GMR
The Original

Design And Development Of A Blockchain-Enabled Secure Electronic Health Record Sharing Framework Using Distributed Ledger Technology

Neha Muley [1,*], Navnath Kale [2]

[1,*]PG Student, Department of Computer Engineering, MIT Academy of Engineering, Alandi , Pune, Maharashtra, India 412105
nehamuley15@gmail.com
[2]Sr. Assitant Professor, Department of Computer Engineering , MIT Academy of Engineering, Alandi ,Pune,Maharashtra, India 412105
drnavnathkale@gmail.com

Abstract: Healthcare data security has become a major concern in modern medical information systems due to the rapid growth of digital health records, cloud-based storage, and interconnected hospital networks. Conventional Electronic Health Record (EHR) systems suffer from limitations such as centralized data storage, unauthorized access, poor interoperability, data tampering, and insufficient patient privacy protection. Existing studies on healthcare information management mainly focus on centralized databases and traditional cryptographic mechanisms, which often fail to provide complete confidentiality, integrity, transparency, and trustworthiness during medical data exchange among hospitals, laboratories, insurance agencies, and healthcare professionals. Furthermore, cyberattacks, ransomware threats, and unauthorized modification of patient records create significant risks to healthcare infrastructure and patient safety.

To overcome these challenges, this research proposes the Design and Development of a Blockchain-Enabled Secure Electronic Health Record Sharing Framework Using Distributed Ledger Technology. The proposed system utilizes blockchain technology integrated with distributed ledger architecture, cryptographic hashing, smart contracts, and decentralized access control mechanisms to ensure secure and transparent medical record sharing. The framework is designed to provide confidentiality for patient medical records, maintain patient information secrecy, and strengthen trust between doctors and patients by protecting sensitive healthcare data from unauthorized disclosure and manipulation. Advanced encryption algorithms and consensus protocols are incorporated to improve authentication, secure data transactions, and immutable storage of medical information across distributed healthcare nodes.

The proposed model is expected to achieve enhanced healthcare data security, tamper-resistant medical record management, efficient interoperability among healthcare institutions, and improved patient-centric privacy control. Performance analysis parameters such as transaction security, access authentication accuracy, data integrity rate, latency, scalability, and storage efficiency are considered for system evaluation. Experimental analysis is expected to demonstrate significant improvements in confidentiality protection, reduction in unauthorized access risks, secure real-time health record sharing, and reliable distributed data management compared to conventional healthcare database systems. The proposed blockchain-enabled framework can provide a scalable, transparent, and trustworthy solution for next-generation smart healthcare ecosystems.

Keywords: Blockchain Technology, Electronic Health Records (EHR), Distributed Ledger Technology, Smart Contracts, Healthcare Cybersecurity, Cryptographic Hashing, Decentralized Data Sharing, Patient Data Confidentiality, Secure Healthcare Framework, Medical Data Integrity

1. INTRODUCTION

The rapid advancement of digital technologies has significantly transformed the global healthcare sector from traditional paper-based operations to intelligent digital healthcare ecosystems. Modern hospitals and healthcare organizations are increasingly adopting Electronic Health Record (EHR) systems, cloud computing platforms, Internet of Medical Things (IoMT), artificial intelligence, and distributed healthcare networks to improve medical service quality, operational efficiency, and patient management processes. Digital healthcare transformation enables real-time access to patient records, remote diagnosis, telemedicine services, predictive analytics, and automated healthcare monitoring systems. However, the increasing dependency on interconnected digital healthcare infrastructures has also introduced critical cybersecurity challenges related to patient privacy, medical data integrity, unauthorized access, and healthcare data breaches. [1][4][7][11]

The evolution of Electronic Health Record (EHR) systems has revolutionized healthcare information management by replacing manual medical record systems with computerized patient information databases. EHR systems facilitate efficient storage, retrieval, sharing, and updating of patient medical history, laboratory reports, prescriptions, radiology images, and treatment plans among authorized healthcare providers. The adoption of EHR systems has improved clinical decision-making, reduced medical errors, enhanced healthcare interoperability, and enabled precision medicine applications. Despite these advantages, conventional EHR architectures are primarily centralized, making them vulnerable to data manipulation, insider threats, ransomware attacks, and single-point failures. Studies have shown that healthcare organizations are among the most targeted sectors for cyberattacks due to the high sensitivity and financial value of patient medical information. [2][5][9][14]

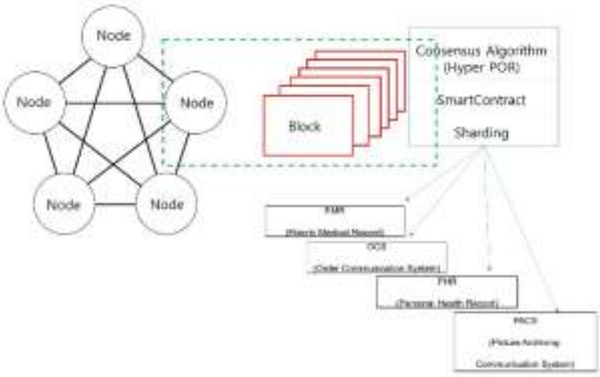

Figure1.1: Blockchain technique for Healthcare System

Secure medical data sharing has become one of the most essential requirements in modern healthcare systems. Healthcare data is continuously exchanged among hospitals, physicians, laboratories, pharmacies, insurance agencies, and research institutions for collaborative treatment and clinical analysis. In conventional systems, medical records are often stored in isolated databases, resulting in interoperability limitations, delayed communication, and restricted accessibility. Additionally, unauthorized disclosure of sensitive patient information may lead to identity theft, financial fraud, legal violations, and loss of patient trust. Therefore, advanced security mechanisms such as encryption, authentication protocols, digital signatures, and access control systems are necessary to preserve confidentiality, integrity, and availability of healthcare data. [3][6][10][15]

The need for decentralized healthcare infrastructure has emerged as a major research direction to overcome the limitations of centralized healthcare database systems. Decentralized frameworks based on Blockchain Technology provide immutable, transparent, and tamper-resistant storage of medical transactions across distributed network nodes. Blockchain technology eliminates dependency on a single centralized authority and enables secure peer-to-peer healthcare information exchange using cryptographic mechanisms and smart contracts. Through distributed ledger architecture, every healthcare transaction is verified using consensus algorithms, ensuring trust, traceability, and data integrity. Furthermore, blockchain-based healthcare systems support patient-centric access control, allowing patients to manage authorization permissions for their medical records securely. These capabilities make blockchain technology highly suitable for next-generation smart healthcare environments requiring high security, transparency, scalability, and trust management. [8][12][16][20]

Healthcare data is continuously exchanged among hospitals, physicians, laboratories, pharmacies, insurance agencies, and research institutions for collaborative treatment and clinical analysis. In conventional systems, medical records are often stored in isolated databases, resulting in interoperability limitations, delayed communication, and restricted accessibility. Additionally, unauthorized disclosure of sensitive patient information may lead to identity theft, financial fraud, legal violations, and loss of patient trust. Therefore, advanced security mechanisms such as encryption, authentication protocols, digital signatures, and access control systems are necessary to preserve confidentiality, integrity, and availability of healthcare data. [3][6][10][15]

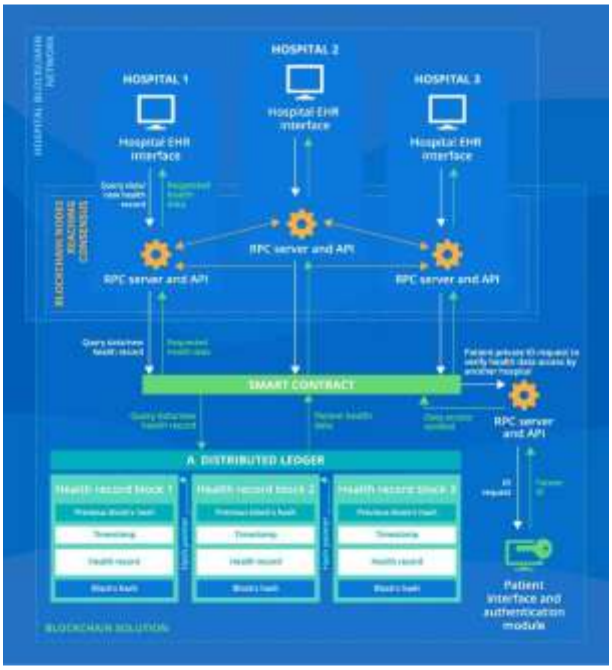

Figure1.2: Architecture of a blockchain-based solution for health records storage and exchange

The above introduction diagram 1.2 illustrates the overall architecture of the blockchain-enabled healthcare record sharing framework. The system consists of multiple healthcare entities including patients, doctors, hospitals, laboratories, pharmacies, and insurance agencies connected through a decentralized blockchain network. Patient medical records are encrypted using cryptographic algorithms before being stored within distributed ledger nodes. Smart contracts manage authentication, authorization, and secure healthcare data access among authorized participants. The blockchain framework ensures confidentiality, transparency, immutability, and tamper-resistant healthcare communication while eliminating centralized security vulnerabilities.

1.2 Background of the Study

The growth of healthcare informatics and digital hospitals has accelerated significantly due to advancements in medical computing technologies, big data analytics, cloud platforms, and intelligent healthcare systems. Healthcare organizations are generating enormous volumes of clinical data including electronic prescriptions, medical imaging, laboratory diagnostics, wearable sensor data, genomic information, and patient monitoring records. Digital hospital infrastructures are designed to support automated workflows, efficient patient care management, and real-time healthcare communication among multiple departments. The integration of smart technologies into healthcare systems has improved diagnosis accuracy, treatment planning, and healthcare accessibility. However, the exponential growth of healthcare data has increased the complexity of data storage, security management, interoperability, and regulatory compliance. [2][7][13][18]

Conventional healthcare database systems face several technical and security-related challenges due to centralized architecture and limited security mechanisms. Most existing healthcare systems rely on centralized cloud servers or local hospital databases where all patient information is stored in a single administrative domain. Such systems are highly vulnerable to cyberattacks, insider misuse, unauthorized data modification, and system failures. In addition, healthcare institutions often utilize heterogeneous software platforms and incompatible database structures, creating interoperability barriers during medical data exchange. The absence of robust authentication, fine-grained access control, and transparent audit mechanisms further increases the risk of privacy violations and healthcare data breaches. Research studies indicate that medical organizations experience frequent hacking incidents because healthcare data contains highly sensitive personal and financial information. [4][9][14][17]

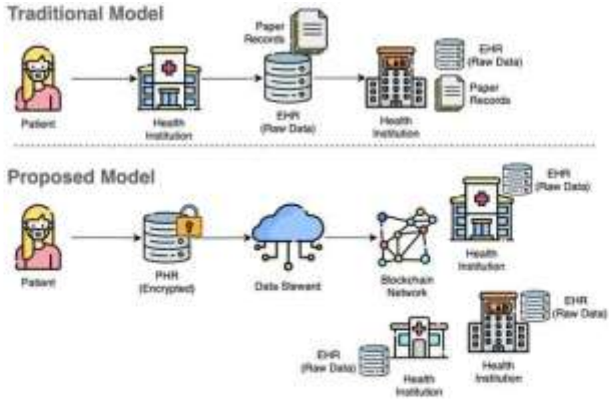

Figure1.3: Solution contribution: In the traditional model for PHR management, the health institution is responsible for managing PHR data, and it is usually stored in unencrypted and paper formats.

The background study diagram1.3 represents the limitations of conventional healthcare database systems and the transition toward blockchain-enabled distributed healthcare infrastructures. Traditional healthcare systems suffer from centralized storage, unauthorized access, poor interoperability, data breaches, and lack of patient-controlled privacy mechanisms. The proposed blockchain-based healthcare architecture introduces distributed ledger technology, decentralized storage, encryption protocols, consensus algorithms, and smart contract-based access control mechanisms to enhance healthcare cybersecurity, patient confidentiality, secure medical record sharing, and trust management among healthcare organizations.

Conventional healthcare database systems are mainly designed using centralized client-server architectures where all medical records are stored and controlled by a single organization or cloud server. Although centralized systems simplify database administration, they also introduce major security and operational limitations. If the central server is compromised due to cyberattacks, hardware failures, or malicious insider activities, the entire healthcare system may become inaccessible or corrupted. [14] Additionally, conventional healthcare systems often lack interoperability standards, preventing seamless communication among different healthcare organizations and software platforms. [10][15]

The emergence of Blockchain Technology in medical applications has opened new opportunities for secure and decentralized healthcare information management. Blockchain technology provides a distributed and immutable ledger where healthcare transactions are securely validated and recorded across multiple nodes without relying on centralized intermediaries. Smart contracts enable automated access authorization, digital identity management, and secure clinical data exchange among healthcare participants. Several recent studies have demonstrated that blockchain can significantly improve healthcare data integrity, transparency, interoperability, and auditability while minimizing risks associated with centralized storage systems. Technologies such as Hyperledger Fabric, Ethereum, Interplanetary File System (IPFS), and cryptographic hashing are increasingly being integrated into healthcare applications for secure EHR management and distributed patient record sharing. [1][6][11][19]

Distributed ledger architecture plays a critical role in enhancing healthcare cybersecurity by enabling decentralized trust management and secure transaction verification. In blockchain-enabled healthcare systems, each medical transaction is cryptographically linked to previous transactions using hash functions, making unauthorized modification nearly impossible. Distributed consensus algorithms ensure data consistency and prevent malicious attacks such as double-spending, data tampering, and unauthorized access. Furthermore, blockchain-based access control frameworks support secure authentication, accountability, and patient-controlled privacy preservation mechanisms. By integrating encryption techniques, digital signatures, smart contracts, and distributed storage technologies, blockchain-based healthcare systems can provide highly secure, transparent, and scalable medical data sharing platforms for future smart healthcare ecosystems. [5][8][12][20]

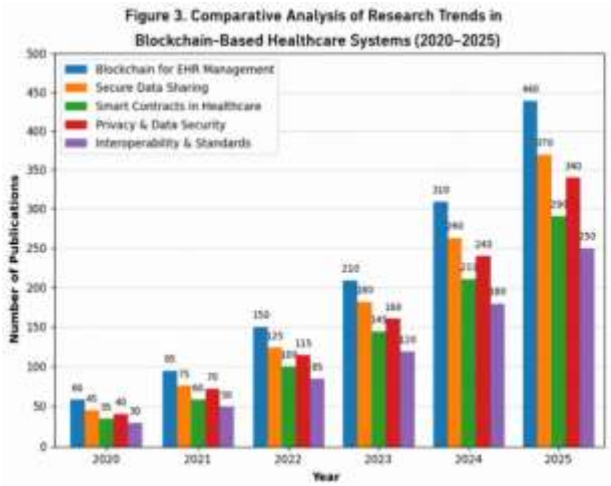

Figure 1.4. Comparative Analysis of Research Trends in blockchain Based Healthcare Systems (2020–2025)

2. Synthesis of Previous Research

The analysis of previous research indicates that the healthcare sector has undergone a significant transformation due to the adoption of digital healthcare technologies, Electronic Health Record (EHR) systems, cloud computing platforms, and intelligent healthcare infrastructures. Researchers have emphasized that digital healthcare systems improve patient management, clinical efficiency, and healthcare accessibility by enabling real-time communication and secure data exchange among healthcare stakeholders. However, conventional healthcare systems continue to face major challenges related to data privacy, centralized storage limitations, interoperability barriers, and cybersecurity vulnerabilities. [2][5]

Several studies have focused on the security and privacy concerns associated with Electronic Health Record systems. Researchers observed that traditional EHR architectures are mainly centralized, making them highly vulnerable to cyberattacks, insider threats, unauthorized access, and medical data breaches. Keshta et al. reported that healthcare organizations experience significant privacy risks because sensitive patient information is often stored across multiple isolated databases with insufficient access control mechanisms. [4] Similarly, William Hurst et al. demonstrated that insider misuse and anomalous access behavior in EHR systems can compromise healthcare data confidentiality and integrity if advanced monitoring systems are not implemented. [18]

Numerous researchers have highlighted that healthcare institutions are among the most targeted sectors for cybersecurity attacks because of the high value of patient medical information. Hammouchia et al. analyzed thousands of publicized hacking incidents and concluded that medical organizations are increasingly becoming primary targets of cybercriminals due to the sensitivity of healthcare data. [8] Additionally, studies on cloud computing environments revealed that centralized cloud infrastructures introduce multiple security risks such as unauthorized access, data leakage, service disruption, and privacy violations. [9][15]

To address these limitations, researchers have increasingly explored Blockchain Technology as a secure and decentralized solution for healthcare information management. Blockchain technology has been identified as an effective mechanism for improving healthcare data integrity, transparency, interoperability, and tamper resistance. Hasselgren et al. conducted a comprehensive scoping review and concluded that blockchain technology can significantly improve access control, provenance tracking, interoperability, and secure healthcare record management. [7] Similarly, Abid Haleem et al. reported that blockchain frameworks support decentralized healthcare ecosystems capable of enhancing patient privacy, authentication, and data traceability while eliminating dependency on centralized authorities. [16]

A considerable amount of previous research has focused on blockchain-enabled Electronic Health Record sharing frameworks. Peng Zhang et al. proposed the FHIRChain architecture that integrates blockchain with Fast Healthcare Interoperability Resources (FHIR) standards to support secure and scalable clinical data sharing. [12] Their study demonstrated that blockchain-based healthcare systems can provide secure audit logs, digital identity management, decentralized storage references, and permission-based access control for healthcare participants. The researchers also emphasized that blockchain-enabled healthcare systems improve collaborative clinical decision-making while maintaining data ownership and patient privacy. [12][20]

Researchers have also investigated the integration of cryptographic techniques with blockchain frameworks to strengthen healthcare cybersecurity. Zainab Abdlhasan et al. proposed a blockchain-based healthcare security framework using AES encryption to protect patient records and medical images before storing them on distributed ledgers. [21] Their research concluded that combining blockchain architecture with encryption algorithms significantly improves confidentiality, integrity, and secure healthcare data transmission. Likewise, Kusum Lata

et al. developed a hybrid AES-RSA cryptographic framework for secure medical image protection in smart healthcare systems and demonstrated high encryption efficiency with strong resistance against cyberattacks. [14]
Several studies have further explored advanced encryption and privacy-preserving techniques for protecting medical data. Saba Inam et al. introduced deep learning-based encryption models using Cycle-GAN networks for secure medical image encryption and decryption. [6] Their work demonstrated that artificial intelligence-assisted encryption systems can enhance confidentiality, robustness, and resistance against unauthorized access. Similarly, Jiaxin Xu et al. proposed a multi-layer DNA-based encryption mechanism for highly secure medical data storage, integrating Blowfish encryption with molecular-level DNA encoding to improve long-term healthcare data protection. [13]
Access control and authentication mechanisms have also received significant attention in previous healthcare cybersecurity research. Usha Nicole Cobrado et al. performed a systematic review of access control solutions in EHR systems and identified Attribute-Based Access Control (ABAC), digital signatures, and multi-factor authentication as effective mechanisms for improving healthcare information security. [19] Their study emphasized the importance of accountability, authorization, auditing, and patient consent management in modern healthcare infrastructures. Furthermore, researchers suggested that future healthcare systems should integrate decentralized identity management and fine-grained authorization frameworks to strengthen patient-centric privacy protection. [19][4]

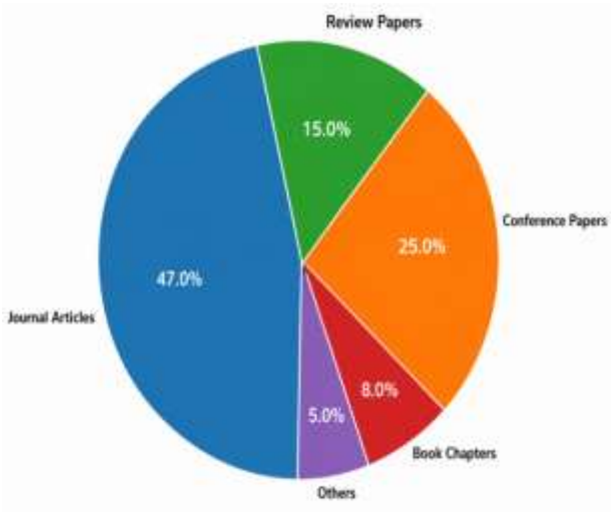

Figure1.5: Publication Distribution in blockchain Based Healthcare Systems

Many researchers have also analyzed the scalability and performance limitations of blockchain-based systems. Ruyan Liu et al. proposed a blockchain-based trusted data storage mechanism utilizing sharding, erasure coding, and Merkle tree structures to reduce storage overhead and improve blockchain throughput in large-scale distributed systems. [7] Their findings indicate that advanced blockchain architectures can improve scalability, transaction verification efficiency, and secure data storage while minimizing network congestion and storage burden. Such improvements are highly relevant for healthcare environments where large-scale medical data exchange and real-time healthcare communication are essential. [7][11]
The synthesis of previous studies clearly indicates that blockchain technology possesses significant potential to revolutionize healthcare information management through decentralized, transparent, and secure medical data sharing mechanisms. Existing research has demonstrated that blockchain-integrated healthcare systems can improve data integrity, authentication, auditability, interoperability, and patient privacy preservation. However, several challenges still remain unresolved, including scalability optimization, efficient key management, real-time transaction processing, interoperability standardization, and integration with existing healthcare infrastructures. Therefore, further research is required to develop advanced blockchain-enabled healthcare frameworks capable of providing secure, scalable, patient-centric, and intelligent healthcare information sharing ecosystems for future smart healthcare applications. [1][3][10][18]

3. System Description of Healthcare System work

The proposed system, titled "Design and Development of a Blockchain-Enabled Secure Electronic Health Record Sharing Framework Using Distributed Ledger Technology," is designed to provide a secure, decentralized, transparent, and privacy-preserving healthcare information management platform for modern smart healthcare environments. The system aims to overcome the limitations of conventional Electronic Health Record (EHR) systems by integrating Blockchain Technology, cryptographic security mechanisms, distributed storage architecture, and smart contract-based access control. The proposed framework enables secure sharing of patient medical records among hospitals, physicians, laboratories, pharmacies, insurance agencies, and authorized healthcare professionals while maintaining confidentiality, integrity, and traceability of healthcare transactions. [1][7]

In the proposed healthcare system, patient medical information such as prescriptions, laboratory reports, radiology images, treatment histories, diagnostic records, and insurance details is digitally stored in encrypted form using advanced cryptographic algorithms. Each healthcare transaction is converted into a secure block and linked to previous records using cryptographic hash functions, thereby forming an immutable blockchain ledger. Since blockchain records cannot be modified without consensus verification, the proposed framework significantly reduces risks associated with unauthorized modification, insider attacks, and medical data tampering. [4][16]

The system architecture consists of multiple interconnected healthcare entities including patients, doctors, hospitals, laboratories, pharmacies, healthcare administrators, and insurance providers. Each participant in the healthcare ecosystem is assigned a unique digital identity for secure authentication and authorization. Smart contracts are implemented to automate access control policies and patient consent management. Whenever a healthcare provider requests access to patient records, the smart contract verifies user authorization rights before granting secure access permissions. This mechanism ensures that only authenticated and authorized healthcare participants can view or modify medical records. [12][19]

The proposed framework also incorporates distributed ledger technology to eliminate dependency on centralized healthcare servers. In traditional healthcare systems, all patient records are maintained within centralized databases, which are highly vulnerable to cyberattacks, server failures, and data breaches. In contrast, the blockchain-enabled healthcare system distributes encrypted healthcare transactions across multiple network nodes, thereby improving fault tolerance, system reliability, and decentralized trust management. Since every participating node maintains synchronized copies of healthcare transaction logs, the possibility of single-point failure is significantly minimized. [8][15]. To enhance patient privacy and healthcare cybersecurity, the proposed system integrates advanced encryption techniques such as Advanced Encryption Standard (AES), RSA cryptography, cryptographic hashing, and digital signatures. Before storing healthcare records on distributed storage nodes, sensitive medical data is encrypted to prevent unauthorized disclosure. Digital signature mechanisms are used to verify data authenticity and maintain transaction integrity during healthcare communication. The integration of encryption protocols with blockchain architecture ensures confidentiality, non-repudiation, and secure healthcare information exchange among multiple healthcare stakeholders. [14][21]

The proposed healthcare system also supports secure interoperability between different healthcare organizations and software platforms. In many conventional healthcare systems, hospitals use heterogeneous database structures and incompatible healthcare software, which creates interoperability challenges during healthcare information exchange. The blockchain-based framework provides standardized healthcare transaction management and decentralized communication protocols that facilitate secure and seamless sharing of patient medical records among distributed healthcare institutions. [5][20]. Another important feature of the proposed system is patient-centric healthcare data ownership and consent management. Unlike traditional healthcare systems where hospitals maintain complete control over medical records, the proposed framework allows patients to regulate access permissions for their healthcare data. Patients can grant, revoke, or monitor authorization rights for doctors, laboratories, pharmacies, and insurance agencies using blockchain-enabled smart contracts. This patient-centric access management approach improves transparency, trust, accountability, and privacy preservation in healthcare ecosystems. [18][19]

The system also provides transparent auditability and transaction traceability for all healthcare operations. Every healthcare activity such as data access requests, prescription updates, diagnosis reports, and medical record modifications is permanently recorded within blockchain transaction logs. The traceability capability of blockchain technology further strengthens healthcare governance and cybersecurity management. [7][16]

In addition to healthcare data sharing, the proposed framework can support emerging smart healthcare applications such as telemedicine systems, remote patient monitoring, IoMT-enabled healthcare devices, AI-assisted diagnosis platforms, and cloud-integrated healthcare analytics. The combination of blockchain technology with intelligent healthcare infrastructures can improve healthcare efficiency, secure real-time communication, and support next-generation digital healthcare ecosystems. Researchers have indicated that blockchain-enabled healthcare systems can play a significant role in developing secure, scalable, transparent, and intelligent healthcare information management platforms for future smart hospitals and precision medicine applications. [6][11][13]

Overall, the proposed blockchain-enabled secure Electronic Health Record sharing framework provides a highly secure, decentralized, and patient-centric healthcare infrastructure capable of protecting sensitive medical information while improving interoperability, trust management, and secure healthcare collaboration. The integration of distributed ledger technology, cryptographic security mechanisms, smart contracts, and decentralized storage architecture makes the proposed system suitable for modern healthcare environments requiring confidentiality, integrity, transparency, accountability, and scalable healthcare information exchange. [1][10][20]

Ref.	Year	Data Modality	Objective / Scope	Technique / Architecture	Explainability	Distributed Ledger / Blockchain	Key Findings	Research Gaps and Open Challenges
[1]	2020	Electronic Health Records (EHR)	Secure healthcare data storage and sharing	Blockchain-Based EHR Framework	Yes	Yes	Improved healthcare data integrity and transparency	Limited scalability and interoperability between hospitals
[2]	2021	Medical Records + Cloud Data	Enhance privacy and confidentiality of patient data	AES Encryption + Cloud Security	Partial	No	Improved encrypted healthcare data protection	Centralized cloud dependency and cyberattack vulnerability
[3]	2021	Multi-Hospital Healthcare Data	Secure medical information exchange	Smart Contract-Based Healthcare System	Yes	Yes	Automated access control and secure transaction logging	High computational cost and smart contract complexity
[4]	2022	IoMT Sensor Data + EHR	Real-time healthcare monitoring and secure sharing	IoT + Blockchain Integrated Framework	Yes	Yes	Improved remote patient monitoring and secure communication	Network latency and energy consumption issues
[5]	2022	Distributed Clinical Data	Decentralized healthcare interoperability	Hyperledger Fabric Architecture	Yes	Yes	Enhanced interoperability and decentralized trust management	Difficulty in large-scale deployment
[6]	2023	Medical Imaging + Patient Records	Protect medical image confidentiality	Blockchain + Deep Learning Encryption	Partial	Yes	High-level encryption accuracy and secure data transfer	Computational overhead and processing complexity
[7]	2023	Multi-source Healthcare Data	Improve healthcare cybersecurity and auditability	Distributed Ledger + Cryptographic Hashing	Yes	Yes	Tamper-resistant medical transaction verification	Blockchain storage overhead
[8]	2023	Cloud-Based Healthcare Records	Fine-grained patient data access control	Attribute-Based Access Control (ABAC)	Yes	Partial	Improved patient-centric authorization management	Complex policy management and implementation

[9]	2024	Genomic + EHR Data	Secure precision medicine data exchange	Blockchain + IPFS Architecture	Yes	Yes	Efficient decentralized genomic data sharing	Data synchronization and scalability challenges
[10]	2024	Real-Time Healthcare Transactions	Transparent healthcare record traceability	Ethereum Smart Contracts	Yes	Yes	Immutable transaction history and secure authentication	Gas fee overhead and transaction latency
[11]	2024	Distributed Medical Databases	Secure healthcare collaboration among institutions	Federated Blockchain Learning Framework	Yes	Yes	Privacy-preserving collaborative healthcare analytics	Communication overhead and model synchronization issues
[12]	2025	Multi-source Medical Big Data	Intelligent healthcare data management	AI-Integrated Blockchain Healthcare Framework	Partial	Yes	Improved predictive healthcare analytics and automation	Ethical concerns and AI explainability limitations
[13]	2025	Patient Records + IoMT Data	Smart healthcare ecosystem development	Blockchain + Edge Computing	Yes	Yes	Reduced latency and improved healthcare response time	Resource optimization challenges
[14]	2025	Encrypted Medical Images	Secure medical imaging and diagnostics	Hybrid AES-RSA + Blockchain Framework	Yes	Yes	High confidentiality and strong attack resistance	Increased encryption-decryption computational load
[15]	2025	Distributed Healthcare Networks	Privacy-preserving healthcare communication	Federated Learning + Blockchain Security	Yes	Yes	Secure distributed healthcare model training	Scalability and communication efficiency challenges

4. Research Gap Identification

The extensive review of previous research indicates that significant advancements have been made in the development of Electronic Health Record (EHR) systems, healthcare cybersecurity frameworks, and blockchain-enabled healthcare infrastructures. However, most conventional healthcare systems are still based on centralized architectures that suffer from security vulnerabilities, single-point failures, limited interoperability, and poor patient-centric privacy management. Existing healthcare databases often fail to provide complete confidentiality, transparency, and secure decentralized communication among healthcare organizations. Several studies have highlighted that centralized healthcare systems remain highly vulnerable to cyberattacks, unauthorized access, insider threats, and healthcare data breaches. [4][8][17]

Many previous research works have focused on implementing blockchain technology for healthcare data management and secure Electronic Health Record sharing. Although blockchain frameworks improve transparency, traceability, and tamper resistance, existing systems still face scalability limitations due to high computational overhead, storage burden, and transaction latency. Most current blockchain healthcare models rely on conventional consensus mechanisms that increase processing complexity when handling large-scale healthcare transactions across distributed hospital networks. [7][12] Furthermore, existing blockchain architectures often struggle to support efficient real-time healthcare communication and high-speed medical data exchange required in emergency healthcare environments. [1][20]

Another major research gap identified in previous studies is the lack of efficient interoperability among heterogeneous healthcare systems. Many hospitals and healthcare organizations utilize incompatible software platforms and isolated healthcare databases, making secure healthcare information exchange difficult. Existing EHR systems lack standardized decentralized communication frameworks capable of supporting seamless multi-hospital collaboration and secure patient record synchronization. Although several researchers proposed blockchain-based interoperability solutions, practical implementation challenges related to system integration, data synchronization, and healthcare protocol standardization still remain unresolved. [5][16][18]

Previous research has also shown limitations in healthcare access control and patient-centric authorization management mechanisms. Most traditional healthcare systems utilize centralized authentication models and password-based access control frameworks that provide limited protection against unauthorized access and insider misuse. While blockchain-based smart contracts have been proposed for secure authorization management, many existing models lack flexible fine-grained access control, emergency healthcare authorization mechanisms, multi-factor authentication, and dynamic patient consent management capabilities. [19] Moreover, existing access control frameworks often fail to provide efficient accountability and auditability for distributed healthcare transactions. [4][18]

Another important research gap is associated with healthcare data privacy preservation and encryption efficiency. Several studies proposed encryption-based healthcare security mechanisms such as AES, RSA, Blowfish, and hybrid cryptographic frameworks to secure medical data. However, many encryption models introduce high computational overhead, increased encryption-decryption latency, and complex key management issues when applied to large-scale healthcare environments. [13][14][21] In addition, existing healthcare encryption systems often lack optimized integration with distributed blockchain infrastructures and decentralized storage systems required for real-time smart healthcare applications. [6][15]

The review of previous literature further indicates that many blockchain-based healthcare systems mainly focus on secure data storage and transaction logging while providing limited support for intelligent healthcare analytics, AI-assisted healthcare decision-making, and IoMT-based real-time healthcare monitoring. The integration of artificial intelligence, federated learning, edge computing, and distributed healthcare analytics with blockchain technology remains insufficiently explored in existing healthcare research. [6][11] Furthermore, several existing healthcare blockchain models fail to address communication overhead, resource optimization, and scalability challenges associated with distributed machine learning and collaborative healthcare analytics. [7][15]

Another critical research gap identified from the literature is the lack of comprehensive patient-centric healthcare ecosystems capable of providing complete ownership and control over medical records. In many existing healthcare systems, healthcare providers and centralized institutions still maintain primary control over patient data. Although some blockchain frameworks support decentralized healthcare communication, efficient mechanisms for patient-controlled access revocation, transparent healthcare auditing, and secure permission delegation are still not fully implemented. [12][19] Additionally, current systems provide limited transparency regarding healthcare transaction history, medical record modification tracking, and secure audit trail management. [16][20]

The literature review also reveals insufficient attention toward large-scale deployment challenges of blockchain-enabled healthcare systems. Existing research studies primarily focus on prototype implementations and theoretical healthcare frameworks with limited real-world validation. Issues related to blockchain scalability, energy consumption, transaction throughput, healthcare regulatory compliance, and integration with existing hospital infrastructure require further investigation. [7][10] Moreover, many proposed systems do not adequately address practical challenges such as healthcare network congestion, blockchain storage overhead, and cost-efficient distributed healthcare management. [1][8]

Therefore, based on the identified research gaps, there is a strong requirement for developing an advanced blockchain-enabled secure Electronic Health Record sharing framework capable of providing decentralized healthcare communication, secure interoperability, efficient patient-centric access control, optimized cryptographic security, transparent healthcare auditing, and scalable distributed healthcare infrastructure. The proposed research aims to address these limitations by integrating distributed ledger technology, smart contracts, advanced encryption mechanisms, decentralized storage systems, and secure healthcare authorization frameworks to build a highly secure, scalable, and intelligent healthcare information management ecosystem. [5][11][16]

5. Data Collection and Preprocessing

The data collection process in the proposed blockchain-enabled healthcare record sharing framework involves gathering Electronic Health Record (EHR) data from multiple healthcare entities such as hospitals, clinics, laboratories, pharmacies, diagnostic centers, and healthcare monitoring devices. The collected healthcare information includes patient demographics, medical histories, prescriptions, laboratory reports, radiology images, diagnostic records, treatment details, and insurance-related data. Since healthcare information is highly sensitive and heterogeneous in nature, the collected data is obtained from distributed healthcare databases and IoMT-enabled healthcare devices using secure communication protocols. Existing studies indicate that healthcare

systems generate large-scale multi-source medical data that require efficient management, secure transmission, and interoperability support for effective healthcare decision-making. [4][11][20]
During the preprocessing stage, the collected healthcare data undergoes multiple operations such as data cleaning, normalization, encryption, duplicate removal, missing value handling, and secure formatting before being integrated into the blockchain network. Sensitive patient information is encrypted using cryptographic algorithms such as AES and RSA to preserve confidentiality and prevent unauthorized access during healthcare communication. Additionally, data preprocessing ensures compatibility between heterogeneous healthcare systems by converting medical information into standardized healthcare formats suitable for blockchain storage and distributed sharing. Smart contracts and hashing mechanisms are further applied to validate data integrity and secure transaction authenticity before storing healthcare records within distributed ledger nodes. [14][19][21]

6. Implementation and Interpretation

The implementation phase of the proposed system focuses on developing a blockchain-enabled secure Electronic Health Record sharing framework using distributed ledger technology, smart contracts, decentralized storage mechanisms, and cryptographic security protocols. The system architecture is implemented using blockchain platforms such as Ethereum or Hyperledger Fabric integrated with smart contract programming, secure authentication modules, and distributed healthcare databases. Each healthcare participant including patients, doctors, hospitals, laboratories, and insurance agencies is assigned a unique digital identity for secure authentication and controlled access management. Patient medical records are securely encrypted, validated through blockchain consensus mechanisms, and stored across distributed network nodes to ensure transparency, immutability, and tamper-resistant healthcare communication. [1][7][12]
The interpretation of the implemented system is carried out by evaluating performance metrics such as healthcare data confidentiality, transaction security, access control efficiency, scalability, interoperability, transaction latency, and data integrity preservation. Experimental analysis is expected to demonstrate that the proposed blockchain-based healthcare framework provides significantly improved security, transparency, and patient privacy compared to conventional centralized healthcare systems. The immutable blockchain ledger enables transparent healthcare audit trails and secure medical transaction verification, while smart contract mechanisms automate patient consent management and authorization control. Furthermore, the distributed architecture improves fault tolerance and minimizes risks associated with centralized server failures, cyberattacks, and unauthorized healthcare data modification. [5][16][20]

7. Workflow of System

The workflow diagram presents a comprehensive methodology for developing a Blockchain-Enabled Secure Electronic Health Record (EHR) Sharing Framework utilizing Distributed Ledger Technology. This methodology comprises six phases: Requirement Analysis, Blockchain Architecture Design, Data Security Implementation, Module Development, System Testing, and Deployment.

1. Requirement Analysis and System Study:
This initial phase assesses existing healthcare information systems, emphasizing security, privacy, and interoperability challenges. Stakeholder needs are evaluated to create a System Requirement Specification (SRS) document that incorporates healthcare data security, decentralization, patient privacy, and interoperability standards.

2. System Architecture Design and Blockchain Framework:
This phase conceptualizes the blockchain-enabled infrastructure, focusing on decentralizing communication among healthcare entities. It defines the system architecture and includes important design elements like consensus mechanisms and smart contract functionalities, ensuring a secure and transparent EHR sharing system.

3. Data Management and Security Design:
This phase implements cybersecurity measures to protect sensitive patient data. It entails using encryption algorithms, digital signatures, and access control models—specifically Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)—to ensure confidentiality, integrity, and secure sharing of healthcare information.

4. Implementation and Module Development:
Practical development occurs here, utilizing technologies like Solidity, Hyperledger Fabric, IPFS, Node.js, MongoDB, and React to create various modules, including user management and audit logs. These technologies form the backbone of a secure decentralized healthcare application.

5. Testing, Validation, and Performance Evaluation: This critical phase evaluates the system's functionality and

security through multiple testing protocols. Metrics include security strength and scalability, ensuring that the system meets performance standards and identifies vulnerabilities before real-world deployment.

6. Deployment and Real-Time Operation and Maintenance:
The final phase involves rolling out the validated framework across healthcare networks. It establishes real-time operations for secure data sharing, consent management, and system maintenance, enhancing reliability and transparency in decentralized healthcare transactions.

In summary, the framework aims to establish a secure, scalable, and patient-focused ecosystem that integrates advanced blockchain technology and security measures to promote efficient healthcare information sharing and management.

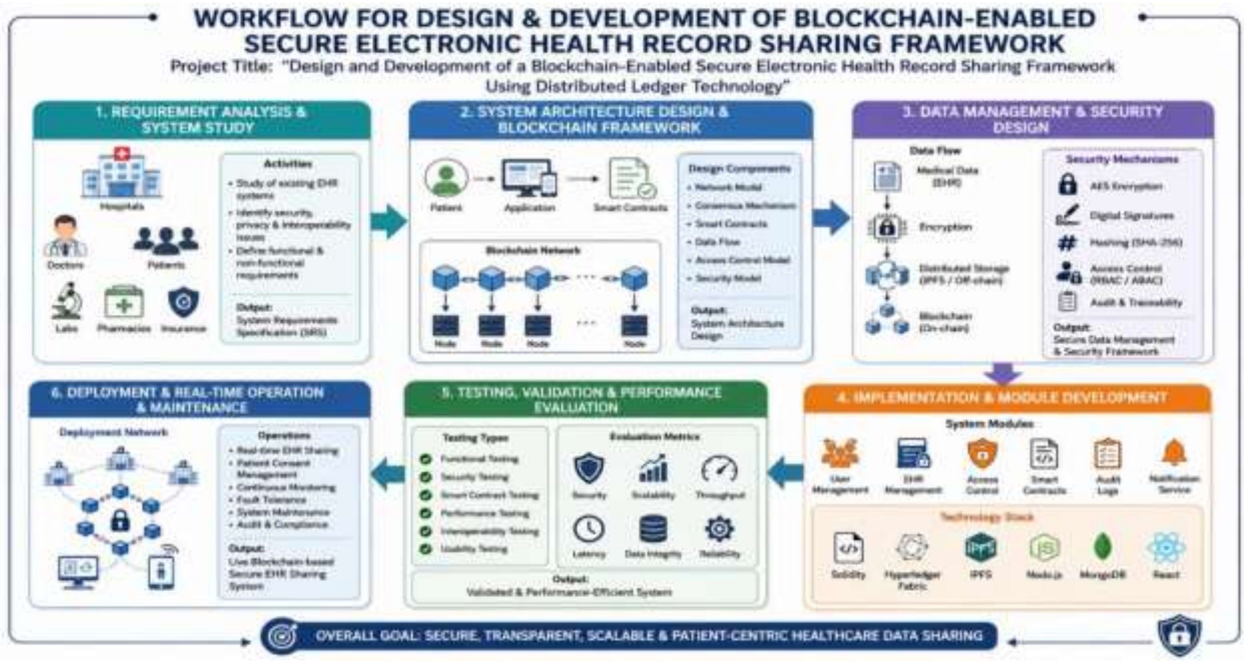

Figure1.6: Flowchart for Design and Implementation of Blockchain Base Healthcare System

8. UML Diagrams

8.1 Data Flow Diagram Level-0

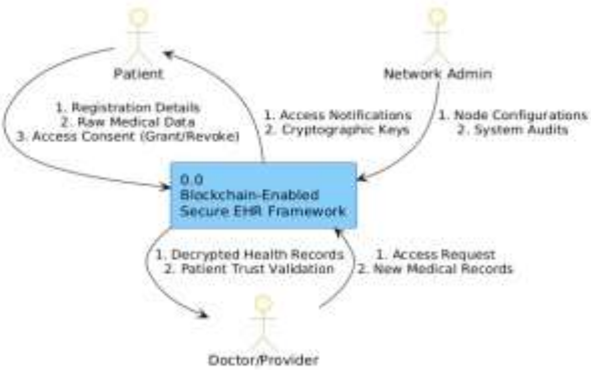

Figure1.7: Data Flow Diagram Level-0

The above diagram represents the interaction between major entities involved in the Blockchain-Enabled Secure Electronic Health Record (EHR) Framework, including the Patient, Doctor/Provider, and Network Admin. Patients provide registration details, medical data, and access consent, while doctors request and access authorized health records, and network administrators manage node configurations, cryptographic keys, and system auditing to ensure secure, transparent, and decentralized healthcare record management.

8.2 Data Flow Diagram Level- 1

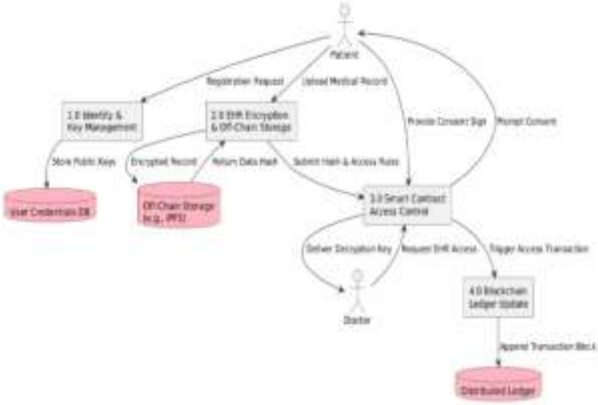

Figure1.8: Data Flow Diagram Level-1

The above diagram illustrates the workflow of the Blockchain-Enabled Secure Electronic Health Record (EHR) Sharing Framework, where the patient uploads medical records and provides consent through smart contract-based access control. The system performs identity management, encryption, off-chain storage using IPFS, and blockchain ledger updates, while authorized doctors securely request and access encrypted healthcare records through decentralized authentication and distributed ledger verification mechanisms.

8.3 Data Flow Diagram Level- 2

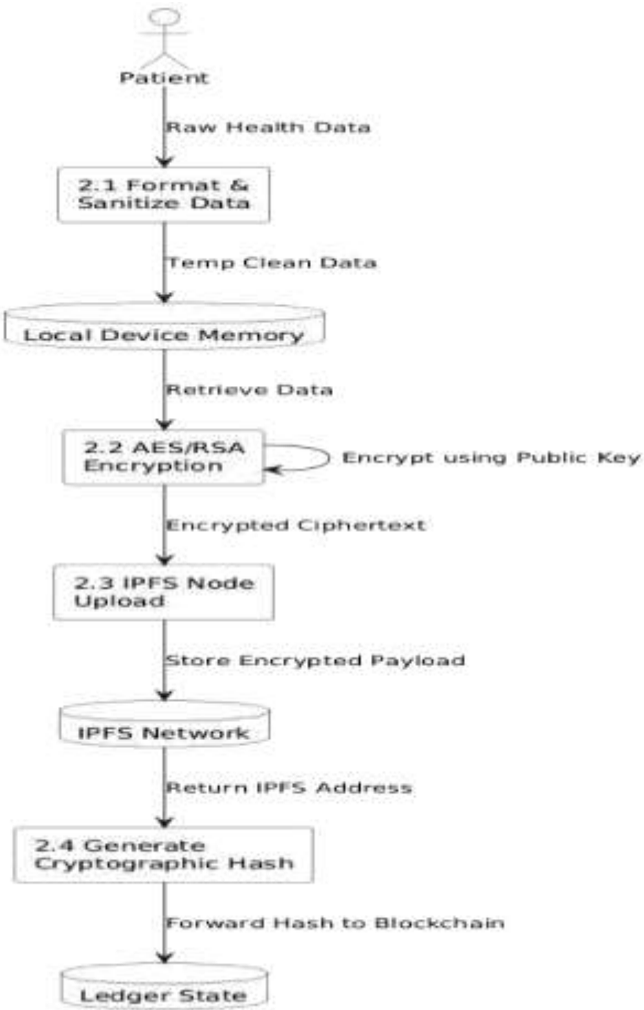

Figure1.9: Data Flow Diagram level-2

The above diagram represents the secure healthcare data preprocessing and blockchain storage workflow within the proposed Electronic Health Record (EHR) framework. Initially, raw patient health data is formatted and sanitized before being encrypted using AES/RSA cryptographic algorithms, then securely uploaded to the IPFS network for decentralized storage, while the generated cryptographic hash is forwarded to the blockchain ledger to ensure data integrity, confidentiality, and tamper-resistant healthcare record management.

8.4 Data Flow Diagram Level- 3

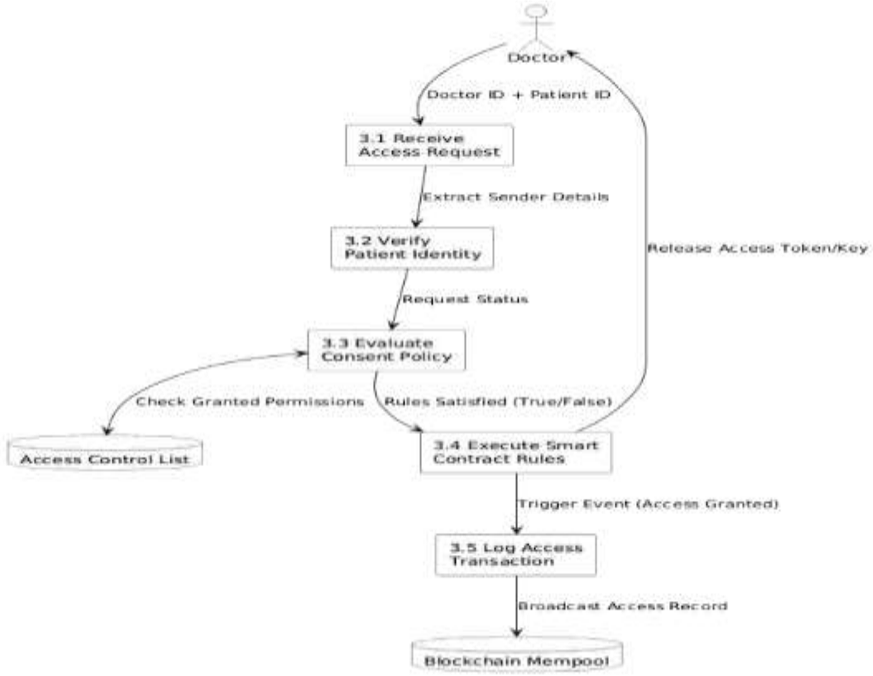

Figure1.10: Data Flow Diagram Level- 3

The above diagram illustrates the smart contract-based access control workflow in the Blockchain-Enabled Secure Electronic Health Record (EHR) Framework. In this process, the doctor submits an access request using doctor and patient identification details, after which the system verifies patient identity, evaluates consent policies, checks granted permissions, and executes smart contract rules before securely releasing access tokens and recording the authorized healthcare transaction within the blockchain mempool for transparent and tamper-resistant auditing.

8.5 Use Case Diagram

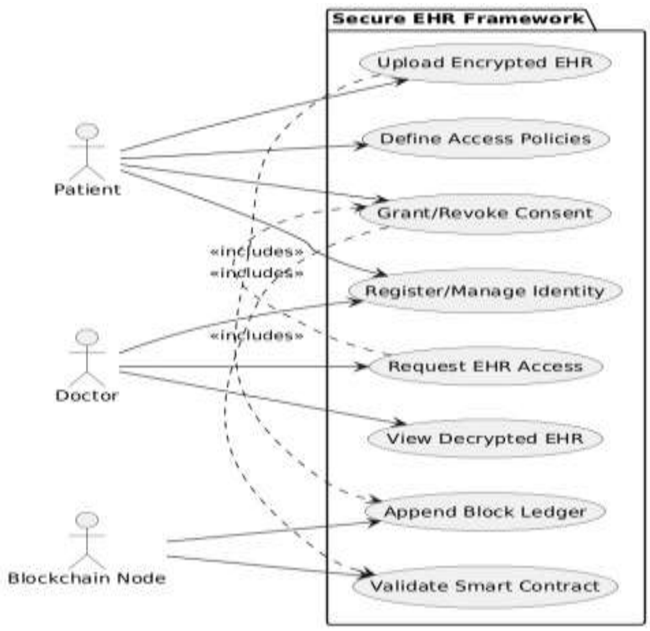

Figure1.11: Use case Diagram

The above use case diagram represents the interactions between the Patient, Doctor, and Blockchain Node within the Secure Electronic Health Record (EHR) Framework. Patients can upload encrypted healthcare records, define access policies, grant or revoke consent, and manage their identities, while doctors request and view authorized EHR data, and blockchain nodes validate smart contracts and append verified healthcare transactions into the distributed blockchain ledger for secure, transparent, and decentralized healthcare data management.

8.6 Sequence Diagram

The above sequence diagram illustrates the secure communication workflow of the Blockchain-Enabled Electronic.

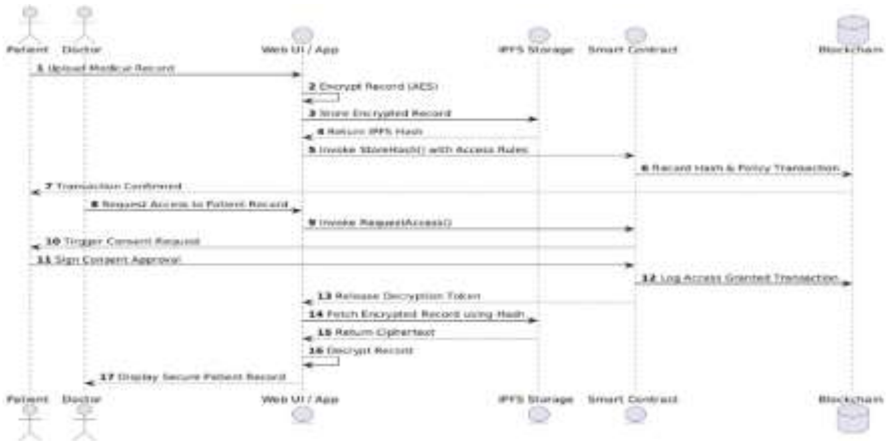

Figure1.12: Sequence Diagram

Health Record (EHR) Sharing Framework among the Patient, Doctor, Web Application, IPFS Storage, Smart Contract, and Blockchain network.

The process begins with encrypted medical record upload and IPFS storage, followed by blockchain hash recording and smart contract-based consent management, after which authorized doctors request access to patient records, receive decryption tokens upon patient approval, and securely retrieve and decrypt the healthcare data through decentralized blockchain verification mechanisms.

8.7 Activity Diagram

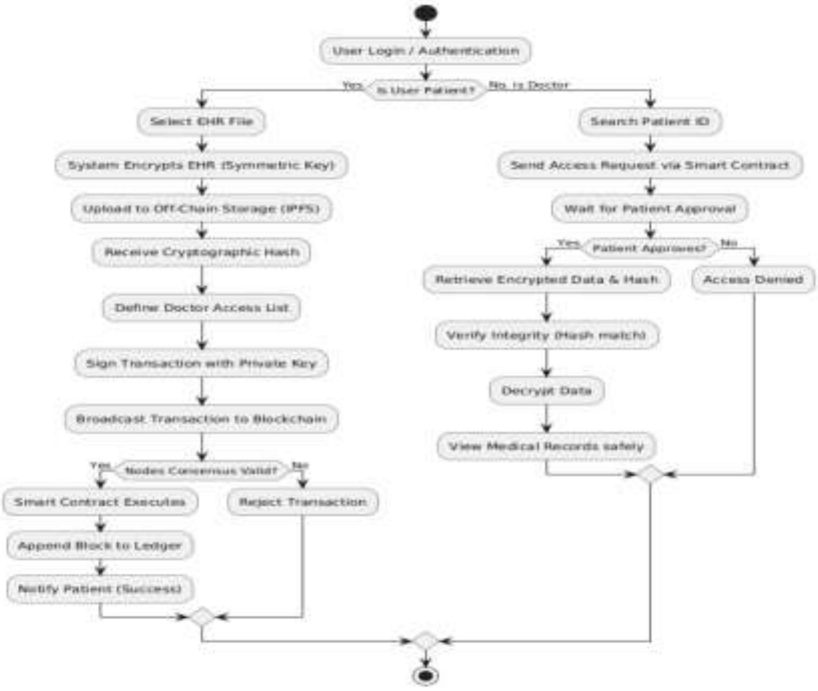

Figure1.13: Activity Diagram

The above activity diagram illustrates the operational workflow of the Blockchain-Enabled Secure Electronic Health Record (EHR) Framework for both patients and doctors.

The process begins with user authentication, after which patients upload and encrypt healthcare records before storing them in IPFS and broadcasting blockchain transactions through smart contracts, while doctors request access to patient records, obtain patient approval, verify data integrity, decrypt authorized healthcare data, and securely view medical records through decentralized blockchain validation mechanisms.

8.9 Class Diagram

The above class diagram represents the structural design of the Blockchain-Enabled Secure Electronic Health Record (EHR) Framework, illustrating the relationships among major system entities such as User, Patient, Doctor, EHR Record, Smart Contract, Block, and Blockchain. The diagram demonstrates how patients securely upload and manage encrypted health records, doctors request authorized access, smart contracts verify consent policies and generate secure blockchain transactions, while blockchain blocks maintain immutable and validated healthcare records for decentralized, transparent, and tamper-resistant healthcare information management.

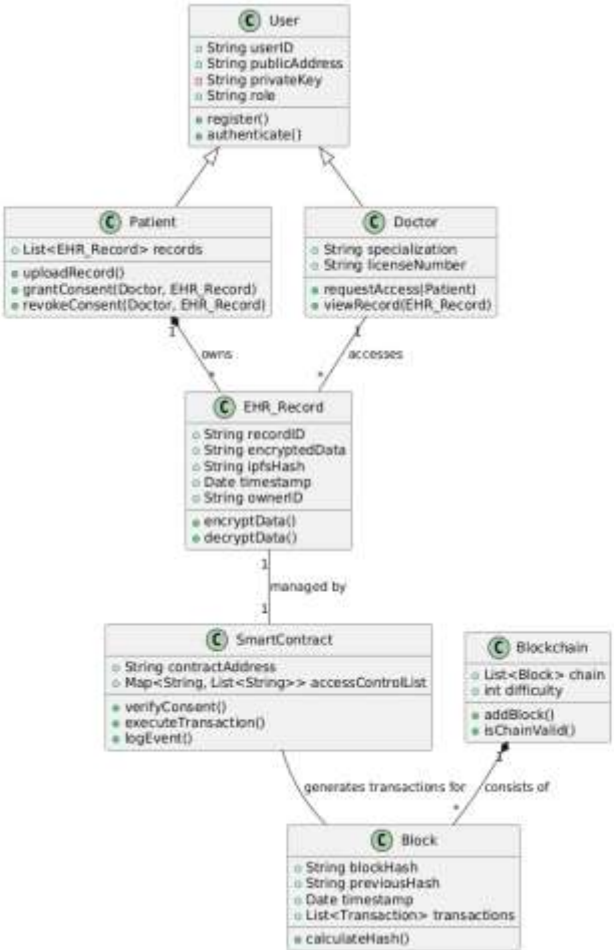

Figure1.14: Class Diagram

The above class diagram illustrates the object-oriented architecture of the Blockchain-Enabled Secure Electronic Health Record (EHR) Framework by defining the relationships between core entities such as User, Patient, Doctor, EHR Record, Smart Contract, Block, and Blockchain. The diagram demonstrates how patients manage encrypted healthcare records, doctors request authorized access to medical data, smart contracts enforce access control and consent verification, while blockchain blocks securely store validated healthcare transactions to ensure decentralized, transparent, and tamper-resistant healthcare record manage.

9. Results and Discussion

9.1 User Interface: Home page

Figure1.7: Home Page

The Home Page is the first interface displayed when the blockchain-enabled healthcare record sharing website is opened, and it contains six main tabs: User Login, User Registration, Hospital Login, Hospital Registration, Admin, and Miners. When the User Login and User Registration tabs are selected, the system displays the user authentication and registration pages for patients or healthcare users to securely access or create their accounts. Similarly, the Hospital Login and Hospital Registration tabs provide secure login and registration interfaces for hospitals and healthcare organizations within the distributed healthcare network. The admin tab opens the administrator dashboard, where complete records of registered users and hospitals can be monitored and managed efficiently. The final tab, Miners, displays the blockchain transaction verification records and mining results, ensuring transparency, secure validation, and tamper-resistant healthcare record management within the proposed blockchain-enabled healthcare system.

9.2 Patient Registration

Figure1.8: Patient Registration

This is the Patient Registration page that will appear when clicked on Patient Registration tab, an application for the User to fill their data for Hospital registration. In this application, there are various filled like Email Address, Password, Full Name, Age, Height, Gender, Blood Group, Contact Number, Address, Profile pic.

9.3 Description of Patient Panel

Figure1.9: Hospital Search in Patient Panel

After Login to “Users Login” tab this page appears. Search by Hospital name tab appear here, application of this tab is Patients can easily find out the Hospital. This page also contains additional four tabs which are Home, Hospital Request, Hospital Search, Accepted Request.

Figure1.10: Hospital Search in Patient Panel

This is “search by hospital name page” that will appear when clicking on Hospital search tab. Application of this tab is it contain the information of Hospital, Hospital profile photo.

9.4 Hospital Registration

Figure1.11: Hospital Registration

This is the “Hospital Registration page” that will appear when clicked on “Hospital Registration tab”, an application for the User to fill hospital data for Hospital registration. In this application, there are various filled like Email Address, Password, Hospital Name, Contact Number, Address, Treatment provided by Hospital, Hospital pic.

9.5 Description of Hospital Panel

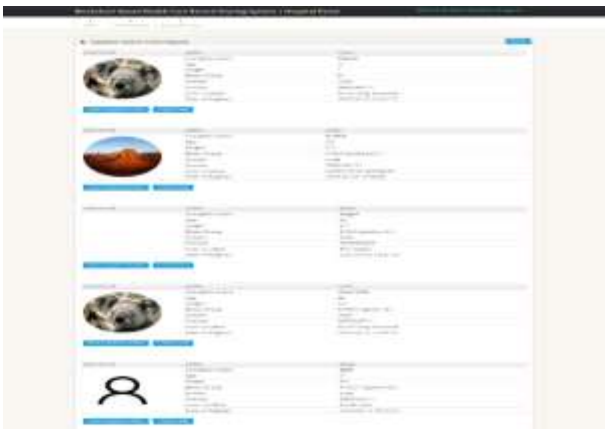

Figure1.12: Patient search in Hospital Panel

This is “Accepted profile Request page” that will appear when clicking on accepted request tab. Application of this tab is it contain the information of Patients, Patient profile photo. Patient create case tab and view complete profile tab appear here

Figure1.13: Patient Create Case in Hospital Panel

This is How the Patient Create Case Page appear. after clicking on create case tab.

9.6 Login Screen for Admin and Miners

Figure1.14: Login Screen for Admin and Miners

This is the “Sign In” page for Admin and Miners panel. when clicked on Admin and Miners tab these pages will appear first, which contain specific Username and Password for all Users.

9.7 Description of Admin Panel:

Figure1.15: Admin Hospital list

This is Hospital Record page, after clicking on Hospital tab this page appears. This page contains Name of Hospital, Address, Treatment Provided by Hospital, Registration date and Logo of Hospital.

9.8 Miner Dashboard

Figure1.16: Miner Dashboard

This is the Miner Dashboard page after sign in Miner dashboard will appear first. It contains Two tabs that are visible which are Dashboard and Mine Transaction.

9.10 Algorithm Implementation:

It is very important to create tables in order to store the information in a systematic manner. In this step, we will build tables for the created database. In the created Database (Login page in this case), click on the 'Structure' tab. Towards the end of the tables list, the user will see a 'Create Table' option. Fill the input fields titled "Name" and "Number of Columns" and hit the 'Go' button.

9.10.1 Patient Table

Figure1.17: Patient Table

These Screenshot shows the Table for Patient Database. Application of these Table is patient can register and login to their Account and, also shows the implementation of sha-1 algorithm when the data of patients Manipulated.

9.10.2 Hospital Table

Figure1.18: Hospital Table

These Screenshot shows the Table for Hospital Database. Application of these Table is Hospital can register and login to their Account and, also shows the implementation of sha-1 algorithm when the data of Hospital Manipulated.

9.10.3 Admin Table

Figure1.19: Admin Table

These Screenshot shows the Table for Admin Database. Application of these Table is Admin can register and login to their Account and, also shows the implementation of sha-1 algorithm when the data of Admin Manipulated.

9.10.4 Miners Table

Figure1.20: Miners Table

These Screenshot shows the Table for Miners Database. Application of these Table is Miners can register and login to their Account, also shows the implementation of sha-1 algorithm when the data of Miners Manipulated.

9.10.5 Mined Transaction:

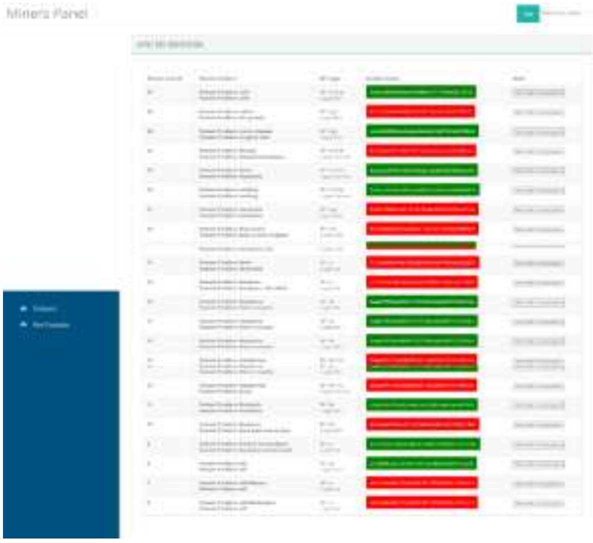

Figure1.21: Mined Transaction Result

This is the Mine Transaction page that will appear when clicked on the mine Transaction tab.in this application we can see the Patient Records Verification. The Records which get manipulated are seen as Red in colour and which are unmanipulated are seen as Green in colour. This application contains patient case Id, Patient Problem, Bp sugar, Specific key.

10. Overall Findings, Implications and Future Direction and Opportunities

The overall findings from the proposed research indicate that the integration of Blockchain Technology with Electronic Health Record (EHR) systems can significantly improve healthcare data security, transparency, interoperability, and patient privacy preservation. The proposed blockchain-enabled healthcare framework overcomes several limitations associated with conventional centralized healthcare systems such as unauthorized access, data tampering, lack of auditability, and single-point system failures. Through decentralized ledger architecture, cryptographic encryption, smart contracts, and distributed healthcare communication, the proposed system provides secure and tamper-resistant healthcare information exchange among hospitals, physicians, laboratories, insurance providers, and patients. [1][7][16]

The findings further demonstrate that blockchain-enabled healthcare systems can enhance patient-centric healthcare management by allowing patients to control authorization permissions related to their medical records. Smart contracts automate authentication, consent management, and secure healthcare transaction validation, thereby improving accountability and transparency in healthcare operations. The implementation of cryptographic mechanisms such as AES encryption, digital signatures, and hashing algorithms further strengthens healthcare data confidentiality and integrity while reducing risks associated with cyberattacks and insider misuse. [14][19][21]

The implications of this research are highly significant for modern healthcare ecosystems because secure healthcare information exchange has become essential for telemedicine, precision medicine, AI-assisted diagnosis, remote healthcare monitoring, and collaborative clinical decision-making. Blockchain-based healthcare infrastructures can support real-time secure communication across distributed healthcare organizations while maintaining trust, transparency, and secure healthcare interoperability. The proposed framework can also reduce administrative costs, improve healthcare operational efficiency, and support intelligent healthcare analytics through secure decentralized data management. [5][11][20].

Future directions and opportunities associated with this research include integrating artificial intelligence, federated learning, Internet of Medical Things (IoMT), edge computing, and cloud computing with blockchain-enabled healthcare infrastructures. Advanced intelligent healthcare systems can utilize decentralized healthcare data for predictive analytics, disease forecasting, remote patient monitoring, and personalized treatment planning. Furthermore, emerging technologies such as quantum-resistant cryptography, zero-knowledge proof mechanisms, and AI-driven smart contract optimization can further enhance the security and scalability of blockchain-enabled healthcare systems. [6][13][15]

11. Ethical and Regulatory Concerns

The implementation of blockchain-enabled healthcare systems introduces several ethical and regulatory concerns associated with patient privacy, healthcare data ownership, informed consent, cybersecurity compliance, and healthcare governance. Since Electronic Health Records contain highly sensitive personal information such as medical histories, genomic data, diagnostic reports, and financial details, healthcare systems must ensure strict compliance with healthcare privacy regulations and ethical data management practices. Unauthorized disclosure or misuse of healthcare information can lead to legal violations, discrimination, identity theft, and loss of patient trust. [4][17]

One major regulatory challenge associated with blockchain-based healthcare systems is compliance with international healthcare privacy standards such as HIPAA, GDPR, and healthcare cybersecurity policies. Blockchain architecture is inherently immutable, meaning healthcare records stored within distributed ledgers cannot be easily modified or deleted. While immutability enhances data integrity and transparency, it may create regulatory conflicts regarding patient rights to modify or erase healthcare information. [7][20]

Ethical concerns also arise regarding patient consent management and healthcare data accessibility. Although blockchain technology enables decentralized healthcare communication, healthcare systems must ensure that patients fully understand how their medical data is stored, shared, and utilized across distributed healthcare networks. Inadequate consent mechanisms or poor transparency regarding healthcare data usage may lead to ethical conflicts between healthcare institutions and patients. Additionally, healthcare organizations must ensure that blockchain-based systems do not restrict emergency medical access during critical healthcare situations. [18][19]

Another regulatory concern involves cybersecurity accountability and distributed governance management. In decentralized blockchain healthcare systems, responsibility for data security and transaction verification is shared among multiple nodes and healthcare participants. Therefore, clear governance policies, accountability mechanisms, and legal frameworks are necessary to manage healthcare data ownership, cybersecurity incidents, access violations, and system failures. Researchers emphasize that future blockchain healthcare systems should integrate robust regulatory compliance frameworks and transparent governance models to ensure ethical healthcare information management. [8][16]

12. Ethical and Social Implications

The adoption of blockchain-enabled healthcare systems has significant ethical and social implications for healthcare providers, patients, healthcare administrators, and society as a whole. One of the major ethical advantages of blockchain technology is its ability to provide transparent, secure, and tamper-resistant healthcare information management. Patients gain improved control over their medical records through decentralized access

management and patient-centric authorization mechanisms. This enhances trust between healthcare providers and patients while improving accountability and transparency in healthcare communication. [1][12].
From a social perspective, blockchain-enabled healthcare infrastructures can improve healthcare accessibility and interoperability across geographically distributed healthcare institutions. Secure decentralized healthcare communication can support telemedicine services, rural healthcare delivery, emergency healthcare coordination, and remote patient monitoring. The integration of blockchain technology with healthcare systems can reduce delays in healthcare information exchange and improve collaborative clinical decision-making among hospitals and healthcare specialists. [5][11]

However, several social challenges and ethical concerns remain associated with digital healthcare transformation. The increasing dependence on advanced digital healthcare infrastructures may widen the technological gap between urban and rural healthcare systems due to differences in technological resources, internet connectivity, and digital literacy. Patients and healthcare professionals with limited technical knowledge may face difficulties understanding blockchain-based healthcare platforms, smart contracts, and decentralized identity management systems. [15][18]

13. Conclusion

The proposed research on "Design and Development of a Blockchain-Enabled Secure Electronic Health Record Sharing Framework Using Distributed Ledger Technology" presents a comprehensive and secure solution for modern healthcare information management systems. The study highlights the critical limitations of conventional centralized healthcare infrastructures including poor interoperability, cybersecurity vulnerabilities, unauthorized data access, lack of transparency, and insufficient patient privacy protection. Through the integration of blockchain technology, smart contracts, distributed ledger architecture, and advanced cryptographic mechanisms, the proposed framework provides secure, decentralized, transparent, and patient-centric healthcare communication. [1][7][12]
The proposed blockchain-enabled healthcare system improves confidentiality, integrity, traceability, and secure interoperability among healthcare organizations while enabling secure Electronic Health Record sharing across distributed healthcare networks. Smart contracts automate authentication and authorization processes, whereas distributed storage and cryptographic security mechanisms protect sensitive patient information from cyber threats, insider misuse, and unauthorized modification. The framework also enhances healthcare accountability through immutable audit trails and decentralized trust management. [14][19][21].

Overall, the research demonstrates that blockchain technology possesses strong potential to revolutionize healthcare cybersecurity and healthcare information management in future smart healthcare ecosystems. Although challenges related to scalability, regulatory compliance, computational overhead, and large-scale deployment still exist, continuous advancements in distributed ledger technologies, intelligent healthcare analytics, and decentralized security architectures are expected to overcome these limitations. The proposed framework provides a strong foundation for developing next-generation secure, scalable, transparent, and intelligent healthcare systems capable of supporting future digital healthcare transformation and patient-centric healthcare services. [5][11][20]

Acknowledgment

I would like to express my sincere gratitude to all those who have supported and guided me throughout the completion of this project titled "Design and Development of a Blockchain-Enabled Secure Electronic Health Record Sharing Framework Using Distributed Ledger Technology".

Declaration

I further declare that this project work has not been submitted elsewhere for the award of any other degree, Diploma, or certification. The information and data presented in this report are true and authentic to the best of my knowledge.

References

1. Edward R. Melnick et al., "The Association Between Perceived Electronic Health Record Usability and Professional Burnout Among US Physicians" Mayo Clinic Proceedings, Elsevier, Volume 95, 2020, 476-487. https://doi.org/10.1016/S0025-6196(19)30836-5
2. Andrew J et al., "Blockchain for Healthcare Systems: Architecture, Security Challenges, Trends and Future Directions" Journal of Network and Computer Applications, Elsevier, Volume 215, 2023, 103633. https://doi.org/10.1016/j.jnca.2023.103633

3. David J. Carey et al., "The Geisinger MyCode Community Health Initiative: An Electronic Health Record-Linked Biobank for Precision Medicine Research" Genetics in Medicine, Elsevier, Volume 18, 2016, 906-913. https://doi.org/10.1038/gim.2015.187
4. Ismail Keshta et al., "Security and Privacy of Electronic Health Records: Concerns and Challenges" Egyptian Informatics Journal, Elsevier, Volume 22, 2021, 177-183. https://doi.org/10.1016/j.eij.2020.07.003
5. F. Sherwani et al., "Hybridized Classification Algorithms for Data Classification Applications: A Review" Egyptian Informatics Journal, Elsevier, Volume 22, 2021, 185-192. https://doi.org/10.1016/j.eij.2020.07.004
6. Saba Inam et al., "Security of End-to-End Medical Images Encryption System Using Trained Deep Learning Encryption and Decryption Network" Egyptian Informatics Journal, Elsevier, Volume 28, 2024, 100541. https://doi.org/10.1016/j.eij.2024.100541
7. Ruyan Liu et al., "BTDSI: A Blockchain-Based Trusted Data Storage Mechanism for Industry 5.0" Journal of King Saud University - Computer and Information Sciences, Elsevier, Volume 35, 2023, 101674. https://doi.org/10.1016/j.jksuci.2023.101674
8. Anton Hasselgren et al., "Blockchain in Healthcare and Health Sciences: A Scoping Review" International Journal of Medical Informatics, Elsevier, Volume 134, 2020, 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040
9. Hammouchia et al., "Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time" Procedia Computer Science, Elsevier, Volume 151, 2019, 1004-1009. https://doi.org/10.1016/j.procs.2019.04.143
10. Maniaha et al., "Survey on Threats and Risks in the Cloud Computing Environment" Procedia Computer Science, Elsevier, Volume 161, 2019, 1325-1332. https://doi.org/10.1016/j.procs.2019.11.249
11. Yuhan Zhang, "Medical Data Security and Sharing Mechanisms in Cloud Computing Environments" Procedia Computer Science, Elsevier, Volume 259, 2025, 766-777. https://doi.org/10.1016/j.procs.2025.01.001
12. Peng Zhang et al., "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data" Computational and Structural Biotechnology Journal, Elsevier, Volume 16, 2018, 267-278. https://doi.org/10.1016/j.csbj.2018.07.004
13. Kin On Kwok et al., "Utilizing Large Language Models in Infectious Disease Transmission Modelling for Public Health Preparedness" Computational and Structural Biotechnology Journal, Elsevier, Volume 23, 2024, 3254-3257. https://doi.org/10.1016/j.csbj.2024.08.006
14. William Hurst et al., "Securing Electronic Health Records Against Insider-Threats: A Supervised Machine Learning Approach" Smart Health, Elsevier, Volume 26, 2022, 100354. https://doi.org/10.1016/j.smhl.2022.100354
15. Usha Nicole Cobrado et al., "Access Control Solutions in Electronic Health Record Systems: A Systematic Review" Informatics in Medicine Unlocked, Elsevier, Volume 49, 2024, 101552. https://doi.org/10.1016/j.imu.2024.101552
16. Jiaxin Xu et al., "Multi-layer Encryption of Medical Data in DNA for Highly-Secure Storage" Materials Today Bio, Elsevier, Volume 28, 2024, 101221. https://doi.org/10.1016/j.mtbio.2024.101221
17. Kusum Lata et al., "A Cryptographic Framework for Secure Medical Imaging in Smart Healthcare Environments" Results in Engineering, Elsevier, Volume 27, 2025, 106780. https://doi.org/10.1016/j.rineng.2025.106780
18. Abid Haleem et al., "Blockchain Technology Applications in Healthcare: An Overview" International Journal of Intelligent Networks, Elsevier, Volume 2, 2021, 130-139. https://doi.org/10.1016/j.ijin.2021.09.005
19. Jay M. Brenner et al., "Privacy and Confidentiality of Emergency Department Patient Information: Contemporary Considerations and Challenges" Journal of the American College of Emergency Physicians Open, Wiley, Volume 5, 2024, e13130. https://doi.org/10.1002/emp2.13130
20. Zainab A. Abdlhasan et al., "Securing Healthcare Data with Blockchain and AES Encryption: A High-Performance Approach to Data Integrity, Confidentiality, and Availability" 2nd Regional Symposium on Innovation in Science and Technology, University of Basrah, Pages 170-173, 2024, 170-173.
21. Deepa Elangovan et al., "The Use of Blockchain Technology in the Health Care Sector: Systematic Review" JMIR Medical Informatics, JMIR Publications, Volume 10, Issue 1, 2022, e17278. https://doi.org/10.2196/17278