Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 5, pp. 2061–2069, DOI 10.12694/scpe.v26i5.4905

THE BLOCKCHAIN IN THE DESIGN OF ELECTRONIC MEDICAL RECORD SYSTEM SUPPORTING MULTIMEDIA COMMUNICATION TECHNOLOGY

XIONG JIAN*, RAJAMOHAN PARTHASARATHY†, YINQING TANG‡, AND BINWEN HUANG§

Abstract. This paper proposes the design of electronic medical record system supported by multimedia communication based on blockchain technology. Blockchain technology ensures the secure storage and sharing of patient information through distributed ledger and smart contract algorithm. In this system, smart contracts are used to automatically execute cross-institutional data access control and audit functions to ensure the transparency and compliance of data access. At the same time, this paper introduces multimedia communication technology to support the efficient transmission and sharing of medical data, especially in diagnostic images, videos and voice. Simulation results show that the electronic medical record system based on blockchain has significantly improved data processing efficiency, security and reliability compared with traditional systems.

Key words: Smart contract algorithm; Multimedia communication; Electronic medical record system; Blockchain.

1. Introduction. As an important part of modern medical informatization, electronic medical record system (EMR) is gradually replacing the traditional paper medical record management method. However, the existing electronic medical record system still faces many challenges in data security, privacy protection, cross-institutional data sharing and data integrity. Especially when multiple roles such as medical institutions, doctors, and patients are involved, the circulation and security management of data are particularly prominent. Therefore, how to build a safe, reliable and efficient electronic medical record system has become a key issue in the current development of medical informationization.

The introduction of smart contracts enables blockchain to automatically execute pre-defined logical rules without the intervention of external third parties, ensuring that the data sharing and access process is transparent and compliant. Therefore, the application of blockchain in medical information sharing and privacy protection shows broad prospects. Reference [1] proposed a distributed medical information sharing solution based on blockchain, which successfully solved the problem that data in traditional centralized systems are easily tampered with and leaked. The solution achieves multi-party information synchronization through distributed ledgers, ensuring data security and consistency. Reference [2] discussed the application of blockchain in electronic medical record systems and proposed an automated data access control mechanism based on smart contracts, which effectively reduced the potential risks of manual operations and enhanced the transparency of the system. Reference [3] designed a cross-institutional information sharing framework based on blockchain, which solved the trust problem in information flow between different medical institutions and strengthened the protection of patient privacy. Reference [4] discusses the application of multimedia communication technology in medical systems, solving the problem of insufficient timeliness of medical data during transmission, especially in the real-time transmission of diagnostic images, videos, and voice data.

This paper proposes a blockchain-based electronic medical record system design. The system not only supports multimedia communication technology, but also realizes automatic access and sharing management of data through smart contracts. The core goal of this system is to solve the trust barriers and privacy leakage risks in traditional electronic medical record systems in data sharing, and significantly improve the efficiency and security of information transmission.

*Modern Educational Technology Center, Hainan Medical University, Haikou, Hainan, 571199, China; Faculty of Engineering, Built Environment and Information Technology SEGi University, Kuala Lumpur, 47810, Malaysia
†Faculty of Engineering, Built Environment and Information Technology SEGi University, Kuala Lumpur, 47810, Malaysia
‡Modern Educational Technology Center, Hainan Medical University, Haikou, Hainan, 571199, China
§Modern Educational Technology Center, Hainan Medical University, Haikou, Hainan, 571199, China (Corresponding author, huangbinwen88@126.com)

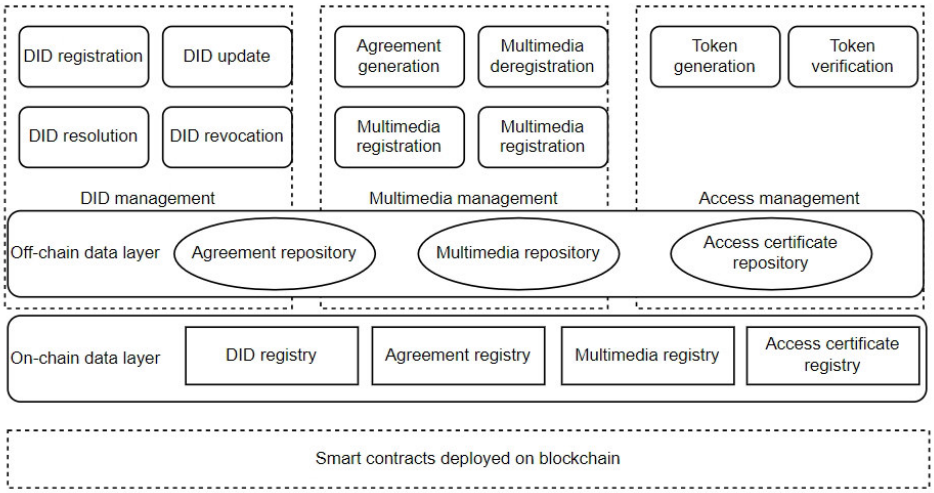

Fig. 2.1: Blockchain and multimedia communication integration architecture.

2. System architecture design.

2.1. Integration architecture of blockchain and multimedia communication. In order to solve the shortcomings of traditional electronic medical record systems, this paper proposes an electronic medical record system architecture based on blockchain and multimedia communication technology. The system architecture is shown in Figure 2.1.

The blockchain network layer is responsible for recording all data operations related to electronic medical records. Through the distributed ledger method, the data is tamper-proof and transparent. All operations, including the creation, access, and modification of medical records, will be recorded and executed through smart contracts.

The smart contract layer is used to realize automated medical record data management, especially the access control of data. Each query, sharing, or update of medical records will trigger the corresponding smart contract to ensure the legality and compliance of data access.

The multimedia communication layer is mainly used to process multimedia information in medical data. Through advanced communication protocols and technologies, this layer can efficiently transmit large-capacity data such as medical images and diagnostic videos, while ensuring the security of data transmission.

Due to the diversity and large volume of medical data, it is not feasible to rely solely on blockchain storage. Therefore, this system adopts a distributed storage solution to store data in various nodes and ensure the security of data through encryption mechanisms.

2.2. Application of smart contracts in medical record data management. Smart contracts play a key role in this system, especially in medical record data management. Through smart contracts, the system can realize automatic processing and access control of medical record data [5]. Smart contracts predefine the permissions of various roles, such as doctors, patients, insurance companies, etc. Only users who meet the permission requirements can access the corresponding medical record data through smart contracts.

In addition, smart contracts are also used to record logs of each data operation. Whenever a user queries or updates a medical record, the smart contract automatically records the time, operator, and content of the operation [6]. This logging mechanism not only ensures the transparency of data access, but also facilitates data auditing. Smart contracts can also realize multi-party data sharing. For example, in cross-institutional medical cooperation, different medical institutions can achieve secure data sharing through smart contracts without worrying about data leakage or tampering. At the same time, smart contracts can automatically execute data sharing agreements without the intervention of third parties, reducing the risk of human intervention.

2.3. Data encryption and storage. To ensure the security of data during transmission and storage, this system uses a variety of encryption and security algorithms, including elliptic curve encryption (ECC), hash algorithms, and distributed storage. The following are the main technologies used by the system and their mathematical descriptions.

2.3.1. Elliptic Curve Encryption. ECC is an efficient public key encryption technology, especially suitable for resource-constrained environments [7]. Compared with the traditional RSA algorithm, ECC requires a shorter key length while providing the same level of security, so it is more computationally efficient. The basic formula of ECC is as follows:

$$y^2 = x^3 + ax + b(\text{mod}) \tag{2.1}$$

a and b are the parameters of the elliptic curve, and p is a prime number. Through this formula, the system can generate public and private keys for encrypting and decrypting medical record data.

2.3.2. Hash algorithm. In the blockchain system, hash algorithms are widely used to verify the integrity of data. The system uses the SHA-256 hash function to generate a unique identifier for the data, ensuring that the medical record information remains intact during storage and transmission without any modification [8]:

$$H(m) = h_1\left(h_2\left(\ldots h_n(m)\right)\right) \tag{2.2}$$

m represents the input data, and $H($ m) is the generated hash value. The algorithm is calculated through multiple iterations to ensure that any small data change will lead to a significant change in the hash value.

2.3.3. Data encryption and decryption. In this system, each electronic medical record will be encrypted by ECC before storage. Assuming that the medical record data is D, its encryption process can be expressed as:

$$C = E(D, k) = D \cdot k(\text{modp}) \tag{2.3}$$

Among them, k is the encryption key, and C is the encrypted medical record data. The decryption process is:

$$D = C \cdot k^{-1}(\text{modp}) \tag{2.4}$$

This encryption and decryption mechanism ensures the security of medical record data. Even if the data is intercepted during transmission or storage, the attacker cannot decrypt the content [9].

2.3.4. Distributed storage mechanism. This system adopts a distributed storage mechanism [10]. Medical record data will not be stored directly on the blockchain, but will be stored through distributed nodes. The blockchain only saves the index and hash value of the data. The distribution of data in the distributed storage network is as follows:

$$D = (D_1, D_2, \ldots, D_n) \tag{2.5}$$

$D_1, D_2, \ldots, D_n$ represent different parts of the medical record data after being sharded. These fragments are distributed and stored in different nodes [11].

3. Application of blockchain technology.

3.1. The role of blockchain in the electronic medical record system. In the electronic medical record system, blockchain technology plays a vital role, mainly in the storage, security verification and sharing of information. First, the distributed ledger structure of blockchain ensures the security and tamper-proof nature of data storage. Whenever an electronic medical record is operated, a corresponding block is created, and a consensus mechanism is used to ensure that these operations are consistent and verifiable throughout the network. The distributed storage of data not only reduces the possibility of single point failures, but also enhances the redundancy and security protection of information [12].

Secondly, blockchain also plays a key role in the verification of medical record data. Each data operation generates a hash value, and the integrity and legitimacy of the operation are verified by a hash function. For example, assuming there is a medical record data D, its corresponding hash value $H(D)$ can be obtained by the following formula:

$$H(D) = \text{hash}(D) \tag{3.1}$$

This hash value is compared with the historical data records in the blockchain. If the hash values are consistent, the verification is passed, indicating that the data has not been tampered with. Otherwise, the system will prompt that the data may be tampered with or damaged.

3.2. Medical record transmission and verification under multimedia communication technology. In the medical environment, medical records are not just text data, but more often include complex multimedia information, such as medical images, videos, audio, etc. Therefore, how to efficiently and securely transmit these multimedia medical record data is one of the focuses of system design [13]. The combination of blockchain and multimedia communication technology provides an ideal solution for this. The distributed structure of blockchain can effectively protect multimedia data from tampering during transmission. Each piece of multimedia data will be encrypted before transmission and a unique hash value will be generated to ensure the integrity and consistency of the data. For example, for a medical image I, the encrypted ciphertext $E(I)$ and the corresponding hash value $H(E(I))$ can be expressed as follows:

$$\begin{aligned} E(I) &= \text{encrypt}(I, k) \\ H(E(I)) &= \text{hash}(E(I)) \end{aligned} \tag{3.2}$$

k is the encryption key, $E(I)$ is the encrypted image data, and $H(E(I))$ is the hash value of the data. After the data transmission is completed, the receiver can verify the integrity and consistency of the data through decryption and hash verification.

3.3. Design and implementation of smart contracts. The role of smart contracts in blockchain cannot be ignored, especially in electronic medical record systems, where its main functions are reflected in permission management, data auditing and automated processing.

Smart contracts allow the system to assign different access rights to different users. Taking doctors, patients and medical insurance companies as examples, different roles have different access rights [14]. For example, patients can view all their medical records, while doctors can only view relevant medical records. Every creation, modification or access operation of medical record data will be recorded by the smart contract on the blockchain to form an unalterable log. In this way, when a security incident occurs, the system administrator can use these logs to audit the data and track the source, time, and content of each data operation. Smart contracts can also automate the management of medical records. For example, when a doctor enters a new diagnosis, the system automatically activates the smart contract and sends the diagnosis information to the patient and related medical institutions without any human intervention. This automated operation significantly improves the efficiency of the system and reduces the potential risks of human intervention [15]. The execution efficiency and stability of smart contracts depend on the design quality of the underlying code. During the design phase, the system must ensure the accuracy of the contract logic to avoid security vulnerabilities and logical errors. The execution process of a smart contract is as follows:

$$T_i = C\left(x_i\right) \tag{3.3}$$

T_i represents the execution result, C is the logic function of the smart contract, and x_i is the input data. The contract processes the input data according to the preset rules and outputs the corresponding results.

3.4. Privacy protection mechanism of blockchain. Patients' medical information is very sensitive, so the system must have an effective privacy protection mechanism.

Zero-knowledge proof is a cryptographic technology that allows users to prove the legitimacy of their possession of certain data without disclosing specific information [16]. For example, a user can prove that he

Table 4.1: Experimental data set

Data type	medical records (n)	Data size (GB)	Data content
Plain text medical records	1000	0.5	Plain text information such as diagnosis reports and prescriptions
Image medical records	1000	5.2	MRI images, CT scan images
Video medical records	500	20	Ultrasound videos, dynamic image records
Voice medical records	500	1.5	Doctor's diagnosis voice records

has access to a medical record without revealing the specific contents of the medical record. The mathematical model of zero-knowledge proof is as follows:

$$P(x) \to V \tag{3.4}$$

Among them, $P(x)$ represents the secret data held by the prover, and V is the verifier. In the zeroknowledge proof process, the specific content of $P(x)$ will not be passed to V, but the verifier can still confirm the legitimacy of the prover. Homomorphic encryption allows encrypted data to be directly operated without decryption. In the process of medical data processing, homomorphic encryption can ensure that the data remains encrypted during processing and analysis, thereby protecting data privacy [17]. For example, suppose there are two encrypted medical data $E(A)$ and $E(B)$. Homomorphic encryption allows the encrypted data to be added, and the result is:

$$E(A+B) = E(A) \oplus E(B) \tag{3.5}$$

Combined with zero-knowledge proof and homomorphic encryption technology, the application of blockchain in medical record system can effectively protect patient privacy and ensure that data will not be leaked during storage, transmission and processing.

4. Experiment and performance analysis.

4.1. Design of experimental data set and multimedia medical record. In this experiment, electronic medical record data sets from multiple sources are selected, and multimedia medical record data are introduced for testing. Traditional electronic medical record data sets contain text records, diagnosis reports, drug prescriptions, etc., while multimedia medical records are extended to include medical images, video records, and voice diagnosis. In order to simulate the actual medical scenario, this paper obtained 3,000 medical records from the hospital system, including 1,000 MRI data with images, 500 dynamic ultrasound videos, and 1,500 medical records containing voice records [18]. To ensure the breadth and representativeness of the experiment, this paper divides the data set into three categories: plain text medical records, multimedia medical records (images and videos), and medical records combined with multimedia and text. Different types of medical records have different storage, transmission and processing requirements in the system. Through these multi-dimensional data experiments, the integration effect of blockchain and multimedia communication technology can be more comprehensively evaluated. The specific contents of the experimental data set are shown in Table 4.1.

4.2. Evaluation Indicators. In order to evaluate the performance of this system in the multimedia electronic medical record scenario, this paper selects system performance, storage efficiency, communication delay and security analysis as the main evaluation indicators. The results of the system performance evaluation are shown in Table 4.2.

The system has high performance when processing plain text medical records, while the processing efficiency of image and video medical records is relatively low due to the large data volume, but it can still meet the actual application needs.

Table 4.2: The results of the system performance evaluation.

Metrics	Plain text medical records	Image medical records	Video medical records	Voice medical records
Throughput (records/s)	1200	850	450	750
Response time (milliseconds)	200	400	600	350
Contract execution time (s)	0.8	1	1.5	1.1

Table 4.3: Comparison of the three consensus mechanisms in system performance.

Consensus Mechanism	Throughput records	Response time (ms)	Consensus time (s)
PoW	500	800	2.5
PoS	1000	300	1.2
PBFT	1200	200	0.8

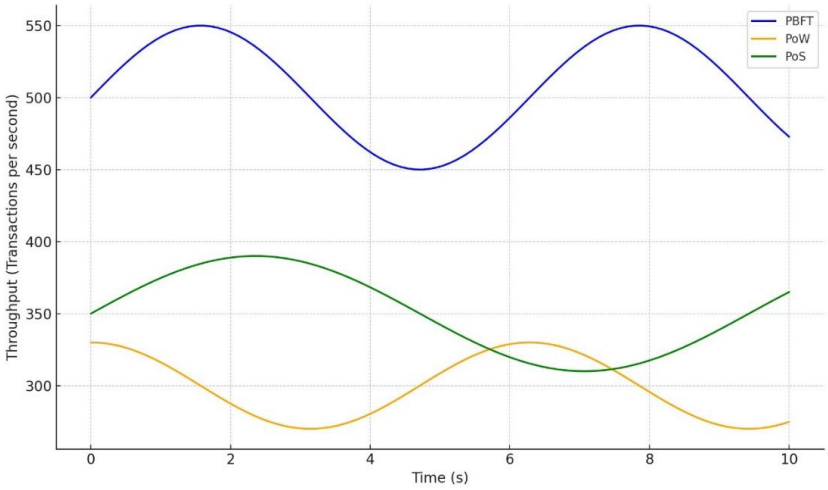

Fig. 4.1: Performance trends of different consensus mechanisms in terms of processing throughput.

4.3. Performance comparison analysis of blockchain systems. This paper compares the performance differences of proof of stake (PoS), practical Byzantine fault tolerance (PBFT) and proof of work (PoW) when processing electronic medical record data. Table 4.3 shows the comparison of the three consensus mechanisms in system performance.

PBFT has the best overall performance and is suitable for deployment in medical data environments that require high efficiency. Figure 4.1 shows the performance trends of different consensus mechanisms in terms of processing throughput.

4.4. Evaluation of the effectiveness of data encryption and distributed storage. In order to ensure the security and storage efficiency of medical record data, the system adopts a solution that combines elliptic curve cryptography (ECC) with distributed storage. In the experiment, this paper compares the changes in the storage efficiency of the system before and after using distributed storage, as well as the performance overhead caused by encryption during data transmission. First, the storage efficiency of the system in both encrypted and unencrypted conditions is evaluated. Table 4.4 shows the storage size comparison of various medical record data in encrypted and unencrypted states:

Table 4.4: The storage size comparison of various medical record data in encrypted and unencrypted states.

Medical record type	Original size (GB)	Encrypted size (GB)	Storage Optimization Ratio
Plain text medical record	0.5	0.6	-20%
Image medical record	5.2	4.9	6%
Video medical record	20	18.5	7.50%

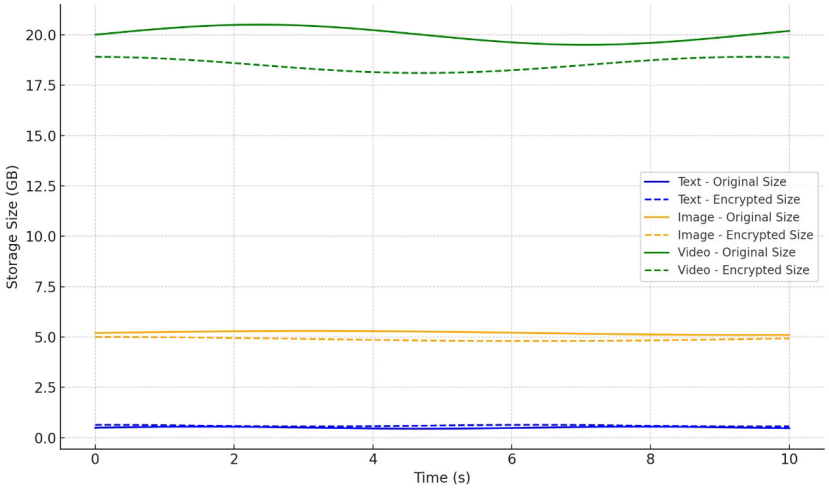

Fig. 4.2: Comparison of storage efficiency of different medical record type.

It can be seen that for multimedia data, the encryption process does not significantly increase the storage space requirements, but reduces the storage cost through the optimization of distributed storage. Figure 4.2 shows the storage efficiency comparison of different medical record types.

Secondly, the impact of the data encryption process on communication delay was evaluated. The experimental results show that although data encryption increases a certain amount of computational overhead, the delay increase is small for plain text data; while for video data, the delay caused by the encryption process is more obvious. Overall, the system can provide acceptable communication delay while ensuring data security. Figure 4.3 shows the impact of data encryption on communication delay of different medical record types.

5. Conclusion. This system can ensure the secure storage and access control of medical data. Smart contracts automatically execute permission management, ensure the transparency and compliance of data, and reduce the security risks caused by manual operations. At the same time, the application of multimedia communication technology improves the transmission efficiency of medical data, especially in supporting the transmission of large amounts of information such as diagnostic images and videos. The simulation results show that the electronic medical record system based on blockchain has significant improvements in security, reliability and data processing efficiency compared with traditional systems. The system improves the redundancy and anti-tampering ability of data storage through a distributed structure, while the smart contract algorithm effectively solves the trust problem in cross-institutional data sharing. Combined with multimedia communication technology, the system can meet the needs of modern medicine for efficient, convenient and reliable data sharing, especially in the application scenarios of telemedicine and multi-party collaboration.

6. Acknowledgements.

1. Research project on education and teaching reform of colleges and universities in Hainan Province: Application of medical data sharing in hospital virtual simulation teaching. (NO: Hnjg2019-53).

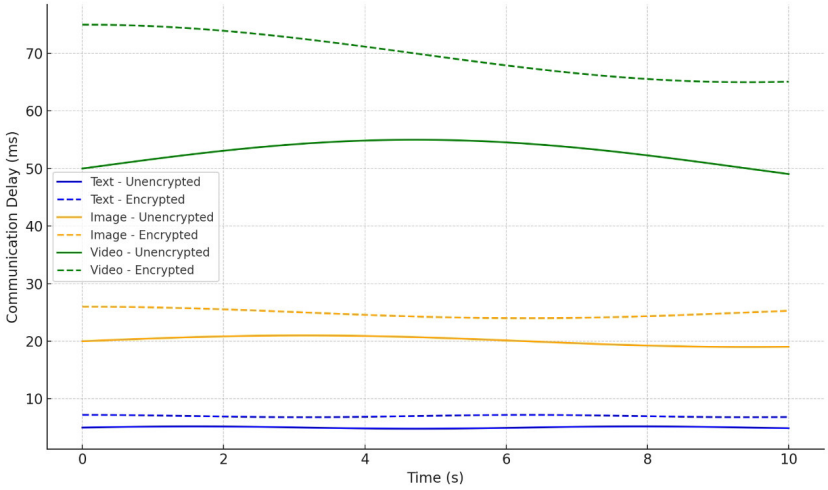

Fig. 4.3: The impact of data encryption on communication delays of different medical record types.

2. Major science and technology projects in Hainan Province: New intelligent multi-point trigger early warning and diagnosis technology for emerging and sudden infectious diseases. (NO:ZDKJ2021029).
3. Industry-university cooperation coordination education project of the Ministry of Education in 2022 (No.220604719293004).

REFERENCES

[1] Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. *Healthcare informatics research*, *26*(1), 3-12.

[2] Mahajan, H. B., & Junnarkar, A. A. (2023). Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. *Multimedia Tools and Applications*, *82*(28), 44335-44358.

[3] Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *17*(2s), 1-17.

[4] Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2023). RETRACTED ARTICLE: Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, *13*(3), 2329-2342.

[5] Abbate, S., Centobelli, P., Cerchione, R., Oropallo, E., & Riccio, E. (2022). Blockchain technology for embracing healthcare 4.0. *IEEE Transactions on Engineering Management*, *70*(8), 2998-3009.

[6] Stafford, T. F., & Treiblmaier, H. (2020). Characteristics of a blockchain ecosystem for secure and sharable electronic medical records. *IEEE Transactions on Engineering Management*, *67*(4), 1340-1362.

[7] Reegu, F. A., Mohd, S., Hakami, Z., Reegu, K. K., & Alam, S. (2021). Towards trustworthiness of electronic health record system using blockchain. *Annals of the Romanian Society for Cell Biology*, *25*(6), 2425-2434.

[8] Sabu, S., Ramalingam, H. M., Vishaka, M., Swapna, H. R., & Hegde, S. (2021). Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain. *Global Transitions Proceedings*, *2*(2), 429-433.

[9] Liu, Y., Lu, Q., Zhu, C., & Yu, Q. (2021). A blockchain-based platform architecture for multimedia data management. *Multimedia Tools and Applications*, *80*(20), 30707-30723.

[10] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and ubiquitous computing*, *28*(1), 59-72.

[11] Mahajan, H. B. (2022). Emergence of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems: solutions, challenges, and future roadmap. *Wireless Personal Communications*, *126*(3), 2425-2446.

[12] Wang, J., Fan, S., Alexandridis, A., Han, K., Jeon, G., Zilic, Z., & Pang, Y. (2021). A multistage blockchain-based secure and trustworthy smart healthcare system using ecg characteristic. *IEEE Internet of Things Magazine*, *4*(3), 48-58.

[13] Biswas, S., Sharif, K., Li, F., Latif, Z., Kanhere, S. S., & Mohanty, S. P. (2020). Interoperability and synchronization management of blockchain-based decentralized e-health systems. *IEEE Transactions on Engineering Management*, *67*(4), 1363-1376.

[14] Kim, H., Lee, S., Kwon, H., & Kim, E. (2021). Design and implementation of a personal health record platform based on patient-consent blockchain technology. *KSII Transactions on Internet and Information Systems (TIIS)*, *15*(12), 4400-4419.

[15] Shuaib, K., Abdella, J., Sallabi, F., & Serhani, M. A. (2022). Secure decentralized electronic health records sharing system based on blockchains. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5045-5058.

[16] Adegoke, A. (2023). Patients' reaction to online access to their electronic medical records: the case of diabetic patients in the US. *International Journal of Applied Sciences: Current and Future Research Trends*, *19*(1), 105-115.

[17] Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: a systematic mapping study. *Journal of Public Health*, *32*(3), 435-454.

[18] Lewis, A. E., Weiskopf, N., Abrams, Z. B., Foraker, R., Lai, A. M., Payne, P. R., & Gupta, A. (2023). Electronic health record data quality assessment and tools: a systematic review. *Journal of the American Medical Informatics Association*, *30*(10), 1730-1740.

[19] Landolsi, M. Y., Hlaoua, L., & Ben Romdhane, L. (2023). Information extraction from electronic medical documents: state of the art and future research directions. *Knowledge and Information Systems*, *65*(2), 463-516.

Edited by: Hailong Li
Special issue on: Deep Learning in Healthcare
Received: Sep 13, 2024
Accepted: Oct 14, 2024