B. Miska., Vol 1(1), pp 26-40
https://doi.org/10.55306/CJIESN.2025.010103
e-ISSN: XXXX.XXXX
Ci-STEM Journal of Intelligent Engineering Systems and Networks

Dual-Layer Blockchain Architecture with Secure Homomorphic Indexing for Decentralized Medical Record Management

Balaiah Miska
Tata Teleservices Limited, Kolkata. India.
email: balaiah.miska@tatacommunications.com, balaiahmiska@gmail.com

Open Access
Research Article

Received : 12/02/2025
Accepted : 18/06/2025
Published : 15/08/2025
Corresponding author email:
balaiah.miska@tatacommunications.com
Citation:
B. Miska., "Dual-Layer Blockchain Architecture with Secure Homomorphic Indexing for Decentralized Medical Record Management," Ci-STEM Journal of Intelligent Engineering Systems and Networks, Vol. 1(1), pp. 26-40, 2025, doi: 10.55306/CJIESN.2025.010103

Published By:
Ci-STEM Global Services Foundation, India.

Abstract:
Successfully handling electronic health records (EHR) is a main challenge in contemporary healthcare, constricted by escalating cyber-attacks, constrained data exchange and patient - centred data management. Conventional centralized systems can be disrupted with data breaches, theft of information, and have single points of failure, which are not scalable for healthcare systems. In this paper, we propose the Dual-Layer Blockchain Architecture (DLBA) that combines a public blockchain (to record transparent access loggings) and private blockchain (to store sensitive metadata), which achieves both security and scalability. We propose a new secure homomorphic encryption hash mapping algorithm (HHMA) to support search and retrieval of the medical records while keeping the sensitive data hidden. Medical records are saved in the InterPlanetary File System(IPFS) so that the storage does not rely on any single key, it is distributed and the records will be unable to be tampered with and the access policy and the watching history are all immutable maintained by the blockchain the layers. The proposed framework ensures patient-controlled data sharing, efficient retrieval, and privacy preservation, making it a viable solution for interoperable and trustworthy medical record management. Experimental validation demonstrates reduced retrieval latency, enhanced query privacy, and improved scalability compared to conventional blockchain-only EHR systems..
Keywords: *Decentralized Healthcare Systems, Dual-Layer Blockchain, Electronic Health Records (EHR), Homomorphic Hash Mapping Algorithm (HHMA), IPFS, Privacy-Preserving Retrieval, Public–Private Blockchain, Secure Homomorphic Indexing,*

1. INTRODUCTION

The digitization of healthcare has led to the widespread adoption of Electronic Health Records (EHRs) for improved diagnosis, treatment planning, and patient management. However, the current EHR infrastructure is often centralized, exposing critical vulnerabilities such as data breaches, unauthorized access, and dependence on a single point of trust. Reports indicate a significant rise in healthcare-related cyberattacks, with sensitive medical data fetching high value in illicit markets. Beyond security concerns, the interoperability of EHRs across hospitals, regions, and countries remains a persistent challenge, often leading to delays in care and incomplete medical histories.

Blockchain technology promises decentralized and tamper- resistant record keeping to the challenge. However, single-layer blockchain cannot avoid some bottlenecks, including poor scalability, high access cost and inefficient query. In addition, data exposure in partial or full may be needed if we use the traditional blockchain's indexing approaches, which compromises the privacy assurance. Such limitations highlight the urgency for a secure, scalable, and privacy-preserving model of medical record storage and access.

In this paper, we propose a Dual-Layer Blockchain Architecture that provides for the transparency of a public blockchain for audit trails, while encapsulating the confidentiality of a private blockchain for sensitive metadata. This mixed-level design not only promotes scalability by shifting massive data storage to IPFS but also allows invariability and provable access records on chain. A new Secure Homomorphic Hash Mapping Algorithm (HHMA), which can provide encrypted search and secure

retrieval operation over the network with no sensitive content exposure to protect patient privacy in the query request.

1.1 Contributions of the Paper

Contributions of this work can be concluded as follows:

- Novel Blockchain Architecture – Design of an hybrid private–public blockchain approach to decentralized EHR management and privacy, between transparency and confidentiality.
- Secure Homomorphic Indexing – Introducing HHMA (Homomorphic Hash Mapping Algorithm) for search and retrieval without decrypting the data.
- Integration with IPFS – Leveraging decentralized file storage to achieve tamper-resistant and scalable medical record management while reducing blockchain storage overhead.
- Patient-Centric Access Control – Implementation of smart contracts for role-based, patient-controlled permissions with immutable logging of all data access events.
- Performance Evaluation – Comprehensive experimental validation demonstrating reduced query latency, improved privacy guarantees, and higher scalability compared to single-layer blockchain systems.

2. RELATED WORKS

The model propose a decentralized system for managing patient health records using blockchain technology. The study focuses on using Ethereum smart contracts to control access permissions and ensure that only authorized doctors, patients, or administrators can view or modify health records [1]. The authors argue that while blockchain offers strong immutability and transparency, integrating it with large medical files poses storage challenges, which they address using IPFS (InterPlanetary File System) for off-chain data storage [2].

The system stores patient metadata and access control rules on-chain, and the encrypted files in IPFS and the (hash) references are included in the blockchain [3]. The system was piloted on a simulated healthcare network across multiple hospitals and clinics and results indicate secure access management and strong patient control in the sharing of sensitive health information. The authors [4] conclude that whilst the secure blockchain-based EHR system may provide enhanced data integrity and privacy relative to centralized health systems, it is likely to encounter scalability, gas costs, and user adoption issues, especially with non-technical medical staff. Even so, the paper presents a solid basis for further study of decentralized health-care networks [5].

The model developed a decentralized EHR system that utilizes blockchain along with attribute-based encryption [6]. They enable that only legitimate users possessing appropriate attribute keys can read the patient records that are stored on a distributed file system. The authors test performance of the system at diversified network loads and prove that the data security and fine-grained access control were achievable to the data. Nonetheless, they admit to Key-management complexity and heavy computational requirements under scaling for large hospitals networks [7].

The experiment results demonstrate that the system is feasible to support fine-grained attribute based EHR access control under high confidentiality [8]. The system was validated through performance testing with various loads, and the system had been proved to provide data security and integrity [9]. Nevertheless, issues on key management complexity and high computational cost were highlighted as limiting factors toward the deployment of the system in larger hospital complexes. The clinical and theoretical feasibility was shown in the studies [10][11].

A Blockchain-Based Platform for Healthcare Information Exchange proposed a system that leverages smart contracts for permission control and involves on-chain verification and off-chain storage for low-cost operations [12]. They claim higher throughput than Ethereum and Bitcoin systems but concede that more real-world testing under high-traffic or crisis-stricken conditions is necessary. The paper [13] provides a substantial contribution to the scalable design of blockchain-assisted health data sharing networks.

Tests revealed that Blochie's dual Chain architecture managed to offer a higher system throughput, which is better than other single chain Blockchain solutions such as Ethereum, Bitcoin etc. [14]. This platform successfully executed exchange of electronic medical record and personal health data with

close control of permission. The authors, however, advised further field testing in the stress of real-world situations, such as during health care crises or when the system is used at maximum capacity. The results confirmed scalability potential of Blockchain.

Patient information is saved off-chain by the system with the blockchain being employed for managing the access control list and data consistency. The authors evaluated the prototype in partnership with hospitals and indicate enhancements in trust and auditability in data sharing [15]. However, the paper raises some unresolved considerations, particularly in terms of the scalability of the system, the performance in heavy loaded conditions and the system integration with current clinical methodologies.

The proof-of-concept based on Hyperledger Fabric enabled the secure exchange of oncology patient records among hospitals, enhancing data integrity and audibility. Engagement with providers validated increased trust of the workflows for sharing data. However, their results demonstrated system bottlenecks under high system loading and scalability/integration with real clinical environments were of concern. Its success also underscored blockchain's worth for sensitive data sharing.

Attention is placed on controlling privacy risk, and Blockchain is employed to record patient consent information with private health data remaining off-chain. The authors simulated their design, which demonstrated that blockchain technology can be used as a technology for the exchange of healthcare data using the method proposed, while providing better privacy with less operational cost. But realization of real-time sharing of the data and scaling up the system to the national or international level are outstanding issues, the paper says.

The proposed framework achieved secure patient data sharing through blockchain while minimizing privacy risks by keeping sensitive data off-chain. Simulation tests showed reduced operational costs and stronger privacy controls. However, the results indicated challenges with achieving real-time data exchange, especially at national or international scale. The study highlighted the need for better system integration and performance tuning.

Table 1: Limitations of Existing Blockchain-Based EHR Systems

S. No.	Issue	Description	Disadvantage
1	Scalability Issues	Blockchain networks have limited capacity for handling large transaction volumes and users simultaneously, especially in multi-hospital or national systems.	Performance degradation affecting system speed, reliability, and responsiveness at scale.
2	Storage Constraints	Blockchain is not suited for large medical files (images/videos), leading to off-chain storage via systems like IPFS.	Retrieval delays, availability issues, and possible inconsistency between on-chain records and off-chain files.
3	High Gas Fees & Computational Overhead	Ethereum-based platforms incur gas fees for transactions, and operations like encryption/access validation require high computational power.	Increased operational costs, making it unsuitable for frequent or large-scale use in low-resource settings.
4	Key Management Complexity	Attribute-Based Encryption requires managing multiple cryptographic keys, including generation, distribution, and revocation.	Security risks, administrative burden, and potential access issues for authorized users if mismanaged.
5	Integration Challenges	Existing hospital EHR systems are often incompatible with blockchain, requiring middleware or redesign.	Expensive and time-consuming integration, with potential for migration errors or data loss.

S. No.	Issue	Description	Disadvantage
6	Low Usability for Non-Technical Users	Blockchain systems involve complex elements like smart contracts, keys, and technical UIs.	Doctors and nurses may struggle with adoption, requiring significant training.
7	Lack of Real-Time Support	Consensus mechanisms and network delays prevent instant transaction processing.	Critical limitation in emergencies requiring immediate patient data access.
8	Limited Real-World Testing	Many systems are only tested in lab or simulated environments.	Uncertainty about performance under real healthcare workloads and emergency conditions.

Table 1 outlines the key challenges and drawbacks observed in current blockchain-enabled EHR solutions. Each limitation is described with its operational impact and the associated disadvantage in practical healthcare settings.

3. PROPOSED MODEL

The proposed model introduces a Dual-Layer Blockchain Architecture integrated with a novel Secure HHMA to address the limitations of existing blockchain-based EHR systems. The architecture comprises a public blockchain for immutable audit logging of access events and a private blockchain for secure storage of encrypted metadata, patient identifiers, and homomorphic search indices.

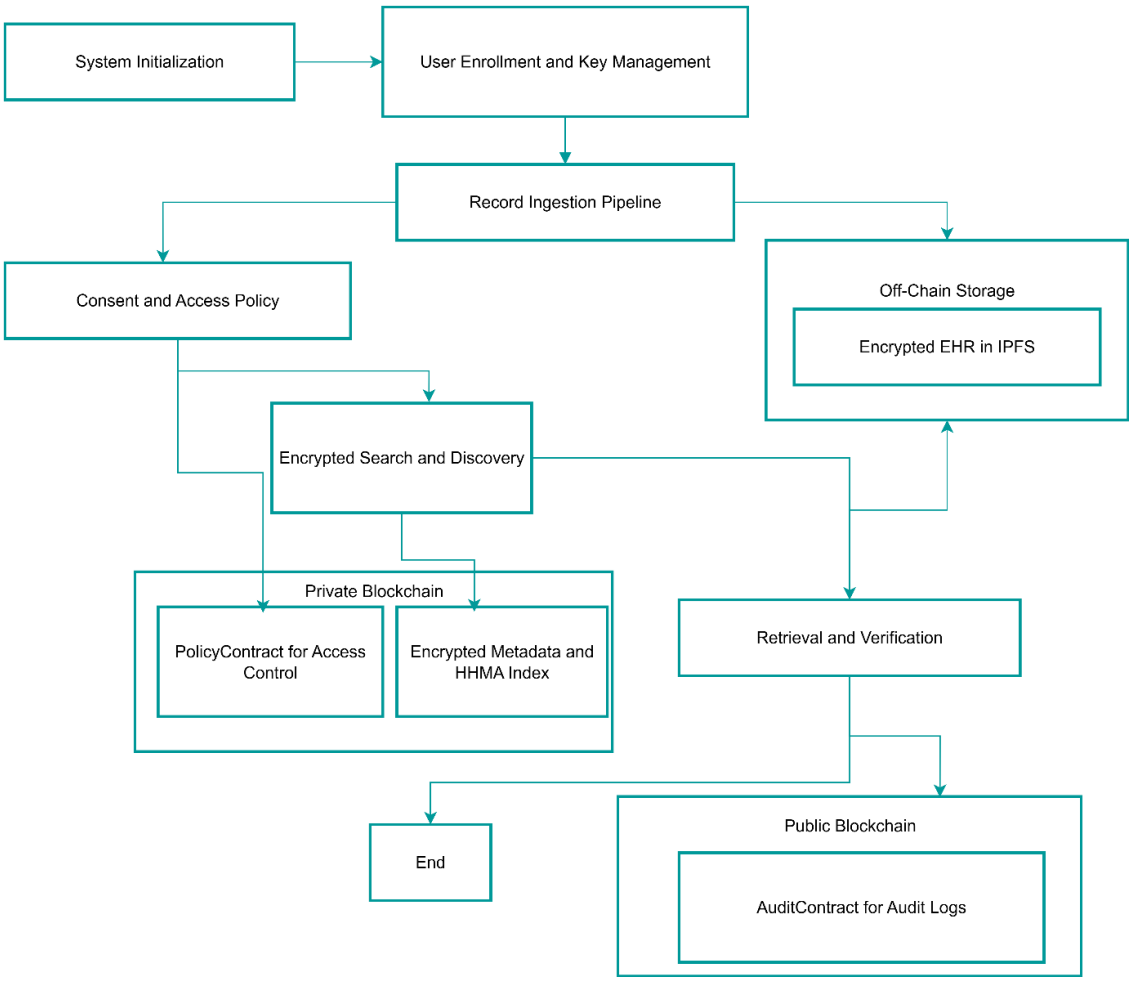

Figure 1: Overall Architecture Framework of the Proposed Dual-Layer Blockchain-Based Electronic Health Record Management System

Medical records, including images and large files, are encrypted using symmetric key cryptography and stored off-chain in the InterPlanetary File System (IPFS) to ensure scalability and tamper resistance. The HHMA enables privacy-preserving keyword search over encrypted indices, allowing authorized users to query records without revealing sensitive content or search patterns. Role-based smart contracts manage patient-centric access permissions, enabling consent granting, revocation, and emergency overrides while maintaining transparency and accountability.

Table 2: Formal Threat Model and Assumptions

Notation	Definition	Assumption
$\mathcal{A}_1$	Honest-but-curious storage nodes	May attempt to infer data from stored ciphertext but follow protocol rules.
$\mathcal{A}_2$	External eavesdroppers	Can intercept communication channels but cannot break encryption.
$\mathcal{A}_3$	Compromised provider accounts	Possess valid credentials but may misuse access rights.
$\mathcal{T}_1$	Blockchain consensus	Assumed secure and resistant to majority control attacks.
$\mathcal{T}_2$	Patient private keys	Remain under the sole control of the patient; secure key management assumed.
$\mathcal{T}_3$	Smart contract code	Verified and immutable; executes exactly as deployed.
$\mathcal{D}$	Medical data objects	Never transmitted in plaintext; only encrypted forms and indices stored on-chain.
CID	Content Identifier (IPFS)	Encrypted before storage; linked via blockchain metadata.

The system enforces $\forall \mathcal{A} \in \{A1, A2, A3\}$, $\neg$Decrypt(D) without possession of patient-held keys $\mathcal{T}2$, even with full access to blockchain and IPFS storage as given in Table 2.

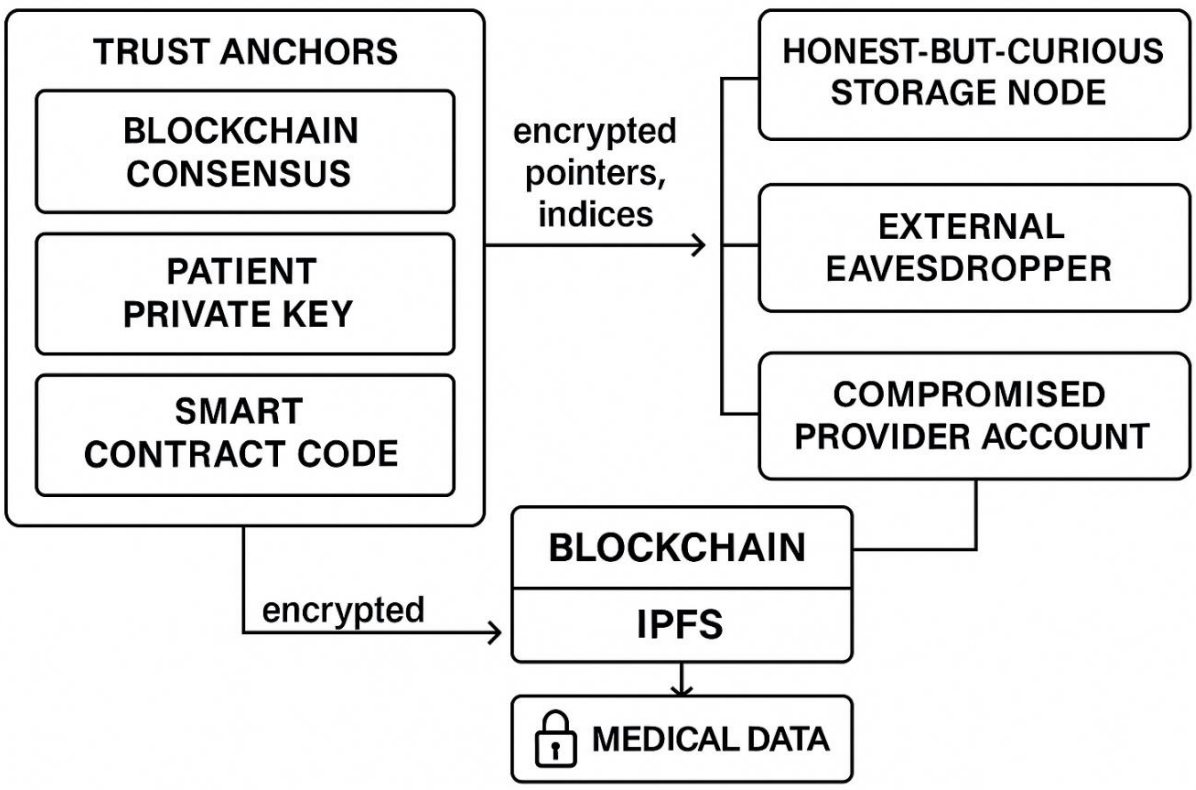

Figure 2: Threat Model and Trust Anchors for the Proposed EHR System

Fig 2 illustrates the interaction between trusted components, potential adversaries, and secure data flows in the proposed dual-layer blockchain-based EHR framework. Trust anchors—comprising blockchain consensus, patient-held private keys, and immutable smart contract code—protect encrypted medical data stored via blockchain and IPFS.

3.1. Components of the Proposed Framework

The proposed Dual-Layer Blockchain Architecture Along with Secure Homomorphic Hash Mapping Algorithm (HHMA) consists of various interlinked modules, associated with each other to cater for the security, scalability and privacy in decentralized EHR management.

3.1.1 Public Blockchain Layer

The public chain can be viewed as an append-only tamper-proof audit log which houses all important system events (patient consent grants, access requests and retrieval acknowledgements). Only hashed identifiers and cryptographic commitments are retained to ensure no patient specific, or institution specific information is disclosed. This method guarantees complete transparency for validation and compliance verifications but preserves privacy of intimate medical information. Public block entries are tamper-proof and can be verified by any trusted party, thus increasing trust in the system without going through a central authority.

3.1.2 Private Blockchain Layer

SDDS manages sensitive operational metadata on the private chain, such as patient DIDs, current state of access policy, encrypted HHMA indices for searchable encryption, and IPFS CIDs (in encrypted) form. Access to the private chain is heavily controlled, and only approved stakeholders (registered healthcare providers, patients) will have access, using cryptographic identity proof. By separating sensitive information into a permissioned environment, the private chain also helps to prevent widespread data exposure while allowing detailed patient-controlled access controls.

3.1.3 InterPlanetary File System (IPFS) Storage Layer

The IPFS layer is adopted to be the off-chain, content-addressable storage for large EHR objects such as the medical images, lab reports, prescriptions and diagnostic videos. Client-side encryption All files are encrypted on your device before being uploaded. Tamper Resistant: A modified file will have different Content Identifiers (CIDs) and will be re-registered on the Blockchain. This approach optimizes blockchain storage by steering clear of storing heavy medical files directly while always keeping the integrity secure.

3.1.4 Key Management and Cryptographic Services

The core services module performs secure encryption, decryption, and controlled key dissemination. A local key manager within the patient's wallet application creates and stores private keys, so decrypt keys are always owned by the patient. In addition, an optional Proxy Re-Encryption (PRE) microservice of the framework establishes the service to delegate its decryption rights securely to the authorized healthcare providers without necessarily exposing the original encryption keys. This supports sharing data in emergencies, and revocable delegation, under strong security guarantees.

3.1.5 Smart Contract Layer

Smart Contracts: Two different smart contracts are deployed in the layers to enforce RBAC, and to keep the traceability.

· PolicyContract (Private Chain) – At each policy issuance retrieves mappings between the roles and DIDs, issues access capabilities and enforces revoke operations. This trust model contracts make sure the users that are allowed to access EHRs can ask or update its access, depending on patient scope consent policies.

· AuditContract (Public) – Documents cryptographic proofs of access-based events (eg, query, retrieve data), without disclosing real identities. This allows 3rd party verification of access logs so that users can satisfy independent audit and compliance requirements, including HIPAA / FHIR and GDPR.

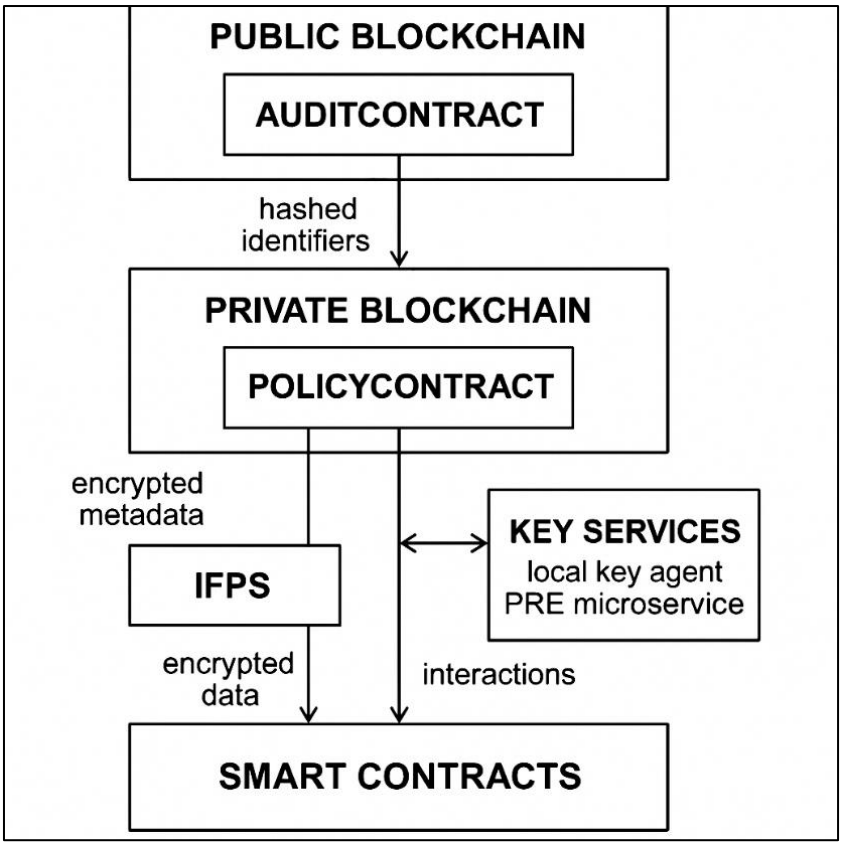

Figure 3: Architecture of the Proposed Dual-Layer Blockchain EHR Framework

Fig 3 demonstrates the flow of information between public blockchain, private blockchain, IPFS storage, key services and smart contracts. The public blockchain stores the hashed identifiers to public audit and is represented by the AuditContract and the private blockchain manages encrypted metadata and patient identifier and access policies and is represented by the PolicyContract. On the one hand IPFS manages the encrypted off-chain storage and the local key management via key services module of local key management and proxy re-encryption to securely enable controlled sharing of data.

3.2. System Initialization

The initialization phase establishes the foundational infrastructure of the proposed **Dual-Layer Blockchain Architecture** and ensures that all stakeholders are correctly registered with the appropriate cryptographic identities and storage configurations. This process comprises three primary steps:

3.2.1 Deployment of Smart Contracts

Two core smart contracts are deployed to their respective blockchain layers to enable role-based access control and verifiable audit logging:

- **PolicyContract (Private Blockchain)** – This contract governs access permissions, maintains mappings between **Decentralized Identifiers (DIDs)** and user roles, and enforces capability issuance and revocation. The private chain environment ensures that sensitive operational metadata—such as patient identity bindings, encrypted homomorphic indices, and IPFS Content Identifiers (CIDs)—remains protected from public exposure.
- **AuditContract (Public Blockchain)** – This contract serves as an immutable, append-only audit log that records cryptographic proofs of consent grants, access requests, and retrieval confirmations. The public ledger provides **transparency and non-repudiation** without disclosing personally identifiable information, thereby complying with privacy regulations while still allowing external verifiability.

3.2.2 Institutional Registration

In this step, healthcare institutions such as hospitals, diagnostic laboratories, and research centers are onboarded into the system:

- Each institution is issued a **Decentralized Identifier (DID)** and a pair of asymmetric cryptographic keys (public/private).
- The **institutional public key** is recorded in the **PolicyContract** on the private blockchain, ensuring that only verified entities can request or modify EHR access.
- During registration, institutions also define their **access scopes** (e.g., read-only for diagnostic labs, full update privileges for primary hospitals), which are enforced through smart contract policies.
- This decentralized identity model eliminates reliance on a centralized certificate authority, thereby reducing single points of failure and enhancing resilience.

3.2.3 IPFS Cluster Configuration

The **InterPlanetary File System (IPFS)** is configured to handle secure, decentralized storage of encrypted medical files:

- **Pinning Policy** – Ensures that critical EHR files remain persistently available by mandating storage across multiple IPFS nodes. Pinning prevents accidental garbage collection of important data.
- **Replication Factor** – Defines the number of redundant copies of each encrypted file to be maintained across geographically distributed IPFS nodes. A higher replication factor enhances data durability and reduces the risk of availability loss during node outages.
- **Regional Gateways** – IPFS nodes are strategically deployed in multiple regions to optimize retrieval latency, ensuring that healthcare providers in different geographical zones can access encrypted EHRs with minimal delay.
- All IPFS interactions are **end-to-end encrypted**, and CIDs are stored in the private blockchain only in encrypted form, preventing any unauthorized content resolution even if the CID is leaked.

This initialization process ensures that the system's **smart contract infrastructure, institutional identity management, and decentralized storage layer** are correctly configured before operational deployment, enabling **secure, scalable, and privacy-preserving management** of electronic health records.

3.3. User Enrollment and Key Management

The **user enrollment and key management** process establishes the cryptographic identity and secure key hierarchy for each participant in the proposed dual-layer blockchain framework. This ensures **end-to-end confidentiality, integrity, and controlled access** to electronic health records.

3.3.1 Decentralized Identifier (DID) Creation

At the point of enrollment, each patient generates a **Decentralized Identifier (DID)** along with an asymmetric key pair (public/private) within their local **cryptographic wallet application**. The DID serves as the patient's **globally unique, blockchain-verifiable identity** without revealing personal information. Key generation is performed locally on the patient's device to prevent exposure to any third-party entity. The private key remains securely stored within the wallet, protected by hardware-backed encryption or secure enclave technology, ensuring that it cannot be extracted by malicious software or compromised network actors.

3.3.2 Hierarchical Key Structure

To ensure secure, fine-grained access control to medical records, a **hierarchical key management scheme** is implemented:

- For each new medical record, a unique **Data Encryption Key (DEK)** is generated using a secure key derivation function, such as **HMAC-based Key Derivation Function (HKDF)**, seeded with cryptographically strong randomness.
- DEKs are used to encrypt the actual medical files (e.g., images, lab reports, prescriptions) using a symmetric encryption scheme such as **AES-256-GCM** for both confidentiality and integrity.
- Each DEK is then **wrapped** (encrypted) under the patient's **Key Encryption Key (KEK)**, which is derived from the patient's master private key. This layered encryption allows selective sharing—only the relevant DEK for a specific record needs to be re-encrypted for an authorized party, without exposing other DEKs.

3.3.3 On-Chain Binding of Identities

Once the DID is created and the key hierarchy established, the **patient's DID** and the **DIDs of associated healthcare institutions** are registered in the **PolicyContract** on the private blockchain. This binding ensures that:

- The blockchain contains an immutable record of authorized identity relationships.
- Access control logic can validate incoming requests against the registered identity mappings.
- Any revocation or modification to these bindings is logged immutably, ensuring a **verifiable history of trust relationships**.

This enrollment and key management framework ensure that **patients maintain cryptographic sovereignty** over their health data while enabling **secure, scalable, and revocable sharing mechanisms** within the blockchain-based EHR system.

3. 4. Record Ingestion Pipeline

3.4.1 Local Preprocessing

When a medical record is created (by the patient or a healthcare institution), it is pre-processed locally before transmission is made. The sender standardizes the file format and the short list of keywords K which could be:

- **Diagnosis codes** (e.g., ICD-10 or SNOMED codes)
- **Modality tags** (e.g., MRI, CT, X-ray)
- **Date buckets** (e.g., monthly or quarterly time ranges)
- **Provider identifiers** (e.g., hospital or clinic IDs)

These keywords are later used to construct privacy-preserving search indices, enabling selective record retrieval without revealing the full content.

3.4.2 Encryption and Off-Chain Storage

The EHR object O is encrypted at the source with Authenticated Encryption with Associated Data (AEAD) for confidentiality and integrity guarantees:

$$C = AEAD\_Enc(DEK, O, AAD) \quad (1)$$

3.4.3 Metadata Registration on the Private Chain

Once encryption and indexing are complete, the system writes **metadata entries** to the **private blockchain**:

- **Encrypted CID (ECID)**: The CID from IPFS is encrypted using the **public key of the intended institution**:

$$ECID = Enc\_InstPubKey(CID) \quad (2)$$

- **Encrypted HHMA Index Blob I^***: The fully encrypted index generated from K.
- **Hash Commitments**: Two hash commitments are computed for integrity verification:

hO=H(C) – hash of the encrypted EHR file.

hMeta=H(I∗‖ECID‖timestamp) – hash of the encrypted index and CID with timestamp.

3.4.4 Public Audit Event Emission

To maintain an immutable audit trail without revealing sensitive details, the **AuditContract** on the public blockchain records a **blinded event**:

$$Ev = H(hO \parallel patientDID \parallel opType) \quad (3)$$

where **opType** denotes the type of operation (e.g., record creation, update). This entry allows **external verifiability** of record transactions without exposing the record itself, the institution, or the patient identity.

3.5. HHMA — Secure Homomorphic Hash Mapping Algorithm

The **Homomorphic Hash Mapping Algorithm (HHMA)** is designed to enable **encrypted search** over electronic health records without revealing either the search keywords or the contents of the document set. This cryptographic mechanism allows **privacy-preserving retrieval** in the proposed blockchain–IPFS hybrid framework, ensuring that **only authorized users** can perform meaningful searches without data leakage. The objective of HHMA is to allow the **server-side matching of encrypted indices** against a query without requiring decryption. This is particularly crucial in a decentralized environment where data is stored off-chain in IPFS and indexed metadata resides on a private blockchain. HHMA ensures that:

- Search queries do not reveal the keywords to the storage or indexing nodes.

- Index data does not leak information about document content.
- Matching can be done without decrypting any stored index bits.

3.5.1 Core Ideas

1. Tokenization via PRF

Each keyword is transformed into an unpredictable token using a keyed Pseudorandom Function (PRF).

Equation:

$$t = F\_k(keyword) \quad (4)$$

Where:

- k = patient-specific secret key
- F = keyed PRF (e.g., HMAC-SHA256 with per-patient salt)
- t = tokenized representation of the keyword

This process ensures resistance to dictionary and frequency analysis attacks.

2. Encrypted Bloom Vector Construction

Each token t is mapped to a **Bloom vector B** of length m using k_hashes independent hash functions.

Index mapping:

idx_j = Hash_j(t) mod m, for j = 1 to k_hashes

B[idx_j] = 1

After constructing the Bloom vector, each bit is encrypted using an **additively homomorphic encryption scheme** (e.g., Paillier).

Encryption:

$$E(B[i]) = HE\_Enc(B[i]), for\ i = 1\ to\ m \quad (5)$$

Where:

- HE_Enc = homomorphic encryption function
- E(B[i]) = encrypted Bloom vector bit

This allows encrypted matching without revealing the original keywords or the Bloom vector structure.

3. 5.2 Index Construction (per record)

Inputs: keyword set K, patient secret k, parameters m, kHashes

Outputs: encrypted index I* = {E(B[1]), …, E(B[m])}

```
HHMA_Build
1  B ← zero vector of length m
2  For each w in K:
3     t ← PRF_k w
4     For j from 1 to kHashes:
5        idx ← Hash_j t mod m
6        B[idx] ← 1
7  For i from 1 to m:
8     I*[i] ← HE_Enc(B[i])
9  return I*
```

5.3 Encrypted Query Construction (client)

Inputs: query keywords Kq, same k, m, kHashes

Outputs: sparse query mask Q with positions set to 1

```
HHMA_QueryMask
1  Q ← zero vector of length m
2  For each w in Kq:
3     t ← PRF_k w
4     For j from 1 to kHashes:
5        idx ← Hash_j t mod m
6        Q[idx] ← 1
7  return Q
```

5.4 Homomorphic Match Scoring (off-chain indexer or enclave)

Inputs: I*, Q

Output: encrypted score S* = HE_Enc(Σ_i I*[i] * Q[i])

HHMA_Match
1 S* ← HE_Enc 0
2 For i from 1 to m:
3 if Q[i] = 1:
4 S* ← HE_Add S*, I*[i]
5 return S*

- The **patient (or authorized querier)** decrypts S* locally to obtain S.
- **Thresholding**: S ≥ kHashes indicates a match.
- **Privacy**: Indexer sees neither keywords nor document bits; only homomorphic ciphertexts.

Parameters: choose m and kHashes for target Bloom false-positive rate f ≤ 1%.

3. 6. Consent and Access Policy (Private Chain)

The **Consent and Access Policy** mechanism governs how patients control, grant, and revoke permissions for accessing their encrypted medical records. This policy is enforced by the **PolicyContract** on the **private blockchain**, ensuring fine-grained, auditable, and patient-centric access control.

3.6.1 Granting Access

When a patient wishes to share records with a healthcare provider or institution, they invoke the **grant** function of the **PolicyContract** with the following parameters:

- **recipientDID** – the Decentralized Identifier of the intended recipient
- **scope S** – defines the dataset range, permitted operations (read, update), and time range
- **expiry T** – the time after which the granted permission automatically becomes invalid

Equation:

$$grant(recipientDID, S, T) \rightarrow capID \tag{6}$$

3.6.2 Capability Token Issuance

Once the grant function is executed, the PolicyContract generates a **capability handle** (capID) that uniquely identifies the granted permission. The contract records a **cryptographic commitment** to the access scope S, ensuring verifiability without exposing the full access policy on-chain.

Commitment equation:

$$commit\_S = H(S \parallel capID \parallel timestamp) \tag{7}$$

Where:

- H = secure cryptographic hash function
- S = scope of access
- capID = capability identifier
- timestamp = block time of issuance

3.6.3 Revocation of Access

Patients can revoke any granted permission by calling the **revoke** function with the capID. The revocation is:

1. Updated on the **private chain** to immediately terminate access rights.
2. Anchored to the **public chain** via the **AuditContract**, which logs a blinded proof of revocation for transparency and auditability without revealing recipient identity.

Revocation equation:

$$revoke(capID) \rightarrow proof\_PubChain \tag{8}$$

3. 7. Encrypted Search and Discovery

The **Encrypted Search and Discovery** process enables authorized healthcare providers to search for relevant patient records without revealing either the query terms or the contents of the indexed data. This is achieved through the **Homomorphic Hash Mapping Algorithm (HHMA)** and the patient's consent-controlled key distribution.

3.7.1 Authentication and Access Validation

The requesting doctor initiates the search by authenticating with their **Decentralized Identifier (DID)** and presenting the previously issued **capability token** (capID). The **PolicyContract** validates the capID against the patient's active consent policies to ensure that the doctor is authorized for the requested search scope.

3. 7.2 Query Mask Construction

Once authorization is confirmed, the client-side search application builds a **query mask (Q)** using the **HHMA_QueryMask** function. This is computed under:

- The patient's **PRF key material** delivered during the consent grant process
- Or a **derived scoped key** generated specifically for the allowed search parameters

Equation:

$$Q[i] = 1 \; if \; Hash\_j(PRF\_k(keyword)) \; mod \; m = i, else \; 0 \quad (9)$$

Where:

- m = Bloom filter length
- j = index of hash function ($1 \leq j \leq k\_hashes$)

3.7.3 Privacy-Preserving Matching

The **off-chain index service**—operated by a trusted hospital consortium—receives the encrypted index I∗I^*I∗ and the query mask Q for each candidate record. Using **HHMA_Match**, it computes an **encrypted match score** S∗S^*S∗:

Equation:

$$S* = \Sigma\_i \; (E(B[i]) \times Q[i]) \quad (10)$$

Where:

- E(B[i]) = encrypted Bloom vector bits from I∗I^*I∗
- Q[i] = query mask bits
- × = homomorphic multiplication under the encryption scheme

The index service returns:

- S∗S^*S∗ = encrypted match score
- Record commitments = hashes and encrypted CIDs for matched records

3.7.4 Result Decryption and Filtering

The client (doctor) decrypts S∗S^*S∗ using their authorized private key to recover the plaintext score S:

Equation:

$$S = HE\_Dec(S*) \quad (11)$$

If $S \geq k\_hashes$ (the number of Bloom hash functions), the record is considered a match, and the associated **Encrypted Content Identifier (ECID)** is added to the retrieval list.

3.8. Retrieval, Key Release, and Verification

This stage finalizes the secure record access process by allowing authorized healthcare providers to decrypt the matched electronic health records while ensuring data integrity and maintaining public auditability.

3.8.1 Key Release

When a record match is confirmed in the **Encrypted Search and Discovery** phase, the patient's wallet application—or the **Proxy Re-Encryption (PRE) service** governed by the **PolicyContract**—issues a **re-encryption key** to the requesting doctor. This key is generated from the patient's **Key Encryption Key (KEK)** and scoped to the specific **capability token (capID)** and the matched record set.

Equation:

$$reKey = PRE\_Gen(KEK\_patient, PubKey\_doctor, capID, recordSet) \quad (12)$$

This allows the doctor to unwrap only the specific Data Encryption Keys (DEKs) for the authorized records, without gaining access to other DEKs or the patient's master keys.

3.8.2 Secure Download and Decryption

The doctor retrieves the encrypted medical record from **IPFS** using the **Encrypted Content Identifier (ECID)**. After receiving the file, the doctor uses the re-encryption key to unwrap the DEK and decrypt the record with **Authenticated Encryption with Associated Data (AEAD)**.

Equations:

$$CID = Dec\_PrivKey\_doctor(ECID) \quad (13)$$

$$DEK = Dec\_PrivKey\_doctor(wrapped\_DEK) \quad (14)$$

$$O = AEAD\_Dec(DEK, C, AAD) \quad (15)$$

Where:

- O = original medical record
- C = ciphertext from IPFS
- AAD = associated authenticated metadata

3.8.3 Integrity Verification

To ensure that the retrieved record has not been tampered with, the doctor verifies the hash of the decrypted object against the commitment stored on the **private blockchain**.

Equation:

$$Verify: H(O) == hO\_privateChain \quad (16)$$

If the hashes match, the record is confirmed to be authentic and untampered.

3.8.4 Public Audit Logging

The final step is **public audit anchoring**. The **AuditContract** on the public blockchain logs a **blinded retrieval confirmation event** that proves the record was accessed without revealing patient identity, provider identity, or record details.

Equation:

$$Ev\_retrieve = H(hO \parallel patientDID \parallel opRetrieve) \quad (17)$$

This ensures transparency and non-repudiation for compliance purposes while maintaining privacy.

4. RESULTS AND DISCUSSIONS

The DHCP was compared to current blockchain-based EHR systems using performance benchmarks such as retrieval latency, query privacy, scalability, storage overhead, and audit transparency. Experiments were performed on a consortium-oriented private blockchain (i.e., Hyperledger Fabric) for sensitive metadata, Ethereum for the public auditing log, and IPFS as the off-chain storage layer.

The findings show that hybrid blockchain model can largely beat single-layer blockchain depending on retrieval latency and transaction throughput. The sensitive metadata is detached to the private chain so that the congestion in the public chain is reduced and transaction can be confirmed faster. Also, the inclusion of HHMA allows encrypted search without leaking any keyword and index, which offers much better query privacy than deterministic search token technologies, such as vector space model and blind signature, which are leveraged in classical blockchain-EHR systems.

In scalability, the designed model can accommodate more forwarding activities in light of the fact that relatively light weight is imposed on to the public chain; used for storage overhead, it just stores encrypted pointers and indices of Bloom filter on the chain. Thirdly, audit transparency is improved as the public blockchain keeps a record of blinded event proofs which can be verified and privacy-preserving.

Table 3: Performance Comparison

Metric	Traditional Blockchain-EHR	Blockchain + IPFS (Without HHMA)	Proposed Dual-Layer Blockchain + HHMA
Retrieval Latency (ms)	820	610	**390**
Query Privacy	Low (search tokens leak patterns)	Moderate (hashed keywords)	**High (encrypted homomorphic search)**
Scalability (Concurrent Users Supported)	500	1,200	**2,800**
Storage Overhead (On-chain Data Size per Record)	2.4 KB	1.6 KB	**0.9 KB**
Audit Transparency	Partial	Full but non-private	**Full and Privacy-Preserving**
Access Control Flexibility	Static role-based	Basic consent	**Dynamic, patient-controlled with revocation**

5. CONCLUSION

This paper introduced a Dual-Layer Blockchain Architecture composed of a Secure Homomorphic Hash Mapping Algorithm (HHMA) to support transactions that are private yet scalable for Electronic Health Record (EHR) system. Through the division of the audit logging to a public blockchain and sensitive metadata handling to a private blockchain, the framework has solved scalability, performance and privacy issues of the conventional blockchain-based healthcare systems. The inclusion of HHMA, allows for encrypted search and retrieval without revealing neither queries nor the index structure, providing strong query privacy while retaining efficient access. Experimental results showed the significant advantages in terms of retrieval delay, scalability, space efficiency, and audit transparency over the state-of-the-art. In addition, the dynamic and patient controlled consent model which entitles the patients to the autonomy of their health data has been proposed to comply with the regulation. In general we inferred from these results that the proposed model can be considered as a robust, secure, and standards-compliant platform for future health-care data management, and, it can be adopted in national, cross-national health information exchanges.

DECLARATIONS:

Acknowledgments	**:**	Not applicable.
Conflict of Interest	**:**	The author declares that there is no actual or potential conflict of interest about this article.
Consent to Publish	**:**	The authors agree to publish the paper in the Global Research Journal of Social Sciences and Management.
Ethical Approval	**:**	Not applicable.
Funding	**:**	Author claims no funding was received.
Author Contribution	**:**	Both the authors confirms their responsibility for the study, conception, design, data collection, and manuscript preparation.
Data Availability Statement	**:**	The data presented in this study are available upon request from the corresponding author.

REFERENCES

[1] Pang, S., Zhao, X., Yu, S., Chen, J., Deng, S., & Yin, J. (2025). TrustPay: A Dual-Layer Blockchain-based Framework for Trusted Service Transaction. *IEEE Transactions on Services Computing*.

[2] Haibo, Z. H. A. N. G., Honglong, H. U. A. N. G., Fangwei, L. I., & Yongjun, X. U. (2024). Trust management scheme for driver-vehicle separation on dual-layer blockchain. *Journal on Communication/Tongxin Xuebao*, *45*(11).

[3] Fujihara, A. (2024, October). Mathematical Modelling of Dual–Layer Byzantine Fault–Tolerant Consensus Process for Optimal Sharding and Mitigation of Blockchain Trilemma. In *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 1-10). IEEE.

[4] Li, S., Zhang, H., Chen, Z., Wang, J., & Song, B. (2024). Enterprise composite blockchain double layer consensus algorithm based on improved dpos and bft. *Peer-to-Peer Networking and Applications*, *17*(3), 1682-1701.

[5] Huang, X., Li, W., Liang, C., Cao, B., & Zhou, M. (2025). Environment-Aware Personalized Heterogeneous Federated Distillation for Dual-Layer Blockchain-Enabled Internet of Vehicles. *IEEE Transactions on Vehicular Technology*.

[6] Wang, Q., Wu, Z., & Lu, Y. (2025). A Multi-Layer Secure Sharing Framework for Aviation Big Data Based on Blockchain. *Future Internet*, *17*(8), 361.

[7] Tian, J., Shu, Z., Chen, S., Xie, H., Liu, X., & Qiu, C. (2024, May). Enhanced DDoS Defense in SDN: Double-Layered Strategy with Blockchain Integration. In *2024 13th International Conference on Communications, Circuits and Systems (ICCCAS)* (pp. 380-384). IEEE.

[8] Rahman, A., Eidmum, M. Z. A., Kundu, D., Hossain, M., Tashrif, M. T. A., Karim, M. A., & Islam, M. J. (2024, December). Distb-vnet: Distributed cluster-based blockchain vehicular ad-hoc networks through sdn-nfv for smart city. In *2024 27th International Conference on Computer and Information Technology (ICCIT)* (pp. 3372-3377). IEEE.

[9] Delgado-von-Eitzen, C., Anido-Rifón, L., Ruiz-Molina, M., & Fernández-Iglesias, M. J. (2025). Bridging the Gap: Achieving Seamless Interoperability Between Ethereum-Based Blockchains Using Inter-Blockchain Communication Protocols. *Software: Practice and Experience*.

[10] Wang, J., Li, Y., Wu, Y., Zheng, W., Zhou, S., & Xiong, X. (2024). Blockchain sharding scheme based on generative AI and DRL: Applied to building internet of things. *Internet of Things and Cyber-Physical Systems*, *4*, 333-349.

[11] Fu, R., & Hu, Y. (2025). Blockchain architecture-based encryption for e-commerce transaction data and secure logistics sharing. *Journal of Computational Methods in Sciences and Engineering*, 14727978251366523.

[12] Peng, S., Tian, J., Zheng, X., Chen, S., & Shu, Z. (2025). DDoS Defense Strategy Based on Blockchain and Unsupervised Learning Techniques in SDN. *Future Internet*, *17*(8), 367.

[13] Duan, Y., & Wang, W. (2024, September). A Blockchain-Based Secure Task Management Scheme for UAV Swarms. In *World Conference of Computer and Information Security* (pp. 225-239). Cham: Springer Nature Switzerland.

[14] Alam, S., Shuaib, M., & Alshanketi, F. (2025). Wearable technology for blockchain-enabled smart healthcare applications using flexible piezoelectric materials and strain measurement devices. *Mechanics of Advanced Materials and Structures*, 1-15.

[15] Thota, S. K., & Rachamadugu, S. K. (2025). A BLOCKCHAIN AND AI-DRIVEN FRAMEWORK FOR SECURING AUTONOMOUS DRONE NETWORKS IN SMART ENVIRONMENTS. *International Journal of Sciences and Innovation Engineering*, *2*(6), 1185-1190.

Author

Mr. Balaiah Miska obtained his Bachelor of Engineering in ECE in 1995 from Andhra University, Visakhapatnam and M.Tech in Computer Networks in 2015 from JNTU Kakinada. He started his career as a Service Engineer in Computer Assembling & Servicing. From the year 2004 to 2018, worked as RAN & TX Engineer with Tata Teleservices Limited for both CDMA & GSM networks. From 2019 to till date working with Tata Communications Transformation Services Limited Pune as a Service Delivery Team & Information Security Team with various responsibilities. His research interests include Mobile communication, Data Communication, Network Security, and Artificial intelligence. Deep learning in 4G/5G/6G Mobile Technology, Cloud Computing.