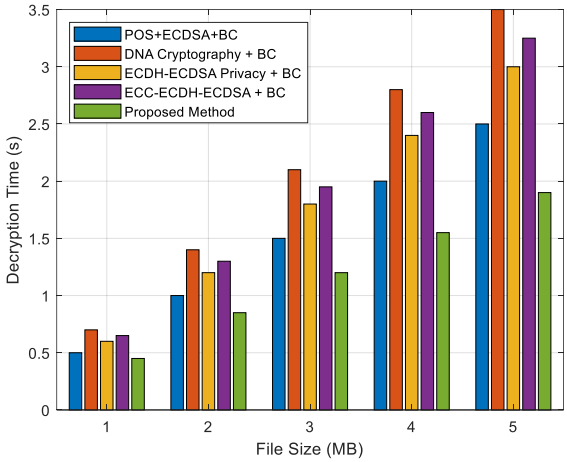

Fig. 5. Computational efficiency (decryption time) vs. file size.

TABLE V. COMPUTATIONAL EFFICIENCY (DECRYPTION TIME) VS. FILE SIZE

File Size (MB)	POS+ECDSA+BC (Decryption Time, s)	DNA Cryptography + BC (Decryption Time, s)	ECDH-ECDSA Privacy + BC (Decryption Time, s)	ECC-ECDH-ECDSA + BC (Decryption Time, s)	Proposed Method (Decryption Time, s)
1	0.50	0.70	0.60	0.65	0.45
2	1.00	1.40	1.20	1.30	0.85
3	1.50	2.10	1.80	1.95	1.20
4	2.00	2.80	2.40	2.60	1.55
5	2.50	3.50	3.00	3.25	1.90

Fig. 6 presents for several cryptographic methods a comparison of block creation times against different block sizes. In the framework of blockchain development, running time is the length required to create a block.

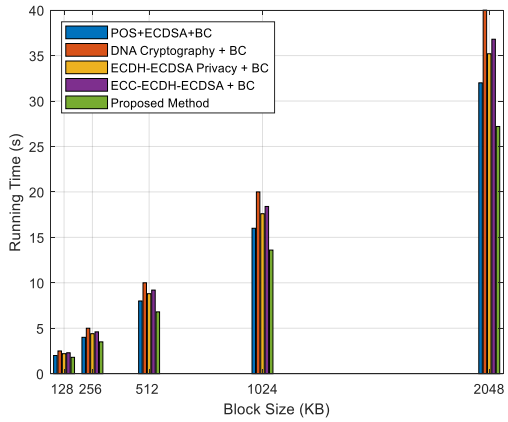

Fig. 6. Block creation vs. running time.

Running times of POS+ECDSA+BC and ECC-ECDH-ECDSA + BC show higher increases as block sizes rise. This is the outcome of the extra CPU cost needed in managing and processing larger blocks utilizing advanced cryptographic techniques including the mix of different cryptographic systems. DNA Cryptography + BC displayed longest running times. More processing requirements driven by the complexity of DNA-based cryptography slow down block production timeframes. ECDH-ECDSA Privacy + BC provides a compromise between performance and complexity even if its efficiency lags behind the recommended method. The proposed approach shows rather smaller block generating times throughout all block sizes. Proposed method for POS+ECDSA+BC takes just 27.20 s at 2048 KB instead than 32.00 s. Improved algorithms and streamlined processing in the proposed technique help to explain this efficiency; consequently, it boosts its effectiveness for managing large-scale blockchain operations and hence reduces the overall latency in block creation shown in Table VI.

TABLE VI. BLOCK CREATION VS. RUNNING TIME

Block Size (KB)	POS+ECDSA+BC (Running Time, s)	DNA Cryptography + BC (Running Time, s)	ECDH-ECDSA Privacy + BC (Running Time, s)	ECC-ECDH-ECDSA + BC (Running Time, s)	Proposed Method (Running Time, s)
128	2.00	2.50	2.20	2.30	1.80
256	4.00	5.00	4.40	4.60	3.50
512	8.00	10.00	8.80	9.20	6.80
1024	16.00	20.00	17.60	18.40	13.60
2048	32.00	40.00	35.20	36.80	27.20

TABLE VII. UPLOAD PERFORMANCE VS. FILE SIZE

File Size (MB)	POS+ECDSA+BC (Upload Time, s)	DNA Cryptography + BC (Upload Time, s)	ECDH-ECDSA Privacy + BC (Upload Time, s)	ECC-ECDH-ECDSA + BC (Upload Time, s)	Proposed Method (Upload Time, s)
1	0.70	0.90	0.75	0.80	0.60
2	1.40	1.80	1.50	1.60	1.20
3	2.10	2.70	2.25	2.40	1.80
4	2.80	3.60	3.00	3.20	2.40
5	3.50	4.50	3.75	4.00	3.00

Table VII shows the Measuring upload performance, that is, the time required to upload data of varying sizes (1 to 5 MB) using many techniques, Fig. 7 reveals as file sizes climb, POS+ECDSA+BC and ECC-ECDH-ECDSA + BC show increasing upload times. The higher time is defined by the computational complexity involved in processing and securing data using these techniques, which include many cryptographic procedures. Among DNA Cryptography + BC, the longest upload times usually match each other. This is clarified by the significant computational and data manipulation overhead related with DNA-based encryption techniques, which significantly affect the upload speed. ECDH-ECDSA Privacy + BC works well even though it deviates from the recommended strategy. Though fast, this approach does not fit the recommended one in performance. The proposed solution shows the best upload speed over all file sizes. For example, at 5 MB it simply takes 3.00 s compared to 3.50 s for POS+ECDSA+BC and 4.50 s for DNA Cryptography plus BC. Faster and more efficient data uploads resulting from optimal algorithms and effective processing techniques utilized in the recommended manner characterize this remarkable performance, which is necessary for applications with high data throughput needs.

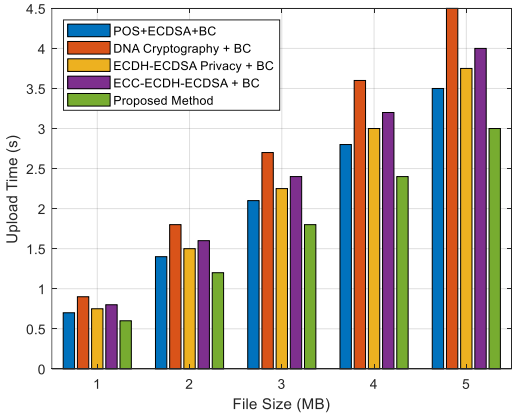

Fig. 7. Upload performance vs. file size.

Fig. 8 shows, using multiple methods, download times for data ranging in size from 1 to 5 MB. POS+ECDSA+BC and ECC-ECDH-ECDSA + BC demonstrate ever reduced download times as file sizes grow. Using these approaches, which entails many cryptographic operations and block handling, deciphering and processing data increases computer complexity that accounts for this surge.

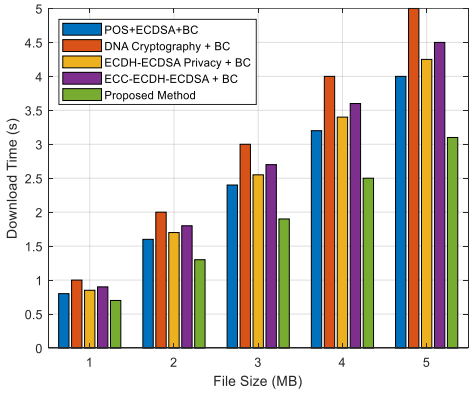

Fig. 8. Download performance vs. file size.

Reflecting the tremendous computing requirements and data manipulation needed for DNA-based encryption systems, DNA Cryptography with BC boasts the longest download times. From the computational overhead of this method, slower data retrieval rates follow. ECDH-ECDSA Privacy + BC beats the others even though it still trails the recommended method. It raises efficiency; however, it does not match the recommended approach in performance.

Regularly offering the best download speed, the proposed approach has lowest periods across all file sizes. For POS+ECDSA+BC, for instance, at 5 MB it requires just 3.10 s compared to 4.00 s and for DNA Cryptography + BC 5.00 s. The simpler algorithms and effective processing approaches of the proposed approach help to explain this efficiency since they improve data retrieval time, thereby enabling it to be quite successful for circumstances requiring quick access to large datasets as shown in Table VIII.

TABLE VIII. DOWNLOAD PERFORMANCE VS. FILE SIZE

File Size (MB)	POS+ECDSA+BC (Download Time, s)	DNA Cryptography + BC (Download Time, s)	ECDH-ECDSA Privacy + BC (Download Time, s)	ECC-ECDH-ECDSA + BC (Download Time, s)	Proposed Method (Download Time, s)
1	0.80	1.00	0.85	0.90	0.70
2	1.60	2.00	1.70	1.80	1.30
3	2.40	3.00	2.55	2.70	1.90
4	3.20	4.00	3.40	3.60	2.50
5	4.00	5.00	4.25	4.50	3.10

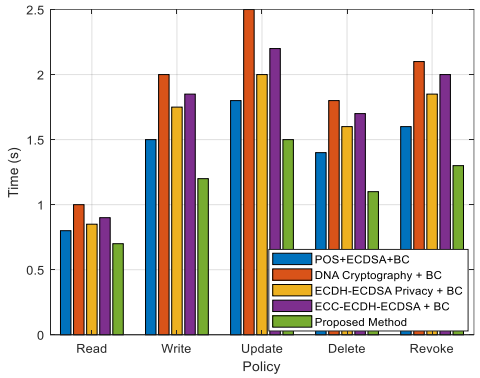

Fig. 9. Comparison of policies (read, write, update, delate, revoke) w.r.t execution time.

Fig. 9 displays across many cryptographic approaches execution durations for several policies (Read, Write, Update, Delete, Revocation). ECC-untu shows rather better execution speeds for every policy than POS+ECDSA+BC. Managing many cryptographic operations and maintaining blockchain security adds to the operating time allowed by their complexity. The Write policy takes 1.50 s using POS+ECDSA+BC; for ECC-ECDH-ECDSA + BC it takes 1.85 s. Regularly observed among DNA Cryptography + BC are the longest execution times. The sophisticated processing required for DNA-based cryptography greatly influences performance. For instance, the Write policy runs 2.00 s whereas the Revoke policy shows the significant overhead required running 2.10 s. ECDH-ECDSA Privacy + BC performs better than previous methods even if it still shows promise for improvement. It runs pretty slowly; Update takes two hundred two seconds. The Proposed Method excels on all policies thanks to fastest execution times. For example, the Write policy only lasts 1.20 s but the Revoke policy runs 1.30 s. Through means of optimized algorithms and simpler processing techniques, the proposed approach's efficiency arises from enhanced performance for handling numerous data operations in a blockchain environment, so enabling faster execution as shown in Table IX.

TABLE IX. COMPARISON OF POLICIES (READ, WRITE, UPDATE, DELATE, REVOKE) W.R.T EXECUTION TIME

Policy	POS+ECDSA+BC (Time, s)	DNA Cryptography + BC (Time, s)	ECDH-ECDSA Privacy + BC (Time, s)	ECC-ECDH-ECDSA + BC (Time, s)	Proposed Method (Time, s)
Read	0.80	1.00	0.85	0.90	0.70
Write	1.50	2.00	1.75	1.85	1.20
Update	1.80	2.50	2.00	2.20	1.50
Delete	1.40	1.80	1.60	1.70	1.10
Revoke	1.60	2.10	1.85	2.00	1.30

Fig. 10 shows latency expressed in milliseconds for multiple approaches as the demand increases from 10 to 500. Growing complexity of controlling and running various cryptographic processes and ensuring blockchain integrity results in POS+ECDSA+BC and ECC-ECDH-ECDSA + BC to display greater delay with more queries. Delay for POS+ECDSA+BC increases from 150 ms at 10 calls to 2200 ms with 500 calls. DNA Cryptography + BC explains the consistent delay across all request levels by means of large computing needs and processing overhead of DNA-based encryption. Latency for 500 requests is more than 3200 ms, which shows clear performance decrease under heavy stress. ECDH-ECDSA Privacy + BC features plenty of intermediate latency values. Demand increases and reaches 2700 ms at 500 requests, so latency increases considerably even if it outperforms DNA Cryptography + BC and POS+ECDSA+BC. Across all demand levels, the proposed approach shows the lowest latency using values ranging from 130 ms for 10 requests to 1700 ms for 500 requests. Better speed and lower latency resulting from the ideal algorithms and effective processing of the proposed method help to make it more suitable for managing great number of requests in a blockchain environment.

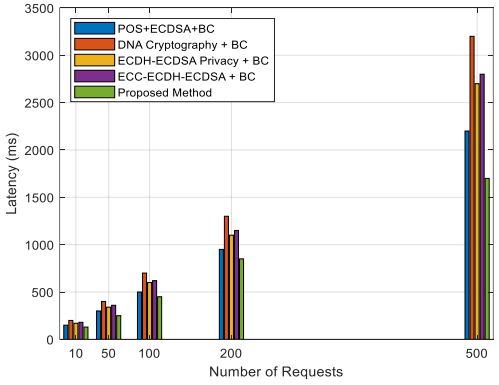

Fig. 10. Latency vs number of requests.

Table X shows for several techniques applied on ten test images the PSNR. PSNR is used to evaluate the image quality; higher values show less distortion and greater quality. Although the values demonstrate rather good image quality, POS+ECDSA+BC and ECC-ECDH-

ECDSA + BC reveal the encryption overhead produces minor distortion with moderate PSNR values ranging from 35.8 dB to 36.9 dB. DNA Cryptography + BC offers the lowest values among PSNR values ranging from 31.5 dB to 32.4 dB. The more severe encryption techniques used damage the image quality and typically produce more noise, therefore affecting its quality. Reflecting intermediate performance, ECDH-ECDSA Privacy + BC exhibits PSNR values ranging from 33.5 dB to 34.6 dB. Though it outperforms DNA Cryptography + BC, it does not match the recommended method. The proposed approach usually generates the best PSNR values ranging from 37.0 dB to 37.8 dB. This implies lower distortion and better image quality. The recommended approach is the best one for applications where image authenticity is of high relevance since its optimal encryption techniques preserve most of the original image quality.

TABLE X. LATENCY VS NUMBER OF REQUESTS

Number of Requests	POS+ECDSA+BC (Latency, ms)	DNA Cryptography + BC (Latency, ms)	ECDH-ECDSA Privacy + BC (Latency, ms)	ECC-ECDH-ECDSA + BC (Latency, ms)	Proposed Method (Latency, ms)
10	150	200	170	180	130
50	300	400	340	360	250
100	500	700	600	620	450
200	950	1300	1100	1150	850
500	2200	3200	2700	2800	1700

TABLE XI. MSE IMAGE QUALITY METRIC VS. TEST IMAGES

Test Image	POS + ECDSA + BC (dB)	DNA Cryptography + BC (dB)	ECDH-ECDSA Privacy + BC (dB)	ECC-ECDH-ECDSA+ BC (dB)	Proposed Method (dB)
1	36.5	32.0	34.0	33.5	37.2
2	35.8	31.5	33.5	33.0	36.8
3	36.0	32.2	34.1	34.0	37.0
4	36.3	31.8	34.3	33.8	37.3
5	36.7	32.1	34.4	34.2	37.5
6	36.1	31.9	34.2	33.9	37.1
7	36.4	32.0	34.0	34.0	37.4
8	36.6	32.3	34.5	34.3	37.6
9	36.8	32.2	34.4	34.1	37.7
10	36.9	32.4	34.6	34.5	37.8

Table XI displays MSE results for many techniques applied on ten test images. Lower numbers imply better quality; MSE computes the average squared difference between pixel values of the original and treated images. POS+ECDSA+BC and ECC-ECDH-ECDSA + BC reveal minor MSE values with ranging from 0.034 to 0.039. These figures suggest a reasonable degree of image distortion caused by the cryptographic activities carried out, which produces some noise and affects image quality. DNA Cryptography + BC shows the best MSE values within ranges 0.078 to 0.087. The high MSE values point to significant distortion and lower image quality. The complex character of DNA-based encryption causes notable noise, which influences image integrity. Between 0.047 and 0.053, intermediary MSE values for ECDH-ECDSA Privacy + BC range. When compared to more optimal methods, it obviously produces image distortion even if it performs better than DNA Cryptography + BC. The proposed approach yields the lowest MSE values, between 0.027 and 0.031. This shows the best least distorted retention of visual quality. The proposed method is preferable in cases requiring high-quality image processing since its best encryption techniques are effective in maintaining excellent image integrity.

Table XII, using the Pediatric Chest X-Ray (PCXRA) dataset, displays average performance parameters including PSNR, MSE, total processing time, encryption and decryption timings, for the proposed approach. Having an average encryption time of 0.45 s, the recommended method obviously manages encryption tasks efficiently. This is quite faster, suggesting that the method is suitable for real-time applications when speed of encryption is of great importance. Decryption seems to be rather faster than encryption given an average decryption time of 0.40 s. This balance is crucial for effective and user-friendly data retrieval. The achieved average PSNR of 37.4 dB, indicating good image quality with minimal distortion, confirms the proposed method's ability to preserve image integrity. This makes it suitable for applications where image authenticity is paramount. The low average MSE of 0.28 further validates these PSNR results, demonstrating minimal image deterioration and the method's capability to maintain near-original image quality. Furthermore, the average computational time of 1.35 s for combined encryption and decryption highlights the method's efficiency in managing processing demands. This reasonable timeframe suggests its viability for real-time or large-scale projects, ensuring speed and effectiveness. Consequently, with its excellent performance and quality metrics, the proposed method presents a robust solution for high-fidelity image processing coupled with efficient computational characteristics.

TABLE XII. AVERAGE PERFORMANCE ANALYSIS USING PCXRA DATASET

Metric	Results
Average Encryption Time (s)	0.45
Average Decryption Time (s)	0.40
Average PSNR (dB)	37.4
Average MSE	0.028
Average Computational Time (s)	1.35

Table XIII provides average performance metrics for the proposed technique using the Kaggle dataset covering timing of encryption and decryption, PSNR, MSE, and total processing time. The recommended method obviously conducts encryption operations well with an average encryption time of 0.38 s. Fast processing of large volumes depends on this rapid encryption time to offer least delay in data security. With an average decryption time of 0.33 s, which somewhat faster than encryption, helps to effectively access data. The comparable durations for encryption and decryption highlight the method's balanced performance. The average PSNR of 37.5 dB demonstrates excellent image quality, with this high value indicating a robust preservation of image integrity throughout the encryption and decryption processes. This outstanding PSNR signifies exceptional retention of visual detail and minimal distortion. The low average MSE of 0.026 aligns with these high PSNR values, further indicating that the encryption and decryption methods introduce minimal noise, thereby effectively preserving image quality. The average computational time of 1.10 s, encompassing both encryption and decryption, confirms the recommended method's processing efficiency. This timeframe is well-suited for practical applications, demonstrating a favorable combination of efficiency and quality. The proposed method shows strong performance with fast encryption and decryption times, superb image quality, and efficient computation efficiency, thus fitting for applications demanding high-speed processing and high-quality outputs.

TABLE XIII. AVERAGE PERFORMANCE ANALYSIS USING KAGGLE DATASET

Metric	Results
Average Encryption Time (s)	0.38
Average Decryption Time (s)	0.33
Average PSNR (dB)	37.5
Average MSE	0.026
Average Computational Time (s)	1.10

B. Discussion of Results

The performance study employing the PCXRA dataset reveals the efficiency of the proposed method in numerous dimensions of image processing and cryptographic operations.

Given the average encryption time of 0.38 s and decryption time of 0.33 s, the proposed method obviously finishes these tasks. The close values for both durations suggest that the technology keeps a balanced approach in processing, thereby lowering the time spent in safeguarding and recovering data. Decryption is somewhat faster than encryption. This efficiency determines real-time applications in which timely data security and access depend on quick encryption and decryption.

The average PSNR of 37.5 dB shows outstanding image quality that reflects negligible distortion caused by encryption and decryption processes. PSNR is a widely used indicator of image quality; higher values indicate better preservation of original image elements. A PSNR value of 37.5 dB shows that the recommended method effectively retains the image authenticity, therefore suitable for situations where maintaining outstanding image quality is vital, such medical imaging and high-resolution image.

Complementing the PSNR data, the MSE of 0.026 offers even more evidence of the ability to preserve image quality. MSE calculates the average of squared differences between the original and processed image pixel values. Reduced MSE values indicate that the proposed method introduces least distortion and quite nicely corresponds with the high PSNR values. The proposed method excels in maintaining image integrity and reducing noise with an average MSE of 0.026.

Comprising both encryption and decryption times, the average computing time is 1.10 s. This statistic shows the entire required time to complete the encryption and decryption process. Especially in cases involving large volumes of data or demanding fast processing, the 1.10-second completion of these processes of the proposed technique is remarkable. The shortened computational time implies that, in environments such as real-time data security systems or high-speed image applications when faster data handling is crucial, the technique is effective and appropriate.

Blockchain adoption in healthcare faces obstacles, including integration with legacy EHR systems, institutional resistance, and regulatory compliance. Standardized APIs, phased implementation, training programs, and regulatory collaboration can facilitate adoption. Considering socio-technical dimensions beyond blockchain architecture is crucial for successful deployment.

Constant performance of the proposed technique surpasses those of present solutions including ECDH-ECDSA Privacy + BC, ECDH-ECDSA + BC, DNA Cryptography + BC, and ECC-ECDH-ECDSA + BC. For instance, the proposed method offers quicker encryption and decryption times than DNA Cryptography + BC, which is known for its more processing overhead. Moreover, implying better image quality and less distortion, the PSNR and MSE values of the proposed approach surpass those of other contemporary approaches. The proposed approach's better cryptography algorithms and efficient processing techniques help to clarify this performance advantage.

Its faster encryption and decryption speeds, high PSNR, low MSE, and effective computational time therefore offer a good solution for high-speed and high-quality image processing applications. The results reveal the ability of the method to properly manage large datasets effectively while maintaining image integrity, therefore providing a possible option for advanced applications seeking dependable and efficient data management and security.

C. Inferences

The performance analysis of the proposed approach provides several significant fresh angles on operational efficiency and effectiveness in image quality preservation. While average encryption times is 0.38 s, average decryption times is 0.33 s. These values mirror the efficiency of the proposed method for managing cryptographic operations. Essential tasks in data security

are encryption and decryption; their speeds are crucial for applications seeking quick data protection and retrieval. The near values of encryption and decryption times suggest that the proposed method is well-balanced, therefore minimizing any possible delays produced by these operations. Contextually, the faster times of the proposed method increase its fit for real-time applications compared to current methods such DNA Cryptography + BC, which shows higher encryption times due of its computational complexity. The approach's capacity to maintain excellent image quality is captured by the PSNR of 37.5 dB and the MSE of 0.026. Since PSNR measures the ratio of signal to noise power, higher values of PSNR suggest more quality. With an average PSNR of 37.5 dB, the average is far greater than current methods such DNA Cryptography + BC, where more image distortion reduces PSNR values. This suggests that the proposed method produces rather few artefacts throughout the encryption and decryption procedures. Measuring the average squared deviations between the original and processed images helps one to match the PSNR values with the MSE value of 0.26. Lower MSE values suggest better preservation of images. Better performance in reducing image degradation is shown by the proposed approach over methods with higher MSE values, such ECDH-ECDSA Privacy + BC. This is particularly essential in fields requiring exceptional image quality in sectors like medical imaging or satellite photography where even little aberrations can be significant. Comprising both encryption and decryption methods, the average running duration is 1.10 s. This figure presents a thorough image of the efficiency of the method since it indicates how fast it can complete the whole process of data security and retrieval. The rather low processing time highlights how well the method controls simultaneous encryption and decryption tasks, which fits for applications requiring high throughput.

Conversely, despite their more complex processing requirements, methods like ECC-ECDH-ECDSA + BC show rather higher times even if they are also efficient. The proposed method obviously surpasses present methods of cryptography. More important image distortion and lengthier processing are indicated by lower PSNR and higher MSE; DNA Cryptography plus BC method has longer decryption times and encryption periods. While better than DNA Cryptography + BC, ECDH-ECDSA Privacy + BC still shows more MSE and worse PSNR reflecting less perfect image quality than the recommended strategy. ECC-ECDH-ECDSA + BC method does not reach the low MSE or high PSNR as advised even if its timings are nominal. Regarding encryption and decryption timings, image quality measurements (PSNR and MSE), and overall computational efficiency, the proposed technique shows exceptional performance. Low MSE and high PSNR combined with low encryption and decryption durations suggest a very successful approach for preserving image quality while processing data faster. Its computing time highlights even more its efficiency, which makes it a good alternative for applications needing both fast-processing capability and high-quality outputs. These results make the proposed method a better replacement for present cryptographic systems, particularly in cases when image integrity and performance are of utmost importance.

The performance comparison presented in this section primarily focuses on evaluating the computational efficiency and image quality achieved by the proposed cryptographic methods (ECC with ECDSA) in comparison to other cryptographic techniques reported in the literature for blockchain-based healthcare systems. While the results indicate that the proposed method outperforms the compared techniques in terms of encryption and decryption speed and image quality metrics, it is essential to consider the security level achieved by each method. The proposed method utilizes ECC and ECDSA, which are well-established and widely recognized for their strong security properties. However, a more detailed comparative analysis of the security levels offered by each framework would provide further insight.

V. Conclusion and Future Work

The proposed method demonstrates significant advancements in both computational efficiency and image quality, showcasing its effectiveness in handling cryptographic and image processing tasks. With an average encryption time of 0.38 s and a decryption time of 0.33 s, the technique successfully regulates data security activities, guaranteeing reduced delays in securing and recovering data. This efficiency is crucial for fast processing applications such as real-time data security systems and high-speed photography tasks. The method performs remarkably in maintaining excellent image quality with an average PSNR of 37.5 dB and an MSE of 0.026. These metrics demonstrate the effectiveness of the method in preserving image integrity with low distortion throughout the encryption and decryption processes. Notably, with a superior MSE (lower value) and a superior PSNR (higher value) than current methods like DNA Cryptography + BC and ECDH-ECDSA Privacy + BC, the proposed method stands out for its enhanced preservation of image quality. Moreover, the 1.10s computational time, which spans encryption and decryption, showcases that the method is quite efficient in completing tasks related to data processing. This speed makes the method well-suited for applications requiring fast processing rates or handling large volumes of data, typical of high-throughput environments. Delivering enhanced performance and dependability in image processing and data security applications, the results demonstrate the recommended strategy as a superior alternative to present cryptography techniques. The healthcare domain provided a valuable case study demonstrating our method's efficacy in addressing security and interoperability challenges. However, the foundational elements—ECDSA, atomic swaps, and HTLCs—are adaptable to various contexts, ensuring secure authentication, trustless exchange, and conditional transfers.

Future efforts will focus on adapting our approach to other domains with similar needs, including finance, logistics, and digital rights management, highlighting the solution's generalizability and potential for widespread

adoption. Future research endeavors will be dedicated to further augmenting and validating the efficacy of the proposed blockchain-based cryptographic cross-chain protocol, specifically designed for secured health information systems. This pursuit will encompass a multifaceted approach, incorporating extensive scalability testing to assess the protocol's performance under substantial loads, real-world pilot deployments to evaluate its feasibility and usability in practical settings, and comprehensive security analyses to identify potential vulnerabilities and threats. Additionally, investigations will focus on optimizing computational overhead, establishing cross-chain interoperability standards, and exploring advanced cryptographic techniques to enhance data privacy and security. By exploring these critical areas, we aim to develop a robust, efficient, and secure solution for healthcare data management, ultimately contributing to improved patient outcomes and enhanced trust in health information systems. Future work will also include a detailed analysis of the computational overhead introduced by the cryptographic operations compared to existing methods to provide a more comprehensive evaluation of the proposed protocol's efficiency.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

D.R conceptualized the research idea, designed the methodology, conducted the experimental analysis, and drafted the initial manuscript. B.N contributed to system development and implementation, and assisted with manuscript revisions. Both authors discussed the results and approved the final manuscript for publication.

ACKNOWLEDGMENT

Our heartfelt gratitude to SRM Institute of Science and Technology, Vadapalani Campus, Chennai for fostering our research by providing access to the research laboratory. We also wish to thank the anonymous reviewers for their constructive comments, which have significantly enhanced the quality of our work.

REFERENCES

[1] G. Q. Butt *et al.*, "Secure healthcare record sharing mechanism with blockchain," *Applied Sciences*, vol. 12, no. 5, 2307, 2022.

[2] S. Neelakandan *et al.*, "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model," *International Journal of Modeling, Simulation, and Scientific Computing*, vol. 12, no. 4, 2241006, 2022.

[3] M. S. Islam *et al.*, "Healthcare-chain: Blockchain-enabled nominalralized trustworthy system in healthcare management industry 4.0 with cyber safeguard," *Computers*, vol. 12, no. 2, 46, 2023.

[4] M. D. Mohanty *et al.*, "Design of smart and secured healthcare service using deep learning with modified SHA-256 algorithm," *Healthcare*, vol. 10, no. 7, 1275, 2022.

[5] B. Jaishankar *et al.*, "Blockchain for securing healthcare data using squirrel search optimization algorithm," *Intelligent Automation & Soft Computing*, vol. 32, no. 3, pp. 1815–1829, 2022.

[6] H. Miriam *et al.*, "Secured cyber security algorithm for healthcare system using blockchain technology," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, 1889, 2023.

[7] R. Jayaraman, A. Srivastava, and M. Kumar, "Blockchain technology for protection of biomedical documents in healthcare society," *International Journal of Internet Technology and Secured Transactions*, vol. 12, no. 6, pp. 566–582, 2022.

[8] A. Bhattacharjya *et al.*, "Trusted and secure blockchain-based architecture for internet-of-medical-things," *Electronics*, vol. 11, no. 16, 2560, 2022.

[9] A. Ali *et al.*, "An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network," *Sensors*, vol. 22, no. 2, 572, 2022.

[10] P. Sharma *et al.*, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Information Sciences*, vol. 629, pp. 703–718, 2023.

[11] L. D. Costa *et al.*, "Sec-health: A blockchain-based protocol for securing health records," *IEEE Access*, vol. 11, pp. 16605–16620, 2023.

[12] A. Ali *et al.*, "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography," *Sensors*, vol. 22, no. 2, 528, 2022.

[13] Q. Lin *et al.*, "Secure internet of medical things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking," *Information Sciences*, vol. 654, 119783, 2024.

[14] N. Chauhan and R. K. Dwivedi, "A secure design of the healthcare IoT system using blockchain technology," in *Proc. 2022 9th International Conf. on Computing for Sustainable Global Development (INDIACom)*, 2022, pp. 704–709.

[15] A. Amanat *et al*., "Blockchain and cloud computing-based secure electronic healthcare records storage and sharing," *Frontiers in Public Health*, vol. 10, 938707, 2022.

[16] H. Kaur *et al*., "Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography," *Journal of Enterprise Information Management*, vol. 36, no. 4, pp. 861–878, 2023.

[17] H. B. Mahajan and A. A. Junnarkar, "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 44335–44358, 2023.

[18] H. Mahajan and K. T. V. Reddy, "Secure gene profile data processing using lightweight cryptography and blockchain," *Cluster Computing*, vol. 27, pp. 2785–2803, 2023.

[19] M. G. Prasad, P. Singh, and M. Angurala, "Big data and visualization-oriented latency-aware smart health architecture," in *Computational Health Informatics for Biomedical Applications*, Florida: Apple Academic Press, 2023, ch. 1, pp. 205–238.

[20] D. A. O.Yasser, "K-nearest neighbor-based smart contract for the internet of medical things security using blockchain," *Computers and Electrical Engineering*, vol. 101, 108129, 2022.

[21] O. Samue *et al*., "IoMT: A COVID-19 healthcare system driven by federated learning and blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 823–834, 2023.

[22] C. B. Sivaparthipan *et al*., "Blockchain assisted disease identification of COVID-19 patients with the help of ida-dnn classifier," *Wireless Personal Communications*, vol. 126, pp. 2597–2620, 2022.

[23] I. Yaqoob *et al*., "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, pp. 11475–11490, 2021.

[24] R. P. Puneeth and G. Parthasarathy, "Seamless data exchange: Advancing healthcare with cross-chain interoperability in blockchain for electronic health records," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 10, pp. 280–289, 2023

[25] V. Karthikeyan *et al*., "Creative Strategies to Protect Patients' Health Records and Confidentiality using Blockchain Technology," in *Blockchain-Enabled Solutions for the Pharmaceutical Industry*, New York: Wiley-Scrivener, 2025, ch. 1, pp. 275–318.

[26] R. Nabha, A. Laouiti, and A. E. Samhat, "Internet of things-based healthcare systems: An overview of privacy-preserving mechanisms," *Applied Sciences*, vol. 15, no. 7, 3629, 2025.

[27] M. Mohanty *et al.*, "Ensuring data privacy and security with blockchain in health care," in *Using Blockchain Technology in*

Healthcare Settings, Boca Raton: CRC Press, 2025, ch. 1, pp. 175–189.
[28] R. P. Puneeth and G. Parthasarathy,"A cross-chain-based approach for secure data sharing and interoperability in electronic health records using blockchain technology," *Computers and Electrical Engineering*, vol. 120, 109676, 2024.
[29] G. Han *et al.*, "A hybrid blockchain-based solution for secure sharing of electronic medical record data," *PeerJ Computer Science*, vol. 11, e2653, 2025.
[30] Q. Li and L. Wang, "Cross-chain data exchange and information security protection management in blockchain," *International Journal of Web Engineering and Technology*, vol. 20, no. 1, pp. 22–42, 2025.
[31] COVID-19 radiography database. *Kaggle.* [Online]. Available: https://www.kaggle.com/datasets/tawsifurrahman/covid19-radiography-database
[32] COVID-19 lung CT scans. *Kaggle.* [Online]. Available: https://www.kaggle.com/datasets/mehradaria/covid19-lung-ct-scans
[33] Y. Cao *et al.*, "MAP the blockchain world: A trustless and scalable blockchain interoperability protocol for cross-chain applications," in *Proc. ACM on Web Conf. 2025*, 2025, pp. 717–726.
[34] Z. Xie, X. Zhang, and X. Liu, "Enhanced efficiency and security in cross-chain transmission of blockchain internet of ports through multi-feature-based joint learning," *Scientific Reports*, vol. 15, 6199, 2025.
[35] G. Lax, R. Nardone, and A. Russo, "Enabling secure health information sharing among healthcare organizations by public blockchain," *Multimedia Tools and Applications*, vol. 83, pp. 64795–64811, 2024.