Patient Centric Access Control for Electronic Medical Record with security via Blockchain

1st Aadhya Shrivastava
Computer Science and Communication
KIIT
Bhubaneshwar, India
2229001@kiit.ac.in

2nd Abhinav Gogoi
Comuter Science and Communication
KIIT
Bhubaneshwar, India
2229003@kiit.ac.in

3rd Aurgho Banerjee
Computer Science and Communication
KIIT
Bhubaneshwar, India
2229022@kiit.ac.in

4th Ayushman .
Computer Science and Commuication
KIIT
Bhubaneshwar, India
2229026@kiit.ac.in

***Abstract*—This paper proposes secure and optimized methods for the storage of electronic medical records and patient-centric access control for these records. The methods suggested for secure purpose are Kyber - 1024 encryption which is a lattice-based encryption method along Zero Knowledge Proofs authentication for accessing the EMR of the user. The above provided method is compared with the already existing methods and hence further worked on to optimize this method.**

***Index Terms*—Blockchain, Kyber - 1024, Zero - Knowledge Proofs, Electronic Medical Records**

I. Introduction

Electronic Medical Records are digital versions of patient paper charts, containing medical histories, diagnoses, medications, treatment plans, immunization records, and lab results. It is different from electronic health records which primarily have interoperability across multiple healthcare providers, EMRs are primarily used within a single healthcare organization. The shift from paper - based records to EMRs has significantly improved healthcare efficiency, reduced errors, and improved patient care, but as this data becomes increasingly digitized , ensuring the security, privacy, and integrity of EMRs has become a critical concern.

Patient data is highly sensitive, and breaches can have severe consequences, including identity theft, insurance fraud, and compromised medical records. Thus, secure EMRs must:

- Only authorized healthcare professionals should access patient records.
- Medical records must remain unchanged and accurate.
- Laws like HIPAA and GDPR mandate strict data protection measures.
- Patients should have transparency and control over who views their data.

Traditional security mechanisms such as password protection, encryption, and role-based access control have been used to safeguard EMRs, but these methods face significant challenges in today's cyber threats landscape.

II. Comparisons

A. Traditional Access Methods Challenges

Challenges in the traditional EMR access mechanism Most EMRs are stored in centralized databases, making them prime targets for cyberattacks. Different healthcare systems use incompatible EMR formats, hindering secure data sharing. Passwords and basic access controls can be surpassed by phishing and hacking. Tracking unauthorized access or modifications is often difficult in conventional systems. Patients have little control over how their medical is shared or used.

B. Blockchain bases storage and acess

Blockchain offers a decentralised, tamper proof and transparent solution to EMR security challenges. Key benefits:

- Decentralised Immutable records :Blockchain stores data across distributed network eliminating single points of failure. Once the data is recorded, it cannot be altered, ensuring integrity and preventing fraud.
- Enhanced Access control Patient Ownership: Smart Contracts can enforce strict access rules, allowing only authorised personnel to view records. They can grant or revoke access using private cryptographic keys.
- Secure Transparent Auditing: Every access or modification is recorded on the blockchain, creating an immutable audit trail.
- Improved Interoperability: Blockchain enables secure cross - institutional data sharing without relying on a central authority.
- Protection against Cyber Threats: Blockchain cryptographic security makes it highly resistant to hacking and unauthorised alterations

C. EMR Sharing Models

EMR have revolutionised healthcare by digitalizing patient data, improving care coordination, and reduce medical errors. However, sharing EMRs comes with privacy, security and interoperability challenges. Three primary models exist today:

Identify applicable funding agency here. If none, delete this.

Centralised: The single database is controlled by one entity. In a centralized EMR system, all patient data is stored in a single, unified database managed by a central authority (e.g., a hospital, healthcare network, or government agency).**Key Features:** (a)Single Database: All patient records are stored in one location. (b)Uniform Access: Authorized users access the same centralized system. (c)Standardized Data Format: Ensures consistency in data entry and retrieval. (d)High Control: Easier to manage security, backups, and updates. **Advantages:** Easy Data Retrieval – No need to query multiple sources. Consistency – Uniform data structure reduces errors. Strong Security – Centralized control over access and encryption. Efficient Updates – Software upgrades apply system-wide. Disadvantages: Single Point of Failure – If the central server fails, access is disrupted. Scalability Issues – Large datasets may slow down performance. Privacy Concerns – Centralized storage may be a target for cyberattacks. Limited Flexibility – May not accommodate diverse healthcare providers easily.

Federated: It contains distributed databases with shared standards. Key Features: Decentralized Storage: Each organization controls its own database.

Interoperability: Uses standards like HL7, FHIR, or DICOM for data exchange.

Patient-Centric Access: Patients or providers can request records from different sources.

Distributed Control: No single entity owns all data.

Advantages: No Single Point of Failure – Resilient against system-wide crashes. Enhanced Privacy – Data remains with the original custodian unless shared. Scalability – New institutions can join without overhauling the central system. Flexibility – Supports diverse healthcare providers (hospitals, clinics, labs).

Disadvantages: Complex Interoperability – Requires strong data standards and APIs. Slower Data Retrieval – Queries may need to fetch data from multiple sources. Security Risks – Each node must be secured individually. Inconsistent Data Formats – May require normalization.

Hybrid: It is a combination of centralised and federated approaches. Key Features: Partial Centralization: Critical data (e.g., patient IDs, allergies) may be centralized.

Federated Components: Specialized data (e.g., radiology, lab results) stays local but is queryable.

Adaptive Architecture: Balances control and flexibility.

Advantages: Balanced Control Flexibility – Combines the best of both models. Improved Interoperability – Easier data sharing than purely federated systems. Redundancy Reliability – Less vulnerable than fully centralized systems.

Disadvantages: Complex Implementation – Requires integration between centralized and federated components. Higher Maintenance – Needs continuous synchronization. Additionally, access control mechanisms like Role Based Access Control and Attribute Based Access Control are used to regulate data access. However, these models face security vulnerabilities, leading to the exploration of blockchain based security solutions for EMRs.

III. Existing Work

A. Action EHR: Patient Centric Blockchain Based Record data management

The paper ACTION - EHR: Patient Centric Blockchain Based Record Data Management for Cancer Care: presents a system aimed at enhancing the management, sharing, and aggregation of Electronic Health Record (EHR) data, particularly in the context of cancer care. The main objective is to empower patients with greater control over their EHR data across various hospitals. Utilizing blockchain technology, the system ensures secure and trustworthy data sharing. It adopts a hybrid approach: metadata is stored on the blockchain, while the actual EHR data is encrypted and stored in a cloud storage solution that complies with HIPAA regulations.

Advantages of Action EHR:

Enhanced Security and Privacy: The system uses encryption and digital signatures to secure EHR data, addressing the privacy concerns associated with sensitive health information. Patient-Centric Approach: Patients can manage their health records and control who has access to their data. **Improved Data Sharing**: The system aims to provide a more efficient and secure way to share EHR data compared to traditional methods like faxing or mailing. **Scalability**: By using a hybrid approach, the system can handle large volumes of EHR data, which is a significant advantage.

Challenges and Limitations:

Complexity of Implementation: Applying blockchain technology in healthcare is challenging due to the highly regulated environment. **Potential Single Point of Failure**: If the system isn't set up correctly (e.g., with a single orderer or Certificate Authority), it could be vulnerable to a single point of failure. **Emergency Access Challenges**: The system may face difficulties in emergency situations where immediate access to a patient's EHR is needed but restricted by access control policies. **Right to be Forgotten" Incompatibility**: The immutability of blockchain can conflict with data deletion requests (the "right to be forgotten"), posing a challenge for compliance with regulations like the General Data Protection Regulation (GDPR).

Problem-Solving Approach The paper addresses the problem of insecure and inefficient EHR data sharing by: Leveraging Blockchain Technology: To provide a secure, transparent, and immutable record of data sharing transactions. Implementing a Hybrid Data Management System: Storing metadata on the blockchain and actual EHR data in encrypted form in cloud storage to balance security and scalability. Developing a Patient-Centric System: Giving patients control over their data and permissions. Using Cryptographic Techniques: Such as asymmetric encryption and digital signatures, to ensure data privacy, integrity, and authenticity.

B. Blockchain Powered Paitent Centric Access Control woth MIDI AES 256 encryption

This paper presents a blockchain-based access control mechanism aimed at improving the security of patient healthcare records. The system employs **MIDI AES-256 encryption**, a modified variant of the Advanced Encryption Standard (AES-256), to ensure strong data protection. The main objective is to empower patients with control over their medical data, facilitating secure sharing with healthcare providers while safeguarding against unauthorized access. **Advantages of the Proposed Technique: Enhanced Security**: MIDC AES-256 improves upon AES-256, making it more resistant to cyberattacks. **Decentralization**: Blockchain eliminates the need for a central authority, reducing data manipulation risks. **Patient-Centric Control**: Patients can grant and revoke access to their medical records, increasing privacy. **Tamper Resistance**: Blockchain ensures that once data is recorded, it cannot be altered or deleted. **Interoperability**: The proposed system can be integrated with existing healthcare information systems.

Disadvantages of the Proposed Technique: High Computational Cost: Encryption and blockchain operations require significant processing power. **Storage Overhead**: Blockchain networks can grow in size, leading to increased storage requirements. **Scalability Issues**: As the number of transactions grows, the system may experience latency. **Adoption Challenges:** Healthcare institutions may face difficulties transitioning from traditional data management to blockchain-based systems.

IV. Proposed Method

"Secure Blockchian-Based EMR system with Lattice Based Encryption and Optimized Access Control" this proposal outlines a highly secure, patient centric EMR system using blockchain technology combined with post-quantum lattice based encryption (Kyber-1024) and zero knowledge proofs (ZKPs) for enhanced privacy. This system provides a tamper-proof storage, fine grained access control and efficient data sharing while minimizing storage overhead and operational cost.

A. System architecture

Our approach consist of three layers:

Application Layer(User Interface): It is the front end interface where patients, doctors and healthcare providers interact with the EMR system. **Key Components: Patient Dashboard:** This dashboard helps in viewing the medical records, grant or revoke access to doctors and track access logs for the patients. **Doctor Portal**: This section requests EMR access via ZKP authentication, view the decrypted records and update prescriptions with patient approval. **Admin Panel:** this manages the healthcare providers, monitors the compliance using HIPAAand audits the access log.

2. Blockchain Layer(Smart Contracts and Consensus): This layer is the decentralised backbone handling the access control, audit logs and data integrity. Key components: **Access Control SC**: This enforces patient defined permissions and uses ZKP verifications **Audit log SC**: This records every EMR access/modification and has immutable timestamping. **Key Management SC**: This stores public keys (Kyber - 1024) and manages teh IPFS CIDs. **Consensus Mechanism**: It uses Practical Byzantine Fault tolerance for fast finality. **Workflow: Request:** A doctor submits EMR access request. **Pre - prepare:** Leader node broadcasts the request. **Prepare/Commit**: Validators reach consensus. **Execution:** Smart contract grants / denies access.

3. Storage Layers (IPFS + Encrypted EMRs): Off Chain storage for encrypted EMRs , ensuring scalability and cost efficiency. **Key Components: IPFS(Off Chain)**: IT stores encrypted EMRs(Kyber - 1024) and returns a content ID for on chain reference. **On Chain metadata:** It stores CID + SHA - 3 Hash for EMR and ensures tamper proofing. **Decryption Module:** The authorised users fetch the CID and this module decrypts with Kyber - 1024 private key.

B. Data Flow

- Patients uploads EMR which is encrypted with Kyber - 1024

$$ciphertext = Kyber.encrypt(pk, EMR)) \tag{1}$$

- Uploads to IPFS which returns the CID

$$CID = ipfs.add(ciphertext) \tag{2}$$

- Stores on blockchain:

$$blockchain.store(CID, SHA - 3(EMR)) \tag{3}$$

C. Core Algorithms

1. Kyber - 1024:It is a post quantum cryptographic algorithm.It provides resistance to quantum attacks as it based on Module Learning with Errors(MLWE) a lattice problem that remains hard even for quantum computers and ensures long term security. It provides strong security with better efficiency with 256 bit security. And is optimised for healthcare use cases.

- Key Generations:

```
    def kyber_keygen():
pk , sk = Kyber1024.keygen()
return (pk,sk)
```

- Encryption:

```
    def kyber_encypt(pk, EMR_data):
ciphertext = Kyber1024.encrypt(pk ,EMR_data
return ciphertext
```

- Decryption:

```
    def kyber_decypt(sk, ciphertext):
plaintext = Kyber1024.encrypt(pk ,EMR_data)
return plaintext
```

2. Zero Knowledge Prooofs Authentication:ZKPs enable secure, privacy - preserving authentication in EMR system by privacy first verification, this proves authorisation without revealing identities or sensitive credentials. Each session generates unique proof which makes the proof non reusable and blockchain becomes attack resistance.

- ZKP setup(zk$_{S}NARKS$) :

```
def zkp_prove(identity, access_policy):
proof = zkSNARKs.generate(identity,
access_policy)
return proof
```

3.Hybrid Storage Optimizations(IPFS + Blockchain) The issue is that storing full EMR on - chain is expensive, so storing only metadata on chain, while the encrypted EMRs reside in IPFS. Workflow: The EMR is initially encrypted with Kyber - 1024 then this encrypted file is uploaded to IPFS, and a Content Identifier (CID) is received. This CID along with has (SHA - 3) is stored in the blockchain.

V. Figures Tables

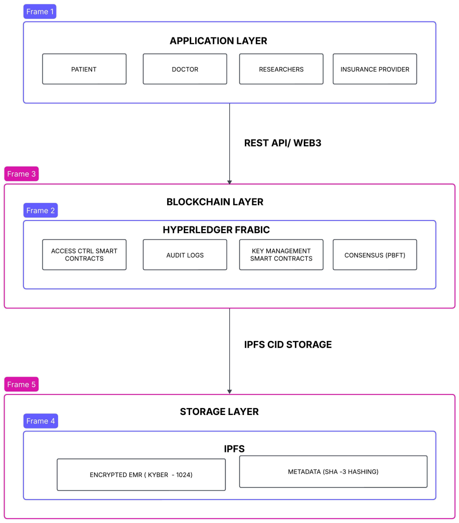


Fig. 1. Architecture Design of Proposed Model

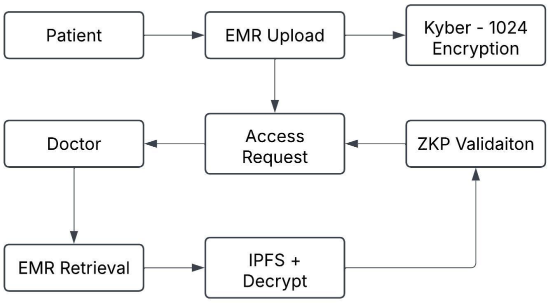
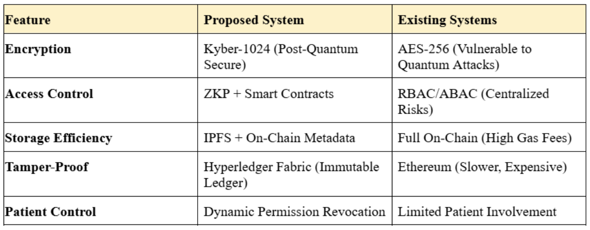
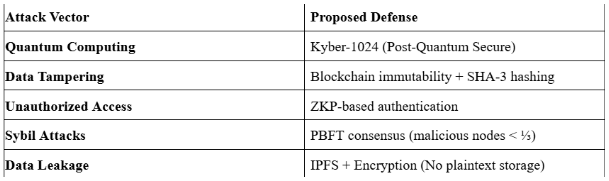


Fig. 2. Workflow Architecture



Feature	Proposed System	Existing Systems
Encryption	Kyber-1024 (Post-Quantum Secure)	AES-256 (Vulnerable to Quantum Attacks)
Access Control	ZKP + Smart Contracts	RBAC/ABAC (Centralized Risks)
Storage Efficiency	IPFS + On-Chain Metadata	Full On-Chain (High Gas Fees)
Tamper-Proof	Hyperledger Fabric (Immutable Ledger)	Ethereum (Slower, Expensive)
Patient Control	Dynamic Permission Revocation	Limited Patient Involvement

Fig. 3. Comparison with existing approach



Attack Vector	Proposed Defense
Quantum Computing	Kyber-1024 (Post-Quantum Secure)
Data Tampering	Blockchain immutability + SHA-3 hashing
Unauthorized Access	ZKP-based authentication
Sybil Attacks	PBFT consensus (malicious nodes < ⅓)
Data Leakage	IPFS + Encryption (No plaintext storage)

Fig. 4. Threat and Security Analysis

VI. Conclusion

Thus the integration of blockchain technology, Kyber - 1024 lattice based encryption and zero knowledge proofs(ZKPs) presents a transformative approach to securing Electronic Medical Records(EMRs) while ensuring patient centric control. This system addresses critical challenges in healthcare data management, including the security breaches, interoperability issues and lack of patient autonomy by providing : Quantum Resistant Security with Kyber - 1024 Privacy preserving access with Zero Knowledge Proofs(ZKPs) Decentralised and Tamper Proof Blockchain Architecture

For future works we can integrated Biometric

ZKPs like fingerprint/ face recognition for seamless access, training AI models on encrypted EMRs without decryption and expanding the secure EMR sharing across healthcare networks.

VII. Acknowledgement

We extend our heartfelt gratitude to **Assistant Professor Dr. Arup Sarkar** for his invaluable guidance, insightful feedback, and unwavering support throughout the process of writing this paper. His expertise in **Electronic Medical Records (EMR) systems** and patient data management greatly enriched our research, helping us refine our understanding of **centralized, federated, and hybrid EMR models**. His mentorship not only enhanced the quality of our work but also encouraged critical thinking and structured analysis. We deeply appreciate his time, patience, and dedication in shaping this paper into a well-researched and coherent document. Thank you, Dr. Sarkar, for being an exceptional mentor and inspiring us to excel in healthcare informatics research.

VIII. Referecences

References

[1] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, *ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care*, J Med Internet Res, vol. 22, no. 8, 2020.

[2] S. Ghaffaripour and A. Miri, *Application of Blockchain to Patient-Centric Access Control in Medical Data Management Systems*, 2019.

[3] 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, vol. 10, no. 6, pp. 3908–3921, 2023.

[4] N. K. Pandit, S. Das, and C. K. Panda, *A Patient-centric EHR Management System using Ethereum Blockchain*, 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS), pp. 1–5, 2024.

[5] Z. Sun, D. Han, D. Li, T. -H. Weng, K. -C. Li, and X. Mei, *MedRSS: A blockchain-based scheme for secure storage and sharing of medical records*, Computers & Industrial Engineering, vol. 183, pp. 109 521, 2023.

[6] D. Kumari, A. S. Parmar, H. S. Goyal, K. Mishra, and S. Panda, *HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data*, Computer Networks, vol. 241, pp. 110 223, 2024.

[7] Y. Hong, L. Yang, W. Liang, and A. Xie, *Secure Access Control for Electronic Health Records in Blockchain-Enabled Consumer Internet of Medical Things*, IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 4574–4583, 2024.

[8] K. P. N. Rao and S. Chinnaiyan, *Blockchain-Powered Patient-Centric Access Control with MIDC AES-256 Encryption for Enhanced Healthcare Data Security*, Acta Informatica Pragensia, vol. 13, no. 3, 2024.

[9] M. Sharmitha, M. P. Theeraj, P. V. Ranjith, and S. Anitha, *BLOCKCHAIN BASED PATIENT CENTRIC MEDICAL RECORDS SHARING WITH PRIVACY PRESERVATION*, 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–6, 2024.

[10] U. Chelladurai, S. Pandian, and K. Ramasamy, *A blockchain based patient centric electronic health record storage and integrity management for e-Health systems*, Health Policy and Technology, vol. 10, pp. 100 513, 2021.