RESEARCH ARTICLE OPEN ACCESS

Block chain-Enabled Decentralized Secure EHR System with Cryptographically Enforced Consent Control and Scalable Off-Chain Storage Architecture

Laukik Parashare, Alok Bhorunde, Rohan Roy, Harsh Shah, Wrushabh Sirsat
Department of Information Technology, Zeal College of Engineering & Research,
Pune, India

ABSTRACT
The digital disruption in the healthcare systems has resulted in an enormous adoption of Electronic Health Record (EHR). hospital/clinic systems. Despite the strengths of the centralized EHR design in terms of operation, the traditional design suffers serious flaws like data. Single point of failure vulnerability, lack of transparent audits, low quality patient data ownership, and silos. exposure to victimizing by cyber-attacks. The increasing trend of healthcare data breach demonstrates that centralized trust models are not only not becoming outdated, but also on the contrary, they are increasing in number. structurally insufficient. The proposed paper architecture is an EHR management system, which is decentralized, cryptographically secured and scaled in such a way as to incorporate permissioned blockchain technology encrypted off-chain. distributed storage sometimes referred to as InterPlanetary File System (IPFS), high-intensity relational database systems, and distributed caching systems. The proposed system can ensure that there is a patient-oriented ownership, air-tight medical record repositories, consent-based access statistics, and auditing trails of large hospital systems. The medical files are encrypted using AES-256 symmetric encryption and the hash in order to get decentralized storage. introducing the file identifiers to the blockchain, only the cryptographic hash of the file identifiers has been stored to guarantee integrity. storage overhead. RBAC and ABAC models are implemented alongside. access control implementation, which is valid as smart contract logic. Cryptographic security is mathematically modeled to conduct a formal analysis of system robustness. hashing, authentication validation and metrics of system performance. Security analysis is resistant to unauthorized access, re-use, manipulation by an insider and re-use. tampering. The high consistency, throughput and regulatory grade compliance that is provided by this hybrid architecture proposal is high. suitable in a modern healthcare ecosystem.

Keywords — Electronic Health Records, blockchain, Hyperledger fabric, IPFS, AES-256, consent. RBAC, management, ABAC, distributed system, healthcare security, PostgreSQL, Redis.

I. INTRODUCTION

Information medical has overtaken the medical sector in a radical way. systems digitization. The paper-based records have been replaced with Electronic Health Records and have enabled improved clinical. distance consultations, coordination, predictive analytics, and data-driven medical research. However, the digitization not only expands the availability and efficiency of operations but presupposes with itself. the major concerns of security and privacy. The traditional EHR systems are typically designed on the foundation of centralised client server systems in which the server is centralised. patient records are stored in controlled but disconnected environments in hospitals data bases. The structural susceptibility of such a centralized structure encompasses the nature of this structure e.g. the symmetry.

The structural vulnerability of such centralized models of storage is structural vulnerability e.g. the risk of huge information data breaches, insider misuse, ransomware, and unauthorized access and data manipulation. Healthcare information is highly confidential and thus the privacy takes precedence. This is unlike financial information since medical records contain lifelong diagnostic history and genetic information. and personal identifiable information that cannot be undone once it has been spilled into the wild. Hence, EHR systems jeopardize outcomes in privacy violation which cannot be reversed. In addition, central systems provide an implicit faith of the administrative authorities and therefore limiting data. ownership and patient autonomy. Patients are in no position to exert a direct control in accessibility of their records and auditing systems. are in-house more than cryptographically verifiable.

The mathematical interpretation of structural constraint of the centralized trust models is reliance on one authority node. Suppose we refer to one of the centralized healthcare databases as a node (S), all the transactions (T_i) rely on (S) then the concept of system integrity is:

$$Integrity_{system} = f(S)$$

where the compromise of (S) is a direct compromise of the entire system. This brings one area of system vulnerability.

A distributed consensus mechanism is a new form of trust presented by blockchain technology. A distributed ledger has replications of transactional data at several nodes instead of having one trusted party. The cryptographic hash of the block before it is stored in each block in the chain, which makes the block immutable, using chained integrity:

$$H_i = SHA256(Data \,//\, H_{i-1})$$

Any change in ($Data_i$) leads to change in (H_i) thus disjoining the chain and revealing attempts to tamper with. The given property makes blockchain especially applicable to healthcare audit and consent log.

Nonetheless, it is infeasible to store medical files directly on blockchain, like MRI scans, CT reports and high-resolution diagnostic reports because of storage capacity limitations and overhead in terms of performance. The medical imaging file in question can be in the hundreds of megabytes, but blockchain storage is designed to store small transaction records. Thus, on-chain/off-chain designs are needed. In these systems, the cryptographic hash of the identifiers of medical files is stored on-chain only, the encrypted version is stored in decentralized storage networks e.g. IPFS.

where (M) is a medical record file. The encryption algorithm of AES-256 can be represented as follows:

$$C = E_{AES256}(M, K)$$

and (K) is the encryption key which is symmetric and (C) is the ciphertext. The file is uploaded onto IPFS generating a Content Identifier (CID):

$$CID = SHA256(C)$$

This (Hash (CID)) is then stored in the blockchain which means that any modification in the encrypted file will yield a different CID making the verification of integrity useless.

Secure access control is essential besides data integrity. The healthcare systems should also implement fine-grain authorization policy according to user roles, contextual features, and patient consent. Traditional Role-Based Access Control is defined as the permission granted to a predefined role. Healthcare situations are however prone to contextual choices including emergency overrides or time-based consent validity. Hence, the interaction of RBAC and the Attribute-Based Access Control facilitates the dynamic policy analysis. The access validation can be presented as:

$$Access\ (U, R, A, C) = 1,\ if\ policy\ satisfied;\ 0,\ otherwise$$

in which (U) is the user, (R) is the requested resource, (A) is user attributes and (C) is consent conditions.

Infrastructure backend should be high performance to ensure the large-scale hospital networks are scaled. Stateless RESTful APIs can be scaled horizontally in which the code is written in Node.js and Express. PostgreSQL ensures relational integrity of the structured data such as the records of consent as well as metadata is ACID compliant. Redis distributed caching reduces the time taken to reply to the query and rate limits to curb abuse. It is possible to have the model of system throughput as follows:

$$Throughput = Amount\ of\ Requests/Time.$$

and caching improves throughput by minimizing irrelevant repetitive database access.

One of the proposed architectures is the Decentralized Secure Electronic Health Record Management System which integrates all these layers into a harmonized architecture where the ownership of the patients is the main consideration, ability to resist tampering, ability to keep records as well as scaling capabilities. The system overcomes the natural limitations of centralized EHR infrastructures with the blockchain immutability, encrypted distributed storage, secure API gateways, relational consistency and distributed caching.

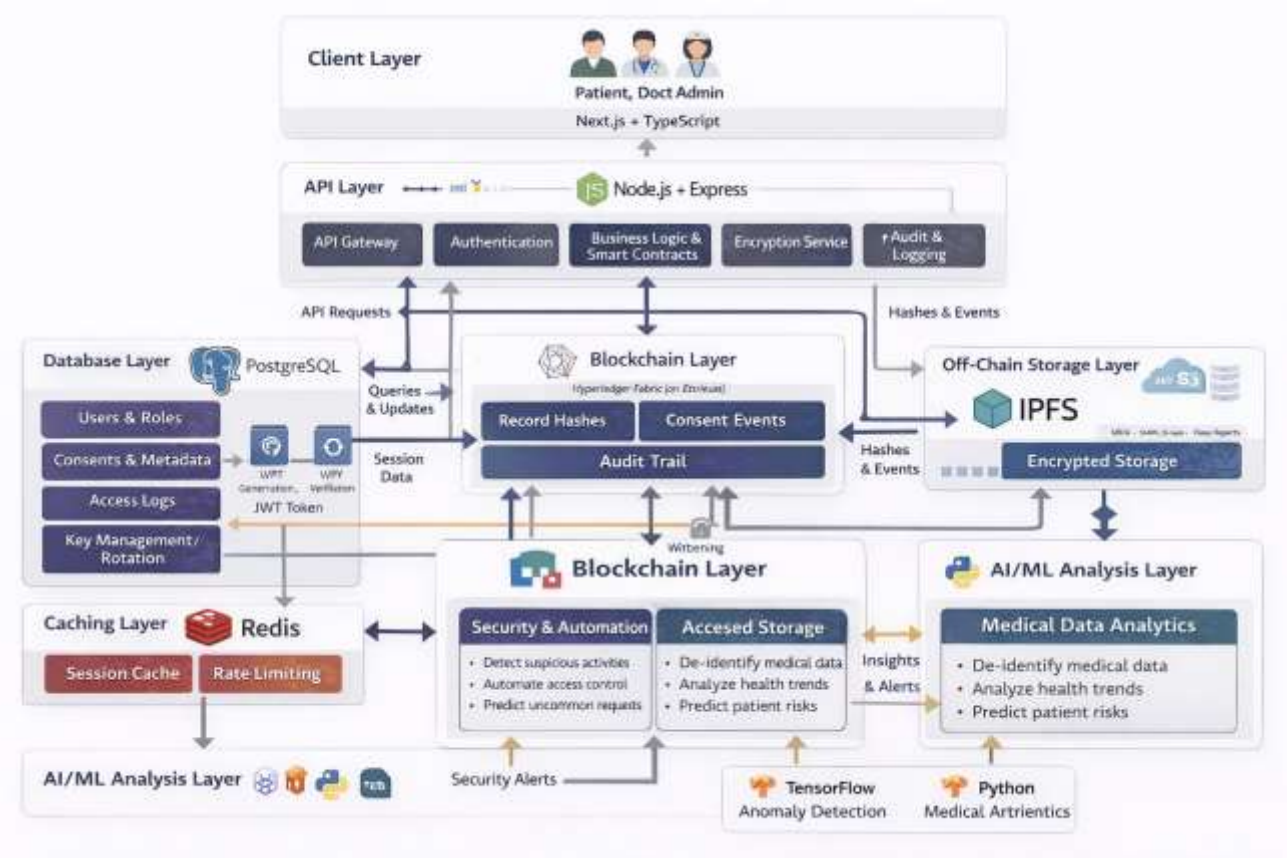

Fig. 1 System Architecture Diagram

II. Related Work (Literature Review)

The fit between blockchain technology and medical information systems has been the subject of significant research inquiries in the past decade owing to the increasing concerns. in regard to the safety of medical information, its privacy, the capability to interoperate and audit medical information. The conventional Electronic health records are primarily centralized meaning that the system is a monolith. hospital or a health care organization that has a separate database that holds records of the patients. Whereas these architectures facilitate the control of administration, they highly lack vulnerability, as includes data breaches, unauthorized access, lack of interoperability among the institutions, and poor access control transparency. There are other researches that made attempts to eliminate these disadvantages with the use of distributed ledger technologies and secure. data sharing systems. The initial research into blockchain-based healthcare systems had been premised largely on blockchain immutability. to ensure medical records integrity. Zhang et al. came up with a proposed medical data sharing platform utilizing blockchain that the records of transactions received in the form of access events were saved on a distributed ledger. Their method showed that cryptographic hashing might be used to make sure that when a medical information is stored it is impossible to change it without being detected. Nonetheless, the direct storage of the entire medical records on the blockchain created scalability challenges due to the fact that blockchain networks are not programmed to support large amounts of information. On the same note, Kumar et al. explored the use of blockchain as a secure medical record exchange system and determined that though blockchain offers trust among distributed healthcare systems, storage overheads are impractical when addressing large medical images like CT lesions or MRI data.

In order to defeat storage constraints, later studies proposed hybrid off-chain/on-chain designs. The authors of this article, Chen et al., suggested a decentralized storage system that combines InterPlanetary File System (IPFS) with blockchain to allow distributing encrypted medical records. Within this architecture, medical records are off-chain and blockchain is kept on the hash of file identifiers. Such an approach saves a lot of blockchain storage space, but verifiable integrity is preserved. The integrity checking system is based on cryptographic hash functions which are specified as

$$H(x) = SHA256(x)$$

Where x is the block of data. In the event the stored data is modified, the resulting hash value would differ hence indicating attempts of tampering.

The other direction in research is on the access control and consent management mechanisms. Wang et al. suggested a healthcare data sharing model, based on the smart contract, where patient permission is coded into smart contracts in the blockchain. The smart contract automatically confirms the permission of a requesting entity to access medical records. The

use of this automated enforcement eliminates the use of centralised access control authorities. Nonetheless, the context-dependent nature of complex healthcare use cases, in which permission can be conditioned on contextual attributes like treatment purpose, emergency cases or time limits, might not be adequately represented by purely role-based models. To resolve this problem, some studies suggested to use Role-Based Access Control (RBAC) alongside with Attribute-Based Access Control (ABAC) models.

Another significant research issue is security of medical information when storing and transmitting it. Encryption systems have been also highly implemented in ensuring confidential healthcare data. AES-256 symmetric encryption algorithm was studied by Sharma et al and Gupta et al who analyzed the effectiveness of these algorithms in securing medical data.

$$C = E(M, K)$$

Decryption restores the original message:

$$M = D(C, K)$$

Besides the issue of security of storage, a number of researchers investigated the methods of optimizing the system scalability and optimizing performance. Redis is a distributed caching system that has been suggested to shorten the query latency time on databases in healthcare systems. Kapoor et al. have shown that caching of metadata that is accessed very often by medical systems brings about a significant enhancement to the system throughput and alleviates the load on the backend database.

System throughput can be mathematically described as

$$Throughput = Number\ of\ Requests / Execution\ Time$$

The decrease in latency of the database query directly enhances the system throughput which is very important in the case of the large hospital networks that receive thousands of concurrent requests.

III. PROBLEM STATEMENT

The systems of data management in healthcare encounter a myriad of technical, operational, and security issues that do not facilitate effective and reliable exchange of medical information. Conventional centralized EHR designs make use of servers controlled by the hospital and store sensitive patient information in remote institutional databases. Although this architecture makes control easier, it, by definition, makes control and trust in the hands of one administrative unit. Concerning security, this kind of concentration of trust creates systemic vulnerabilities since the failure of the central database may reveal the whole dataset.

The total system integrity can be modeled as

$$Integrity_{System} = f(S)$$

where S represents the centralized database node containing all transactions T_i.

It is important to note that the integrity and availability of the entire system are completely reliant on the reliability of node S. Any compromise, assault, or misuse of this node means a massive compromise.

Centralized systems also restrict patient autonomy besides access security weaknesses. Patients hardly have the authority to control the way their medical information is exchanged among institutions. Hospital administrators usually handle access permissions in-house, and the auditing mechanisms are usually opaque.

Another significant problem is the barriers of interoperability. The use of incompatible information systems is common in healthcare institutions and is not compatible with each other. Consequently, there is a tendency to have divided patient records in several hospitals hence it is hard to have access to complete medical histories by the physicians.

System design is further complicated by the rapid increase in the amount of medical data including high-resolution imaging data, genomic data, wearable monitoring records, and clinical notes.

There are other security threats which are not external attacks such as insider misuse and accidental data modification.

Thus, the essential issue tackled in this study is the creation of a decentralized, scalable, and secure healthcare record management system that satisfies the following goals:

- Medical records immutability
- Patient-controlled consent mechanisms
- Secure distributed storage of large medical files
- High system throughput for large hospital networks
- Verifiable audit logs for regulatory compliance

IV. SYSTEM MODEL AND PROPOSED METHODOLOGY

The proposed decentralized EHR management system embraces a layered system architecture integrating secure frontend interfaces, scalable backend APIs, relational data management systems, distributed caching, blockchain-based integrity verification, and decentralized storage systems.

The client layer is implemented using Next.js and TypeScript which provides responsive dashboards for patients, doctors, and administrators.

Communication between client and server occurs through HTTPS using TLS 1.3.

The backend API layer functions as the core processing system responsible for authentication, authorization, data validation, encryption, and blockchain interactions. Node.js and Express are used because of their event-driven architecture and high concurrency support.

Authentication uses JSON Web Tokens (JWT).

$$Signature = HMACSHA256(Header.\ Payload,\ Secret\ Key)$$

The metadata including user profiles, consent policies, and record identifiers are stored in PostgreSQL which provides ACID-compliant relational database transactions.

Redis distributed caching improves system performance by storing frequently accessed metadata in memory.

Hyperledger Fabric is used as the permissioned blockchain infrastructure. Instead of storing complete medical files on-chain, only cryptographic hashes of records and access events are recorded.

Medical files are encrypted using AES-256 and stored in the InterPlanetary File System (IPFS). IPFS generates a unique content identifier (CID) for each file based on its cryptographic hash.

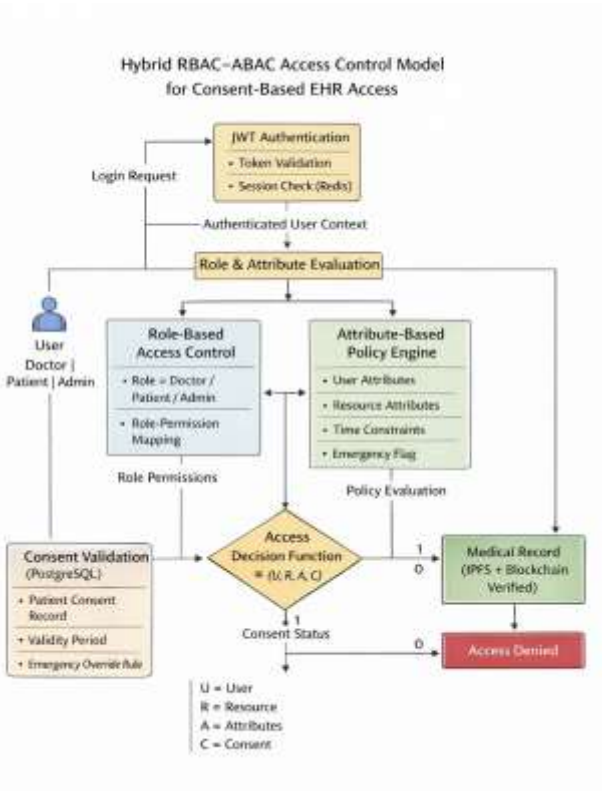

Fig. 2 Sequence Diagram for Medical Record Update and Access

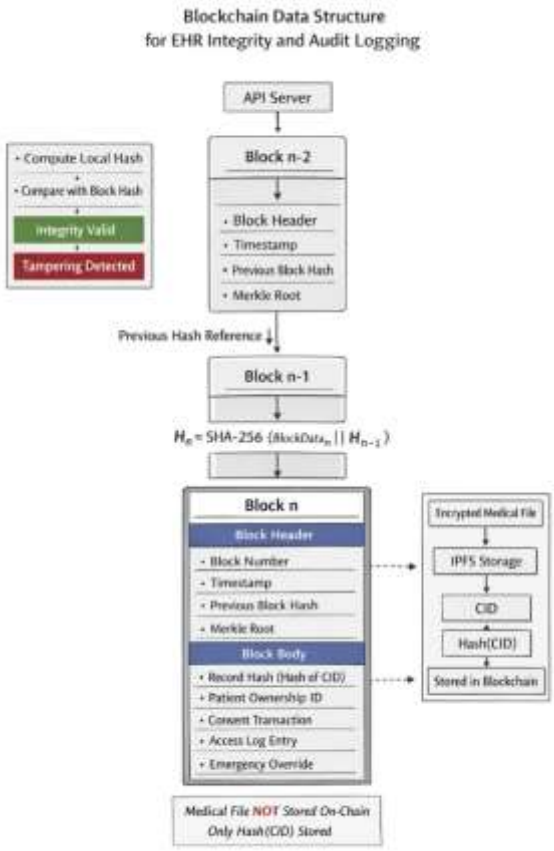

Fig. 3 Blockchain Data Structure Diagram

V. MATHEMATICAL MODELLING

The decentralized EHR system can be formally described using mathematical models representing encryption, blockchain verification, authentication validation, and system performance metrics.

AES-256 encryption of a medical record M with key K produces ciphertext C:

$$C = E_{AES256}(M, K)$$

Decryption restores the original record:

$$M = D_{AES256}(C, K)$$

RSA encryption using public key (e, n) is defined as

$$C = M^e \bmod n$$

Decryption using private key d:

$$M = C^d \bmod n$$

Blockchain integrity verification relies on chained cryptographic hashing:

$$H_i = SHA256(Data_i \parallel H_{i-1})$$

IPFS content identifiers are generated using

$$CID = SHA256(File)$$

System throughput is defined as

$$Throughput = Total\ Requests / Processing\ Time$$

Latency is measured as

$$Latency = T_{response} - T_{request}$$

Caching reduces latency by minimizing direct database queries and thereby improving system responsiveness.

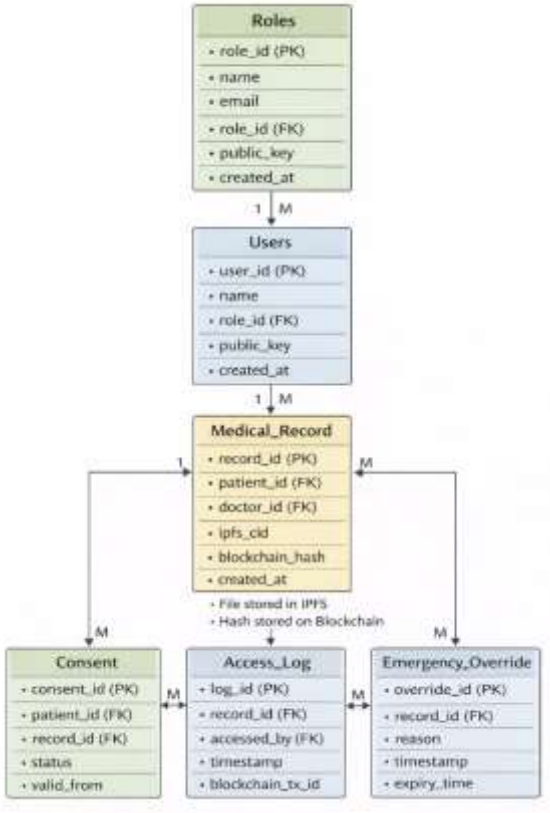

Fig. 4 Database Entity Relationship Diagram

VI. IMPLEMENTATION DETAILS

The development of the offered decentralized Electronic Health Record (EHR) management system is modelled in the multi-layer format incorporating the latest web technologies, distributed storage systems, blockchain infrastructure, relational databases, and high-speed caching systems. The implementation is aimed at making sure that the network of large hospitals supports scalability, security, and effective access to data without doing anything to undermine the tight control of patient data ownership and access permissions.

The system client side is created based on the Next.js framework and TypeScript, and it allows creation of a responsive and scalable user interface that can store various user types, including patients, doctors, and administrators. Next.js also offers server-side rendering, as well as efficient routing processes, which have a considerable effect on improving the performance and scalability of an application. TypeScript has high levels of type safety and minimizes the likelihood of runtime errors and enhances the maintainability of large-scale applications. Under this layer, patients will be given dashboards to upload medical records, control consent policies and check access histories, and healthcare providers can request access which is controlled by the patient.

The dialogue between the client application and the backend system is based on secure RESTful APIs with the development of Node.js and Express. The event-based architecture of the Node.js platform enables the system to effectively support high volumes of requests that are airing at once, which is essential where healthcare systems are concerned since several hospitals and medical professionals can be using the system at the same time. All API endpoints are secured with the help of middleware elements that perform authentication and authorization, input validation, and rate limitation.

Authentication is based on JSON Web Tokens (JWT) that can be used to check identities that are stateless and do not need any session storage on the server side. The JWT token is made of three parts such as a header, a payload that carries a user information, and a signature that ensures the integrity of the token. The signature can be created with the HMAC-SHA256 algorithm in the following manner:

$$Signature = HMACSHA256(Header. Payload, Secret Key)$$

Whenever a request is presented, the backend verifies the signature of the token and checks the expiration time and accepts a request to the secured resources.

System operations utilize structured data which is stored in a PostgreSQL relational database. PostgreSQL is used because it is highly effective in ACID-compliant transactions whereby database activities remain consistent even when multiple connections are present. The ACID guarantees that every transaction meets the following requirements: atomicity, consistency, isolation, and durability.

A Redis distributed caching layer is added to the system architecture to enhance performance as well as minimize the overhead of database queries. Redis is a key-value in-memory store, which can access regularly deployed data with sub-milliseconds latency. The tokens in the session, access permissions, and metadata of medical records that are commonly requested are also stored in cache to minimize the number of database queries.

$$T_{cache} \ll T_{db}$$

This difference proves that load balancing speed in the form of cache retrieval saves a serious load of time in response time.

The system uses Hyperledger Fabric, a permissioned blockchain framework that is implemented with the blockchain component of the system. In contrast to the public blockchains, which are based on energy-intensive consensus systems like Proof-of-Work, Hyperledger Fabric employs modular consensus protocols that can be applied to the private organizational network.

Instead of storing medical records and access events, the blockchain ledger holds cryptographic hashes of them only.

The InterPlanetary File System (IPFS) is a distributed peer-to-peer storage network which stores large medical files off-chain and is addressed by their cryptographic content hash. The backend uses AES-256 encryption to encrypt a file before uploading it to IPFS. The file is then uploaded to IPFS, which creates a unique content identifier (CID) of the file. This CID hash is stored in the blockchain, and a point of reference to determine the data integrity in the future is generated.

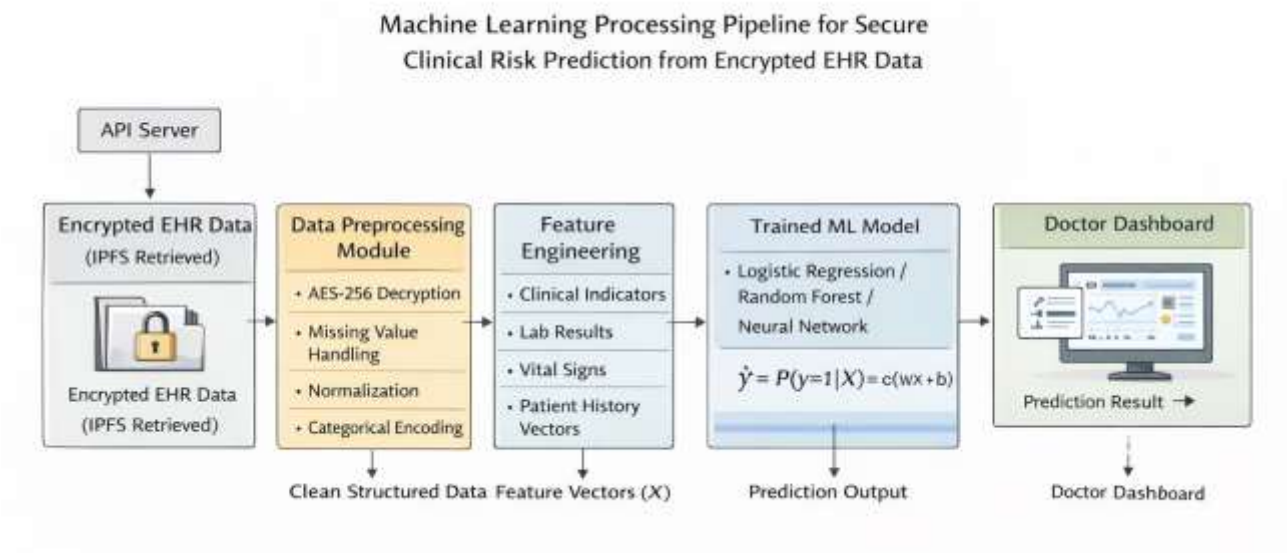

Fig. 5 Machine Learning Processing Pipeline Diagram

VII. Security and Privacy Analysis

Healthcare systems require strict security and privacy protection because medical data is extremely sensitive. The proposed decentralized EHR model incorporates multiple layers of cryptographic protection, authentication mechanisms, access control systems, and audit logging processes.

AES-256 symmetric encryption is used to guarantee confidentiality of medical records stored in distributed storage.

$$C = E_{AES256}(M, K)$$

where M represents the plaintext medical record and K represents the encryption key.

Asymmetric cryptographic algorithms such as RSA or Elliptic Curve Cryptography are used to securely distribute encryption keys.

RSA encryption:

$$C = M^e \bmod n$$

RSA decryption:

$$M = C^d \bmod n$$

Blockchain ensures integrity through cryptographic hashing.

$$H_i = SHA256(Data_i \,//\, H_{i-1})$$

Any modification in previous block data changes the resulting hash and invalidates the chain.

The system implements a hybrid Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) model. Access control can be defined mathematically as:

$$Access\ (U, R, A, C) = 1,\ if\ authorization\ conditions\ are\ met;\ 0,\ otherwise$$

where U represents the user requesting access, R represents the requested resource, A represents contextual attributes, and C represents patient-defined consent policies.

JWT tokens also prevent replay attacks by including expiration timestamps and cryptographic signatures.

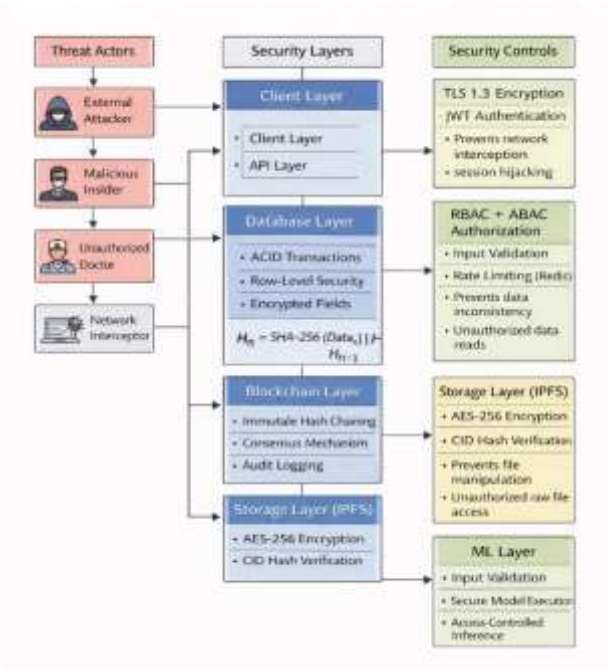

Fig. 6 Threat Model and Multi-Layer Security Defence Diagram

VIII. Performance Evaluation

The performance of a decentralized healthcare system must be evaluated through computational efficiency and scalability metrics.

System throughput represents the number of requests processed within a certain time period.

$$Throughput = Total\ Requests / Processing\ Time$$

Higher throughput indicates the ability of the system to handle larger workloads without performance degradation.

Latency measures the time difference between request submission and system response.

$$Latency = T_{response} - T_{request}$$

The latency is determined by a number of factors such as database query time, network delays, blockchain transaction confirmations, and IPFS file retrieval.

Latency is cut down drastically by the Redis caching method since most metadata that is used is loaded directly out of memory rather than accessing the database.

The throughput of Hyperledger Fabric is better than that of the public blockchain networks due to its ability to run in a permissioned environment (no mining).

Distributed storage of medical files is made possible by IPFS that divides the data into several nodes.

IX. COMPARATIVE ANALYSIS

To determine the efficiency of the proposed architecture, the comparison can be made with the conventional centralized Electronic Health Record systems.

The conventional EHR systems have been using centralized databases that are run by the respective healthcare institutions. Institutional data centers and internal access control policy are used to store patient records.

Nonetheless, the centralized architectures are vulnerable to the single point of failure, not being transparent, and not providing patients with the control over the sharing of the data.

Centralized systems rely on security of one database server in order to maintain data integrity. Attackers have the ability to alter the records or erase them without being noticed in case the server is compromised.

The suggested blockchain-based architecture, in its turn, writes cryptographic hashes of medical records in a distributed registry. Because blockchain data structures are immutable, any alteration of the data stored in the data structure will instantly cause the hash value of the data to change which then causes inconsistencies to be revealed.

The other significant distinction is patient data ownership. The conventional healthcare model views medical records as an institutional resource where the decentralized model provides patients with access permission through blockchain-based consent policies.

In terms of scalability, centralized systems tend to become bottlenecks due to the growth in the number of users in the databases. The proposed architecture is a system that allocates the responsibilities of the system to the various components such as Redis caching, distributed IPFS storage, and horizontally scalable backend APIs.

Encryption protocols ensure confidentiality, blockchain ensures integrity and auditing, and hybrid access control models are a guarantee of stringent authorization policies.

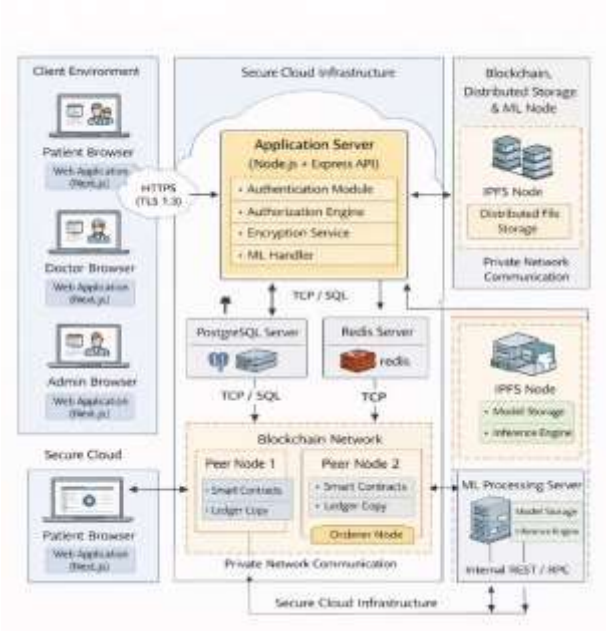

Fig. 7 Deployment Architecture Diagram

X. DISCUSSION

One of the means through which the new distributed technologies can significantly improve the security, transparency as well as scalability of the infrastructures of healthcare information is the suggested decentralized Electronic Health Records management system. The conventional healthcare system is predominantly centralized database based where the control and trust are centralized within individual institutions. Even though it has been noted that such architectures ease management of operations, it is also known to pose a great risk in regards to unauthorised access, data tampering and system failures. The decentralized system suggested in the work delivers the trust to several nodes involved in the process with the help of blockchain but it does not allow reliance on one node and makes the system much more resilient.

Immutability of the records of transactions is one of the greatest advantages of involving blockchain and healthcare data systems. All access requests, updates to consents and record changes are commemorated to the blockchain ledger, forever. The cryptographic hash of one block is based on the previous block and therefore blockchain data structure is linked together, any attempt to modify past information will change the respective hash values and invalidate the ledger. This property provides verifiable evidence of integrity of data, and it allows the healthcare institutions to keep open audit trails in order to meet regulations.

Separated storage of data and integrity check is another advantageous impact of the proposed architecture. Placing large medical files on the blockchain networks would pose horrendous scalability problems due to the block size restriction and cost of transactions. The hybrid architecture can address this shortcoming by relying on a decentralized storage network to store encrypted data (the medical files) like IPFS and only

the cryptographic hash of file identifiers on the blockchain. In such a manner, it will ensure that blockchain would maintain the integrity confirmation and storage layer would address the high volumes of data in an efficient manner.

Machine learning is even more likely to make the difference in healthcare information management systems when it is coupled with these types of architectures. It is possible to process large volumes of medical records with the help of machine learning models to facilitate predictive diagnostics, personalized treatment suggestions, and risk analysis of illness. Nevertheless, machine learning applications also pose a threat to privacy as they have access to sensitive patient information, which in many cases is required to train machine learning models. The privacy-preserving practice like encrypted storage and authorized access policies in a decentralized architecture may guarantee that machine learning can be carried out on authorized data without necessarily exposing raw patient data.

Moreover, the application of distributed caching and high-performance backend systems assists in enhancing the speed of the system within large healthcare networks. In healthcare, there are many requests being processed by a doctor, a patient, a laboratory and administration, at the same time, in the thousands. The Redis caching incorporates the data caching into the application and reduces the load of the application database queries due to the fact that commonly used metadata can be found faster in the memory. Such architecture is designed in such a way that it cannot have unacceptable performance overhead of security mechanisms.

All in all, the suggested system demonstrates that a carefully considered combination of blockchain, distributed storage, cryptographic security means, relational databases, and scalable backend services can address most of the shortcomings associated with the conventional healthcare data infrastructures.

XI. LIMITATIONS

Though the advantages of decentralized healthcare data management systems are numerous, there is a great number of limitations that should be considered in case decentralized data management systems are implemented in real healthcare environments. One of the biggest challenges is the difficulty of implementation and maintenance of blockchain networks. Hyperledger Fabric as a permissioned blockchain system requires to be configured using peer nodes, ordering service, and certificate authority. The development of this infrastructure in other healthcare facilities may be a complicated task regarding its technical expertise and integration between corporations.

The other weakness is attributed to key management of cryptography. In data confidentiality and control in decentralized systems, the encryption keys play a very crucial role. Encrypted medical records do not manage to be recovered in case of the loss or breach of the encryption keys, or unauthorized access can be faced. Management systems that are formulated to be user friendly and secure become very significant to implement in actual life.

The communication with distributed blockchain networks can also have problems with latencies in networks. Although permissioned blockchain systems may require more transaction throughput than the open blockchain systems, a transaction still needs additional processing time as compared to the normal database writes. It is also the responsibility of system designers to make sure that blockchain interactions are optimized in healthcare situations where real-time access to patient data is of the highest priority and delaying due to emergency cases should be prevented.

The other big limitation is regulatory and legal factors. Strict privacy legislation applies to healthcare information as well with HIPAA, GDPR, and other local privacy regulations. The emergence of blockchain technology in the healthcare system may meet the problem of data ownership, the transfer of information across the borders, and compliance with the existing regulatory standards. The policymakers and healthcare organizations must thus collaborate to establish the guidelines of a safe and legal implementation of blockchain use.

Finally, infrastructure may be more expensive at the preliminary deployment phase. Both distributed storage networks and blockchain nodes and secure server environments require computing resources and network bandwidth. Such costs could be minimised as time progresses as technology matures, but initial implementation cost could be high.

XII. FUTURE SCOPE

The proposed decentralized EHR system is an excellent point of departure in the progress and creation of further research and technological advancements in the safe healthcare data management models. There are several research areas that may be applied to enhance the system capabilities and efficiency.

One area of research that is prominent in the future work is that more advanced machine learning models capable of handling decentralized medical data should be presented. Machine learning algorithms, natural language processing models, and predictive analytics algorithms are the artificial intelligence methods that may assist physicians in diagnosing diseases and the trends of their treatment and patient outcomes. Machine learning can be used to ensure the provision of intelligent clinical decision support and the maintenance of data security in the context of decentralized healthcare systems.

The second potential solution is the use of privacy-aware techniques of computation called federated learning and homomorphic encryption. Federated learning is a machine learning model that can also be trained in multiple institutions without having to move raw patient data to a central server. Instead, the model is locally trained at each of the participating institutions, and model updates are only shared. This has been amalgamated to get a world model. Such approaches also reduce the risk of exposing sensitive information and these approaches offer the opportunity to pursue collaborative research in medicine.

Also, the deployment of zero-knowledge protocols of proving that belong to blockchain networks could be enhanced. Zero-knowledge proofs allow one party to verify that he indeed

possesses some information without revealing the information. Such protocols can be applied in the health care sector to confirm the eligibility or health standards of the patients without exposing their personal information of a sensitive nature.

Internet of Medical Things (IoMT) is another research opportunity. The wearable health device is an unending source of physiological records such as the heartbeat, blood pressure and glucose. Implementation of such kind of data streams into decentralized healthcare systems is a possible potential solution in terms of the real time monitoring of patients and preventing medical anomalies at their early stages of the development.

The cross-institutional interoperability standards are also to be taken into consideration to facilitate a perfect data exchange among other hospitals that utilize alternative healthcare systems. The medical data standard protocols and formats of communications will become the key to achieving the connectivity in healthcare ecosystem.

XIII. CONCLUSION

The research has suggested an elaborate, decentralized structure of safe and scalable management of Electronic Health Records utilizing the blockchain technology, distributed storages, cryptography security devices, and the high-performance infrastructure (back-end). The proposed system will be able to address some of the key limitations associated with the old centralized healthcare data structure, such as the vulnerability to the data breach, the lack of visibility in the access control, and the inability to transfer medical records ownership to the patient.

With blockchain, the system will ensure that record access and consent transactions events are stored in an undisrupted distributed ledger in a permanent manner. Cryptographic hashing also guarantees that identity of any attempt to alter records that have already been stored earlier is established instantly. In the meantime, the decentralized storage network has been incorporated such as IPFS that allow the storage of large medical files in their proper place without overloading the blockchain network.

It is also well encrypted in terms of methodology, and secure authentication schemes in addition to hybrid access control frameworks that incorporates role and attribute-based authorization. These systems will ensure that patient records are not accessed by unauthorized healthcare providers and that they are carefully guarded as far as privacy is concerned. Performance optimizations of the system will also be done using Redis caching and scalable backend API to make sure that the system has the capacity to support large hospital networks without influencing efficiency.

Overall, the proposed model of decentralized healthcare record management demonstrates that the existing shared technologies can transform the security and transparency of medical information system. The system will provide a realistic basis of the future of healthcare data platforms in that it will enable patients to own some data, no proof of tampering by auditors, and scalable infrastructure.

REFERENCES

[1] A. Zhang, X. Lin, and H. Wang, "A Blockchain-Based E-Healthcare System with Provenance Awareness," IEEE Journal, 2023.

[2] Y. Li et al., "A Secure Medical Information Storage and Sharing Method Based on Multiblockchain Architecture," IEEE Journal, 2023.

[3] H. Chen et al., "A Privacy-Preserving Quantum Blockchain Technique for Electronic Medical Records," IEEE Journal, 2023.

[4] S. Nakamoto et al., "A Survey on Blockchain Technology Evolution," IEEE Access, 2023.

[5] K. Sharma et al., "A Survey on Blockchain for Healthcare Challenges, Benefits, and Future Directions," IEEE Access, 2023.

[6] J. Liu et al., "An Integrated Healthcare Service System Based on Blockchain Technologies," IEEE Access, 2023.

[7] M. Chen et al., "Blockchain-Based Medical Data Asset Sharing Framework for Healthcare 4.0," IEEE Internet of Things Journal, 2024.

[8] R. Gupta et al., "Blockchain-Based Medical Decision Support System," IEEE Access, 2024.

[9] S. Patel et al., "Blockchain-IoT Healthcare Applications and Trends: A Review," IEEE Access, 2023.

[10] T. Nguyen et al., "Blockchain and Machine Learning in EHR Security: A Systematic Review," IEEE Access, 2023.

[11] M. Khan et al., "Blockchain Meets Federated Learning in Healthcare: A Systematic Review with Challenges and Opportunities," IEEE Access, 2023.

[12] Y. Zhao et al., "Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System," IEEE Transactions on Network Science and Engineering, 2024.

[13] X. Yang, X. Qi, and X. Zhou, "Deep Learning Technologies for Time Series Anomaly Detection in Healthcare: A Review," IEEE Access, vol. 11, 2023.

[14] P. Singh et al., "Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review," IEEE Access, 2023.

[15] Q. Zhang, X. Xue, and J. Yang, "Blockchain-Enabled Trustworthy Healthcare Data Sharing Mechanism for Reliable 6G-IoT Networks," IEEE Internet of Things Journal, 2026.

[16] M. Khan et al., "Blockchain Meets Federated Learning in Healthcare: A Systematic Review With Challenges and Opportunities," IEEE Access, 2023.

[17] X. Wang et al., "Large-Scale Medical Records Analysis by AI-Driven Method in Healthcare Consumer Electronics," IEEE Transactions on Consumer Electronics, vol. 71, no. 1, 2025.

[18] Q. Feng, M. Du, N. Zou, and X. Hu, "Fair Machine Learning in Healthcare: A Survey," IEEE Transactions on Artificial Intelligence, vol. 6, no. 3, 2025.

[19] G. Peng, A. Zhang, and X. Lin, "Patient-Centric Fine-Grained Access Control for Electronic Medical Record

Sharing With Security via Dual-Blockchain," IEEE Transactions on Network Science and Engineering, 2023.
[20] U. Ullah and B. Garcia-Zapirain, "Quantum Machine Learning Revolution in Healthcare: A Systematic Review of Emerging Perspectives and Applications," IEEE Access, 2024.
[21] S. Gupta, R. Patel, and A. Sharma, "Secure access control for electronic health records in blockchain-enabled consumer Internet of Medical Things," IEEE Access, vol. 12, pp. 1--15, 2024.
[22] K. Zhang, Y. Li, and H. Chen, "Real-time tracking of diagnostic discrepancies in electronic health records for improved predictive modeling," IEEE Journal of Biomedical and Health Informatics, vol. 28, no. 2, pp. 1--12, 2024.
[23] W. Zheng, T. Anwlnkom, and Y. Liu, "TRUST-Med6G: A secure and trustworthy medical data privacy protection mechanism in 6G-IoT," IEEE Internet of Things Journal, vol. 13, no. 5, pp. 8248--8260, Mar. 2026.