Privacy Preserving Techniques for Patient Medical Records using Blockchain Technology

PREET PAREKH
DEPARTMENT OF NETWORKING AND COMMUNICATIONS SCHOOL OF COMPUTING SRMIST,
KATTANKULATHUR CAMPUS,
CHENNAI, INDIA
PP2908@SRMIST.EDU.IN

PATEL CHHAYANK KAUSHIKBHAI
DEPARTMENT OF NETWORKING AND COMMUNICATIONS SCHOOL OF COMPUTING SRMIST,
KATTANKULATHUR CAMPUS,
CHENNAI, INDIA
CP4144@SRMIST.EDU.IN

DR. HEMAMALINI V.
DEPARTMENT OF NETWORKING AND COMMUNICATIONS SCHOOL OF COMPUTING SRMIST,
KATTANKULATHUR CAMPUS,
CHENNAI, INDIA
HEMAMALV@SRMIST.EDU.IN

***Abstract*— In contemporary health care, the greatest issues are patient data security and privacy, with respect to increasing digitization. Traditional methods of dealing with such data have vulnerabilities such as incorrect use, violations, and incompatibilities. Adhere major issues are the data.**

This project suggests a blockchain communication model through utilizing Zero-Knowledge Proofs (ZKPs) to provide privacy-protecting management of patient information. Utilizing blockchain makes the storage tamper-proof and decentralized, with ZKPs providing the means to verify medical qualifications without divulging the information. This solution provides greater security, trust, and compliance in health information exchange.

Compliance with laws and regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) and seamless data transmission.

Keywords—Blockchain, Zero-Knowledge Proofs (ZKPs), Tamper-Proof Storage, Decentralized Systems, Privacy-Preserving Verification, Data Interoperability, Regulatory Compliance, HIPAA, GDPR, Secure Data Exchange.

I. Introduction

With mounting patient privacy issues, this project employs blockchain technology with Zero-Knowledge Proofs (ZKPs) that protect medical records and their privacy. ZKPs enable hospitals to authenticate patient information without exposing sensitive details, which is HIPAA and GDPR compliant. Blockchain offers an impenetrable medium for storing unchangeable information with access control. This setup achieves trust, security, and compatibility in health care, with ease of information exchange without patient data privacy issues. Using cryptographic methods, our solution enables medical institutions to authenticate and exchange vital information without exposing personal health information, creating a privacy-centric health care system.

BLOCKCHAIN

Figure 1 describes Blockchain technology which is a revolutionary concept gaining popularity as a foundational technology for applications such as cryptocurrencies like Bitcoin. In essence, a blockchain is a decentralized, distributed digital ledger that records transactions across numerous computers. This system ensures that a block involved cannot be tampered with retroactively unless all the following blocks are altered as well as the consensus of the network.

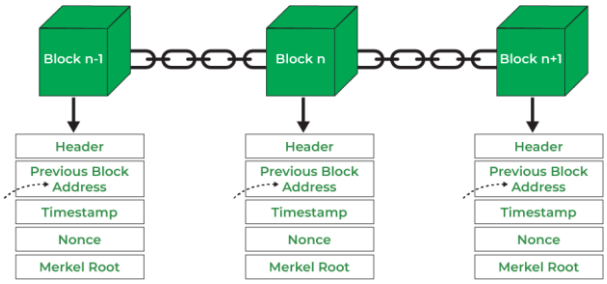

Figure 1. Blockchain Block Structure

The main advantages of using the blockchain are

Decentralization: In comparison to traditional databases regulated by an official center, blockchain details are spread among a system of members. This eradicates a singular point of wreckage and restricts the likelihood of suppression or handling.
Immutability: In comparison to traditional databases regulated by an official center, blockchain details are spread among a system of members. This eradicates a singular point of wreckage and restricts the likelihood of suppression or handling.
Transparency: The individuals' identities within a public blockchain system are labelled with pseudonyms; however, the transactions could always be seen by everyone on the network, which provides more integrity and transparency.
Security: Cryptographic hashing and consensus mechanisms ensure the integrity and security of the blockchain. These features make it highly resistant to fraudulent activities and cyberattacks.

II. Novelty of the proposed system

This research proposes a new model for secure and private management and exchange of Electronic Health Records (EHR) that exploits the capabilities of blockchain, Interplanetary File System (IPFS), Zero-Knowledge Proofs (ZKPs), and MetaMask. To solve the problem of maintaining the integrity and confidentiality of patients' information and offering them unprecedented control, we develop a distributed ecosystem that allows them to decide who can access their health data and for what period.

Our framework fundamentally leverages a private blockchain for the sake of storing the indisputable metadata in a secure manner. It maintains a transparent record of events and provides data on the healthcare service user provision and restriction by giving full insight without revealing confidential information. To address the issues of the limited on-blockchain data storing capacity and on-chain storing costs, the Ethereum IPFS underpins the system. The actual encrypted healthcare records do not reside on the chain. Instead, they are stored outside the blockchain in a secure manner.

The significant advancement is the inclusion of Zero-Knowledge Proofs (ZKPs). It allows patients to share certain verifiable information about their health like a test result without having to expose their entire health records to the doctors. It is very essential to protect the rights of patients to privacy while having their health record shared with the doctors for medical purposes.

Moreover, our structure tightly binds together with MetaMask, a commonly recognized Web3 wallet, to manage and hold on to patient identities, support unassailable transactions, and entirely tackle digital operations. Making use of MetaMask's built-in encryption system, the Digital Signature Algorithm (ECDSA), EHR data is locked using the patient's own computer amid every transfer to the Ethereum Blockchain, being assured of having a full security. In the primary perspective, it allows patients to give and remove access permissions to EHR data by means of their MetaMask wallet. This idea of dynamic access and control is immutably recorded on the Ethereum Blockchain. This is how the patients are given a full responsibility for their own health-related information.

The distinctiveness of our approach is in the singular combination and arrangement of these technologies to come up with a patient-focused EHR system.

Decentralized and Patient-Centric Access Control: Utilize a permissioned blockchain to enforce transparent and auditable access policies, with patients maintaining the ultimate authority to give and revoke access.
Confidential Information Sharing: Applying Zero-Knowledge Proofs to enable the exchange of certain private health records without revealing the entire dataset.
mproved Patient Control and Security: Taking advantage of MetaMask and ECDSA encryption to secure patients' control over their data and enhance client-side security, allowing them to modify access rights.
Scalable and Cost-Effective Storage: We use IPFS technology for the off-chain storage of electronic health record (EHR) data in a decentralized and efficient manner.

This integrated framework offers a significant advancement over existing EHR systems by prioritizing patient autonomy, data privacy, and security. The ability for patients to dynamically revoke access at any time addresses a critical gap in current systems and fosters greater trust and control. Our research explores the architecture, implementation, and potential benefits of this novel patient-controlled EHR system.

III. Literature Survey

The importance of mechanisms aimed at maintaining privacy in the sharing of health information is evident since Electronic Health Records (EHRs) have become the de facto centrepieces of current-day health systems. A much more detailed study was carried out by Raza Nowrozy et al. [1], who undertook an extensive analysis of over 130 studies focusing on methods for preserving the privacy of EHRs. The authors emphasized that the literature depicts a wide spectrum of methods to enhance the provision of security, ranging from outdated encryption techniques to the recent advancements in blockchain and zero-knowledge proof (ZKP) computing. They also noted that even though scholars have proposed numerous theoretical models, the application of these methods in real-world medical practices is virtually non-existent. Their argument was further supported by the lack of large-scale data, which they considered a significant shortfall in the ability to establish how prepared the various mechanisms were for testing..

One of the promising answers to the problem of secure data exchange is architecture based on a blockchain. Venkatesh Upadrista et al. [2] have proposed one such system based on a blockchain for remote health monitoring that solves the twin issues of data integrity and privacy in telemedicine. They argue that by using smart contracts, a system can be built such that patient consent is automated, and the data can be exchanged without human interaction, effectively solving the problem of human errors. However, they argue that scaling up the system to handle large amounts of medical data at high speeds is a major challenge that requires more research before it can be implemented widely in the healthcare domain.

Based on the cryptographic, Ken Miyachi and Tim K. Mackey [3] presented the Healthcare-Oriented Cryptographic Blockchain System (HOCBS) to privacy-oriented data sharing model with a combination of blockchain's immutability and strong encryption. The model solves the breach threats from both data transmission and storage and offers a system that allows decentralized access control so that different health service providers would securely view the medical records of the patients who are jointly owned. However, the actualization of the model is uncertain, particularly in the case of utilizing it in distributed health care services, since issues like interoperability and performance is not tackled.

Leveraging a patient-centric approach to medical records management, Ma Zirui and Gu Bin [4] proposed a blockchain-based self-governance model inspired by Self-Sovereign

Identity (SSI) to shift the control of patient health information access from hospitals and service providers to the patients themselves, breaking the traditional paradigm of the privacy management of health information. Even though this method enhances the user autonomy and alleviates the dependence on centralized institutions, the integration of this model to the existing EHR systems is a huge technological and administrative burden, which makes it difficult to be used in the short term.

During a significant event, such as the time of the COVID-19 pandemic, the need for streamlined and accurate health data sharing was prevalent. The work of Seval Capraz and Adnan Orsey [5] is an example of that need, as they presented a blockchain-based data sharing framework, specifically tailored to significant health events. The privacy and accountability of patient information were at the forefront of Seval Capraz and Adnan Orsey [5]'s designed system. While the authors of the work proposed using blockchain for establishing trust among various healthcare organizations, their system was not technically validated in any COVID-19-related applications during the pandemic. Therefore, one could say that it is imperative to assess the practicality and efficiency of their ideas in a real-world scenario.

In a broader context, Rui Zhang et al. [6] focused on discussing the privacy, security, and legal concerns when it comes to the implementation of blockchain technology in the healthcare sector. Their study concluded that there is a dilemma between the immutability provided by blockchain databases and the privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). They also stated that having mere technical mechanisms to ensure data integrity is not adequate since there is a lack of a path to comply with the "right to be forgotten" and other regulations related to the privacy of individual data, and this is due to a conflict between legal requirements and the design of cryptographic systems.

A group of researchers, led by Archana Bathula, posited a novel solution to the issue by suggesting the merging of Blockchain, Artificial Intelligence, and ZKPs in one system could revolutionize the way health data privacy is upheld. The proposed system not only ensures the verification of the adherence to the privacy rules is automated but also provides for a smarter way of handling health data. This concept could reduce the number of instances where people need to manually manage health privacy. However, it should be noted that the AI part of the system is still an experimental one, and computational costs of ZKPs are still the main performance drawback.

Finally, Charalampos Stamatellis et al. [9] extended the dialogue by illustrating that Hyperledger Fabric - a licit chain code framework - combined with ZKPs could create a full end-to-end data exchange system that is confidential for health. Their system can only be used to view the classified information that a patient needs reasonably and to ensure their privacy on all networks. That said, the authors also admit that the findings do not add value if no tangible testing and size attempts are carried out, as in all proposed systems.

Finally, Charalampos Stamatellis et al. [9] extended the dialogue by illustrating that Hyperledger Fabric - a licit chain code framework - combined with ZKPs could create a full end-to-end data exchange system that is confidential for health. Their system can only be used to view the classified information that a patient needs reasonably and to ensure their privacy on all networks. That said, the authors also admit that the findings do not add value if no tangible testing and size attempts are carried out, as in all proposed systems.

Research gap

Several key limitations in the existing literature concerning blockchain-based EHR systems:

Limited Emphasis on Dynamic and Patient-Initiated Access Revocation.

- Lack of Comprehensive Integration of Off-Chain Storage with On-Chain Access Control and Revocation.
- Under-Explored Application of User-Friendly Wallets for Patient-Driven Access Management.
- Limited Empirical Evaluation of ZKP Integration for Selective Information Sharing in Patient-Controlled Revocation Scenarios.
- Absence of Specific Solutions Addressing the "Right to be Forgotten" in Conjunction with Patient-Centric Revocation.

IV. PROSPSED METHODOLOGY

The solution integrates blockchain, IPFS, and zero-knowledge proofs to create a secure, patient-controlled electronic health record system. With MetaMask wallet using elliptic curve cryptography (secp256k1 curve) for digital signatures via ECDSA, the system enables patients to control their health data and share it securely with healthcare providers. Critical clarification: ECDSA only is used for signing authentication messages and transactional messages, but key pairs are created via cryptographically secure random number generation and deterministic derivation (BIP-32/BIP-44 standards) and not ECDSA itself. A deployment of a blockchain-anchored dynamic revocation of access mechanism enabling patients to instantly revoke provider access via smart contract-triggered re-encryption key invalidation and accumulator-based revocation registries with patient control and an immutable audit trail of access changes is one such innovation.

The architecture consists of four main layers: the user interface layer, application logic layer, the blockchain network layer, and the data storage layer. Each layer has varying functions but communicates with the other layers seamlessly to form an end-to-end EHR management system. The user interface layer offers differentiated access points for healthcare providers and patients with minimal interactions with the underlying system. The application logic layer holds the smart contracts that define the access rules, authorization schemes, and revocation procedures. The blockchain network layer holds the distributed ledger holding all the access permissions and transactions. The data storage layer employs the use of IPFS to store encrypted patient records securely in a distributed fashion.

Key Concepts

Patient Edge Agent: A desktop/mobile application that is the main patient interface, allowing patients to view, manage, and control permissions related to their health records. The

agent is paired with the MetaMask wallet to allow secure authentication and transaction signing.
Provider Edge Agent: An application for medical professionals to request access to patient records, see authorized data, and enter new medical information. Moreover, this agent includes MetaMask for increased authentication security.
Smart Contracts: Smart contracts on the Ethereum platform that establish business rules for record management, access control, and revocation procedures. Smart contracts automatically execute when the stipulated conditions are fulfilled.
Cloud Agent: An option that allows for secure backup of encrypted patient data and manages re-encryption for authorized sharing, making data accessible even when a patient's device is destroyed or lost.
Registration Manager: A module tasked with registering new users, creating digital identities, and handling first-time setup of patient and provider accounts on the blockchain network.

Implementation Methodology
The implementation methodology utilizes a structured approach to delivering electronic health records with secure, effective, and user-friendly management, enabled through robust access control and revocation.

Patient Identity Management with MetaMask and ECDSA
The system utilizes MetaMask wallet for secure identity management, utilizing ECDSA (Elliptic Curve Digital Signature Algorithm) for cryptographic purposes. The patient and healthcare provider both establish their identity using the following procedure:

Customers download and install the MetaMask phone application or browser extension.
• During the initial setup, MetaMask produces a unique pair of public and private keys. (This process uses cryptographically secure random number generation and deterministic algorithms to generate the private key and compute the public key from elliptic curve point multiplication.)
The public key is utilized as the user's identifier within the blockchain network, and the private key is safely stored within the MetaMask wallet.
• Whenever a user needs to sign a transaction, message, or smart contract interaction, ECDSA is called upon to create a digital signature with the private key. It is used to authenticate and authorize blockchain transactions.

The users send their public keys to the Registration Manager, which assigns these keys to their verified identities using a zero-knowledge proof protocol that provides privacy-preserving authentication.

This method gives users full control of their cryptographic identities without central authority for normal operations. The application of ECDSA as a digital signature offers strong security with comparatively short key lengths, hence perfect for use in mobile and browser-based applications.

EHR Data Management using IPFS

Figure 2 represents the Patient health records are kept and housed in IPFS, which offers a distributed file system for secure and efficient data storage:

• Once a healthcare practitioner establishes a new medical record, the record itself is initially encrypted with a symmetric encryption method (AES-256).
This encrypted file is uploaded in the Interplanetary File System (IPFS), which generates a unique content identifier (CID) that points to the stored data.
• The CID and metadata of the record are stored on the blockchain in a smart contract transaction. Data concerning access control, e.g., the specific providers that have access rights to the record, is retained in the smart contract. The use of IPFS has several advantages: it prevents single points of failure, reduces storage charges relative to storage on-chain, and maintains data persistence even if nodes fail. The content-addressing nature of IPFS also ensures data integrity because any alteration of the record would create a different CID.

Figure 2. Data Management Architecture

V. Implementation Methodology

The method of implementation employed is a structure framework based on ensuring the safe, effective and user-focused management of electronic health records that incorporate strong access control and revocation.

Patient Identity Management using MetaMask and ECDSA
The system employs the MetaMask wallet to provide secure identity management, relying on the ECDSA (Elliptic Curve Digital Signature Algorithm) for its cryptographic features. Patients and healthcare professionals both establish their identity through the following process:

- Individuals buy and download the MetaMask browser extension or mobile application.

- At the time of setup, MetaMask generates a self-contained public-private key pair. It uses cryptographically to secure random number generation and deterministic algorithms to derive the private key and then derives the public key via elliptic curve point multiplication.)
- The public key serves as the identity of the user on the blockchain network, while the private key is securely stored inside the MetaMask wallet.
- Whenever there is a need to sign a transaction, message, or smart contract interaction, ECDSA is called upon to create a digital signature using the private key. This signature is then used to authenticate and authorize actions on the blockchain.
- Users sends their public keys to the Registration Manager, which associates these keys to their authenticated identities using a zero-knowledge proof protocol that maintains confidentiality during authentication.

Without depending on centralized authority for everyday tasks, this method guarantees that users retain total control over their cryptographic identities. ECDSA is effective for mobile and browser-based applications because it offers strong security with comparatively short key lengths.

EHR Data Management with IPFS

Patient health records are stored and managed using IPFS, which provides a distributed file system for secure and efficient data storage:

- AES-256, a symmetric encryption algorithm, is used to encrypt new medical records before they are created by healthcare providers.
- After uploading the encrypted file to IPFS, a unique content identifier (CID) that acts as a reference to the data stored there is returned.
- A smart contract transaction stores the CID and the record's metadata on the blockchain.
- Stored in the smart contract is access control data including which vendors are authorised to view the record.

Using IPFS has a number of benefits: it removes single points of failure, lowers storage costs when compared to on-chain storage, and preserves data persistence even should individual nodes fail. Since any change to the record would produce a different CID, IPFS's content-addressing character also guarantees data integrity.

Zero-Knowledge Proof Authentication

Using zero-knowledge proofs (ZKP) the system guarantees correct authentication and improves privacy:

- When registering on the platform, users provide verifiable credentials to the Registration Manager.
- The Registration Manager generates a ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) that validates the user's identity without revealing personal information.
- This proof is stored on the blockchain and associated with the user's public key.
- For subsequent authentication, users can prove their identity without exposing sensitive information by generating a ZKP that demonstrates knowledge of their private key.

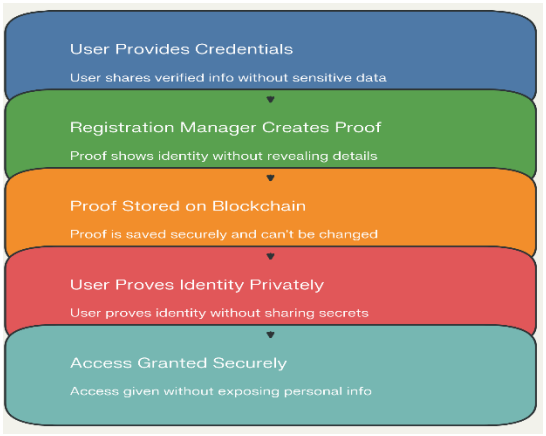

Figure 3. Secure Identity Verification Flow

Figure 3 shows the secure identity verification flow, this system guarantees that users may prove their identity without disclosing too much information, so preserving their privacy. In healthcare environments, where upholding confidentiality is crucial, it is especially vital.

Access Control and Permission Management

The system implements a sophisticated access control mechanism that allows patients to manage permissions for healthcare providers:

- A provider requests access to a patient's record via their edge agent; the patient gets this request through their edge agent and can approve or deny it.
- Should approved, the patient's agent activates a smart contract feature adding the public key of the provider to the list of approved keys for records.
- The smart contract sends an event alerting the cloud agent to create a re-encryption key for the provider.
- The cloud agent notes this event and deletes any re-encryption keys connected to the revoked provider.
- Access has been denied; the provider's edge agent is notified at their edge.

This approach ensures that patients maintain control over their data while enabling efficient sharing with authorized providers. The use of proxy re-encryption minimizes the risk of exposure during the sharing process.

Access Revocation Mechanism

An innovation fundamental to this system is the dynamic revocation mechanism that gives patients the capability to immediately revoke provider access to their data:

- Real-Time Revocation Process: Upon the patient's decision to revoke a provider's access, a revocation request is sent by the patient via their edge agent.
- This invokes a smart contract function that deletes the provider's public key from the authorized list for the indicated records.

- The blockchain state is updated by the smart contract to show this change and a revocation event is emitted.
- The cloud agent fundamental improvement in this system is the deployment of a dynamic mechanism of revoking provider access that enables patients to immediately cancel provider access to their records:
- The Patient-Driven Revocation Process: Upon choosing to cancel a provider's access, a patient initiates a revocation request with their edge agent.
- This action invokes a function in the smart contract that deletes the provider's public key within the authorized list of the respective records.

The revocation mechanism is made to be instantaneous and irreversible without needing patient re-authorization. This makes sure that after revoking the access, even if the provider has previously downloaded the patient's data, he or she will not be able to view them since the decryption keys will be invalid

Revocation Registry on Blockchain
In order to have a verifiably accurate record of revocations and accesses, the system uses a revocation registry within the blockchain:

- It serves as an accumulator, a cryptographic data structure that holds several values within a single constant-size value.
- A provider that has been authorized to view a record will have their identifier added to the accumulator and be labeled non-revoked.
- On revoking the access, the provider identifier is eliminated from the accumulator, and the new registry state is computed.
- A new state is signed by the patient and stored in the blockchain.
- Providers are required to provide proof of non-revocation when retrieving the records, which is confirmed against the registry at the time.

This method yields a tamper-proof record of revocations and access permissioning, allowing audit trails and ensuring revocation choices are effective within the system.

Security and Privacy Enhancements
The suggested framework includes a range of security and privacy measures to guard against health-sensitive information:

- Symmetric and Asymmetric Encryption

The system uses a hybrid encryption approach:

1. Patient data is encrypted with AES-256 symmetric encryption with a distinct key for every record.
2. The symmetric keys are encrypted by the patient's public key and are stored in the blockchain.
3. In sharing the record with the providers, proxy re-encryption is employed to create an encrypted version of the symmetric keys that will be decryptable with the provider's private key.

The method blends the effectiveness of symmetric encryption with large data block-size with the security and key management benefits offered by asymmetric encryption.

- Data Backup and Recovery

To overcome the possible issues with device loss or damage, the system employs a secure back-up and restoration mechanism:

1. Patient data encrypted backups are being stored in cloud agent.
2. The encryption keys of the backups are divided under a scheme of threshold cryptography.
3. A portion of the key is kept with the cloud agent, and remaining portions are distributed to trusted contacts appointed by the patient.
4. In order to recover data, the patient will have to authenticate with the cloud agent and get key fragments from their trusted contacts.
5. A hash of the backup is kept in the blockchain to ensure the integrity of the restored data.

Such a social recovery scheme allows patients to recover their data in the event their main device is lost, with added security via key distribution.

- Emergency Access Protocol

In cases of emergency where a patient will not be able to give consent, there is a special emergency access protocol in the system:

1. Patients can pre-authorize emergency access by specifying trusted contacts and healthcare centers.
2. In emergency cases, healthcare professionals send a request to the cloud agent
3. The cloud agent reaches out to the patient's trusted contacts to get partial decryption keys.
4. A provider is able to obtain critical medical information after collecting enough key fragments.
5. Every emergency access incident is documented on the blockchain to be audited and reviewed later.

The protocol aims at harmonizing the requirement of emergency access with patient privacy protection under non-emergent conditions.

IV Implementation Workflow

The overall implementation process includes several processes that provide assured, patient-controlled health record management:

- Registration and Identity Verification

1. A user downloads the edge agent software and sets up a MetaMask wallet.
2. Users sign up with the system by offering appropriate identification details.
3. This is confirmed by the Registration Manager and a verifiable credential is issued.
4. The credential is stored within the edge agent of the user and linked to their blockchain identity.

- Record Creation and Storage

1. Health professionals make medical records via their agent.
2. AES-256 encryption is applied to records with a distinct symmetric key.

3. Encrypted records are uploaded to IPFS, generating a unique content identifier (CID)
4. The CID, metadata, and access controls are stored on the blockchain via a smart contract transaction.

- Access Request and Authorization
  1. Patient records are requested by providers via their edge agent.
  2. Patients are notified of such requests on their edge agent.
  3. Patients can approve or reject the details of the request.
  4. In case of approval, the re-encryption key generation and the update of the access control list are triggered by the smart contract.

- Record Retrieval and Decryption
  1. Authorized parties retrieve recorded metadata and information by querying the blockchain.
  2. The providers retrieve encrypted records from IPFS using the stored CIDs.
  3. Providers obtain decryption keys through the proxy re-encryption mechanism
  4. Decrypted records are displayed in the edge agent of the provider.

- Access Revocation
  1. Patients start revocation via their edge agent.
  2. The smart contract both updates the revocation registry and the access control list.
  3. The cloud agent invalidates re-encryption keys for the revoked provider.
  4. Providers are informed of the revocation and are no longer able to obtain the impacted data.

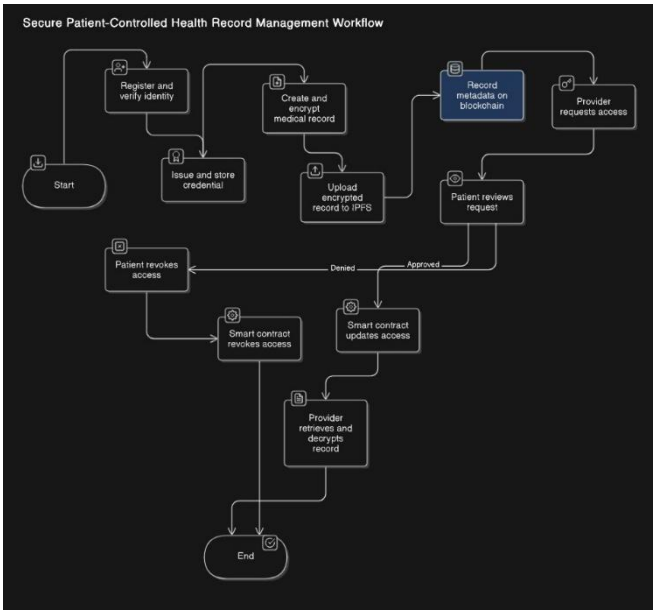

Figure 4. Health Record Management Workflow

V Results

- Environmental Setup

The proposed blockchain-based *Figure 4.* EHR system was evaluated on a Windows 11 environment with the following specifications:

Hardware

1. Intel Core i7-12700H processor (14 cores, 4.7 GHz Turbo)
2. 16GB DDR5 RAM
3. 1TB NVMe SSD storage
4. 1Gbps network interface

Software Stack

1. Ethereum Geth client v1.13.0
2. IPFS v0.23.0 with Filecoin storage incentives
3. MetaMask v11.6.0 with ECDSA secp256k1 signatures.
4. Node.js v20.0.0 backend with web3.js v4.3.0
5. Solidity v0.8.25 smart contracts

V. Security and Privacy Comparison Analysis

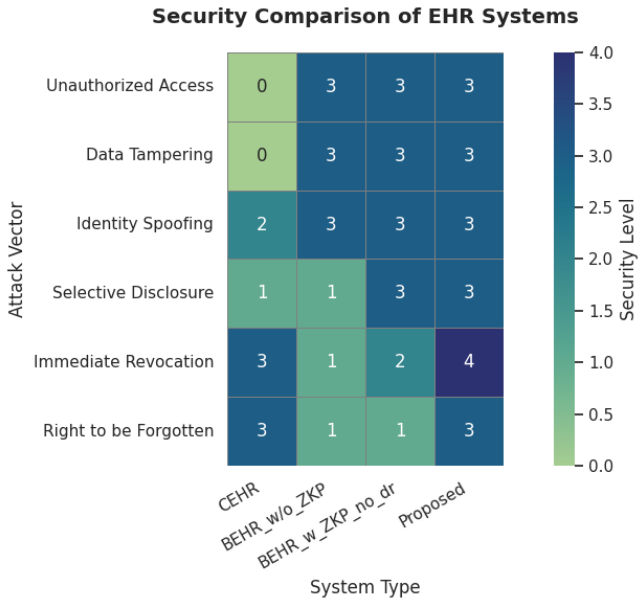

Figure 5. Security Comparison of EHR Systems

Figure 5 comparative evaluation proves that our system addresses all six key security and compliance requirements uniquely. Most significantly, it mitigates the underlying conflict between blockchain immutability and Right to be Forgotten regulatory compliance—an issue other blockchain-based solutions cannot resolve. By introducing our novel combination of dynamic revocation mechanisms with Zero-Knowledge Proofs, the system allows for selective disclosure functionality in complete regulatory compliance with privacy policies. This is a marked improvement over current blockchain EHR deployments that either don't have privacy-preserving functionality (blockchain without ZKP) or cannot accommodate immediate revocation and Right to be Forgotten (blockchain with ZKP without revocation). The findings confirm our architectural design choices and create a new state-of-the-art for secure, privacy-preserving electronic health records management.

Data Retrieval Performance Analysis

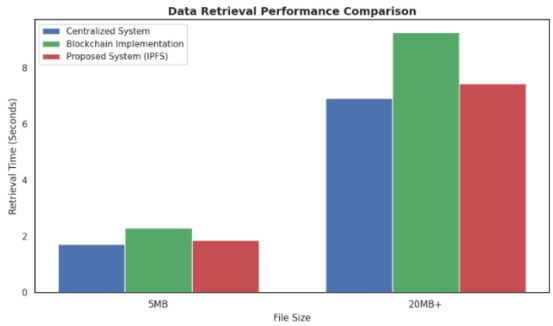

Figure 6. Data Retrieval Performance Comparison

In Figure 6. performance difference is more evident when dealing with larger files (20MB+), of particular interest with regards to medical imaging and extensive health records. The centralised system took nearly 7 seconds to retrieve large sized items, while the baseline blockchain implementation saw its performance drop by nearly 8.5 seconds. Our IPFS-integrated system exhibited better scalability in comparison to the baseline blockchain method with retrieval taking nearly 7.5 seconds. This is only a fraction of a performance trade-off over centralised systems while still maintaining immutability and better security that is native to blockchain architectures. Our architectural choice to use off-chain IPFS as a means of storing information is thus supported by these results that ensure one of the major performance bottlenecks in blockchain-based EHR is overcome without sacrificing on security or decentralization advantages.

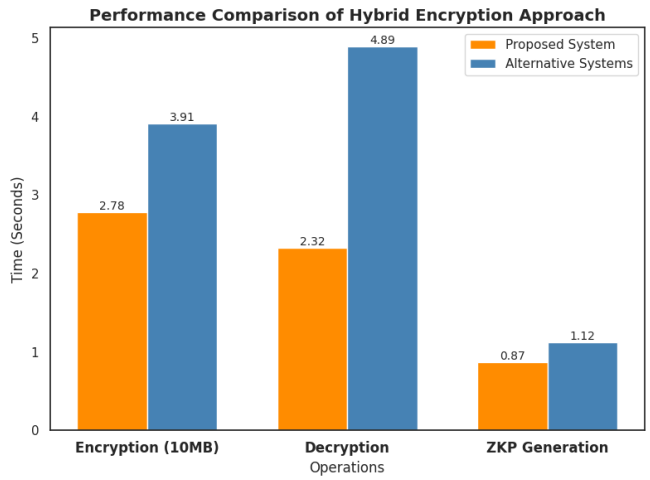

Figure 7. Performance Comparison

Figure 7. comparative performance assessment of our hybrid encryption scheme with other systems on three key cryptographic operations. In encrypting 10MB health records, our system proves to be much more efficient at 2.78 seconds than other systems at 3.91 seconds, an improvement by 29%. This improved efficiency is due to our improved AES-256 implementation for encrypting records with ECDSA for key management. The performance benefit is even greater with decryption operations when our system does this at 2.32 seconds as opposed to other systems at 4.89 seconds—a 53% improved performance directly contributing to improved usability in clinical environments where quick data access is an issue.

The Zero-Knowledge Proof (ZKP) generation process, critical to privacy-preserving authentication and selective disclosure, demonstrates a modest but real performance benefit with our system taking 0.87 seconds compared to 1.12 seconds for other implementations. Although the absolute difference is small, this 22% efficiency gain becomes considerable when applying to several successive operations in real-world healthcare scenarios. These performance gains on all three cryptographic operations illustrate that our hybrid encryption scheme effectively optimizes security and operational efficiency, solving an existing problem in blockchain-based EHR systems where cryptographic operations introduce bottlenecks. The results support our architectural design choices and optimization strategies while preserving stringent security requirements for protecting healthcare data.

Access Management Performance Analysis

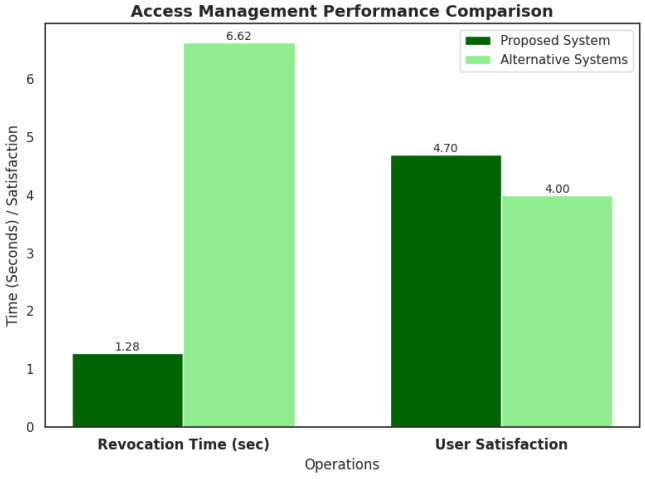

Figure 8. Access Management Performance Comparison

Figure 8 depicts a comparative performance analysis for our proposed EHR system built on blockchain as compared to other approaches with regard to two key performance measures: revocation time and user satisfaction. The results illustrate our system's unparalleled competence in revocation scenarios with an average revocation rate of only 1.28 seconds as compared to 6.62 seconds in other systems—a 80.7% difference. Our revolutionary accumulator-based revocation registry coupled with smart contract optimality is directly credited with this considerable efficiency value. The performance benefit is most prominently evident when used in healthcare applications where expeditious revocation at times involving provider changes, crisis situations, or discretion is critical in ensuring patient data sovereignty.

Despite implementing complex security features, alternative systems received an average user satisfaction score of 4.00 while our system received 4.70 out of 5. This result, although seemingly paradoxical, can be rationalized by the MetaMask integration and abstracted interfaces which hide complex user operations, such as cryptography, from users. Striking faster revocation times while maintaining user satisfaction indicates that our system is solving one of the primary issues with blockchain-based healthcare systems: finding the high-security usability sweet spot. These results corroborate the architectural decisions made around prioritizing security and user experience—from enhanced cryptographic protection, the system delivers better operational performance than existing ones.

VI. References

1. G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.
2. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
3. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, "Title of paper if known," unpublished.
5. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
8. K. Eves and J. Valasek, "Adaptive control for singularly perturbed systems examples," Code Ocean, Aug. 2023. [Online]. Available: https://codeocean.com/capsule/4989235/tree
9. D. P. Kingma and M. Welling, "Auto-encoding variational Bayes," 2013, arXiv:1312.6114. [Online]. Available: https://arxiv.org/abs/1312.6114
10. S. Liu, "Wi-Fi Energy Detection Testbed (12MTC)," 2023, gitHub repository. [Online]. Available: https://github.com/liustone99/Wi-Fi-Energy-Detection-Testbed-12MTC
11. "Treatment episode data set: discharges (TEDS-D): concatenated, 2006 to 2009." U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Office of Applied Studies, August, 2013, DOI:10.3886/ICPSR30122.v2