RESEARCH PAPER

Blockchain-Powered Distributed Medical and Drug Record Sharing with Integrity and Access Control

Dr. P. C. Prabhu Kumar[1], P. Poojitha[1], K. Satheesh Kumar[1], M. Charan Kumar[1], S. Monisha[1], T. Bharath Kumar[1]

[1]Department Of Computer Science And Engineering, Mother Theresa Institute of Engineering and Technology, Palamaner, Andhra Pradesh, India

ABSTRACT

The rapid digital transformation of the healthcare and drug sector has increased the reliance on cloud infrastructures for storing and exchanging Electronic Health Records (EHRs), raising significant concerns regarding privacy breaches, unauthorized access, and data integrity. To overcome these challenges, this project proposes a secure, patient-centric medical and drug data-sharing framework that integrates blockchain technology with distributed cloud storage. In this system, patients upload encrypted Personal Health Records (PHRs) to an untrusted cloud server while maintaining complete control over access permissions. A semi-trusted Setup and Re-Encryption Server (SRS) manage cryptographic key generation and re-encryption processes, enabling healthcare providers to access only the data explicitly authorized by the patient. All access requests, key operations, and permission updates are immutably recorded on a blockchain ledger, ensuring transparency, traceability, and accountability. The design further enforces forward and backward access control, automatically revoking past privileges when permissions are modified. Experimental evaluation demonstrates that the framework effectively ensures confidentiality, integrity, and access control while resisting tampering and supporting efficient real-time medical services, making it a promising solution for secure and scalable e-Health data exchange.

Keywords: Blockchain Technology, cryptography, electronic health record, Interplanetary File System, Higher education, medical health record, security

How to cite this article: Kumar P C P, Poojitha P, Kumar K S, Kumar M C, Monisha S, Kumar T B. Blockchain-Powered Distributed Medical and Drug Record Sharing with Integrity and Access Control. Int J Drug Deliv Technol. 2026;16(13s): 553-563. DOI: 10.25258/ijddt.16.13s.62.

Source of support: Nil

Conflict of interest: None

INTRODUCTION

The history of medical records dates back more than a thousand years, with earlier roots in prehistoric societies. Initially, medical records primarily served educational purposes until the 19th century, when they began to play additional roles in insurance and judicial proceedings. Historically, paper records were used by medical offices to maintain patient information. However, the migration from paper-based records to electronic solutions has brought significant advantages. Healthcare institutions are increasingly adopting electronic records due to evolving patient privacy regulations and the ability to access patient files regardless of where the patient is being treated, which improves convenience and continuity of care. As the internet has become deeply integrated into everyday life and has grown rapidly over the past few decades, data security has emerged as a major concern for individuals and organizations alike. [1][2][3]. It has been emphasized that digital information security needs to be strengthened, as the security of digital files during cloud transmission remains a major concern. Higher education organizations today place a strong priority on data security because colleges and universities are frequent targets of cyberattacks. Higher Education Institutions (HEIs) are particularly vulnerable since they handle, process, and store a significant amount of sensitive data,

including Personally Identifiable Information (PII) related to staff, students, and parents. Similarly, when medical records and data are shared or disseminated outside the secure cloud environments of institutions, patients' privacy may be compromised. One of the most significant scientific advancements in computing architecture has been the development and implementation of cryptography to protect sensitive information [4][5]. The use of cryptographic tools and protocols, along with data classification, implementation of access controls, regular updates, and security patches, are some of the important practices that higher education institutions should consider to mitigate specific types of information vulnerabilities. Implementing these techniques helps ensure the confidentiality, integrity, authentication, and

non-repudiation of data during storage, transmission, and access [6].

Blockchain technology relies heavily on cryptography to maintain the security and trustworthiness of information. It enables secure storage and sharing of data without requiring a central authority to oversee the process. Over the years, blockchain has emerged as one of the most innovative application models due to its ability to integrate consensus mechanisms, distributed data storage, digital encryption technologies, peer-to-peer transmission, and other advanced computing techniques. Various sectors such as banking, government, defence, and education are increasingly exploring blockchain technology. Many researchers believe that blockchain will challenge and transform several industries, including higher education institutions, and may represent the next "big" wave in digital technology [7][8]. Universities are likely to be significantly affected by the emergence and growth of blockchain technology, which has the potential to become a powerful disruptive innovation. Blockchain technology can also support the development of secure methods for financial transactions and data protection, which are critical requirements in higher education environments. In addition, domains such as academic libraries and human resource management are exploring the potential and advantages of blockchain technology, particularly in areas related to information storage, preservation, and secure sharing [9][10][11].

OBJECTIVES

To design a real-time access recognition and authentication framework for medical health records that ensures immediate identification, validation, and authorization of all users accessing sensitive patient data using blockchain-based event logging and smart contracts.

To enforce fine-grained forward and backward access control policies through smart contract–driven permission verification, ensuring that only users with legitimate, updated, and role-appropriate privileges can access encrypted medical records.

To integrate blockchain with distributed off-chain storage for the secure, efficient, and tamper-resistant retrieval of encrypted medical records using content-addressable hashing and real-time integrity verification mechanisms.

To implement a secure real-time re-encryption and decryption mechanism that allows authorized healthcare personnel to access required medical data without exposing patient cryptographic keys or increasing key management complexity.

To ensure data integrity, privacy, and availability in real clinical environments by validating every access request, file retrieval, and decryption step in real time without introducing significant latency.

To enable continuous real-time monitoring and anomaly detection for identifying suspicious or malicious access patterns in medical data access systems [12][13][14].

Many institutions are already considering the application of blockchain technology to enhance their instructional processes and foster cooperation among parents, teachers, and students. Scholarly studies on the integration of this technology in education indicate that research on blockchain implementation is still in its early stages. These studies highlight that the two primary uses of blockchain technology in education currently involve certificate issuance and blockchain-based cryptocurrency payment processing [15]. Furthermore, blockchain technology has introduced several improvements to the teaching and learning process in the educational sector; however, there remains significant potential for growth and further benefits, particularly in enabling collaboration and partnerships among educational institutions. The incorporation of blockchain technology could significantly impact education by reducing costs, improving trust and transparency, and providing a secure platform for sharing student data [16]. Through this study, we aim to explore how blockchain technology can facilitate collaboration between the healthcare sector and educational institutions. In addition, this research investigates the feasibility of incorporating blockchain technology with multi-factor authentication mechanisms to enhance security in sensitive data-sharing environments [17][18].

LITERATURE SURVEY

Security is a top priority for covered entities because medical records contain some of the most sensitive and valuable forms of data. This highlights the need to maintain a delicate balance between trusting institutions and their infrastructures with personal and medical information. The major challenge lies in developing an effective and secure cryptosystem capable of safeguarding sensitive information during storage, transmission, and sharing. Furthermore, the distribution and exchange of information in the healthcare industry present several significant challenges. According to the study in [19], the digitalization of medical records can open new opportunities for improving healthcare services. The authors argue that the immutability, transparency, distributed ledger structure, and decentralization capabilities of blockchain technology can be utilized to securely store personal medical data. They further suggest that the integration of blockchain technology into healthcare systems is expected to have a significant impact. Their study also highlights a comparison between the proposed system and conventional systems. We analysed and considered their approach when conceptualizing the architecture of our proposed framework. Similarly, the study presented in [20] suggested blockchain technology as a potential solution

for the efficient management and maintenance of medical records. Based on these findings, we believe that blockchain technology can also be effectively applied in academic environments, drawing inspiration from the methodologies proposed in these studies. The authors believed that blockchain technology might be used in an academic setting because of their proposed work. The proposed system examined how previous studies integrated blockchain technology to support a patient-driven model for medical record keeping and maintenance. In addition, we investigated how smart contracts can enhance secure data sharing between users and the healthcare network. The protection of sensitive data has become a rapidly growing area of interest for blockchain technology. Since the healthcare sector faces significant organizational risks and handles highly sensitive data, it requires robust security mechanisms to safeguard patient information.

The study presented in [21] proposes the design of a blockchain-based medical record management system aimed at improving the security, accessibility, and reliability of healthcare data. Such systems demonstrate the potential of blockchain technology in ensuring transparency, integrity, and secure data exchange within healthcare environments. Furthermore, several studies have explored the broader applications of blockchain technology in other sectors. For instance, some institutions are considering the use of blockchain technology to enhance instructional processes and foster cooperation among parents, teachers, and students [22]. Scholarly outputs in [23] and [24] indicate that research on the integration of blockchain technology in the education sector is still in its early stages. These studies highlight that the primary applications of blockchain technology in education currently include certificate issuance and blockchain-based cryptocurrency payment processing. In addition, researchers have noted that blockchain technology has introduced improvements to teaching and learning processes in the educational sector. However, there remains considerable potential for further development, particularly in promoting collaboration and partnerships among educational institutions. Because blockchain technology was initially developed for the financial industry, its adoption in other domains, including education, has been relatively limited but continues to grow as new applications are explored [25]. This serves as the driving force behind this study, which aims to investigate the integration of blockchain technology into higher education institutions for the purpose of maintaining medical health records. The incorporation of this technology may significantly impact the education sector by reducing costs, improving trust and transparency, and providing a secure platform for sharing students' data [24]. Through this study, we aim to explore how blockchain technology can facilitate collaboration between the healthcare sector and educational institutions. In addition, this research investigates the feasibility of implementing blockchain-based systems such as MedChain for secure medical data management.

MedChain is designed to enhance existing healthcare systems by providing patients, healthcare providers, and authorized third parties with secure, efficient, and interoperable access to medical records while preserving patient privacy. The system utilizes time-based smart contracts to manage access to Electronic Medical Records (EMRs) and regulate transactions, while also employing advanced encryption techniques to strengthen data security. Furthermore, the study introduces a novel incentive mechanism that encourages healthcare professionals to maintain and update medical data efficiently. Educational institutions, particularly those at the tertiary level, face multiple challenges related to data security, interoperability, and privacy. Blockchain technology has been identified as a promising solution with the potential to transform both the healthcare and education sectors. Electronic Medical Records (EMRs) contain detailed information about patient diagnosis and treatment, and these records often need to be shared among healthcare professionals. However, the possibility of medical records being compromised or disclosed during transmission creates significant challenges for secure data sharing.

The study presented in [26] demonstrates a similar blockchain-based approach that provides a secure and efficient mechanism for patient and physician data access. The proposed method in their work is capable of protecting patient privacy while ensuring secure data exchange. Their security analysis shows that the system can effectively withstand well-known attacks while maintaining system integrity. Moreover, the feasibility of their proposed framework has been validated through an implementation based on the Ethereum blockchain platform.

Securing and managing the confidentiality and privacy of patients' medical records is crucial for protecting sensitive personal information and maintaining trust in healthcare systems. Without proper safeguards, unauthorized access to medical records can lead to privacy breaches, identity theft, and even medical fraud. To address these challenges, robust security measures and privacy policies must be implemented to safeguard medical records and uphold patient confidentiality. A study presented in [27] proposes a system based on a smart contract methodology combined with Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) mechanisms. The integration of these approaches enables decentralized, dynamic, and fine-grained access control management for secure Electronic

Health Record (EHR) systems. Through the use of blockchain technology, their solution functions as a secure distributed ledger, providing system stakeholders with transparency, reliability, credibility, and immutability. Similarly, the study in [28] presents a promising architecture that combines Interplanetary File System (IPFS) and blockchain technology to store medical data in a distributed off-chain manner, offering a solution to the limitations of the current centralized storage paradigm in the healthcare sector. The authors argue that the misuse of patient data and medical reports, as well as unauthorized access to sensitive information such as personal identification details and disease records, pose significant threats to patient privacy. In this study, we examined and considered the architecture proposed in this literature, particularly regarding the adoption of an off-chain storage solution for managing patient medical records.

The literature on integrating blockchain technology with the Inter Planetary File System (IPFS) for storing and managing medical health records presents a compelling opportunity to transform healthcare data management. This approach combines blockchain's decentralized ledger and cryptographic security with IPFS's distributed file system, thereby addressing longstanding challenges such as security vulnerabilities, privacy concerns, and interoperability issues in medical record management. Researchers have proposed innovative framework models that emphasize the integration of blockchain-based solutions with IPFS technologies. These frameworks provide a conceptual blueprint for higher education institutions seeking to implement secure and efficient medical record management systems. By adopting blockchain and IPFS technologies, institutions can enhance data security, protect patient privacy, enable seamless data exchange, and effectively scale their medical record management infrastructures. Consequently, this integration offers significant benefits for medical data management within higher education environments.

METHODOLOGY

This study employs a structured methodology to develop a secure and decentralized medical health record management approach for the Medical and Dental Health Unit (MDHU). The process begins with an assessment of the existing manual workflow, where medical reports submitted by faculty members and students are stored in physical file cabinets and retrieved by MDHU staff, nurses, and doctors. This traditional approach presents several challenges, including slow retrieval, the risk of unauthorized access, lack of traceability, and poor data security. To overcome these limitations, the proposed methodology integrates encryption, blockchain-based auditing, and distributed off-chain storage to enhance confidentiality, integrity, and access control. Medical reports are digitized and encrypted before being uploaded, ensuring confidentiality even when stored on untrusted servers. The encrypted files are stored in a distributed storage layer that generates a content-addressable hash, which is used for secure data retrieval. Blockchain technology is incorporated to maintain immutable logs of all access requests, permission updates, and data-related transactions, thereby ensuring transparency and resistance to tampering.

A semi-trusted re-encryption mechanism enables healthcare personnel to access only the authorized portions of patient data without exposing private keys. Smart contracts enforce permission rules, verify user roles, and automatically manage forward and backward access control, ensuring that updated permissions affect both past and future access rights.The research environment at the San Carlos Campus provides a real-world setting for system development, alpha testing, and beta evaluation to measure system performance, usability, and security. This comprehensive methodology ensures a more efficient, secure, and privacy-preserving system for managing medical records in an educational healthcare environment. This section also outlines the current manual process of the Medical and Dental Health Unit (MDHU) in recording, storing, and retrieving student medical records. These practices may vary among different institutions. Additionally, the system incorporates authentication and access control mechanisms to ensure that only authorized personnel can access sensitive medical information.

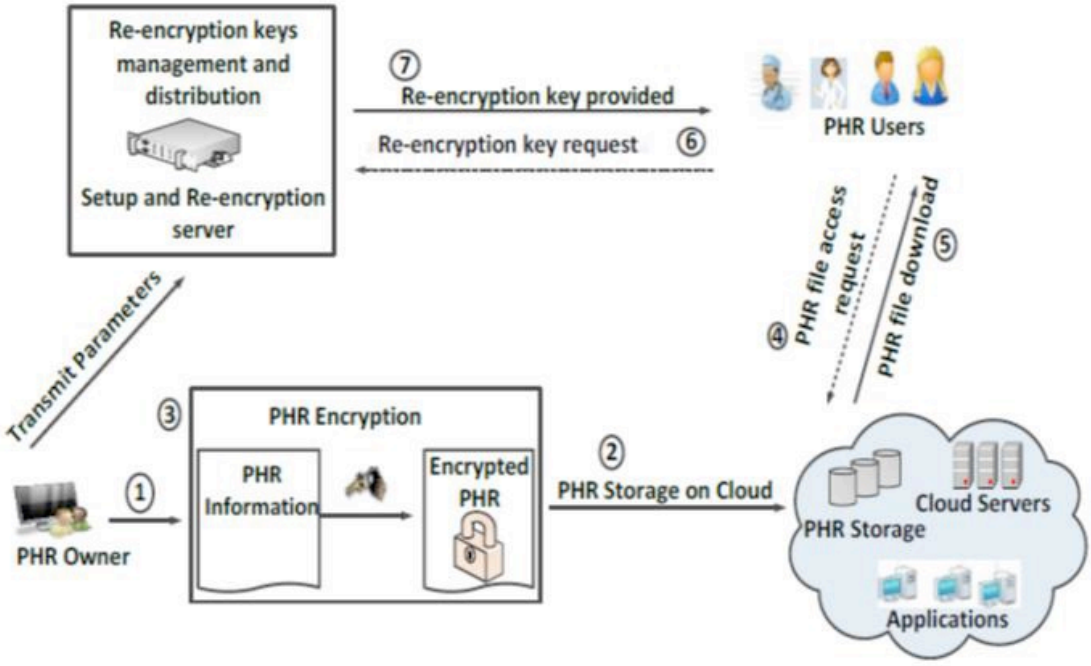

Figure 1: Current process of MDHU for medical and diagnostic report storage/ retrieval.

Most Medical and Dental Health Units (MDHUs) in Higher Education Institutions (HEIs) require the following procedures during the enrolment or employment of faculty members and students.

Student/Faculty Registration**:** Students and faculty members are required to submit their medical examination reports upon enrolment or employment at the institution. They are also required to complete a registration form containing their personal and contact information when they first visit the MDHU. Typically, this information is collected manually using paper-based forms. In addition, patients are required to complete a medical history form in which they disclose details regarding their current medical conditions, past illnesses, surgeries, allergies, medications, and other relevant medical information. In most cases, paper forms are used to collect and store this data.

Health Examination Report: A health examination report is a document that provides an overview of an individual's general health status. Universities and other educational institutions commonly require this report as part of the enrolment or admission process. The purpose of the report is to ensure that students and faculty members are healthy and capable of safely participating in academic activities.

The specific contents of a health examination report may vary depending on the requirements set by the educational institution. However, it typically includes personal information, results of physical examinations, laboratory and diagnostic test results, and medical history. Some institutions may also require standardized forms that must be completed by a licensed healthcare professional, such as a physician or nurse practitioner. As indicated in figure 1, the selected research environment still follows a traditional manual process for storing and retrieving the medical records of faculty members and students. File cabinets provide a conventional means of storing medical reports; however, they present several disadvantages related to accessibility, security, organization, compliance, and operational efficiency. These limitations are particularly evident in educational institutions such as universities and schools, where efficient record management is essential. Transitioning to Electronic Health Record (EHR) systems can address many of these challenges and significantly improve the efficiency and security of medical record management. In the current scenario, it is important to note that the shift from manual record-keeping to EHR systems is becoming increasingly common [30]. Electronic systems offer numerous benefits [31], including easier record retrieval, improved data accuracy, and enhanced coordination of patient care. These observations motivated the researchers to conceptualize a blockchain-enabled digital system designed to address the challenges of security, privacy, and storage of medical health records in Higher Education Institutions (HEIs).

REAL-TIME RECOGNITION

Real-time recognition in the proposed system focuses on the immediate identification, validation, and processing of all access requests and permission-related actions involving medical health records. Whenever a doctor, nurse, or staff member attempts to access a patient's encrypted medical file, the system instantly triggers an event that is recorded on the blockchain. This mechanism ensures that the user's identity, role, and current authorization privileges are recognized immediately. By leveraging smart contracts, the system verifies permission rules, checks updated access rights, and ensures that each request complies with both forward and backward access control policies. This real-time validation mechanism helps prevent unauthorized access and ensures that medical records are accessed only by individuals with legitimate and up-to-date permissions.

Once an access request is authenticated, the system rapidly retrieves the corresponding encrypted file from the distributed off-chain storage layer. Since each medical record is stored using a unique content-addressable hash, the system can quickly locate the appropriate file without relying on traditional indexing structures. The real-time recognition mechanism ensures that the file retrieval process is both efficient and tamper-resistant by comparing the stored hash with the requested hash to verify file integrity. Only after successful verification does the system proceed to the next phase, ensuring that every step in the retrieval pipeline is securely validated without introducing unnecessary delays.

The next component of real-time recognition involves secure decryption through a controlled re-encryption process. Instead of exposing patient keys or requiring healthcare personnel to manage complex cryptographic operations, a semi-trusted re-encryption server instantly transforms the ciphertext so that it becomes decryptable only by the requesting authorized user. This transformation is performed in real time, ensuring that the decrypted information is available immediately while still maintaining strong cryptographic protection. This approach guarantees that each user receives only the data they are authorized to view, while full control remains with the patient or the system administrator. As a result, the system provides a secure, fast, and privacy-preserving data access mechanism suitable for real clinical environments

Finally, the system continuously monitors user activities and system events to detect unusual or potentially malicious patterns in real time. Failed login attempts, repeated access requests, unusual time-of-day access, or attempts to retrieve multiple records within a short period are instantly detected using rule-based or intelligent anomaly detection mechanisms. When abnormal behaviour is identified, the system can automatically trigger protective actions such as revoking access, requiring multi-factor authentication, or alerting system administrators. By combining automated auditing, instant validation, controlled decryption, and continuous monitoring, the real-time recognition component ensures that the entire medical record management process remains secure, transparent, and responsive to emerging threats.

DISCUSSION

To define the system requirements and objectives of this study, the overall system architecture must be designed while considering the integration of blockchain technology with an off-chain storage solution. Electronic Health Record (EHR) management systems play a vital role in modern healthcare by facilitating the storage, retrieval, and sharing of patient data. In the comparative analysis presented in Table 1, six literature sources are examined based on the following criteria: (1) blockchain-based systems, (2) off-chain storage using the Interplanetary File System (IPFS), (3) access control mechanisms, (4) privacy considerations, and (5) applicability in educational settings. Through this analysis, the study aims to provide insights into the strengths and limitations of various EHR management systems across these criteria.

Table 1 Literature Comparison Table

Parameters	**[19]**	**[20]**	**[21]**	**[26]**	**[27]**	**Proposed Model**
Block Chain Based	YES	YES	YES	YES	YES	YES
Off Chian Storage (IPFS)	YES	NO	NO	NO	YES	YES
Access Controlled Based	NO	YES	YES	YES	YES	YES
Privacy	YES	YES	YES	YES	YES	YES
Education Settings	NO	NO	NO	NO	NO	YES

A. Blockchain-Based systems

Blockchain is primarily taken into consideration for EHR due to its inherent capacity to use cryptography and decentralisation to ensure security and immutability of data [34]. All examined literatures emphasize the potential of blockchain in enhancing the security and integrity of their developed EHR systems. Each study integrated blockchain technology into their proposed framework model, highlighting its pivotal role in creating tamper-proof audit trails, facilitating secure data sharing among authorized entities, and ensuring data immutability. This consistent adoption underscores the consensus for us regarding the promising prospects of blockchain in revolutionizing EHR systems to the improved medical record management of an HEI.

B. Off-chain storage (IPFS)

Off-chain storage, particularly through the use of the Interplanetary File System (IPFS), provides a decentralized approach to data storage by reducing reliance on centralized servers and enhancing data availability. Studies in [19] and [28] highlight the advantages of IPFS in ensuring data availability and resilience against single-point failures. While the potential of off-chain storage using IPFS was acknowledged as a promising solution in the comparative analysis, it is notable that not all literature sources [20], [21], [26], and [27] implemented IPFS in their proposed frameworks. Instead, these studies relied solely on the storage capabilities of blockchain technology. However, blockchain-based storage inherently presents certain limitations, including scalability challenges and increased computational overhead. Recognizing these limitations, this study considers the integration of IPFS as an off-chain storage solution within the proposed framework. By combining blockchain technology with IPFS, the system aims to achieve a more scalable, efficient, and secure approach to managing medical health records. storage, particularly utilizing IPFS, provides a decentralized approach to data storage, reducing reliance on centralized servers and enhancing data availability. Literature [19] [28] highlight the benefits of IPFS in ensuring data availability and resilience against single-point failures. While the potential of off- chain storage using Interplanetary File System (IPFS) was acknowledged as a promising solution in the comparative analysis, it's notable that not all literature sources [20][21][26][27] implemented IPFS in their proposed frameworks. Instead, they relied solely on the storage capacity of blockchain technology, which inherently possesses limitations such as scalability issues and increased computational overhead. However, it is important to highlight that we recognized the drawbacks of solely relying on blockchain for storage and considered integrating IPFS as an off-chain storage solution in our proposed frameworks.

C. Access Control Mechanisms

Access control mechanisms are essential for safeguarding patient privacy and ensuring that only authorized personnel can access sensitive medical data. The studies in [20], [21], [26], and [27] emphasize the importance of robust access control mechanisms in Electronic Health Record (EHR) systems to mitigate the risk of unauthorized data access or security breaches. By implementing mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), these systems can effectively regulate data access based on predefined user roles and attributes. This approach ensures that sensitive medical information is accessed only by authorized personnel while also enabling granular control over who can view, modify, or delete specific data elements within the EHR system. Based on these findings, this study incorporates advanced access control mechanisms into the proposed framework model to further strengthen data security and privacy protection.

Access control mechanisms are crucial for safeguarding patient privacy and ensuring that only authorized personnel can access sensitive medical data. The studies in [20], [21], [26], and [27] emphasize the importance of robust access control mechanisms in Electronic Health Record (EHR) systems to mitigate the risk of unauthorized data access or security breaches. By implementing mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), these systems can effectively regulate data access based on predefined user roles and attributes. This approach ensures that sensitive medical information is accessed only by authorized personnel while enabling granular control over who can view, modify, or delete specific data elements within the EHR system. Based on these findings, this study incorporates advanced access control mechanisms into the proposed framework model to further enhance data security and privacy protection.

D. Privacy Considerations

In all the literature sources reviewed, a consistent and paramount focus is placed on privacy considerations within proposed models for EHR management systems. Each study recognizes the critical importance of adhering to privacy regulations and laws, understanding the nuanced differences that exist between institutions and countries. The complexity of privacy regulations underscores the necessity for EHR management systems to be adaptable and compliant with various legal frameworks governing data privacy and security. As such, researchers emphasize the integration of robust privacy measures into their proposed models, ensuring that patient confidentiality is upheld while meeting the diverse regulatory requirements across different jurisdictions.

E. Applicability in Educational Settings

While most of the examined literature primarily focuses on the application of Electronic Health Record (EHR) management systems within healthcare sectors, the limited exploration of these systems in educational settings presents an intriguing opportunity for further research. Considering the widespread adoption of blockchain technology and the InterPlanetary File System (IPFS) for enhancing data security, there exists a potential opportunity to leverage these technologies to secure electronic record management systems in higher education institutions (HEIs).If the proposed investigation proves feasible and successful, demonstrating the applicability of blockchain and IPFS in educational environments for managing medical health records would highlight the novelty and versatility of the proposed model.

This expansion of scope not only contributes to advancing data security practices in healthcare but also extends the benefits of innovative technological solutions to other sectors, demonstrating their potential impact beyond traditional healthcare environments.

RESULTS

The comparative analysis of existing Electronic Health Record (EHR) management systems reveals that while blockchain technology is widely adopted to enhance data integrity, security, and auditability, many solutions rely heavily on on-chain storage or only partially integrate decentralized storage mechanisms. Such approaches often suffer from scalability limitations, increased computational overhead, and higher transaction costs when managing large volumes of medical data.

Although some studies acknowledge the use of off-chain storage, its implementation remains inconsistent. Furthermore, the absence of a fully integrated blockchain–IPFS architecture limits system efficiency, scalability, and data availability.

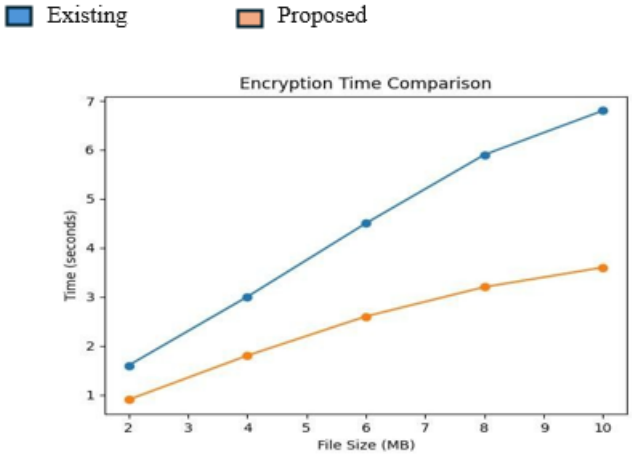

Figure 2. Encryption Time Comparison Graph

Figure 2 illustrates that the proposed blockchain–IPFS-based system significantly reduces encryption time compared to the reference cloud-based blockchain system. As the file size increases, the encryption time rises linearly in both systems. However, the proposed system consistently demonstrates lower processing time due to optimized encryption mechanisms and reduced reliance on on-chain operations.

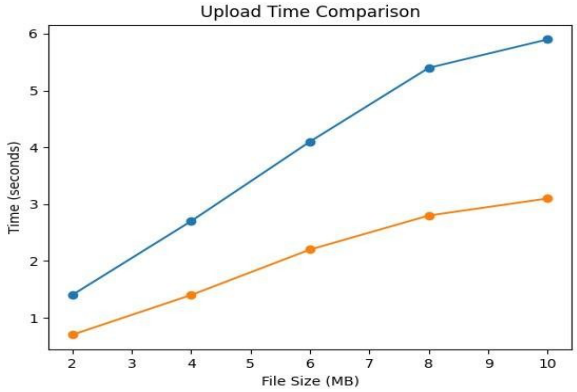

Figure 3. Upload Time Comparison Graph

Figure 3, demonstrates that the upload time in the proposed system is significantly lower than that of the reference system. The improvement can be attributed to the use of Interplanetary File System (IPFS) for off-chain storage, which reduces blockchain transaction overhead and enhances scalability when handling large file uploads. Figure 3, demonstrates that the download time comparison shows that the proposed system enables faster file retrieval across all file sizes. By storing only file hashes on the blockchain and retrieving the actual data from the Interplanetary File System (IPFS), the proposed architecture achieves improved access speed while maintaining data integrity.

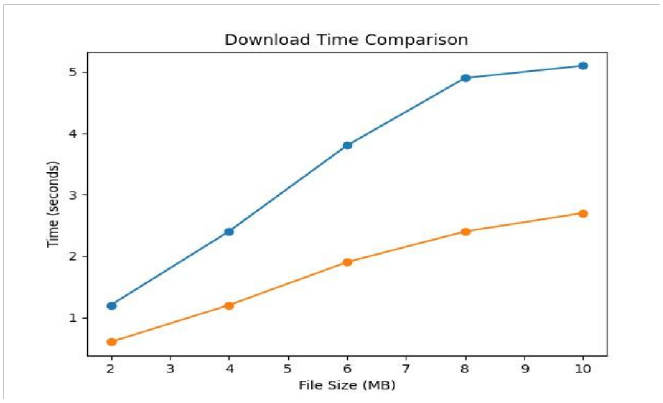

Figure 4. Down Load Time Comparison Graph

CONCLUSION

The proposed decentralized medical health record management system, which integrates blockchain technology with an off-chain storage model such as the InterPlanetary File System (IPFS), presents a highly promising solution for addressing the critical challenges faced by educational institutions in managing sensitive medical data. By ensuring immutability, transparency, and secure auditability through blockchain, the system effectively minimizes risks related to unauthorized access, data tampering, and inconsistent record handling—problems commonly observed in traditional centralized or manual processes. The use of distributed, content-addressed off-chain storage significantly reduces the load on the blockchain while maintaining strong guarantees of data integrity and availability, resulting in a more scalable and efficient approach to health record management.

Furthermore, the proposed architecture enhances interoperability and secure data exchange between the Medical and Dental Health Unit (MDHU) and authorized users such as faculty members and students. With its emphasis on privacy preservation, consent-based access, and role-based access control, the system reinforces trust in digital healthcare systems within higher education environments. The design enables seamless sharing of encrypted medical records while ensuring that sensitive information remains protected at every stage—from storage and retrieval to access logging and permission updates. If implemented successfully, this framework can significantly strengthen institutional data governance practices and establish a new benchmark for secure digital health systems in academic settings.

Overall, the development and deployment of this system represent a significant advancement in modernizing healthcare data management within universities. It not only provides a robust technical foundation for secure medical record management but also opens opportunities for future innovation in areas such as large-scale data analytics, automated health monitoring, and institution-wide digital transformation. As educational institutions continue to adopt emerging technologies, this framework can serve as a model for enhancing security, efficiency, and user trust in medical data administration.

REFERENCES

1. J. Lorkowski and M. Pokorski, “Medical Records: A Historical Narrative,” Biomedicines, vol. 10, no. 10. 2022. doi: 10.3390/biomedicines10102594.
2. C. J. McDonald, “The Barriers to Electronic Medical Record Systems and How to Overcome Them,” J. Am. Med. Informatics Assoc., vol. 4, no. 3, pp. 213–221, May 1997, doi: 10.1136/jamia.1997.0040213.
3. A. M. Qadir and N. Varol, “A Review Paper on Cryptography,” in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1–6. doi:10.1109/ISDFS.2019.8757514.
4. S. Rani, S. Rani, and V. Singh, “Security Enhancement Using Cryptography in Cloud-Based Education Portals,” in Proceedings of 3rd

International Conference on Artificial Intelligence: Advances and Applications: ICAIAA 2022, 2023, pp. 505–516.
5. O. Reyad, Cryptography and Data Security: An Introduction. 2018. doi: 10.13140/RG.2.2.30280.16646.
6. L. A. Alexei and A. Alexei, “Cyber security threat analysis in higher education institutions as a result of distance learning,” Int. J. Sci. Technol. Res., no. 3, pp. 128–133, 2021.
7. K. Al Harthy, F. Al Shuhaimi, and K. K. J. Al Ismaily, “The upcoming Blockchain adoption in Higher Education Requirements and process,” in 2019 4th MEC International Conference on BigData and smart City(ICBDSC),2019,pp oi:10.1109/ICBDSC.2019.8645599.
8. H. Haugsbakken and I. Langseth, “The blockchain challenge for higher education institutions,” Eur. J. Educ., vol. 2, no. 3, pp. 41–46, 2019.
9. E. P. Fedorova and E. I. Skobleva, “Application of blockchain technology in higher education.,” Eur. J. Contemp. Educ., vol. 9, no. 3, pp. 552–571, 2020.
10. H. Abid, “Uses of blockchain technologies in library services,” Libr. Hi Tech News, vol. 38, no. 8, pp. 9–11, 2021.
11. D. Salah, M. H. Ahmed, and K. ElDahshan, “Blockchain applications in human resources management: Opportunities and challenges,” in Proceedings of the 24th International Conference on Evaluation and Assessment in Software Engineering, 2020, pp. 383– 389.
12. S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, “Blockchain technology in healthcare: A comprehensive review and directions for future research,” Appl. Sci., vol. 9, no. 9, p. 1736, 2019.
13. G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” Sustain. cities Soc., vol. 39, pp. 283–297, 2018.
14. H.-S. Huang, T.-S. Chang, and J.-Y. Wu, “A secure file sharing system based on IPFS and blockchain,” in Proceedings of the 2nd International Electronics Communication Conference, 2020, pp. 96– 100.
15. J. Benet, “Ipfs-content addressed, versioned, p2p file system,” arXiv Prepr. arXiv1407.3561, 2014.
16. P. Kang, W. Yang, and J. Zheng, “Blockchain Private File Storage Sharing Method Based on IPFS,” Sensors, vol. 22, no. 14, p. 5100, 2022.
17. K. Azbeg, O. Ouchetto, and S. J. Andaloussi, “BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security,” Egypt. Informatics J., vol. 23, no. 2, pp. 329– 343, 2022.
18. Geetha, G., PC Prabhu Kumar, V. Suriyaraj, and J. Naveen Kumar. "Smart Prediction of Shelf Life and Tomato Sorting Using Deep Learning." Asian Journal of Advances in Agricultural Research 25, no. 10 (2025): 53-67.G. Lodha, M. Pillai, A. Solanki, S. Sahasrabudhe, and A. Jarali, “Healthcare system using blockchain,” in 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 274–281.
19. V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte, “Health record management through blockchain technology,” in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1411–1415.
20. E.-Y. Daraghmi, Y.-A. Daraghmi, and S.-M. Yuan, “MedChain: A design of blockchain-based system for medical records access and permissions management,” IEEE access, vol. 7, pp. 164595–164613, 2019.
21. C. Atienza-Mendez and D. G. Bayyou, “Blockchain technology applications in education,” Int. J. Comput. Technol., vol. 6, no. 11, pp. 68–74, 2019.
22. A. Machado, M. Sousa, and Á. Rocha, “Blockchain technology in education,” in Proceedings of the 4th International Conference on ECommerce, E-Business and E-Government, 2020, pp. 130–134.
23. A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, “Blockchainbased applications in education: A systematic review,” Appl. Sci., vol. 9, no. 12, p. 2400, 2019.
24. N. Lutfiani, Q. Aini, U. Rahardja, L. Wijayanti, E. A. Nabila, and M. I. Ali, “Transformation of blockchain and opportunities for education 4.0,” Int. J. Educ. Learn., vol. 3, no. 3, pp. 222–231, 2021.
25. V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, “Secure and efficient data accessibility in blockchain based healthcare systems,” in 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 206–212.
26. H. Mhamdi, M. Ayadi, A. Ksibi, A. Al-Rasheed, B. O. Soufiene, and S. Hedi, “SEMRAchain: A Secure Electronic Medical Record Based on Blockchain Technology,” Electronics, vol. 11, no. 21, p. 3617, 2022.
27. R. Kumar, N. Marchang, and R. Tripathi, “Distributed off- chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain,” in 2020 International conference on communication systems & networks (COMSNETS), 2020, pp. 1–5.
28. S. Hai-Jew and S. Hai-Jew, “Alpha testing, beta testing, and customized testing,” Des. Instr. Open Shar., pp. 381–428, 2019.
29. Maramba, A. Chatterjee, and C. Newman, “Methods of usabilitytesting in the development of eHealth applications: a scoping review,” Int. J. Med. Inform., vol. 126, pp. 95–104, 2019.

30. S. Kruse, A. Stein, H. Thomas, and H. Kaur, “The use of electronic health records to support population health: a systematic review of the literature,” J. Med. Syst., vol. 42, pp. 1–16, 2018.
31. M. Abouali, K. Sharma, O. Ajayi, and T. Saadawi, “Blockchain framework for secured on-demand patient health records sharing,” in 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021, pp. 35–40.
32. M. Alharby and A. Van Moorsel, “Blockchain-based smart contracts: A systematic mapping study,” arXiv Prepr. arXiv1710.06372, 2017.
33. S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, “Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey,” Comput. Secur., vol. 97, p. 101966, 2020.