ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (38-44), Month: October 2025 – March 2026, Available at: www.paperpublications.org

An efficient EHR sharing model using blockchain and decentralised storage technologies

[1]Mr. Nitish, [2]Mr. Anuj Kumar Sharma, [3]Mr. Kamal Kumar, [4]Mr. Bharat Kumar, [5]Mr. Kunal Yadav

[1](Assistant Professor), Galgotias College of Engineering & Technology

[2,3,4,5,] Galgotias College of Engineering & Technology

DOI: https://doi.org/10.5281/zenodo.18724447

Published Date: 21-February-2026

Abstract: **Due to issues with respect to security breaches and expensive storage capacity, the secure sharing and maintenance of Electronic Health Records (EHRs) remains a concern within the healthcare industry. To ensure mystery, versatility, and reliability in sharing information, this article gives an successful EHR sharing view based on blockchain and decentralized storage technologies. It includes smart contracts, proxy re-encryption, and a hybrid on-chain/off-chain architecture to the Blockchain-based Secure Access and Sharing (BCAS) system. This strategy integrates Filecoin as a decentralized, incentive-driven storage layer to ensure tough and verifiable data availability, in contrast to conventional IPFS-only solutions. Filecoin and IPFS manages the storage of encrypted medical data, whereas Blockchain handles identity verification, access control, and transaction auditing.**

Smart contracts ensure the transparency and confidential ownership of health data by automating access tracking and authorization administration. Security testing verified the system's defenses against common threats like DDoS, spoofing and MITM attacks. When compared to current blockchain-based EHR systems, the performance evaluation demonstrates extraordinary throughput, low computational overhead, and faster recovery. The proposed approach provides an effective, secure, and patient-focused solution for EHR data management and sharing among healthcare centers using Filecoin's decentralized economy with immutability of blockchain.

Keywords: **InterPlanetary File System (IPFS), Filecoin, Secure Data Sharing, Smart Contracts, Electronic Health Records (EHR), Blockchain Technology.**

1. INTRODUCTION

Electronic Health Records (EHRs), which facilitate effective medical data sharing, accurate diagnoses and better patient outcomes, are being utilized more regularly as a result of the healthcare industry's rapid digital transformation. However, the sensitive nature of medical information raises critical issues regarding scalability, security, and privacy. Unauthorized access, data manipulation, and single-point failures are common with conventional centralized EHR organization frameworks. Since of its decentralization, immutability, and transparency, blockchain innovation has pulled in a part of consideration as a arrangement to these issues. By utilizing smart contracts and proxy reencryption for secure and traceable EHR sharing, the Blockchain-based Secure Access and Sharing (BCAS) engineering displayed a potential.

Despite its advantages, the BCAS paradigm faces several drawbacks. For off-chain data storage, it generally depends on IPFS, which lacks both the financial incentives and guaranteed data durability. Moreover, BCAS's implementation is reliant on resource-intensive cryptographic processes, and it has scalability issues when managing large volumes of medical data. Besides, its practical deployment in large-scale healthcare systems is limited by the lack of incentive mechanisms for data providers and the insufficient reduction of storage costs.

This study recommends an effective EHR sharing methodology utilizing blockchain and decentralized storage technologies to address these issues. By combining Filecoin's incentive-driven plan with IPFS, the proposed arrangement enhances BCAS and ensures secure, cost-effective, and durable for long term. The technique improves scalability, ensures patient privacy, and strengthens the robustness and effectiveness of healthcare data exchange by combining smart contracts, proxy re-encryption, and hybrid on-chain/off-chain mechanisms.

2. PROBLEM STATEMENT

The healthcare industry's move toward digital technology has led to the widespread use of Electronic Health Records(EHRs). These records allow medical facilities to easily store, manage and communicate patient data across various platforms. EHRs encourage clinical workflows, increase collaboration among providers, and improves the accuracy of diagnoses. However, as the volume and sensitivity of medical data continue to grow, maintaining the security and scalability of EHR systems has ended up a major concern. Centralized healthcare databases have big weaknesses. They face threats like data being secretly altered, illegal access to records and the danger of the whole system collapsing if a single component fails. These failures undermine patient privacy and weaken confidence in modern digital healthcare.

Blockchain technology's decentralization, permanence, and traceability have made it a game-changer for healthcare information administration. Various inquire about have appeared how blockchain can ensure EHR capacity and give patient-controlled get to utilizing savvy contracts and intermediary reencryption. One such think about is the Blockchain-based protect Access and Sharing (BCAS) conspire. In spite of the fact that BCAS viably makes strides security and straightforwardness, its far reaching utilize is still compelled by viable issues. In spite of the fact that successful conveyance is made conceivable by its reliance on the InterPlanetary Record Framework (IPFS) for off-chain capacity, long-term steadfastness and information lastingness are not ensured. Framework execution is assist hampered by the tall computational cost of keen contract execution and the need of motivating force components for information providers. Overseeing expansive restorative datasets over a few colleges too presents versatility challenges.

A more successful and long-lasting blockchain-based EHR sharing approach is frantically required to urge over these limitations. By consolidating Filecoin, a decentralized and incentive-driven capacity arrange based on IPFS, into the EHR organization method, this ponder fills in these gaps. The arrangement proposes a secure, conservative, and patientfocused EHR exchange system by melding blockchain innovation, smart contracts, proxy re-encryption, and Filecoin-based storage.

3. OBJECTIVE

The primary objective of this project is to utilize blockchain and decentralized capacity innovations to provide an effective, secure, and decentralized framework for sharing and storing Electronic Health Records (EHRs). The proposed architecture overcomes the scalability and cost challenges of current blockchain healthcare systems, resulting in improved data security, privacy, and strength. The study extends the BCAS framework by utilizing Filecoin as an incentive-driven decentralized storage solution to ensure long-term data availability and verifiable persistence compared to old IPFS methods. Through smart contracts and intermediary re-encryption, the architecutre makes a patient-centric environment where individuals keep up total ownership of their health information and can control access rights, permitting for fine-grained, secure exchange with authorized institutions. The hybrid architecture ensures transparency, scalability and confidentiality, while Filecoin's incentive structure supports network stability and long-term data sustainability. Also, the investigate points to maximize framework execution by minimizing vitality utilization, idleness, and computing overhead without relinquishing security. Intensive examinations will affirm that the framework is safe to attacks like man-in-the-middle, spoofing, and DDoS. The model's extreme objective is to supply a versatile, privacy-preserving, and monetarily reasonable EHR sharing arrangement that advances believe and interoperability in decentralized healthcare healthcare ecosystems.

4. RELATED WORK

Broad think about into blockchain-based Electronic Health Record (EHR) frameworks with the objective of progressing information security, judgment, and decentralized administration has been provoked by later advancements in healthcare information administration. In spite of the fact that a number of inquire about have made a considerable commitment to the advancement of secure and adaptable EHR sharing systems, a number of issues still ought to be tended to.

In arrange to secure EHR sharing through keen contracts and intermediary reencryption, the Blockchain-based Secure Access and Sharing (BCAS) plot recommended a half breed on-chain/off-chain engineering utilizing blockchain and IPFS. BCAS has issues with adaptability, solidness, and capacity motivating forces indeed in the event that it improved get to control and mystery. In a comparable vein, Ramesh et al. (2023) displayed TAC-EHR, a tamper-proof EHR concept that combines decentralized IPFS-based cloud capacity with blockchain innovation. In spite of the fact that their arrangement utilized blockchain exchanges to ensure information unchanging nature, mystery, and astuteness, it was all things considered tormented by over the top computational taken a toll, a need of long-term capacity confirmations, and dependence on exterior cloud administrations.[3], [5]

Blockchain and IPFS were brought together in the work of Alsabaan and others. Decentralized login and safe sharing of information. File Storage (2025) idea for sharing files across different locations. Verifying identities in healthcare systems. It seems your message got cut off. Could you please provide the full text that you'd like me to rewrite in simple words. lowered risks of problems and made things better Scalability was still limited by high transaction costs. high costs and poor motivation systems for the long term Data availability means that information is accessible and can be reached when needed. In the same way, by using edge nodes and. fast agreement methods to reduce delay Using up bandwidth, the Blockchain-Based Electronic Health Record (EHR) For Edge Computing (2024), the focus is on important design choices. safety and affordable prices. Even though it went up computing speed and how fast you can get data, it had issues with different systems working together and keeping data forever.

Elliptic curve encryption (ECC) and conveyed records were utilized in A Decentralized and Privacy-Preserving System for Electronic Health (2025), another critical exertion, to move forward protection and give finegrained get to control. In any case, the approach needed a maintainable decentralized capacity layer, and real-time handling was affected by the critical encryption exertion. [4]

In spite of the fact that there are still holes in information lastingness, adaptability, fetched adequacy, and capacity motivating forces, the inspected works appear eminent advance toward secure and decentralized healthcare information administration. The proposed think about combines solid get to control, longterm information toughness, and successful fetched administration for viable healthcare applications by coordination Filecoin as an incentive-driven decentralized capacity layer inside a blockchain-based EHR design. [1]

5. METHODOLOGY

The Blockchain-based Secure Access and Sharing (BCAS) engineering, which combines blockchain innovation, and intermediary re encryption to make a secure, decentralized, and patient-focused EHR administration framework, is the establishment of this study's approach [3]. The proposed approach employments a half breed on- chain/off-chain plan to maximize proficiency whereas ensuring privacy, get to control, and traceability. [3], [5]

Blockchain acts as the trust layer for exchange recording, review path upkeep, and client character administration all through the primary stage of framework plan and architecture construction [1], [3]. Each organization within the healthcare environment, counting protections companies, healing centers, labs, and patients, is given a particular blockchain personality that's associated to both open and private cryptographic keys [1], [2]. By putting away fair vital metadata and get to rights, the blockchain record minimizes excess information and maximizes throughput.

Access control and information encryption are implemented within the moment organize. Intermediary re-encryption is utilized by the BCAS show to defend private EHR data whereas it is being shared. Some time recently being spared, an EHR record transferred by a quiet is scrambled utilizing their private key. Intermediary re-encryption guarantees fine-grained and privacy-preserving get to control by empowering authorized healthcare experts to decode the information without straightforwardly getting to the patient's private key [3]. Patients can allow or expel get to at any minute since to this cryptographic approach's arrangement for energetic authorization [1], [3].

Integration of decentralized information capacity is the most accentuation of the third organize. The approach leverages the InterPlanetary File System (IPFS) as the off-chain capacity layer since it is unreasonable to store huge therapeutic information straightforwardly on-chain. EHR records are part up, hashed, and scattered among IPFS hubs. The blockchain stores the delivered content identifiers (CIDs), setting up a secure association between disseminated record capacity and the unchanging record. Single focuses of disappointment, which are ordinary in centralized frameworks, are dispensed with and adaptability is moved forward by this plan.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 12, Issue 2, pp: (38-44), Month: October 2025 – March 2026, Available at: www.paperpublications.org

The deployment and evaluation of shrewd contracts make up the final arrange. Get to control, exchange examining, and character confirmation are all mechanized through savvy contracts. They halt undesirable control and transparently uphold get to controls. Testing the model's adaptability, response time, CPU utilization, and security against conceivable dangers like DDoS and spoofing assaults are all portion of execution assessment [2], [4], [5]. The BCAS methodology's potential for secure and viable EHR information trade is affirmed by the exploratory comes about, which appear awesome effectiveness, moo computing overhead, and great flexibility to cyber attacks [3].

6. PROPOSED SYSTEM ARCHITECTURE

The deployment and evaluation of shrewd contracts make up the final arrange. Get to control, exchange examining, and character confirmation are all mechanized through savvy contracts. They halt undesirable control and transparently uphold get to controls. Testing the model's adaptability, response time, CPU utilization, and security against conceivable dangers like DDoS and spoofing assaults are all portion of execution assessment [2], [4], [5]. The BCAS methodology's potential for secure and viable EHR information trade is affirmed by the exploratory comes about, which appear awesome effectiveness, moo computing overhead, and great flexibility to cyber assaults [3].

To oversee off-chain information capacity, the decentralized capacity layer combines Filecoin and IPFS. EHR records that have been scrambled are part up into a few parts, hashed, and scattered among IPFS known as content identifiers (CIDs), are put away on the blockchain [2], [3]. In differentiate to conventional IPFS-only frameworks, Filecoin integration makes a decentralized motivation framework that compensates capacity suppliers for maintaining information changelessness and accessibility over time [5]. This dual-layer procedure ensures long-term, reasonable, and reliable information capacity whereas bringing down the blockchain's capacity stack [5].

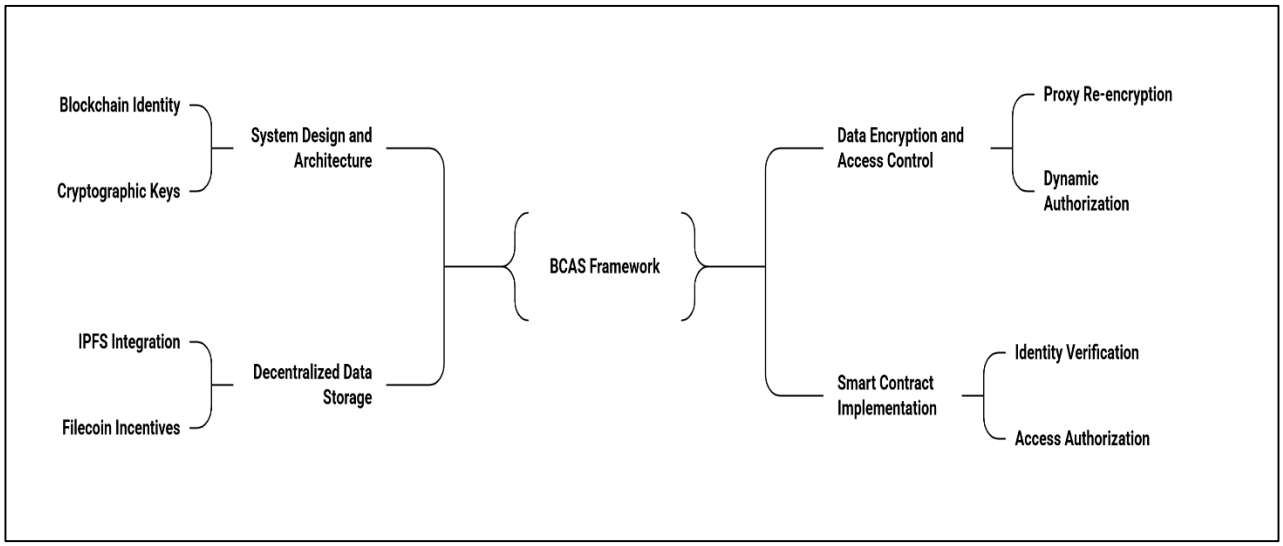

Figure1: Blockchain-based Secure Access and Sharing Framework

The proposed system's engineering is separated into four interconnected levels that participate concordantly to ensure information security and useful adequacy. A assortment of healthcare partners, counting patients, doctors, clinics, labs, and protections companies, make up the client layer. Through blockchain-based identity registered and given a cryptographic key pair that digital signatures to dynamically give or withdraw creates a safe online identity [1], [2]. Patients maintain total access privileges, control over their medical records, and they can use administration, each member is interestingly [1], [3]. The blockchain layer serves as the system's foundation for coordination and believe. It holds metadata relating to EHR get to and sharing, keeps review logs, and records unchangeable exchanges. This layer's smart contracts automate functions like exchange approval, access control, and identity verification without the require for a centralized authority. These contracts formally define data access parameters for healthcare providers, ensuring faireness and security.

To oversee off-chain information capacity, the decentralized capacity layer combines Filecoin and IPFS. EHR records that have been scrambled are part up into a few parts, hashed, and scattered among IPFS hubs. To guarantee information keenness and unquestionable status, the hash values, moreover

Operational level secure data sharing is achieved using proxy re-encryption(PRE), which allows selected parties to decrypt patient data without exposing the initial encryption keys [3]. A profoundly secure, viable, and durable system for overseeing and dispersing EHRs over different healthcare situations is created by combining blockchain straightforwardness, keen contract mechanization, and Filecoin-based storage incentives.

7. OPERATIONAL MECHANISM

The operational component gives the consecutive method for securely uploading, storage, sharing, and recovering Electronic Health Records (EHRs) within the decentralized healthcare organize given by blockchain. Through the integration the blockchain, smart contracts, pre- reencryption, IPFS, and Filecoin, this system achieves scalability and cost effectiveness while ensuring security and controlled access [1], [3], [5].

Every entities, including patients, doctors, hospitals, and insurance companies, must first complete with registration and authentication on the blockchain platform. A unique cryptographic id are assigned to each entity utilizing public-private key sets [1], [2]. By managing user authorization and confirmation, smart contracts eliminate the need for centralized middlemen. Upon enrollment, patients retains total control over their EHR data and are able to grant or revoke access rights to specific healthcare suppliers [1], [3].

The data is secured and encrypted when a patient submits an EHR. To ensure that only those with consent may access the record, it is first encrypted utilizing the patient's private key [1], [3]. The encrypted data is split up into several pieces and kept off-chain within the InterPlanetary File System (IPFS). A distinct hash, referred to as a Content Identifier (CID), is given to each part [2], [5]. To ensure data traceability and keenness, these CIDs are securely put on the blockchain record along with related metadata like timestamps and access rights [3], [5].

The architecture uses Filecoin as an incentive-driven storage layer atop IPFS to ensure long-term accessibility and persistence [5]. Through token-based incentives, Filecoin's decentralized economy persuades storage providers to keep information available [5]. Compared to cloud systems, this integration dramatically brings down storage costs whereas at the same time moving forward data life span.

Proxy re-encryption is utilized to encourage secure key delegation for data access. When patient consent is provided to a healthcare professional the system generates re-encryption key [3]. This allows provider to decrypt the specific data without compromising the patient’s private key. For ensuring responsibility and transparency, each transaction including access requests and retrieval logs is permanently recorded on the blockchain [1], [3], [5].

The framework ensures verification and security recorded by performing review logging and confirmation. By making a transparent and trustless environment, this decentralized workflow diminishes the risk of data tampering, illegal access, and failures caused by reliance on a single system [1], [2], [5]. Blockchain integrity, IPFS decentralization, and Filecoin incentives work together to provide a framework for EHR data sharing across healthcare networks that's effective, secure, and long-lasting.

8. COMPARATIVE ANALYSIS

Several existing blockchain-based healthcare models, such as the Blockchain-based Secure Access and Sharing (BCAS) system, TAC-EHR, HealthChain, and Decentralized Authentication and Secure Distributed File Storage (DASDFS) systems, have been analyzed and compared with the proposed Filecoin integrated EHR sharing system. While these models significantly improve patient privacy and data security they still face limitations in healthcare data systems, they have downsides with respect to scalability, computational fetched, and capacity toughness [1], [3], [5]. The comparative analysis shows that the recommended approach successfully overcomes these restrictions.

The BCAS system enables secure HER sharing by integrating blockchain with proxy re-encryption, ensuring data privacy and traceability [3]. However, since IPFS does not ensure long-term file accessibility when hubs go offline, the system’s heavily dependence on IPFS for offchain storage restricts data persistence [3], [5]. Filecoin, an incentive-based storage network that ensures data durability by rewarding storage miners through cryptoeconomic rewards [5]. This improvement reduces reliance on centralized storage systems and ensures continuous data accessibility.

Compared to TAC-EHR, which relies on blockchain for tamper-proof medical data storage, the proposed framework provides a more cost-effective solution [5]. TAC-EHR relies heavily on on-chain data verification, which increases

processing overhead and gas costs [5]. In contrast, the proposed hybrid architecture stores large EHR data off-chain and records only metadata and content identifiers (CIDs) on-chain, significantly improving throughput, reducing operational costs, and minimizing blockchain congestion [3], [4].

Unlike HealthChain, which primarily focuses on interoperability and access control among healthcare providers, the proposed approach enhances system performance through the use of proxy re-encryption and smart contract automation [3], [4]. This approach eliminates unnecessary authentication steps and enables fine-grained access control without exposing private keys [3]. Smart contracts are used to automate verification, reducing latency and improving real-time data availability [4].

The primary objective of the DASDFS model, which integrates IPFS and blockchain for secure distributed storage, is to improve authentication efficiency. Although it manages user access efficiently, the model involves high transaction costs and lacks a sustainable data storage strategy [2], [5]. In contrast, the Filecoin-powered architecture leverages resource optimization and decentralized incentives to achieve both cost efficiency and reliable authentication [5].

Overall, the comparative analysis shows that the proposed framework performs significantly better in terms of scalability, cost efficiency, data persistence, and access control. By combining blockchain security with Filecoin's decentralized storage network, the approach provides a more robust, privacy-preserving, and future-ready solution for managing and sharing Electronic Health Records across distributed healthcare environments [1], [3], [5].

Framework	Main Features	Limitations
BCAS (Blockchainbased Secure Access and Sharing)	Secure access control, decentralized record sharing	Relies only on IPFS; lacks data persistence; limited scalability
TAC-EHR (Blockchainbased Tamper proof HER)	Tamper-proof storage, auditability, improved data confidentiality	High computational and gas cost; dependence on cloud providers
HealthChain (Blockchain for Healthcare Interoperability)	Cross-institution interoperability, data traceability	Limited support for off-chain storage; moderate latency
DASDFS (Decentralized Authentication and Secure Distributed File Storage)	Distributed authentication, secure data transmission, reduced single-point failures	Lacks incentive mechanism for persistent storage; higher transaction cost
Proposed Filecoin Integrated Model	Secure and scalable EHR sharing; incentive-driven persistent storage	Requires initial setup cost and Filecoin integration effort

9. CONCLUSION & FUTURE SCOPE

This study presents a secure and efficient framework for sharing Electronic Health Records (EHRs) by integrating blockchain technology with decentralized storage platforms such as Filecoin and IPFS. To achieve patient-centric access control, data privacy, and long-term reliability, the proposed framework addresses the limitations of the Blockchain-based Secure Access and Sharing (BCAS) system by introducing a hybrid on-chain/off-chain architecture supported by smart contracts and proxy re-encryption. The framework guarantees that medical data remains continuously accessible, tamper-proof, and cost-effective by leveraging Filecoin's incentive-based storage system.

Performance comparisons with existing models demonstrate that the proposed framework provides greater scalability, improved data-sharing efficiency, and enhanced data reliability, making it a practical and sustainable solution for secure healthcare information management.

In the future, the framework can be further enhanced by integrating federated learning and artificial intelligence (AI) to provide advanced healthcare data analytics while preserving patient privacy. Future research could also focus on developing cross-chain interoperability to enable seamless data exchange between different blockchain networks and healthcare institutions. Integrating IoT-enabled medical devices and lightweight protocol mechanisms can further enhance real-time monitoring and flexibility, especially in resource-constrained environments. With these enhancements, the proposed framework could evolve into a comprehensive, decentralized healthcare ecosystem that ensures secure, efficient, and trustworthy global medical data exchange

REFERENCES

[1] A decentralized and privacy-preserving framework for electronic health records using blockchain. Saad Alahmari, Amal Alshardan Omar Alghushairy, Raed Alsini, Fahd N. Al-Wesabi, Alaa. Khadidos, Shaymaa Sorour, Mesfer Al Duhayyim. 2025

[2] Decentralized Authentication and Secure Distributed File Storage for Healthcare Systems Using Blockchain and IPFS. Maazen Alsabaan, Jasmin Praful Bharadiya, Vishwanath Eswarakrishnan, Adnan Mustafa Cheema, Zaid Bin Faheem and Jehad Ali. 2025

[3] BCAS: Blockchain-based secure access and sharing scheme for EHR data. Biao Jin, Xinhong Chen, Jinbo Xiongb, Xuan Li, Li Lin, Zhiqiang Yao . 2024

[4] A Blockchain-Based Electronic Health Record (EHR) System for Edge Computing Enhancing Security and Cost Efficiency. Valerio Mandarino, Giuseppe Pappalardo and Emiliano Tramontana. 2024

[5] Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage. Dharavath Ramesh, Rahul Mishra, Pradeep K.Atrey, Damodar Reddy Edla, Sanjay Misra, Lianyong Qi. 2023

[6] A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme. Honglei Li ,XiaoYang ,Hongxin Wang, Wujia Wei, and Weilian Xue.2022

[7] Secure internet of medical things based electronic health records scheme in trust decentralized loop federated learning consensus blockchain. Megha Kuliha, Sunita Verma.2024

[8] Patient centric decentralizing health records: a gas-efficient Soulbound token framework for EHR management. Mayank Sharma1, Namrta Tanwar. 2025

[9] Machine learning for effective EHR management in blockchain-cloud integration. Birendra Kumar Saraswat1, Aditya Saxena1, P. C. Vashis. 2024

[10] [10] Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. Dinh c. Nguyen, Pubudu N. Pathirana, Ming Ding, Aruna Seneviratne. 2019