International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Automated Medical Record Authentication and Verification with Blockchain Technology: A Study

Bindushree K P[1], Rashmi C R[2], Shantala C P[3]

[1]M.Tech Candidate, Department of Computer Science and Engineering, Channabasaveshwara Institute of Technology, Gubbi
[2]Assistant Professor, Department of Computer Science and Engineering, Channabasaveshwara Institute of Technology, Gubbi
[3]Professor and Head, Department of Computer Science and Engineering, Channabasaveshwara Institute of Technology, Gubbi

ABSTRACT
A health record is a crucial component of patient follow-up, encompassing healthcare professionals' observations, prescriptions, diagnoses, and all relevant data about the patient. Multiple stakeholders—including the patient, doctor, and pharmacist—are involved in the management and sharing of this record. Electronic Medical Records (EMRs) can be accessed by authorized individuals from anywhere, facilitating the sharing of information among various healthcare providers. However, this sharing process requires strict security and confidentiality measures. Current medical systems face challenges such as potential system failures and malicious attacks, which can undermine service reliability. Additionally, managing centralized access control can be difficult. This paper introduces SEMRAchain, a system integrating role-based access control (RBAC), attribute-based access control (ABAC), and smart contracts. This combination enables decentralized, fine-grained, and dynamic access management for EMR systems. By leveraging blockchain technology as a secure distributed ledger, SEMRAchain offers stakeholders not only visibility but also trustworthiness, credibility, and immutability.

Keywords: Blockchain; smart contract; Ethereum.

1. INTRODUCTION

The global scientific device market is projected to grow at a compound annual growth rate (CAGR) of 4.5%, reaching $409.5 billion by 2025. This growth is expected to be driven by advancements in technology that enhance patient care and data management. One significant development is the ability to disconnect patients from a hospital's centralized system while still enabling communication with their healthcare providers. Given the sensitivity of medical records, effective privacy and security are paramount. Traditionally, these records are stored in various locations and managed by multiple healthcare professionals. However, with the rise of technologies such as the Internet of Things (IoT) and artificial intelligence (AI), medical records are increasingly stored electronically. This digitalization allows for secure storage and real-time updating of patient information with proper consent, ensuring

confidentiality. To address security concerns, cryptographic methods have been developed to protect healthcare data from cyberattacks, particularly in IoT systems.

To tackle the challenges of decentralization, automation, security, and trust management in healthcare, the integration of blockchain technology and multi-agent systems (MAS) presents a promising solution. Blockchain technology offers a distributed and secure ledger, enabling patients to oversee and control access to their data, while ensuring interoperability among various health stakeholders. Additionally, in emergency situations, healthcare services can access patient data directly without requiring patient consent at that moment. MAS facilitates the automation of interactions within a decentralized system, improving communication between systems and ensuring vendor security. By utilizing smart contracts and role-based access control (RBAC) and attribute-based access control (ABAC) methods, this approach eliminates the need for a central authority, reducing maintenance costs and mitigating risks associated with centralized systems.

In the healthcare sector, tracking electronic medical records with blockchain technology aims to enhance security and trust among system agents by automating interactions through smart contracts, without human intervention. Key principles for safeguarding patient information include robust authentication and access control mechanisms.

The main contributions of this paper can be summarized as follows:

- Proposing a Blockchain-Based Platform: The paper introduces a blockchain-based platform specifically designed for managing electronic patient records, enhancing the security and integrity of sensitive medical data.
- Utilizing Access Control Techniques: It leverages access control methods, particularly Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC), to regulate access to the system and prevent unauthorized external intrusion.
- Integrating Smart Contracts: The paper combines smart contracts with access control mechanisms to ensure both the safety and confidentiality of the managed data, automating and securing interactions within the system.

2. LITERATURE REVIEW

Blockchain technology offers an immutable, decentralized network where all participating nodes utilize consensus algorithms and smart contracts to validate transactions. This approach has been adopted by various healthcare systems to enhance privacy and security in communication. Table 1 will later illustrate the study gaps and outline our research motivations. In this paper, the authors have employed smart contracts to develop a remote patient monitoring system that alerts healthcare professionals in emergencies.

The proposed system ensures patient privacy and security through blockchain technology and features three main components and three key actors. The first component involves the registration of patients and doctors on the platform. They access it via a mobile phone, securely entering and updating their information, such as identity, name, and age. Patient monitoring is conducted through data collected from IoT sensors, which is then securely stored on the blockchain via smart contracts. This facilitates real-time tracking of patients by doctors. The final component addresses the organization and medical devices, where a smart contract is established between the organization and the patient upon purchasing a device, registering it under the patient's name, and ensuring that the data collected by the IoT device is recorded at the care center.

To address issues encountered in cloud-based systems, the authors proposed an architecture named BIoMT. This architecture ensures security through the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) and proof-of-work as a consensus mechanism.

3. PROPOSED SYSTEM

The proposed system, SEMRAchain, is a platform designed for the exchange and sharing of patient medical information. This solution integrates blockchain technology with multi-agent systems to enhance security and manage data across various stakeholders. To safeguard the data handled by different parties, the system utilizes access control mechanisms, specifically Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC), along with smart contracts.

The system must fulfill several requirements to function effectively. First, it needs to establish the identity of individuals authorized to participate in the digital medical record management process. Participants must authenticate themselves to access resources, and each has a predefined role in handling patient records, with access restricted to what is necessary for their responsibilities. Given the large volume of data exchanged in healthcare and the growing scale of the network as new users join, scalability is a critical factor. Therefore, the digital medical record system must feature a flexible user interface that simplifies and streamlines resource use.

Additionally, the application must adhere to the CIA triad—confidentiality, integrity, and availability. It is crucial to protect patient data from unauthorized viewing or modification to maintain its reliability and accuracy while ensuring that legitimate users can access the information when needed.

As illustrated, various vendors access patient information, which is aggregated and stored on the blockchain. Smart contracts manage consultations and updates to the electronic medical record (EMR). Each agent must be authenticated to handle the data relevant to their role within a specified timeframe. For example, after examining a patient, a doctor's agent records prescriptions, scans, and test results as operations. Pharmacies and laboratories also record transactions and analyses on the blockchain. Through smart contracts, patients can use digital tokens for online consultations and medication purchases, further integrating blockchain into the healthcare ecosystem.

Within the EMR system, multiple vendors exchange data through a web application designed for managing health information. To access this application, users must undergo authentication. Depending on the user type, smart contracts facilitate the secure and automated transfer of data. Information stored on the blockchain is then presented through the appropriate interface. This approach leverages the transparency and immutability of blockchain technology to assign access roles and maintain the security of patient information, protecting it against potential attacks.

The system's architecture comprises two main components: a Multi-Agent System (MAS) that facilitates communication among vendors and a public blockchain network (BC) that stores all transactions and smart contracts. The proposed model is based on three key principles:

- Smart Contracts: Smart contracts are integral to the blockchain framework, performing essential functions. For our system, we deploy various smart contracts for stakeholder enrollment and authentication, which govern and verify electronic medical records (EMR).
- Authentication: Access to the system requires personal authentication via Ethereum addresses assigned to each agent. Upon successful authentication, patients and healthcare professionals can interact and exchange information.

- Access Control: Access control ensures that only authorized entities can manage and update data. In this system, healthcare professionals request access through smart contracts, which verify the requester's identity and permissions before authorizing data modifications.

4. CONCLUSION

With the onset of COVID-19, the shift to telemedicine highlighted the risks of patient information exposure. To address these concerns, our study integrates blockchain technology with multi-agent systems and access control. The system prioritizes security, using strategically placed smart contracts to manage access requests, policy enforcement, and misconduct checks. The total transaction cost for the proposed system is 0.01751596 ETH, equivalent to £58.61. Specifically, the execution cost for the EMR management contract is 0.00890416 ETH, the registration contract is 0.0086118 ETH, and the agent enrollment contract is 0.008752 ETH. A thorough evaluation based on five criteria—blockchain technology, access management, security, integrity, and multi-agent systems—demonstrates that the platform excels in security, availability, and privacy.

Future work will involve expanding the system to include a platform with three main components: a hospital directory, electronic medical records (EMRs), and a network of ambulances. These components will be interconnected via a blockchain network, allowing users to locate the nearest medical services and ambulances in case of an emergency.

REFERENCES

1. Goyal, S.; Sharma, N.; Bhushan, B.; Shankar, A.; Sagayam, M. IoT Enabled Technology in Secured Healthcare: Applications,Challenges and Future Directions. In Cognitive Internet of Medical Things for Smart Healthcare. Studies in Systems, Decision andControl; Hassanien, A.E., Khamparia, A., Gupta, D., Shankar, K., Slowik, A., Eds.; Springer: Cham, Switzerland, 2021; Volume 311.
2. Mhamdi, H.; Soufiene, B.O.; Zouinkhi, A.; Ali, O.; Sakli, H. Trust-Based Smart Contract for Automated Agent to AgentCommunication. Comput. Intell. Neurosci. 2022,2022, 5136865.
3. Ben Othman, S.; Almalki, F.A.; Chakraborty, C.; Sakli, H. Privacy-preserving aware data aggregation for IoT-based healthcarewith green computing technologies. Comput. Electr. Eng. 2022,101, 108025.
4. Bharadwaj, H.K.; Agarwal, A.; Chamola, V.; Lakkaniga, N.R.; Hassija, V.; Guizani, M.; Sikdar, B. A Review on the Role of MachineLearning in Enabling IoT Based Healthcare Applications. IEEE Access 2021,9, 38859–38890.
5. Gope, P.; Millwood, O.; Sikdar, B. A Scalable Protocol Level Approach to Prevent Machine Learning Attacks on PUF-basedAuthentication Mechanisms for Internet-of-Medical-Things. IEEE Trans. Ind. Inform. 2021,18, 1971–1980.
6. Ahmed, I.; Jeon, G.; Piccialli, F. A Deep-Learning-Based Smart Healthcare System for Patient's Discomfort Detection at the Edgeof Internet of Things. IEEE Internet Things J. 2021,8, 10318–10326.
7. Almalki, F.A.; Soufiene, B.O. EPPDA: An Efficient and Privacy-Preserving Data Aggregation Scheme with Authentication andAuthorization for IoT-Based Healthcare Applications. Wirel. Commun. Mob. Comput. 2021,2021, 5594159.
8. Cho, C.; Seong, Y.; Won, Y. Mandatory Access Control Method for Windows Embedded OS Security. Electronics 2021, 10, 2478.

9. Recommendation on a European Electronic Health Record Exchange Format. Available online: https://digital-strategy.ec.europa.eu/fr/node/2138 (accessed on 31 July 2022).
10. Mhamdi, H.; Othman, S.B.; Zouinkhi, A.; Sakli, H. Blockchain Technology in Healthcare: Use Cases Study. In Intelligent Healthcare;Chakraborty, C., Khosravi, M.R., Eds.; Springer: Singapore, 2022.
11. Mhamdi, H.; Othman, S.B.; Zouinkhi, A.; Almalki, F.A.; Sakli, H. Blockchain Technology in Healthcare: A Systematic Review.In Blockchain Technology in Healthcare Applications: Social, Economic, and Technological Implications, 1st ed.; Bhushan, B., Rakesh, N.,Farhaoui, Y., Astya, P.N., Unhelkar, B., Eds.; CRC Press: Boca Raton, FL, USA, 2022.
12. Kazmi HS, Z.; Nazeer, F.; Mubarak, S.; Hameed, S.; Basharat, A.; Javaid, N. Trusted Remote Patient Monitoring Using Blockchain-BasedSmart Contracts; BWCCA 2019, LNNS 97; Springer Nature Switzerland AG 2020L: Berlin/Heidelberg, Germany, 2020; pp. 765–776