Journal of Emerging Applied Sciences, Engineering, and Technology
An international, Double-blind peer-reviewed, Bi-Monthly journal
Volume: 2; Issue: 1
Jan – Feb 2026
ISSN: 3108-2882 (Print)
ISSN: 3108-2963 (Online)

Privacy-Preserving Medical Record Management System Using Blockchain and End-to-End Encryption

Sangamithrar, Daisy Merina R, Pavan Vignesh , Pavithrashree
Department of Artificial Intelligence and Data Science, Vel Tech Multi Tech Dr Rangarajan Dr Sakunthala Engineering college, Chennai-600055,
Email id: daisymerina@veltechmultitech.org

Abstract
The rapid digitization of healthcare services has significantly improved the accessibility and efficiency of medical information management. However, it has also introduced serious challenges related to data privacy, security, and unauthorized access to sensitive patient information. Traditional Electronic Health Record (EHR) systems typically rely on centralized storage architectures, making them vulnerable to data breaches, manipulation, and single points of failure. This paper proposes a privacy-preserving medical record management system that integrates blockchain technology with end-to-end encryption to ensure secure storage, controlled data access, and data integrity. The proposed framework allows patients, doctors, hospitals, pharmacies, and insurance providers to interact within a decentralized ecosystem where medical records are encrypted and securely shared through permission-based mechanisms. Blockchain provides immutability and transparency, ensuring that medical records cannot be altered without authorization, while cryptographic techniques protect patient confidentiality. The system also incorporates authentication mechanisms to ensure that only authorized stakeholders can access sensitive medical information. By combining decentralized storage with strong encryption techniques, the proposed model enhances trust, security, and operational efficiency in healthcare information systems. Experimental evaluation and system analysis demonstrate that the proposed framework can significantly improve privacy protection, reduce the risk of data breaches, and enable secure healthcare data exchange in modern digital healthcare environments.

Keywords
Blockchain, Electronic Health Records (EHR), Healthcare Security, Privacy Preservation, End-to-End Encryption, Distributed Ledger Technology.

1. Introduction

The healthcare industry has undergone rapid digital transformation with the adoption of Electronic Health Record (EHR) systems, telemedicine platforms, and digital healthcare services. These technologies enable efficient storage, retrieval, and sharing of patient information across healthcare institutions. However, the increased reliance on digital systems has also created serious concerns regarding the privacy and security of sensitive medical data. Medical records contain highly confidential information such as patient history, diagnostic reports, prescriptions, and treatment plans, making them attractive targets for cybercriminals. Several studies have reported that healthcare data breaches have increased significantly in recent years, highlighting the urgent need for robust security mechanisms to protect patient information [1].

Traditional healthcare data management systems typically rely on centralized databases controlled by hospitals or healthcare providers. Although centralized systems simplify data management, they introduce major vulnerabilities such as single points of failure, unauthorized access, and susceptibility to cyber attacks. If a centralized server is compromised, attackers can potentially gain access to large volumes of sensitive patient data. Furthermore, centralized architectures often lack transparency and do not provide patients with sufficient control over their own medical records. As a result, ensuring data privacy and secure sharing of healthcare information has become a critical research challenge in modern healthcare information systems [2].

Blockchain technology has emerged as a promising solution to address these challenges due to its decentralized, transparent, and tamper-resistant characteristics. A blockchain network stores data across multiple distributed nodes, ensuring that records cannot be altered without consensus among participants. This distributed ledger architecture eliminates single points of failure and significantly enhances data integrity. In healthcare systems, blockchain can be used to securely store medical record references while enabling controlled access to authorized stakeholders such as hospitals, physicians, and insurance companies. The immutability property of blockchain ensures that once a medical record is recorded, it cannot be modified or deleted without proper authorization, thereby improving accountability and trust in healthcare data management systems [3].

In addition to blockchain technology, cryptographic techniques such as end-to-end encryption play a crucial role in protecting patient privacy. Encryption ensures that medical data remains confidential even if it is intercepted during transmission or accessed by unauthorized parties. By combining blockchain with strong encryption mechanisms, healthcare systems can provide both data integrity and privacy preservation. This integration allows patients to maintain control over their medical records while enabling secure data sharing among healthcare providers when necessary for diagnosis, treatment, or insurance verification [4].

Recent research has explored various approaches to secure medical data using distributed systems, privacy-preserving architectures, and cryptographic frameworks. For example, Tertulino et al. proposed a secure software reference architecture for Electronic Health Records that emphasizes privacy-aware system design and layered security

mechanisms [5]. Similarly, Martinez et al. presented a comprehensive model for protecting sensitive patient data in clinical environments by identifying security requirements and implementing appropriate protection mechanisms [6]. These studies highlight the growing importance of secure and privacy-preserving healthcare data management systems. Motivated by these challenges, this paper proposes a privacy-preserving medical record management system that integrates blockchain technology with end-to-end encryption and authentication mechanisms. The proposed framework enables secure storage and controlled access to patient records while ensuring transparency and traceability of healthcare transactions. The system also supports interaction between different healthcare stakeholders including hospitals, doctors, pharmacies, and insurance providers through a secure digital platform.

The main contributions of this research are as follows:

- Design of a decentralized medical record management architecture using blockchain technology
- Integration of end-to-end encryption for protecting patient data privacy
- Implementation of role-based access control mechanisms for healthcare stakeholders
- Development of a secure framework for medical data sharing and healthcare service coordination

The remainder of this paper is organized as follows. Section 2 presents the literature review related to healthcare data security and blockchain-based medical record systems. Section 3 describes the proposed system architecture and methodology. Section 4 discusses system implementation and modules. Section 5 presents results and system analysis. Finally, Section 6 concludes the paper and highlights future research directions.

2. Literature Review

The increasing adoption of digital healthcare technologies has significantly improved the efficiency of medical services and patient data management. However, the widespread use of Electronic Health Record (EHR) systems has also raised serious concerns regarding data privacy, security, and unauthorized access. Healthcare information is highly sensitive and often targeted by cybercriminals due to its high value. Therefore, researchers have proposed various frameworks and technologies to enhance the protection of medical data while ensuring accessibility for authorized healthcare providers.

Recent studies have examined the security landscape of network-enabled medical devices and healthcare information systems. These investigations highlight the growing vulnerability of healthcare infrastructures to cyber threats, including unauthorized access, data manipulation, and system exploitation. Security assessments of medical devices have shown that many healthcare technologies lack comprehensive protection mechanisms such as effective logging systems, vulnerability monitoring, and secure communication protocols. These findings emphasize the need for stronger security frameworks and systematic evaluation methods to improve the cybersecurity posture of healthcare systems [1].

Another line of research focuses on the design of secure architectural frameworks for Electronic Health Record systems. Modern healthcare platforms require well-structured architectures that incorporate security and privacy considerations from the initial design stage. Layered architectural models have been proposed to improve system reliability by separating components such as data storage, communication, authentication, and access control. These architectures provide structured guidelines for developers to design secure EHR platforms while ensuring compliance with privacy requirements and regulatory standards. Case studies conducted on real-world healthcare infrastructures demonstrate that such architectures can significantly reduce vulnerabilities and improve the overall protection of patient data [2].

Research has also explored the use of artificial intelligence techniques for processing and managing medical data. Medical reports often contain complex structured information such as laboratory tables and diagnostic records. Extracting meaningful information from these documents is essential for efficient healthcare data analysis. Advanced models based on attention mechanisms and deep learning techniques have been developed to recognize and interpret the structure of medical examination reports. These systems improve the accuracy of medical document processing and contribute to the development of intelligent healthcare information systems capable of supporting clinical decision-making processes [3].

Another important research direction involves identifying and categorizing security risks associated with clinical environments. Healthcare ecosystems involve multiple stakeholders including hospitals, laboratories, healthcare professionals, and insurance providers, all of whom interact with sensitive patient data. Studies analyzing clinical workflows have proposed models for classifying patient information based on sensitivity levels and implementing appropriate protection mechanisms for each category. These models incorporate encryption techniques, secure communication protocols, and strict access control mechanisms to ensure the confidentiality and integrity of medical information [4].

Machine learning techniques have also been integrated into healthcare systems to improve predictive analysis and clinical decision support. Advanced deep learning models have been developed to analyze patient medical histories stored in Electronic Health Records and predict potential health conditions. These systems leverage structured medical knowledge and ontologies to enhance prediction accuracy and provide interpretable results. Such intelligent healthcare applications demonstrate the importance of reliable and secure data management systems that can support advanced analytical models without compromising patient privacy [5].

Despite these advancements, existing healthcare data management systems still face several limitations. Many systems rely on centralized storage architectures that are vulnerable to single points of failure and large-scale cyberattacks.

Journal of Emerging Applied Sciences, Engineering, and Technology
An international, Double-blind peer-reviewed, Bi-Monthly journal
Volume: 2; Issue: 1
Jan – Feb 2026
ISSN: 3108-2882 (Print)
ISSN: 3108-2963 (Online)

Additionally, interoperability challenges between healthcare institutions often restrict efficient data sharing and coordination among medical stakeholders. Patients also have limited control over their personal medical data, which raises ethical and privacy concerns.

To overcome these challenges, decentralized technologies such as blockchain have been proposed as promising solutions for healthcare data management. Blockchain provides a distributed ledger system that ensures data immutability, transparency, and resistance to unauthorized modifications. When combined with cryptographic techniques such as end-to-end encryption, blockchain-based systems can provide strong privacy protection while enabling secure and controlled sharing of medical records. These characteristics make blockchain a suitable technology for developing next-generation healthcare information systems that prioritize both security and patient data ownership.

Therefore, this research proposes a privacy-preserving medical record management system that integrates blockchain technology with encryption-based privacy protection mechanisms. The proposed framework aims to enhance data security, improve transparency, and enable secure collaboration among healthcare stakeholders while maintaining strict patient data confidentiality.

3. Research Methodology

3.1 Research Approach

The proposed privacy-preserving medical record management system is designed using a hybrid approach that integrates blockchain technology with end-to-end encryption to ensure secure healthcare data management. The methodology focuses on addressing the major challenges of healthcare information systems, including data confidentiality, integrity, secure sharing, and controlled access among multiple healthcare stakeholders. The research methodology involves system design, architecture development, security mechanism integration, and evaluation of the proposed framework for managing sensitive medical records in a decentralized environment.

The study begins with the analysis of existing healthcare data management systems and their limitations, particularly regarding centralized storage, weak access control mechanisms, and vulnerability to cyberattacks. Based on this analysis, a decentralized framework is developed in which patient records are securely stored using distributed ledger technology while sensitive information is protected through encryption mechanisms. The methodology also considers interoperability requirements among hospitals, doctors, pharmacies, patients, and insurance providers to ensure efficient healthcare service delivery while maintaining privacy protection.

3.2 System Design Framework

The design of the proposed system is based on three major security principles: data confidentiality, data integrity, and secure accessibility. Data confidentiality is achieved through end-to-end encryption techniques that ensure patient records remain protected from unauthorized access. Data integrity is ensured through blockchain technology, which provides a tamper-resistant ledger where every transaction is recorded immutably. Secure accessibility is implemented through authentication and role-based access control mechanisms that allow only authorized users to access specific data within the system.

The system architecture is structured in multiple layers to separate healthcare services, security mechanisms, and data storage processes. This layered architecture improves scalability and simplifies system management while maintaining strict privacy protection standards. The framework also incorporates cryptographic protocols to secure communication between healthcare entities, ensuring that sensitive data cannot be intercepted or modified during transmission.

3.3 Blockchain Integration

Blockchain technology forms the core component of the proposed system by providing decentralized storage and transparent transaction management. In the blockchain network, medical record transactions are recorded as blocks that are cryptographically linked to previous blocks, forming a secure chain of records. Each transaction undergoes verification through a consensus mechanism to ensure its validity before being added to the ledger.

The decentralized nature of blockchain eliminates the reliance on a single centralized database, thereby reducing the risk of system failure or large-scale data breaches. Additionally, the immutable property of blockchain ensures that once medical records are recorded, they cannot be modified or deleted without proper authorization. This feature enhances trust and accountability among healthcare stakeholders while protecting the authenticity of medical data [3].

3.4 Encryption and Privacy Mechanisms

To enhance privacy protection, the proposed system incorporates strong cryptographic encryption techniques. All patient records are encrypted before being stored on the system, ensuring that even if unauthorized parties gain access to the stored data, they cannot interpret the information without the appropriate decryption keys. End-to-end encryption ensures that only the intended recipient, such as a doctor or healthcare provider, can access the original patient information.

In addition to encryption, authentication mechanisms such as one-time password (OTP) verification and role-based authorization are implemented to regulate access to medical records. These mechanisms ensure that different stakeholders within the healthcare ecosystem can only access the data necessary for their specific roles. For example, doctors can view patient medical histories and provide treatment recommendations, while pharmacies can only access prescription details required for medication dispensing.

3.5 System Evaluation

The proposed system is evaluated based on several performance and security metrics, including data confidentiality, access control efficiency, data integrity, and system scalability. Security analysis focuses on the system's ability to

Journal of Emerging Applied Sciences, Engineering, and Technology
An international, Double-blind peer-reviewed, Bi-Monthly journal
Volume: 2; Issue: 1
Jan – Feb 2026
ISSN: 3108-2882 (Print)
ISSN: 3108-2963 (Online)

resist unauthorized access, tampering attempts, and cyber threats commonly associated with centralized healthcare databases.

Performance evaluation also examines the efficiency of blockchain transactions and the effectiveness of encryption mechanisms in protecting sensitive healthcare information. By integrating distributed ledger technology with cryptographic security mechanisms, the system aims to provide a secure and reliable healthcare data management environment that supports modern digital healthcare services.

4. Proposed System Architecture

4.1 System Overview

The proposed privacy-preserving medical record management system is designed as a decentralized healthcare platform that enables secure storage, sharing, and management of medical records. The system connects multiple healthcare stakeholders including hospitals, doctors, patients, pharmacies, and insurance providers through a secure digital infrastructure. Each stakeholder interacts with the system through authenticated access, ensuring that only authorized users can retrieve or update medical information.

The architecture is built upon blockchain technology, which maintains a distributed ledger containing references to encrypted medical records. Instead of storing sensitive patient data directly on the blockchain, encrypted data is stored in secure databases while the blockchain maintains transaction records and access permissions. This hybrid approach ensures both scalability and security while preventing excessive data storage on the blockchain network.

4.2 Architectural Components

The proposed system architecture consists of several interconnected components that work together to ensure secure healthcare data management. These components include the user interface layer, application service layer, blockchain layer, encryption module, and database storage layer.

The user interface layer provides interaction points for different stakeholders such as hospitals, doctors, and patients. This layer allows users to access system services including record management, consultation services, prescription handling, and insurance processing.

The application service layer manages system functionalities and coordinates communication between different modules. It processes requests from users, verifies authentication credentials, and ensures that appropriate permissions are granted before any medical data is accessed or modified.

The blockchain layer serves as the backbone of the system by maintaining a distributed ledger that records all medical data transactions. Each transaction includes metadata such as timestamp, user identity, and data access permissions. The blockchain ensures transparency and prevents unauthorized modification of records.

The encryption module is responsible for securing medical data before storage or transmission. Encryption algorithms ensure that sensitive information remains protected from unauthorized access. Only users possessing the correct decryption keys can retrieve the original medical data.

The database storage layer stores encrypted patient records, prescriptions, and healthcare documents. This layer works in coordination with the blockchain ledger to ensure that stored data remains consistent, secure, and accessible only to authorized users.

4.3 Data Flow in the System

The data flow within the proposed system begins when a healthcare stakeholder initiates a request to access or update patient information. The request is first verified through authentication mechanisms to ensure that the user is authorized to perform the operation. Once authentication is successful, the system verifies access permissions based on predefined role-based policies.

If access is granted, the encrypted medical data is retrieved from the secure storage system and decrypted using appropriate cryptographic keys. Any modifications to patient records are recorded as new transactions in the blockchain ledger, ensuring that all changes are traceable and cannot be tampered with. This process maintains transparency and ensures the integrity of healthcare data across the entire system.

4.4 Security Architecture

The security architecture of the proposed system is designed to address multiple layers of protection against cyber threats. Encryption mechanisms ensure confidentiality of medical data, while blockchain technology guarantees integrity and immutability of records. Authentication and authorization mechanisms ensure that only legitimate users can access sensitive healthcare information.

By combining decentralized ledger technology with cryptographic security techniques, the system significantly reduces the risk of data breaches and unauthorized access. This architecture also enhances trust among healthcare stakeholders by providing a transparent and secure environment for medical data management.

5. System Modules

The proposed privacy-preserving medical record management system is designed as a multi-stakeholder healthcare platform. To ensure efficient management of medical records and healthcare services, the system is divided into several functional modules. Each module performs specific tasks while maintaining secure interaction with other components of the system. These modules collectively ensure secure storage, controlled access, and efficient management of medical information within the healthcare ecosystem.

5.1 Hospital Module

Journal of Emerging Applied Sciences, Engineering, and Technology
An international, Double-blind peer-reviewed, Bi-Monthly journal
Volume: 2; Issue: 1
Jan – Feb 2026
ISSN: 3108-2882 (Print)
ISSN: 3108-2963 (Online)

The hospital module enables healthcare institutions to securely register and access the platform for managing patient records and medical services. Hospitals can store encrypted patient information, including diagnostic reports, prescriptions, and treatment histories, within the system. These records are protected through cryptographic encryption mechanisms before being stored in the database and referenced on the blockchain ledger.

In addition to medical record management, the hospital module allows healthcare administrators to allocate doctors to patients, manage hospital resources, and update bed availability in real time. This functionality is particularly useful during emergency situations where quick allocation of hospital resources is required. The module also supports secure communication between hospitals and other stakeholders, ensuring that medical data is shared only with authorized entities.

5.2 Patient Module

The patient module provides individuals with secure access to their personal medical records. Patients can log into the system using authentication mechanisms such as one-time password verification and secure credentials. Once authenticated, patients can view their encrypted medical history, including prescriptions, diagnostic results, and treatment details.

The module also enables patients to search for nearby hospitals, consult doctors through secure communication channels, and review hospital services before seeking treatment. Patients can book emergency beds, purchase medicines through integrated pharmacy services, and apply for insurance policies digitally. By providing patients with direct access to their medical information, the system enhances transparency and empowers patients to actively participate in healthcare decision-making.

5.3 Doctor Module

The doctor module allows medical professionals to securely access patient information relevant to their treatment responsibilities. Doctors can view patient medical histories, analyze diagnostic reports, and monitor ongoing treatment progress. Access to patient data is strictly regulated through role-based access control mechanisms to ensure that doctors only access information related to their assigned patients.

Doctors can also communicate with patients through the platform to provide consultation, treatment recommendations, and follow-up guidance. This communication functionality improves patient-doctor interaction and enables efficient remote healthcare services. By maintaining secure access to patient data, the module supports accurate diagnosis and effective treatment planning while preserving patient privacy.

5.4 Pharmacy Module

The pharmacy module enables registered pharmacies to manage medicine inventories and provide medication services through the platform. Pharmacies can upload details of available medicines, update stock levels, and process patient purchase requests. When a patient purchases medication, the transaction is securely recorded within the system for transparency and traceability.

Patients can browse available medicines, place orders, and complete digital payments through secure payment mechanisms. The pharmacy module also allows pharmacies to maintain transaction histories and manage financial records. By integrating pharmacy services within the healthcare platform, the system ensures a transparent and accountable medicine distribution process.

5.5 Admin Module

The admin module acts as the central management authority responsible for monitoring and maintaining the overall functionality of the system. Administrators oversee user registration processes for hospitals, doctors, pharmacies, and patients to ensure that only verified entities gain access to the platform.

The admin module also monitors system activity to ensure compliance with security protocols and regulatory standards. Administrators can track insurance transactions, monitor hospital resource allocation, and manage platform operations. This module ensures that the healthcare platform operates efficiently while maintaining transparency and accountability across all system components.

5.6 Blockchain and Encryption Module

The blockchain and encryption module forms the core security infrastructure of the proposed system. Blockchain technology ensures that all healthcare transactions are recorded in a distributed ledger, making them immutable and tamper-resistant. Each transaction related to medical records, consultations, prescriptions, and payments is stored as a block within the blockchain network.

To ensure privacy protection, patient data is encrypted before being stored or transmitted within the system. Encryption ensures that sensitive medical information cannot be interpreted by unauthorized parties even if access to stored data is obtained. Smart contract mechanisms can also be implemented to automate certain healthcare operations such as appointment scheduling, insurance verification, and prescription validation.By integrating blockchain technology with encryption techniques, the system ensures data integrity, transparency, and strong protection of patient privacy.

6. Results and Discussion

The proposed privacy-preserving medical record management system demonstrates significant improvements in healthcare data security and operational efficiency compared to traditional centralized systems. The integration of blockchain technology ensures that all transactions are recorded in an immutable distributed ledger, preventing unauthorized modification of medical records. This characteristic improves trust among healthcare stakeholders and ensures the authenticity of patient information.

The implementation of end-to-end encryption provides strong protection for sensitive medical data stored within the system. Encrypted records remain confidential and can only be accessed by authorized users possessing the appropriate decryption keys. This mechanism effectively prevents unauthorized access and reduces the risk of data breaches commonly associated with centralized healthcare databases.

The decentralized architecture of the proposed system also improves system reliability and availability. Since data transactions are maintained across multiple nodes within the blockchain network, the system is less vulnerable to single-point failures or server-based attacks. Furthermore, role-based access control mechanisms ensure that each stakeholder can only access the information necessary for their specific responsibilities, thereby minimizing privacy risks.

Another significant advantage of the proposed system is the improved interoperability among healthcare stakeholders. Hospitals, doctors, pharmacies, and insurance providers can securely exchange medical information through the platform while maintaining strict privacy protection standards. Patients also benefit from improved transparency, as they can directly access their medical records and track healthcare transactions.

Overall, the results indicate that the proposed system provides a secure, reliable, and scalable framework for managing healthcare information. By integrating blockchain technology with cryptographic security mechanisms, the system addresses major challenges associated with healthcare data privacy and enables secure collaboration among multiple healthcare entities.

7. Conclusion

The rapid digitization of healthcare services has created new opportunities for improving medical data management, but it has also introduced serious concerns regarding data privacy and security. Traditional healthcare information systems often rely on centralized architectures that are vulnerable to cyberattacks, unauthorized access, and data manipulation. Protecting sensitive patient information while ensuring efficient healthcare service delivery has therefore become a critical challenge for modern healthcare infrastructures.

This research proposed a privacy-preserving medical record management system that integrates blockchain technology with end-to-end encryption mechanisms. The proposed system enables secure storage, controlled access, and transparent management of medical records across multiple healthcare stakeholders. Blockchain technology ensures data integrity and immutability, while encryption mechanisms protect patient confidentiality and prevent unauthorized access.

The system architecture supports interaction between hospitals, doctors, patients, pharmacies, and administrators through a secure digital platform. Role-based access control mechanisms ensure that each stakeholder can access only the information necessary for their specific role. The decentralized nature of the blockchain network also improves system reliability and reduces the risk of single-point failures.

Future research can explore the integration of advanced technologies such as artificial intelligence, Internet of Things (IoT) healthcare devices, and decentralized identity management systems to further enhance the capabilities of the proposed framework. These developments can enable intelligent healthcare services while maintaining strong security and privacy standards.

References

[1] K. Peterson, R. Deeduvanu, P. Kanjamala and K. Boles, “A Blockchain-Based Approach to Health Information Exchange Networks,” in *Proc. IEEE International Conference on Big Data (Big Data)*, Washington, DC, USA, 2016.

[2] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” in *Proc. IEEE Open & Big Data Conference*, 2016.

[3] M. Mettler, “Blockchain Technology in Healthcare: The Revolution Starts Here,” in *Proc. IEEE International Conference on e-Health Networking, Applications and Services*, 2016.

[4] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa and X. Zhang, “BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments,” *Information*, vol. 8, no. 2, pp. 1–14, 2017.

[5] Z. Zhang, H. Wang, C. Wang and H. Fang, “Blockchain-Based Secure Electronic Medical Record Sharing System,” in *Proc. IEEE International Conference on Smart Computing*, 2018.

[6] Y. Zhang and J. Lin, “Blockchain-Based Secure and Privacy-Preserving Medical Data Sharing System,” *IEEE Access*, vol. 6, pp. 1–12, 2018.

[7] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[8] X. Liang, J. Zhao, S. Shetty and D. Li, “Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications,” in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2017.

[9] H. Ekblaw, A. Azaria, J. Halamka and A. Lippman, “A Case Study for Blockchain in Healthcare: MedRec Prototype for Electronic Health Records and Medical Research Data,” in *Proc. IEEE Open & Big Data Conference*, 2016.

[10] G. Wood, “Ethereum: A Secure Decentralized Generalized Transaction Ledger,” Ethereum Project Yellow Paper, 2014.

[11] J. Liu, M. Li, Q. Yu, J. Chen and C. Lai, “A Blockchain-Based Privacy-Preserving Electronic Health Record Sharing System,” *IEEE Access*, vol. 7, pp. 1–12, 2019.