A Blockchain-Based Approach for Audit Management of Electronic Health Records

Rashmi P. Sarode(✉), Yutaka Watanobe, and Subhash Bhalla

Department of Information Systems, University of Aizu, Aizuwakamatsu, Japan
rashmipsarode@gmail.com, yutaka@u-aizu.ac.jp

Abstract. The maintenance of proper health records is essential to patient health care. Electronic Health Records (EHR) are now replacing traditional Manual Health Records. Audit logs or Audit Trails are a record of events and changes done in a system. Majority of hospitals are required to maintain an audit trail of each and every EHR. Currently, the audit trail is stored in relational databases, which can be easily modified and trust can be lost in the process. Also, third-party audit trails are inefficient, costly, and time-consuming. Replication on Blockchain would be a viable method for securing audit trails so that they are secure, transparent, and immutable without the need for third-party intervention. In this manuscript, we have proposed an Audit Management System where immutable audit trail of EHR can be generated on Blockchain. In this system, a physician or other medical authority having access to this audit trail can easily verify all the consultations, procedures and prescriptions given to the patient in a chronological manner.

Keywords: Electronic health records · Electronic medical records · Audit trail · Audit in blockchain

1 Introduction

A handwritten system was used to keep track of health information in the healthcare field. Manual medical recording systems were sluggish, unsecured, and lacked proper organization. An EHR (Electronic Health Record) and EMR (Electronic Medical Record) system provide better security and ease of access while attempting to provide appropriate access controls [1].

EMRs are medical data in the form of digital records that is easy to store, update, and exchange between healthcare organizations anywhere and anytime. EHR refers to a repository of patient data in digital form, maintained and shared securely, accessible by numerous authorized users [2]. The EHR is classified as an inter-organizational system, whereas the EMR is typically regarded as an intra-organizational system [3]. Patients' EMRs and EHRs are distinct from each other. It is possible for medical professionals, patients, and anyone else with permission, to access electronic medical records accurately and promptly [4].

Some EHRs include applications that provide audit trails for auditing and system transparency. These applications continuously monitor the database of

S. Sachdeva et al. (Eds.): BDA 2022, LNCS 13830, pp. 86–94, 2023.
https://doi.org/10.1007/978-3-031-28350-5_7

the application and generate an audit trail record whenever an object's value changes. Due to the client-server interaction, however, audit trails are susceptible to a single point of failure, allowing an adversary to externally and internally change the database and audit trails. Replicating audit trails across all applications is an apparent method for protecting them against single points of failure. This will increase the cost of an attack for the adversary, as altering audit trails requires an attack on all applications. This replication of audit trails can be accomplished employing blockchain technology to offer safe, transparent, and immutable audit trail management without the requirement for a trusted middleman [5].

In addition, an adversarial party attempting to hack the system will be necessary to replace all logs maintained by each peer. This, in turn, increases the cost and complexity of the attack, thus enhancing the audit log application's total defensive capability [6]. With this in mind, we embark on an effort to build an audit trail using blockchain technology. The goal of this paper is to use blockchain technology as a solution to the problem of distributed data in hospitals and generate an audit trail of consultations and investigations that can be made without making significant changes to the existing hospital database.

The rest of the manuscript is as follows: Sect. 2 consists of Related Works, Sect. 3 describes the Proposed System in detail, Sect. 4 presents the Benefits of the Proposed Architecture, Sect. 5 elaborates on the Challenges and Discussion, and finally, Sect. 6 concludes the manuscript with Summary and Conclusions.

2 Related Works

Numerous researchers have conducted extensive research on Blockchain and Smart Contracts in the Medical field; however, the research in Audit Management is limited.

Kaushik et al. (2022) [7] investigate the potential advantages and applications of blockchain and quantum technology in the fields of medicine, pharmacy, and healthcare systems. The application of blockchain technology in the fight against the COVID-19 outbreak, as well as in other healthcare systems of a similar nature, has proven to be quite beneficial. Modern medical care systems feature sensor data that can be utilised to monitor patients while safeguarding their privacy and medical records' confidentiality. Using technologies like as quantum computing and blockchain could make it possible to manage patient data more rapidly and securely. Both blockchain and quantum technologies have been the topic of considerable speculation. This investigation attempts to determine the existence of operational medical uses for either of these technologies in the present scenario.

Sharma, et al. (2021) [8] proposed a multi-constraint and multi-objective simulation-optimization strategy for scheduling linear and nonlinear dynamic and controlled drone movement models. The current COVID-19 pandemic situation required the development of tools for the precise and rapid distribution of disease, impacts, causes, and treatment-related data. The performance of

both types of drone-based smart healthcare systems can be evaluated based on their ability to maintain a stable attitude for both inside and outdoor activities. This effort began with an introduction to COVID-19, identification of hotspots, monitoring, and effects on social and economic sectors. This work examines drone-based COVID-19 interior and outdoor operations, including sanitization, monitoring, data collecting, and sharing. In results and analysis, the number of patients admitted, the number of drones utilised, and the proportion of individual drone utilisation are reviewed and discussed.

A proposed solution in healthcare by Kumar, et al. (2020) [9] utilises blockchain as a safeguard against the failure of central authority and employs a decentralised strategy. Most of the smart healthcare systems prioritise either data security issues or huge data management. The authors propose a simulation-optimization strategy to enhance the overall system and subsystem performance. The incorporation of blockchain technology into the healthcare system gives a range of characteristics, including automation, transparency, and security, to applications such as healthcare.

BlockTrail, a multilayer blockchain system was proposed by Ahmad, et al. (2019) [5] that utilizes the hierarchical distribution of copies in audit trail applications to minimize system complexity and boost performance. BlockTrail divides a single ledger into many chains managed at different system tiers. The prototype of BlockTrail is based on an audit trail application and uses the PBFT protocol to enhance consensus among copies. Experiments indicate that, compared to typical blockchains, BlockTrail is more efficient, with manageable delays.

Ahmad, et al. (2018) [6] proposed BlockAudit, a blockchain-based audit log system that uses blockchain technology's security capabilities to produce distributed, append-only, and tamper-proof audit logs. The authors put their design into practice using Hyperledger, then assessed the system's performance in terms of latency, network size, and payload size. Three assessment metrics are used to analyze the system's performance: latency, network size, and payload size.

3 Proposed System

We propose a blockchain-based audit management system in which a physician or medical authority with access to a patient's EMR can chronologically verify all consultations, procedures, and prescriptions issued to the patient.

3.1 System Architecture

Consider the case of three hospitals. The hospitals store data on a web-based UI (User Interface) that stores the data on a shared database. A summary of the data collected in the hospital databases is stored on Blockchain so that there is a note in brief about every visit and investigation carried out concerning the patient in a time-stamped manner. The hospitals register on Blockchain through Smart Contract. This is depicted in Fig. 1.

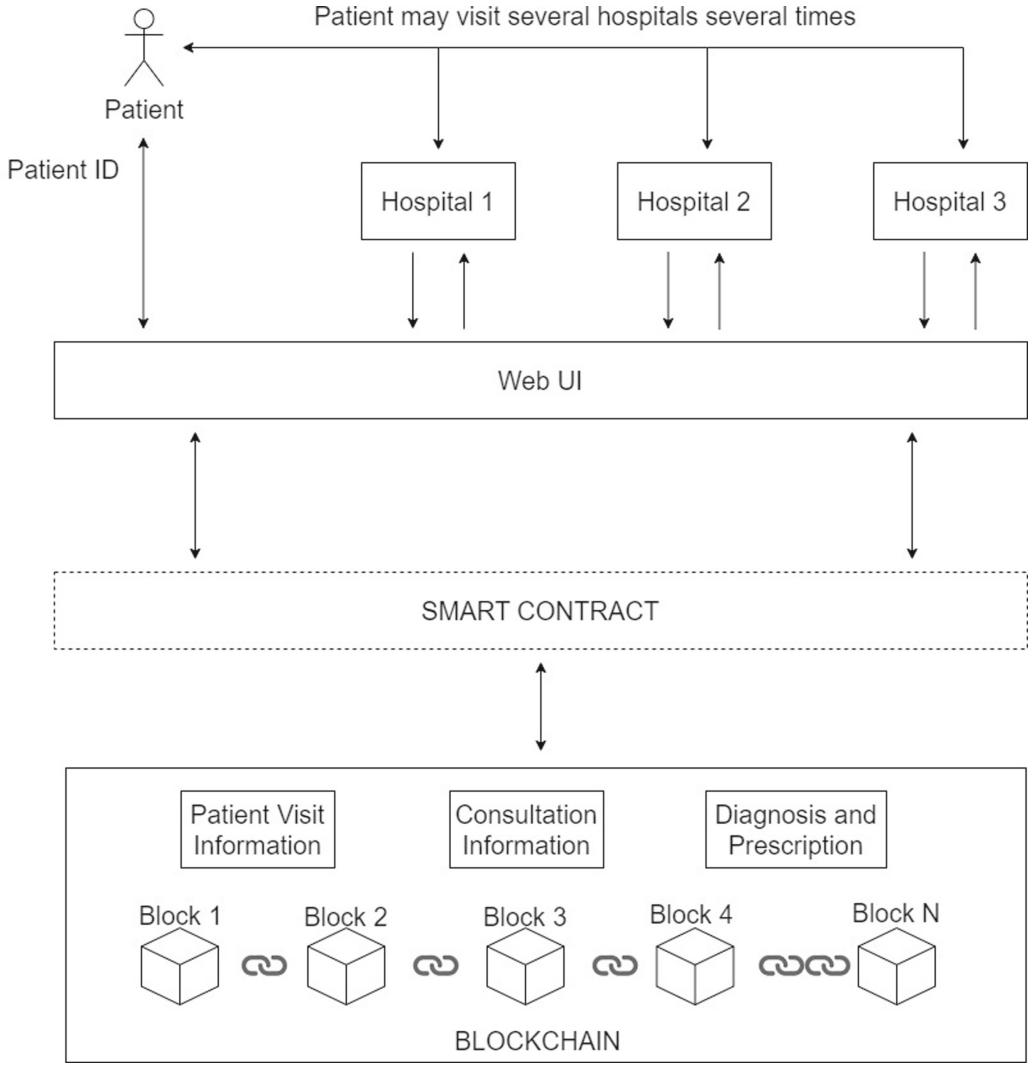

Fig. 1. Proposed System Architecture.

The challenge here is to create an immutable and sequential record of (i) the visits of a patient to these hospitals, (ii) investigations and procedures carried out, (iii) inferences made, and (iv) treatments and medicines prescribed. The steps for the Proposed System process are as follows:

(a) **Registration**: Each hospital has to be registered on the Web UI by providing a unique registration id, a name, an address, and an email address. These facts are verified by medical associations and other regulatory agencies before being recorded in the blockchain and utilized as the unique Hospital-

ID. Adding medical professionals to the blockchain is as simple as supplying the hospital's ID, registration ID, department, and contact information once the hospital has been registered. Every patient will also have to be registered on the Web UI by providing details such as SSN (Social Security Number), First name, last name, gender, and email. Other details of the patient can also be added.

(b) **Smart Contract**: Every hospital registers in the blockchain via a smart contract. Smart Contracts are scripts of code that execute simultaneously on multiple Blockchain nodes. As a blockchain-based program, a smart contract can be correctly executed by a network of mutually distrusting nodes without requiring an externally trusted authority [10]. Each time a Doctor-ID is generated from the smart contract, it can be associated with specific staff, making it easy to track their activities. They are then linked to the patient's medical record.

In the proposed system, patient health records would be created by the registration contract, which would then be kept in blocks of hashed data stored in a database server. A patient goes to a hospital to see a doctor for treatment. Patient's medical and personal data are entered into a Hospital database in the blockchain system; each patient has a unique Patient-ID that identifies each individual in the network. Patients' records, including surgical and diagnostic records, prescription and dosage information, and other medical records, are kept in the patient file once the consultation is complete. Finally, the smart contract receives the data in the proper format.

(c) **Hash Function**:

Using a Hash function to take any input and produce a fixed-size hash is possible. The proposed system will automatically update the hash value if the input data changes, and it uses SHA-256 (Secure Hash Algorithm) hash function for hashing transactions and blocks. Data hashes, not the original data, are stored in the blockchain's repository because it is a protocol for data security.

(d) **Transaction Management**:

The proposed system's smart contract is constructed in such a way that it must generate an n-count number of health blocks. Each block is made specifically for a particular transaction, in this case, every patient's visit to the hospital (consultation). As soon as a patient's medical records are entered into a blockchain, the patient can access their data. With a unique patient-ID, the system automatically accesses prior patient health records. No one can alter the data on a blockchain since it is immutable. Preventing and detecting alterations to a patient's medical record is made easier with the proposed approach, which is very useful while performing audits. A group of pre-approved participants, including the patient, doctor, and an authorized hospital, will be responsible for making necessary changes to the system.

A patient may visit several hospitals and diagnostic centers during his routine, and if all of these are registered on the blockchain, then the entire trail will be available. The patient can access this data via a web UI where he can provide his ID and authentication information to retrieve data.

Further details can be obtained from the respective hospital's databases. However, a complete trail will be available to him so that he does not miss any vital information. Care must be taken to ensure that only one Patient ID is used in all hospitals and diagnostic centres that the patient visits. This ID is provided by the blockchain smart contract used to register the patient. A patient should be registered only once on the blockchain. This can be enforced by using a unique ID such as the patient's social security number while registering.

3.2 Proposed System Implementation

The proposed system is implemented using Ethereum Blockchain Ganache [11] and Truffle [12] that is used to upload smart contracts in Blockchain. The smart contract is critical to implementing the blockchain because it allows the various stakeholders in the system to carry out their agreements.

For auditing, we focus on adding and retrieving hashes on the blockchain in our proposed system. Patients, doctors, and other healthcare professionals can access the blockchain hash. As specified in the registration contract, anyone attempting to do an audit must have permission and approval from the patient being audited. The system sends a false statement if the doctor is not permitted, and the session is terminated. Smart contracts check the patient's and doctor's addresses against information already stored on the blockchain.

We have created the smart contract for Patient Registration and validated it in Blockchain. The patient data is entered into the Web UI, which exists in the hospital. The Node.js module posts the relevant data in the smart contract, which is executed. The code for the createPatient() function in the smart contract is shown in Fig. 2. The data is then stored in the Blockchain via a smart contract transaction which is then validated in Blockchain as seen in Fig. 3. The other smart contracts can be created using a similar method.

4 Benefits of Proposed Architecture

The benefits of such an architecture are that the hospitals can choose any proprietary or web based system to suit their requirements. In addition, a gateway is provided to access the entire history of the patient's health records and investigations. Suppose the patient goes to any other hospital (Hospital 2). In that case, the same Patient-ID could be referred, for example, in situations where a patient would need a second opinion from a different doctor due to relocation or other reasons. Doctors in this situation can review the patient's previous treatment logs to plan subsequent treatment. For further treatment, doctors can access patient records in the blockchain with the patient's permission (the patient provides his unique Patient-ID), and patients can share their health data with any doctor in the network.

In the proposed approach, the patient's medical records are safeguarded. The system allows the registered user (patient) and any authorized health service provider in the blockchain network (in case of emergency) to access and

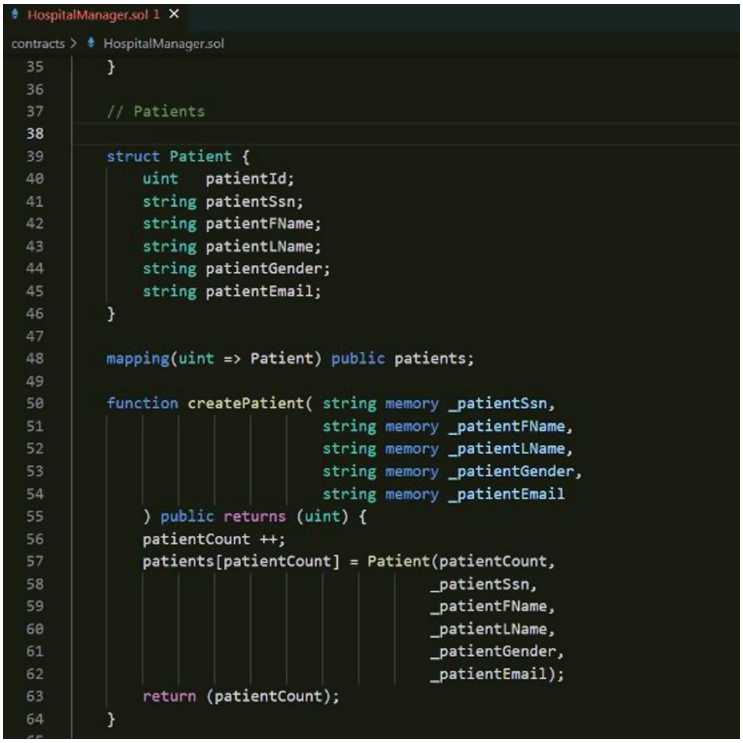

Fig. 2. Smart contract code for patient registration.

view their health records. The authenticity and access control of the audit trail is managed by passwords that are stored against the entities, such as doctors or staff. These passwords will have to be provided to the smart contract while storing patient visit details such as consultations, surgeries, diagnoses, and prescriptions.

The proposed system tries to create a redundant, tamper-resistant, and verifiable record of timestamped information regarding the patient's medical investigations and health records. It is built on blockchain technology, a distributed, fault-tolerant data store. This information can be used by authorized personnel to locate the corresponding detailed records in the Web UI at each hospital which generates a comprehensive patient treatment file for a thorough investigation. The proposed system uses a consortium blockchain, owned and managed by the government or some central medical authority, to provide secure access to the concerned individuals.

We have tried to stress the ease of creating a simple audit trail based on a chronological record of patient investigations and consultations without modifying the existing systems and practices of the medical institutions and hospitals concerned. This system can pave the way for better integration of medical records and a more structured and standardized approach to shared medical data.

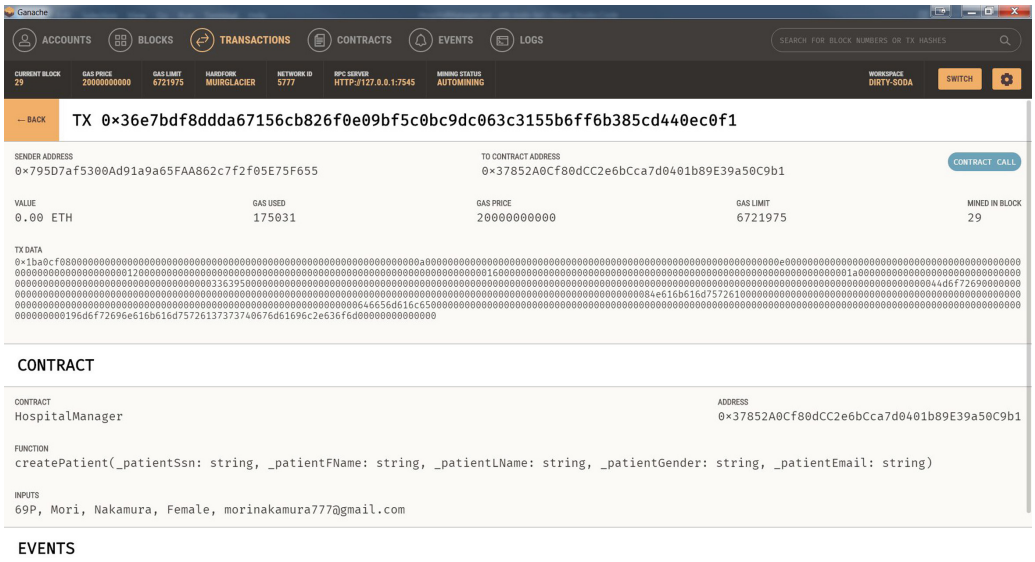

Fig. 3. Smart contract code for patient registration.

5 Challenges and Discussion

We propose the use of blockchain in this system because it is a decentralized database that is immutable. Consider the case of a patient consulting multiple hospitals, each of which maintains its database. No single system has a complete record of all the visits and treatments. Also, consider the case that a particular database is offline or corrupt. The patient or doctor may not know which data has gone missing. In the case of blockchain, as it is a decentralized database with multiple nodes keeping a copy of the data, the entire data will always be available at any given point in time. Also, there is no chance of any corruption or other such failure, which is possible in local databases.

We have proposed the use of Blockchain to eliminate the costs of third-parties and middlemen. However Blockchain technology is inherently complex and expensive; and it would be a challenge to adopt it.

6 Summary and Conclusions

EHR applications include audit trails for auditing and system transparency though each of them can act as a single point of failure. An audit trail has been proposed on Blockchain technology where a patient or a authorized medical personnel has a timeline-based access to all investigations, reports, and procedures conducted during his treatment. The method of facilitating this is through the development of smart contracts, which store the relevant information after providing the necessary checks to ensure the integrity of the data. We have created the Smart Contract for patient registration and validated it in Blockchain. Our proposed approach can meet confidentiality, integrity, and authentication requirements.

A decentralized technology such as Blockchain is used to store EMR and form audit trails. The proposed system can thus solve problems such as fragmentation of medical data across hospitals and possible data loss due to systems being either corrupt or offline. The fault tolerance property of Blockchain and high availability can be utilized to store this information in a distributed manner. This research aims at providing a medium using blockchain technology to maintain an audit management system for current healthcare systems.

For future work, the proposed system can be further enhanced by using an access control system based on asymmetric cryptography with the hospital management systems at the concerned hospitals. Additionally, the hospitals can move towards a decentralized database that would be uniform across all hospitals and incorporate the audit trail blockchain as part of a larger and more comprehensive system.

References

1. Shahnaz, A., Qamar, U., Khalid, A.: Using blockchain for electronic health records. IEEE Access **7**, 147782–147795 (2019)
2. Anshari, M.: Redefining electronic health records (EHR) and electronic medical records (EMR) to promote patient empowerment. IJID (Int. J. Inform. Dev.) **8**(1), 35–39 (2019)
3. Heart, T., Ben-Assuli, O., Shabtai, I.: A review of PHR, EMR and EHR integration: a more personalized healthcare and public health policy. Health Policy Technol. **6**(1), 20–25 (2017)
4. Zhu, H., Hou, M.: Research on an electronic medical record system based on the internet. In: 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), pp. 537–540. IEEE (2018)
5. Ahmad, A., Saad, M., Njilla, L., Kamhoua, C., Bassiouni, M., Mohaisen, A.: Blocktrail: a scalable multichain solution for blockchain-based audit trails. In: ICC 2019–2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2019)
6. Ahmad, A., Saad, M., Bassiouni, M., Mohaisen, A.: Towards blockchain-driven, secure and transparent audit logs. In: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 443–448 (2018)
7. Kaushik, K., Kumar, A.: Demystifying quantum blockchain for healthcare. Security and Privacy, p. e284 (2022)
8. Sharma, K., Singh, H., Sharma, D.K., Kumar, A., Nayyar, A., Krishnamurthi, R.: Dynamic models and control techniques for drone delivery of medications and other healthcare items in COVID-19 hotspots. In: Al-Turjman, F., Devi, A., Nayyar, A. (eds.) Emerging Technologies for Battling COVID-19. SSDC, vol. 324, pp. 1–34. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-60039-6_1
9. Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V., Hossain, E.: A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE Access **8**, 118433–118471 (2020)
10. Zou, W., et al.: Smart contract development: challenges and opportunities. IEEE Trans. Softw. Eng. **47**(10), 2084–2106 (2019)
11. Truffle Suite: Ganache (2022). https://trufflesuite.com/ganache/
12. Truffle Suite: Ganache overview (2022). https://trufflesuite.com/docs/ganache/