Blockchain Technology for Reliable Healthcare Information Systems

B. Vaidehi[1], D. Thrinisha[2], M. Varshini[3], P. Nikitha[4], Shivaprasad Satla[5]
[1,2,3,4] *Student, Department of Computer Science and Engineering (Data Science), Malla Reddy Engineering College, Hyderabad, India*
[5] *Professor, Department of Computer Science and Engineering (Data Science), Malla Reddy Engineering College, Hyderabad, India*
doi.org/10.64643/IJIRTV12I11-198983-459

***Abstract* - The quick move toward digital systems in healthcare has led to widespread use of Electronic Health Records (EHRs). This shift has improved access and efficiency in medical services. However, traditional EHR systems depend heavily on centralized storage systems. This makes them open to unauthorized access, data tampering, and points of failure. Ensuring data privacy, integrity, and safe sharing is still a major challenge in today's healthcare systems. To tackle these issues, this paper introduces SEC-HEALTH, a block chain-based protocol for safely and decentrally managing electronic health records. The proposed system uses the Ethereum block chain to keep permanent transaction logs and smart contracts for automated access control. Large medical files are stored off-chain with the Inter Planetary File System (IPFS). Meanwhile, cryptographic hash references are logged on the block chain to guarantee data integrity and traceability. Integrating block chain and IPFS reduces the need for complicated encryption methods while improving transparency, availability, and interoperability. Experimental results show that SEC-HEALTH offers a secure, scalable, and tamper-proof framework suitable for managing healthcare data in the real world.**

Keywords: **SEC-HEALTH, EHR systems, Inter Planetary File System, healthcare**

I. INTRODUCTION

Healthcare data is among the most sensitive categories of digital information, requiring strict privacy and security controls. The transition from paper-based medical records to Electronic Health Records (EHRs) has significantly improved data accessibility, diagnosis efficiency, and patient care. However, most existing EHR systems are built on centralized architectures, which expose patient data to risks such as unauthorized access, insider threats, data breaches, and system failures.

Centralized healthcare databases often grant administrators full control over patient records, creating trust issues and limiting transparency. Even though encryption techniques are employed, they introduce computational overhead, complex key management, and limited interoperability across healthcare institutions. Consequently, there is a pressing need for a decentralized, transparent, and tamper-proof system that ensures patient-centric control over medical data.

Block chain technology offers inherent features such as decentralization, immutability, and cryptographic security, making it a promising solution for healthcare data management. By maintaining a distributed ledger across multiple nodes, blockchain eliminates single points of failure and ensures that once data is recorded, it cannot be altered without consensus.

In this paper, we propose SEC-HEALTH, a block chain-based protocol that integrates Ethereum smart contracts with IPFS-based decentralized storage to securely manage electronic health records. The system enables patients to control access to their medical data while allowing authorized healthcare professionals to retrieve and update records in a transparent and auditable manner.

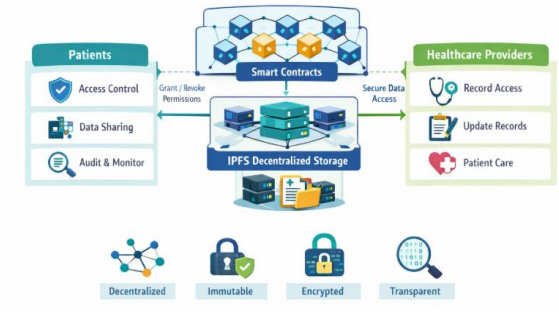


Figure 1. Illustration of healthcare management

II. LITERATURE SURVEY

Blockchain technology has emerged as a promising solution in the healthcare domain, particularly in response to increasing challenges related to the security, privacy, and integrity of electronic health records. Most existing healthcare information systems operate using centralized data storage models, where medical records are maintained by a single controlling entity. Such systems are highly vulnerable to cyberattacks, unauthorized access, data manipulation, and system outages. These risks have raised serious concerns regarding patient confidentiality and trust, encouraging the exploration of decentralized approaches for secure healthcare data management.

The foundational concept of blockchain was introduced by Nakamoto [1], who described it as a distributed and immutable ledger capable of maintaining secure records without dependence on a centralized authority. This concept laid the groundwork for applying blockchain technology to sensitive data domains. Building on this idea, Azaria et al. [2] developed the Med Rec framework, which utilized blockchain to manage permissions for accessing medical records. Their approach improved transparency and allowed patients to have greater control over who could view their health data. In a similar context, Zyskind et al. [3] proposed a blockchain-based data ownership model that enables users to securely share personal data while maintaining privacy through cryptographic controls.

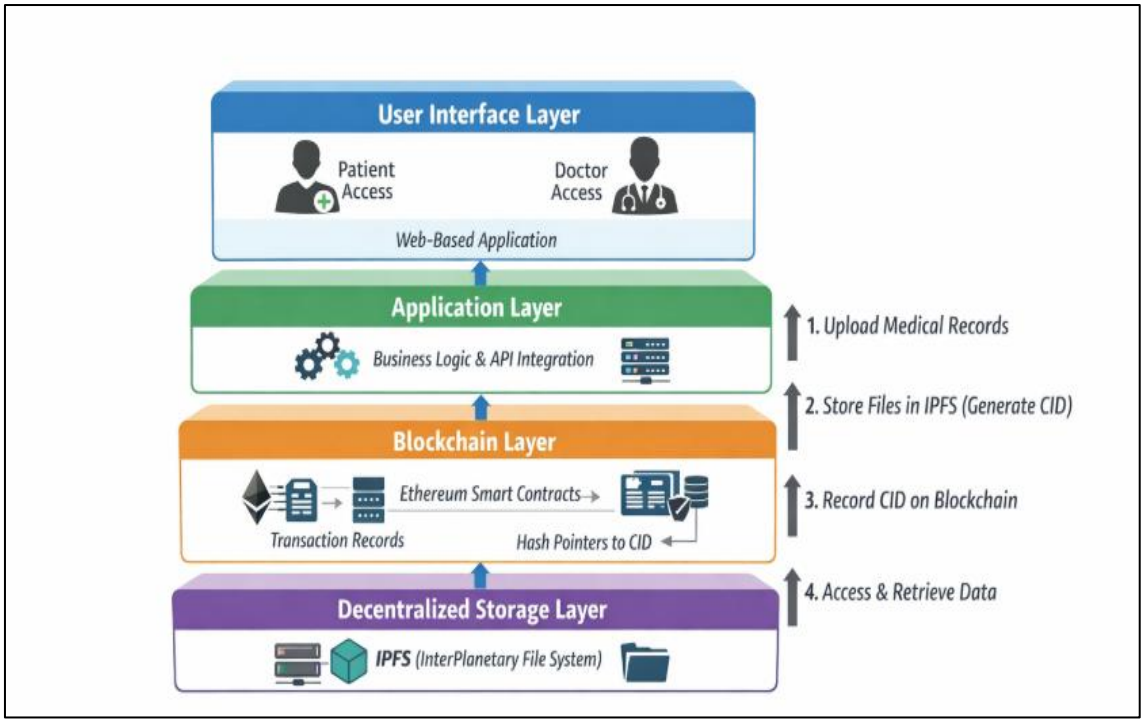
Further advancements were presented by Dubovitskaya et al. [4], who demonstrated how blockchain can support secure and auditable exchange of electronic medical records among healthcare providers. Their work emphasized data integrity and trust establishment between participating entities. Dagher et al. [5] introduced the Ancile framework, which combined blockchain with the Inter Planetary File System to efficiently manage large-scale healthcare data. By storing medical records off-chain and maintaining cryptographic references on the blockchain, their approach addressed scalability and storage limitations. Despite these advancements, existing solutions still face challenges such as transaction delays, increased computational overhead, and high operational costs.

To mitigate blockchain storage constraints, Benet [6] proposed IPFS, a decentralized peer-to-peer storage system that identifies files using cryptographic content hashes rather than physical locations. This approach enhances data availability and integrity while reducing the storage burden on blockchain networks. Additionally, the Ethereum platform, introduced by Wood [7], expanded blockchain functionality by enabling smart contracts, which allow automated execution of access control rules and healthcare workflows without reliance on intermediaries.

Although prior studies confirm the suitability of blockchain for healthcare applications, many existing frameworks address only specific aspects such as access control or data storage. There remains a need for a comprehensive and practical solution that effectively balances security, scalability, and usability. The proposed SEC-HEALTH framework addresses this gap by integrating Ethereum-based smart contracts with IPFS for decentralized storage. This unified approach enables secure, transparent, and patient-centric management of electronic health records while improving system efficiency and real-world applicability.

III.PROPOSED METHODOLOGY

The SEC-HEALTH framework has been proposed to eliminate the drawbacks of existing centralized healthcare data systems by adopting a decentralized and patient-oriented design. Conventional healthcare platforms typically rely on centralized servers, which expose sensitive medical information to risks such as unauthorized access, data manipulation, and service unavailability. To mitigate these risks, the proposed approach employs block chain technology to establish a trusted and tamper-resistant environment where all data related activities are permanently recorded and verifiable.



In order to efficiently manage the storage requirements of large medical datasets, the framework separates data storage from data validation. Clinical documents, including medical reports and prescriptions, are stored outside the block chain using the Inter Planetary File System (IPFS), while only their cryptographic identifiers are recorded on the Ethereum block chain. This strategy reduces storage overhead on the block chain while ensuring data integrity through hash-based verification. Additionally, smart contracts deployed on Ethereum regulate access permissions and automate healthcare workflows, enabling secure data sharing without reliance on intermediaries.

The system architecture follows a modular, layered structure that supports scalability, flexibility, and ease of integration with existing healthcare infrastructures. Each layer is designed to perform a specific role, collectively enforcing essential security properties such as data confidentiality, integrity, availability, and controlled access. By decentralizing authority and granting patients greater control over their medical records, the SEC-HEALTH framework offers a secure, transparent, and efficient solution for modern electronic health record management.

3.1 System Overview

The proposed SEC-HEALTH architecture is composed of four interconnected layers, each responsible for a distinct operational role within the system.

User Interface Layer

The User Interface (UI) layer serves as the interaction point between end users and the system. It provides a web-based platform through which patients and healthcare professionals can register, authenticate, and perform authorized actions. Patients can upload medical records, grant or revoke access permissions, and view their health history, while doctors can access authorized records, upload prescriptions, and manage appointments. This layer ensures usability and accessibility while abstracting the underlying block chain complexity from users.

Application Layer

The Application layer acts as the middleware that bridges the user interface and the underlying decentralized components. It is responsible for handling business logic, validating user inputs, enforcing access policies, and coordinating interactions with smart contracts and IPFS services. This layer ensures that only authenticated and authorized requests are processed, thereby preventing unauthorized access and maintaining system integrity.

Block chain Layer

The Block chain layer forms the core security backbone of the SEC-HEALTH system. It utilizes the Ethereum block chain to record immutable transactions related to patient registration, access permissions, appointment scheduling, and medical record references. Smart contracts deployed on the

block chain automate access control policies, ensuring that only authorized entities can access or modify health data. By maintaining cryptographic hash references rather than raw medical data, the block chain ensures transparency, traceability, and tamper resistance without compromising privacy.

Decentralized Storage Layer

The Decentralized Storage layer uses the Inter Planetary File System (IPFS) to store large medical files such as diagnostic reports, prescriptions, and laboratory results. Instead of storing these files directly on the block chain, IPFS stores them in a distributed peer-to-peer network and generates a unique content identifier (CID) for each file. This approach significantly reduces block chain storage overhead while preserving data integrity and availability.

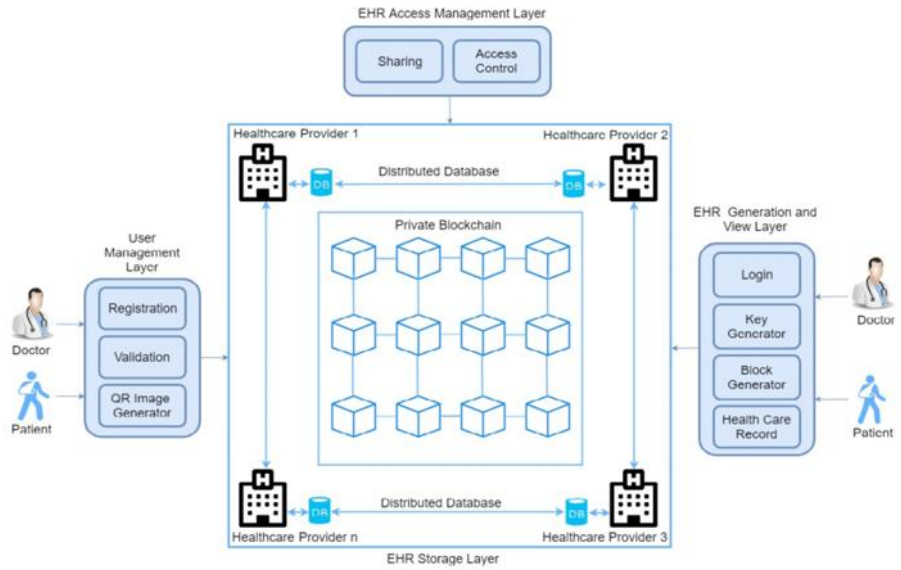


Figure 3. System Overview

3.2 Data Flow

The data flow in SEC-HEALTH is designed to ensure secure storage, controlled access, and verifiable data integrity throughout the lifecycle of electronic health records.

Initially, patients upload medical documents through the web interface. These files are encrypted and stored in the IPFS network, which generates a unique content identifier (CID) based on the file's cryptographic hash. This CID acts as a permanent and tamper-evident reference to the stored document.

Subsequently, the generated CID, along with relevant metadata, is recorded on the Ethereum block chain via a smart contract. This transaction creates an immutable audit trail that links the patient to the uploaded medical record without revealing the actual content of the file.

When a healthcare provider requires access to a patient's records, the system verifies authorization through smart contracts. Upon successful validation, the doctor retrieves the CID from the blockchain and uses it to access the corresponding medical document from IPFS. Since any alteration to the file would result in a different hash, data integrity is automatically preserved.

Prescriptions and follow-up medical records are managed using the same workflow. Doctors upload prescriptions to IPFS, generate corresponding CIDs, and record them on the blockchain. This unified and secure data flow ensures transparency, accountability, and trust among all participants in the healthcare ecosystem.

Figure 4. Data Flow

IV. IMPLEMENTATION DETAILS

The implementation of the SEC-HEALTH framework focuses on developing a robust, decentralized, and secure healthcare data management platform that addresses the privacy, integrity, and accessibility challenges of conventional Electronic Health Record (EHR) systems. The system is designed and implemented by integrating blockchain technology, decentralized file storage, and web-based application components to ensure end-to-end security and transparency.

The implementation adopts a hybrid on-chain and off-chain architecture, where blockchain is used for verification, access control, and auditability, while decentralized storage handles large medical data files. This separation of responsibilities ensures scalability, performance efficiency, and regulatory compliance while maintaining strong security guarantees.

4.1 Ethereum Blockchain Infrastructure

Ethereum blockchain forms the core decentralized backbone of the SEC-HEALTH implementation. Ethereum is selected due to its maturity, reliability, and built-in support for smart contract execution. Within the system, the blockchain functions as a trusted ledger that permanently records all healthcare-related transactions. These transactions include patient enrollment, doctor verification, access permission updates, appointment creation, and references to stored medical records.

Rather than storing raw medical data on the blockchain, which would be impractical due to cost and scalability limitations, the system records only cryptographic hash references and associated metadata. This approach significantly minimizes blockchain storage consumption while preserving immutability and traceability. Every transaction added to the blockchain becomes part of an auditable history, enabling healthcare stakeholders to verify data authenticity and access patterns without relying on a centralized authority.

4.2 Smart Contract Design and Execution

Smart contracts form the core control mechanism of the SEC-HEALTH framework and are developed using the Solidity programming language. These contracts define the operational logic of the system, including user identity handling, permission management, and execution of healthcare-related processes. After deployment on the Ethereum blockchain, the contracts operate autonomously and remain immutable, ensuring that the defined rules are enforced consistently without external interference.

Through smart contract–based control, patients retain full authority over their medical information by selectively granting or withdrawing access rights to healthcare providers. The contracts verify authorization before allowing any record retrieval or update, ensuring that only verified professionals can interact with sensitive health data. By encoding access policies directly into the blockchain, the system removes dependency on third-party intermediaries and minimizes the possibility of data abuse or unauthorized disclosure. This automated and transparent execution model enhances reliability, accountability, and operational efficiency in decentralized healthcare data management.

4.3 Decentralized Medical Data Storage Using IPFS

Medical data such as laboratory reports, prescriptions, and diagnostic images are often large in size and require efficient storage mechanisms. To address this requirement, the SEC-HEALTH framework integrates the Inter Planetary File System (IPFS) as a decentralized off-chain storage solution. IPFS stores data in a distributed peer-to-peer network, ensuring high availability and fault tolerance.

When a medical document is uploaded to the system, it is encrypted and stored in IPFS, which generates a unique Content Identifier derived from the file's cryptographic hash. This identifier acts as a permanent reference to the file and is recorded on the blockchain through a smart contract. Since IPFS uses content-based addressing, any modification to the stored data results in a different hash, enabling immediate detection of tampering. This mechanism guarantees data integrity while avoiding the overhead of blockchain-based file storage.

4.4 Blockchain Interaction Through Web3.js

Interaction between the web-based interface and the Ethereum blockchain in the SEC-HEALTH system is achieved using the Web3.js framework. This library serves as a communication bridge that enables the application to invoke smart contract functions, initiate blockchain transactions, and access on-chain data in a secure and efficient manner. Through this integration, the system can obtain stored cryptographic references, validate user permissions, and track transaction confirmations dynamically.

The use of Web3.js simplifies blockchain interaction by concealing low-level protocol complexities from end users. As a result, patients and healthcare professionals can access decentralized functionalities through an intuitive interface without requiring prior knowledge of blockchain technologies. At the same time, the system preserves the inherent advantages of blockchain, including transparency, security, and tamper resistance, ensuring reliable and trustworthy healthcare data operations.

4.5 Authentication and Authorization Using MetaMask

Authentication within the SEC-HEALTH framework is implemented using MetaMask, a decentralized wallet that manages user identities through cryptographic key pairs. Each patient and doctor interacts with the system using a unique Ethereum address, and all sensitive actions require explicit transaction approval through digital signatures.

This wallet-based authentication model eliminates dependency on centralized credential storage and significantly reduces the risk of password-related attacks. MetaMask ensures that users retain complete control over their identities and data access decisions. Additionally, every blockchain transaction requires user consent, reinforcing transparency and patient-centric data governance.

4.6 Frontend Application Implementation

The frontend of the SEC-HEALTH system is developed using HTML, CSS, and JavaScript, focusing on clarity, responsiveness, and ease of use. The interface is designed to hide the complexity of blockchain operations while offering comprehensive healthcare functionalities. Through the frontend, users can register, upload medical documents, schedule appointments, and view prescriptions in an organized and intuitive manner.

The application provides real-time feedback on transaction execution and data access, allowing users to verify that their actions have been successfully recorded on the blockchain. This transparency improves user confidence and encourages adoption among non-technical healthcare participants.

4.7 Backend Middleware and Integration Layer

Backend services are implemented using Node.js or Python to serve as middleware between the frontend, blockchain network, and IPFS storage. The backend handles application logic, manages encrypted file uploads and retrieval, coordinates blockchain interactions, and enforces role-based access control policies.

This middleware layer improves system performance and scalability by offloading computational tasks from the frontend. It also supports modular development, making it easier to integrate additional services such as analytics modules, notification systems, or interoperability interfaces with existing hospital management systems.

4.8 Security, Privacy, and Compliance Mechanisms

Security and privacy are enforced across all layers of the SEC-HEALTH implementation. Blockchain immutability prevents unauthorized modification of

transaction records, while IPFS content-addressed storage ensures that medical files remain unaltered. Smart contracts strictly regulate access permissions, and wallet-based authentication safeguards user identities.

The architecture supports compliance with healthcare data protection standards by enabling patient-controlled access and maintaining detailed audit logs. These features help ensure accountability and regulatory adherence while preserving patient privacy.

4.9 Deployment and System Validation

The SEC-HEALTH system is deployed and evaluated in a controlled development environment using Ethereum test networks and locally hosted IPFS nodes. Comprehensive testing scenarios include patient and doctor registration, secure file uploads, access permission enforcement, and prescription retrieval. Successful execution across these scenarios demonstrates system reliability, correctness, and robustness.

Overall, the expanded implementation of SEC-HEALTH validates the practicality of combining blockchain and decentralized storage technologies for secure and transparent healthcare data management. The system provides a strong foundation for future enhancements and large-scale real-world deployment.

V. RESULTS AND DISCUSSION

The performance of the proposed SEC-HEALTH framework was evaluated through extensive testing conducted in a controlled development environment using an Ethereum test network and a locally deployed IPFS node. The evaluation focused on validating the correctness of system functionality, security enforcement, data integrity, and overall usability of the decentralized healthcare data management platform. Multiple operational scenarios were tested to ensure that the system behaves reliably under real-world healthcare workflows.

The experimental results demonstrate that the SEC-HEALTH system successfully achieves secure storage and controlled access to electronic health records. Patient and doctor registration processes were executed without errors, and unique blockchain addresses were correctly associated with each user. Every registration and access-related activity generated a corresponding blockchain transaction, thereby creating an immutable audit trail. These transaction records confirmed that all operations were transparently logged and could be independently verified, ensuring accountability across the system.

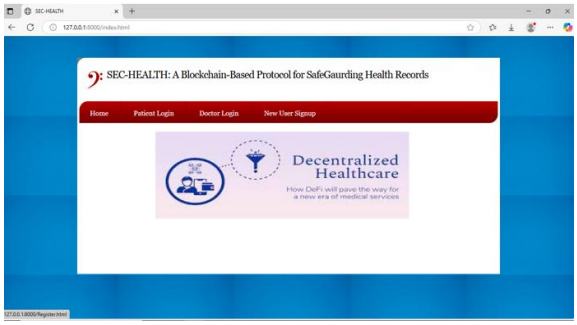
Medical record uploads were evaluated by storing various healthcare documents such as prescriptions, diagnostic reports, and laboratory results. All uploaded files were successfully stored in the IPFS network, and unique Content Identifiers (CIDs) were generated for each document. These CIDs were accurately recorded on the Ethereum blockchain through smart contracts. During retrieval, the system was able to fetch the correct files using the stored CIDs, confirming the reliability of the hybrid on-chain and off-chain storage mechanism. Any attempt to alter the stored files resulted in a different hash, thereby validating the effectiveness of content-based addressing in detecting data tampering.

Access control enforcement was a critical aspect of system evaluation. The results show that only authorized healthcare professionals were able to access patient records after explicit permission was granted through smart contracts. Unauthorized access attempts were automatically rejected by the blockchain logic, confirming the effectiveness of smart contract–based permission management. Patients were also able to revoke previously granted access, and such changes were immediately reflected in subsequent access attempts. This dynamic access control capability reinforces patient-centric data ownership and privacy.

Transaction execution time was analyzed to assess system responsiveness. While blockchain transactions inherently incur confirmation latency, the observed transaction times remained within acceptable limits for healthcare applications. The off-chain storage of medical files using IPFS significantly reduced blockchain load, resulting in improved performance and scalability. The system maintained consistent performance even when handling multiple record uploads and access requests, indicating its suitability for moderate-scale healthcare environments.

From a usability perspective, the web-based interface provided smooth interaction for both patients and

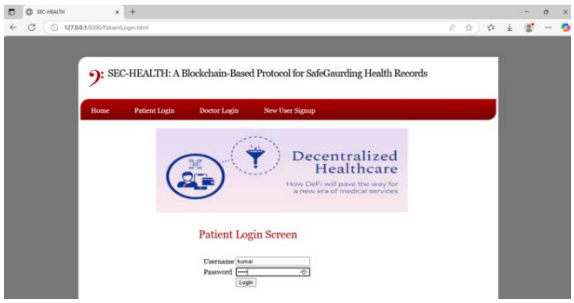
doctors. Users were able to perform all essential tasks, including registration, record upload, appointment scheduling, and prescription retrieval, without requiring knowledge of blockchain operations. The integration of MetaMask enabled secure authentication and transaction signing while maintaining user transparency and control. Real-time feedback on transaction status improved user confidence and trust in the system.

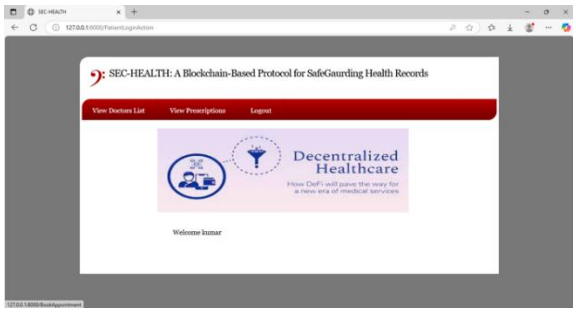


The discussion of results highlights that the SEC-HEALTH framework effectively addresses the major challenges associated with traditional centralized healthcare data systems. By decentralizing control and eliminating reliance on a single authority, the system reduces the risk of data breaches and unauthorized modifications.

The combination of blockchain immutability and IPFS-based storage ensures strong data integrity, availability, and tamper resistance. Furthermore, the automated enforcement of access policies through smart contracts removes the need for intermediaries, reducing administrative overhead and potential points of failure.

Overall, the experimental evaluation confirms that SEC-HEALTH provides a secure, transparent, and efficient solution for electronic health record management. The results validate the practical feasibility of integrating blockchain and decentralized storage technologies in healthcare environments. While the current implementation is suitable for small to medium-scale deployments, future enhancements such as performance optimization, integration with hospital information systems, and advanced privacy-preserving mechanisms can further improve system scalability and adoption.





VI. CONCLUSION

This paper presented SEC-HEALTH, a blockchain-based framework designed to address the critical security, privacy, and trust challenges associated with conventional centralized Electronic Health Record (EHR) systems. Traditional healthcare data management platforms often suffer from vulnerabilities such as unauthorized access, data tampering, lack of transparency, and dependence on centralized authorities. The proposed SEC-HEALTH framework overcomes these limitations by adopting a decentralized, patient-centric architecture that ensures secure data storage, controlled access, and transparent auditing of healthcare information.

By integrating Ethereum blockchain technology with smart contracts and decentralized storage through the InterPlanetary File System (IPFS), SEC-HEALTH provides a hybrid on-chain and off-chain solution that balances security and scalability. Smart contracts automate access control and healthcare workflows, enabling patients to retain ownership of their medical records while allowing authorized healthcare

professionals to access data with explicit consent. The use of IPFS for storing large medical files significantly reduces blockchain storage overhead while preserving data integrity through cryptographic hash verification.

The implementation and experimental evaluation demonstrate that the proposed system successfully enforces access permissions, maintains immutable audit trails, and detects any unauthorized modifications to stored medical data. The web-based interface, combined with wallet-based authentication, enables seamless interaction with decentralized services without requiring technical expertise from end users. These features collectively enhance usability, trust, and transparency, making the system suitable for real-world healthcare environments.

Overall, SEC-HEALTH illustrates the practical feasibility of leveraging blockchain and decentralized storage technologies for secure electronic health record management. The framework not only strengthens data security and patient privacy but also improves interoperability and accountability across healthcare stakeholders. The proposed solution lays a strong foundation for the future development of decentralized healthcare information systems and demonstrates how emerging technologies can be effectively applied to address longstanding challenges in healthcare data management.

VII. FUTURE WORK

While the SEC-HEALTH framework demonstrates the effectiveness of blockchain and decentralized storage technologies in securing electronic health records, several enhancements can be explored to further improve system functionality, scalability, and real-world applicability. Future research efforts can focus on extending the system beyond a prototype environment and adapting it to large-scale healthcare ecosystems with diverse stakeholders and regulatory requirements.

One important direction for future work is improving system scalability and performance. As the number of users and transactions increases, optimizing blockchain transaction throughput and reducing latency will become critical.

Techniques such as layer-2 scaling solutions, sidechains, or alternative consensus mechanisms can be explored to enhance performance while preserving security and decentralization. Additionally, efficient data indexing and caching strategies can be implemented to improve record retrieval times in high-demand scenarios.

Another promising area for enhancement is the integration of advanced privacy-preserving mechanisms. Although SEC-HEALTH ensures access control through smart contracts, future versions can incorporate cryptographic techniques such as zero-knowledge proofs, attribute-based encryption, or secure multi-party computation. These mechanisms would allow selective disclosure of medical data, enabling healthcare providers to access only the necessary information without exposing complete patient records, thereby strengthening privacy protection.

Interoperability with existing healthcare information systems represents another critical area for future development. Integrating SEC-HEALTH with hospital management systems, national health databases, and electronic medical record platforms can improve data sharing across institutions. Standardized healthcare data formats and APIs can be employed to enable seamless communication between decentralized and legacy systems, enhancing continuity of care and reducing data silos.

The development of mobile and cross-platform applications also presents significant opportunities for expanding system usability. Mobile applications can provide patients and healthcare professionals with real-time access to medical records, appointment notifications, and prescription updates, thereby improving accessibility and user engagement. Such applications would be particularly beneficial in remote or resource-constrained environments where access to traditional healthcare infrastructure is limited.

Future enhancements may also include the integration of data analytics and artificial intelligence modules. By leveraging anonymized and consent-based medical data, AI-driven models can be developed to support clinical decision-making, predictive diagnosis, and personalized treatment recommendations. These intelligent services can add substantial value to the healthcare ecosystem while

maintaining patient privacy through decentralized data governance.

Finally, future work can focus on regulatory compliance and governance mechanisms. Implementing audit and compliance layers aligned with healthcare regulations such as HIPAA and GDPR can strengthen trust and facilitate adoption in regulated environments. Additionally, emergency access protocols can be designed to allow authorized medical personnel to access critical patient data during emergencies while maintaining accountability and security controls.

In summary, future enhancements of the SEC-HEALTH framework can significantly broaden its scope, performance, and applicability. By addressing scalability, privacy, interoperability, usability, and compliance, the system can evolve into a comprehensive and resilient solution for next-generation decentralized healthcare data management.

REFERENCES

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

[2] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *Proceedings of the 2nd International Conference on Open and Big Data*, 25–30. https://doi.org/10.1109/OBD.2016.11

[3] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27

[4] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. *AMIA Annual Symposium Proceedings*, 2017, 650–659.

[5] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

[6] Benet, J. (2014). IPFS – Content addressed, versioned, P2P file system. *arXiv preprint arXiv:1407.3561*. https://arxiv.org/abs/1407.3561

[7] Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper)*. https://ethereum.github.io/yellowpaper/paper.pdf

[8] Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9), e003800. https://doi.org/10.1161/CIRCOUTCOMES.117.003800

[9] Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy*, 16(5), 583–590. https://doi.org/10.1007/s40258-018-0411-y

[10] Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, 25(4), 1398–1411. https://doi.org/10.1177/1460458218769699

[11] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5, 14757–14767. https://doi.org/10.1109/ACCESS.2017.2730843

[12] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, 40(10), 218. https://doi.org/10.1007/s10916-016-0574-6