A Secure Electronic Healthcare Information Preservation System Using Blockchain Technology

Modupe Agagu
Department of Computer Science
Olusegun Agagu University of Science and Technology, Okitipupa, Ondo State, Nigeria

Abstract

The role of record keeping and information sharing in the health sector cannot be overemphasized. Such records comprise an individual's health history and other information that facilitates healthcare decisions, therefore easy access to a patient's health information is an important aspect of health-service delivery that must be regulated and monitored because of the sensitivity of the information. Some approaches adopted in many hospitals face challenges of missing files or records, lack of information sharing between healthcare providers, insecure records, and also inaccessibility of patient's health information for healthcare providers that are needed to make informed health decisions. To overcome these challenges, this work proposes an Electronic Health Record (EHR) using Blockchain to store information as well as enhance data privacy and data security. The proposed solution includes Ethereum and smart contracts to establish a medical record system to ensure the privacy of patients. Also, there exists the privilege to deal with and authorize personal medical records in the proposed framework. The practical findings demonstrate that our proposed system offers a practical approach for trustworthy data exchanges in healthcare while safeguarding private health data from dangers. When compared to the current data sharing models, the system evaluation and security exploration show performance gains in the design, minimize delays in patient data retrieval, and high levels of security and data privacy.

Keywords: Electronic Health Records (EHR), Blockchain, Data Privacy, Data Security Ethereum, Smart Contract and Healthcare Provider

1. Introduction

These The process of keeping and evaluating patient medical records to enhance patient care, effectively identify illness causes, produce pharmaceuticals, and create a precise preventative plan is known as healthcare data management. In the early days of data management, patient complaints, diagnoses, and related treatments were manually entered into medical records. Later, as digital data developed, electronic health records, or EHRs, were created [1]. According to [2], an electronic health record, or EHR is a digital record of a patient's medical information that is gathered and stored electronically in a digital format over time by a hospital or healthcare provider. In addition to much more, it has all the data that would be on a paper chart. Past medical history, vital signs, progress notes, diagnosis, prescriptions, dates of vaccinations, allergies, lab results, and imaging reports are all possible inclusions in an electronic health record (EHR). Other pertinent data, like insurance information, demographic data, and even data imported from personal wellness devices, may be included.

The power of an EHR lies not only in the data it contains but how the information contained in it is shared making health information instantly accessible to authorized providers across practices and health organizations, helping to coordinate care efficiently. An EHR can be shared with clinicians and organizations involved in a patient's care, such as labs, specialists, imaging facilities, pharmacies, emergency facilities, and school and workplace clinics.

Before the advent of modern technology, the healthcare sector used paper-based systems to store medical records, i.e., using a handwritten mechanism. This paper-based medical record system was inefficient, insecure, unorganized, and not temper-proof. It also faced the issue of data- duplication and redundancy as all the institutions that patients visited had various copies of patient's medical records [3]. The healthcare industry using EHR has great advantages which include improved patient care, public health improvement, workflow simplicity, etc.

Hospitals all across the world have adopted EHR systems because of its advantages, which include increased cost-effectiveness and security. They are regarded as an essential component of the healthcare industry since they make healthcare considerably more functional. These features include lab test results, patient appointment scheduling, billing and accounts, and electronic medical record storage.

 | DOI: 10.20533/ijehis.2046.3332.2023.0029

Providing safe, unchangeable, and platform-transparent medical records is the main goal of HER systems. Although the idea behind the use of EHR systems in hospitals and other healthcare settings was to raise the standard of treatment, these systems had some drawbacks and fell short of expectations. According to [3], an investigation into the EHR experiences of nursing staff was carried out in Finland. The study's findings indicated that EHR systems had issues with being unreliable and not being very user-friendly. Other issues encountered by the EHR systems includes interoperability, information asymmetry and data breaches.

Healthcare data requires a high level of security and privacy. Privacy refers to persons having the correct rights to allow or disclose personal information to others. This demands consensus among healthcare providers and regulators, and the creation of agreed policies and procedures. Privacy is the starting point for determining who and whom should be allowed to access personal patient information

On the other hand, blockchain is a decentralized network that tracks every transaction. It uses peer-to-peer (p2p) technology to carry out operations. It is devoid of a single point of contact or centralized authority. Instead, a collection of nodes maintains the system's functionality. The storing of a patient EHR on Blockchain using Ethereum makes it secure and hard to be breached by attackers, and the patient can be assured of not having to wake up and see his or her health records trending online. It also enables the care providers to make better and faster decisions and provide care to the patient as soon as possible. Blockchain allows decentralization, data transparency, privacy, confidentiality, etc [4], [5]. The ability of Blockchain technologies to streamline the creation of healthcare apps is one of the industry's most significant advantages. As a result, the interoperability of healthcare databases is enhanced, enabling increased access to patient health records, drug databases, asset records, and the entire device life cycle within the Blockchain infrastructure however still maintains its inaccessibility to outside parties. This proposed system's main objective is to securely store all medical data on the cloud. The list of contributions is as follows. (i) Designing and implementing the front-end platform for the EHR web page (ii) Integrating the EHR mentioned above with the Ethereum blockchain and the smart contract (iii)ensuring that a patient's health record is secure, uniform, and available to all healthcare providers and patient when needed (iv) Testing the blockchain-based system to allow for interoperability, security, and privacy.

2. Related Work

The authors in [6], proposed MedRec: a novel, decentralized record management system to handle EMRs, using blockchain technology. Their system gives patients an immutable log and easy access to their medical information across providers and treatment sites. In [7], the authors proposed a model that focuses on providing healthcare data to researchers for statistical analysis and providing privacy. The model exhibits high data security by combining the customized access control protocol and asymmetric cryptography. It uses a proxy re-encryption method for sensitive medical information sharing. In [5], a new personal health records-sharing scheme with data integrity verifiable based on blockchain was proposed. The study aimed at solving the problems of privacy disclosure, limited keyword searchability, and loss of control rights in the process of personal health record sharing, the new scheme uses searchable symmetric encryption and attribute-based encryption techniques to achieve privacy protection, keyword search, and fine-grained access control. The authors in [3] discussed a framework that could be used for the implementation of blockchain technology in the healthcare sector for EHR. Their proposed framework aimed to implement blockchain technology for EHR and provide secure storage of electronic records by defining granular access rules for the users of the proposed framework. The framework also discusses the problem faced by blockchain technology in general via the use of off-chain storage of the records. It provides the EHR system with the benefits of having a scalable, secure, and integral blockchain-based solution. In [8], the authors developed a scheme based on the ciphertext policy attribute-based encryption system and IPFS storage environment combined with blockchain technology, their work constructed an attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records in the IPFS storage environment. It stores the encrypted electronic medical data in the decentralized InterPlanetary File System (IPFS). In [9], a blockchain-enabled hyperledger fabric architecture for EHR systems was proposed. Their EHR blockchain system created and implemented different Chaincodes to handle the business logic for executing separate EHR transactions. The proposed fabric architecture provides a secure, transparent, and immutable mechanism to store, share, and exchange EHRs in a peer-to-peer network of different healthcare stakeholders. It ensures interoperability, scalability, and availability in adapting the existing EHRs for strengthening and providing an effective and secure method to integrate and manage patient records among medical institutions in the healthcare ecosystem. Also, in [10], blockchain smart contracts were designed to provide a regulated solution to the need of patients, physicians, and health service providers. The proposed system aimed to exchange health information on a blockchain platform to build

 | DOI: 10.20533/ijehis.2046.3332.2023.0029

a smart e-health system. It presented a health model namely immutable patient log creation with a Modified Merkle Tree data structure for secure storage and rapid access of health records, update medical records, health information exchange between different providers, and viewership contracts on the peer-to-peer blockchain network.

3. Methodology

The formal description of the proposed system is explained below.

3.1. System Design and Architecture

The blockchain network is divided into three key components: User, Assets, and Transactions and smart contracts implementation as shown in Figure 1 below. In the blockchain-based EHR system implementation, there exist three main users: the patients, the Medical professional and the System administrator.

i. These users' primary responsibilities are to relate with the system and carry out fundamental operations including creating, reading, updating, and deleting medical records. The system uses a decentralized app that has a Graphical User Interface (GUI) for easy access. Every function that a specific user may access is contained in the GUI. This GUI could be used by the user by their assigned role to communicate with the other layer of the system (see Figure 1).

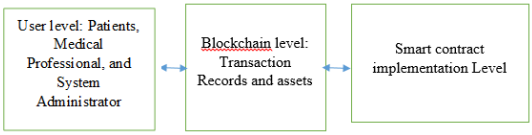

Figure 1. System Design and Architecture of the Electronic Health Record System

- The Patients: As participants in the EHR system, the patients are crucial. The health records they create and add to the blockchain belong to them. They can modify their data. As a result, they can control who can access their records. Patients prevent any unapproved healthcare provider or outsider from accessing their records.
- The medical professionals are the healthcare providers who diagnose patients and compile their medical histories. Only patients who have validated them as authorized professionals and granted them permission to write into their records are accountable for having their health-related information updated. They can modify their profile or personal data.
- Admin is the one who deploys the blockchain network, implements various contracts in the network, generates the key, and handles the encryption-decryption of the transaction data. In this system, medical records are the asset of the network. Each medical record is owned by a patient who is registered on the network. Whenever a transaction is executed the status of the asset changes. Changes are like updates in the records if the patient is diagnosed with some new disease, modifications in medications, test results, etc.

ii. The system's assets and transactions are listed at the blockchain level. A transaction on the Ethereum blockchain is a user's method of updating a record or piece of information that is kept on the network. The Ethereum blockchain views these transactions as assets since they contain information that a user can share with another user or save for later use. In general, blockchain technology computes and completes transactions according to a set of consensus rules. To maintain the blockchain's security and temper-proofness, certain consensus techniques are required. The Proof of Work (PoW) consensus mechanism is used by the Ethereum blockchain. This is done to ensure that the governance of the blockchain is maintained in a trustworthy manner by obtaining approval from all trusted nodes connected to the network. Peer-to-peer networks are used by the Ethereum blockchain. The following is a list of actions and transactions that can be done in the system:

- Adding records that will enable the decentralized app to construct the patient's medical records. Basic medical records for the patient are kept in addition to the IPFS hash of the file that was uploaded with the lab results or other patient documents.
- Updating records would result in updating the patient's medical records. This just modifies the patient's fundamental data; the IPFS hash remains unaltered. IPFS hash is not updateable to guarantee record security.
- View records would allow the user to access a patient's medical records that are kept on file in the decentralized app. Both patients and physicians use the view records tool. By verifying that the patient accesses only his medical records, the system allows the patient to access his records. To guarantee that the patient sees only pertinent medical records, the system leverages the patient's public account address for this purpose. The patient can view his medical records but would not be given access to add or update them:

 | DOI: 10.20533/ijehis.2046.3332.2023.0029

- Delete records: This enables the user to be able to delete records of any patient. The users here would be the doctors who are given the right to delete any patient's record stored on the blockchain.

- Grant / Revoke access: Access to the records can either be granted or revoked. To grant access to each of the above-mentioned transactions, certain users would need to have access to them, i.e., only the doctor or nursing staff can make changes in the records of the patient or add them. So, add and update records would only be accessible to these entities

iii. Smart contract implementation: The system was implemented by using Ethereum and its dependencies. Smart contracts are an important part of decentralized apps as they are used for performing basic operations. The following contracts are included in this framework: Patient Records and user roles. These contracts are used for giving access to the users on the DApp and performing Create, Read, Update, And Delete (CRUD) operations on the records of patients. The Patient Records on the smart contract are made purely for implementing the functionality of the proposed framework (see Figure 2).

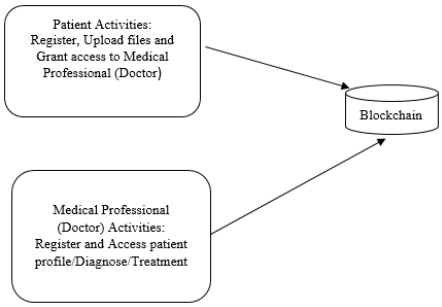

Figure 2. Patient Activities on the Blockchain

3.2. Software Design Illustration

Software design is the most vital part of any framework as it is used for the development of the system from its theory, it serves as a template for programmers to use while they create the application's architecture. The software design pattern of the system describes the back-end design pattern and the front-end design pattern. The most well-known and important components of this framework's implementation are Ethereum and Interplanetary File System (IPFS):

- Ethereum: A decentralized network based on blockchain technology is called Ethereum. It was initially implemented on Blockchain, a well-known cryptocurrency. The intention behind Ethereum's creation was to provide an open-source, blockchain-enabled smart contract platform. Additionally, Ethereum gives programmers access to the Solidity language, which lets them create their blockchains. The last feature is Ethereum's smart contracts, for which it was designed.

- Interplanetary file system (IPFS): This is a peer-to-peer network used by the protocol IPFS to store data. Since data saved on IPFS is shielded from modification, it offers safe data storage. Since any effort to change the data saved on IPFS could only be accomplished by altering the identifier, it utilizes a cryptographic identification to safeguard the data from tampering. A cryptographically produced hash value may be found in every data file saved on IPFS, the IPFS protocol works in the following way:

  i. Files stored on IPFS are assigned a unique cryptographic hash.

  ii. Duplicate files are not allowed to exist on the IPFS network.

  iii. A node on the network stores the content and index information of the node.

3.3. Implementation Tools

i. Ganache: This is a local Ethereum blockchain designed to facilitate the quick development of decentralized apps. Throughout the development cycle, Ganache may be used to deploy, develop, and test in a reliable and secure environment. It functions both as an Ethereum command-line tool and as a desktop application.

ii. MetaMask: It is a point of entry that permits the viewing of the decentralized web in your browser. It eliminates the need to launch an entire Ethereum node in your browser to run Ethereum decentralized applications.

iii. Web3: To communicate with the modules in the chain, transactions must be verified within the chain. Web3 uses the Hypertext Transfer Protocol (HTTP) connection to connect to the Ethereum network via an Ethereum node. MetaMask is a browser-based Ethereum wallet that connects the browser to a Web3 provider class. A Web3 provider is a data structure that provides a link to Ethereum nodes that are publicly available. A user can utilize, save, and maintain public and private keys that are unique to their account with the use of MetaMask. The combination of Ethereum, MetaMask, and web3.js, as well as a web interface, allows for backend–front-end communication.

iv. Truffle: It is a strong Ethereum Virtual Machine

 | DOI: 10.20533/ijehis.2046.3332.2023.0029

development environment that uses blockchains, as well as an asset pipeline and a test framework for the same. It has some features, such as computation, implementation, and maintenance of smart contracts. It also has an environment for testing smart contracts that is fully automated and a deployment and migration framework that can be scripted and expanded. It can create direct communication with the contract and a pipeline with tight integration.

v. VS Code. Microsoft's Visual Studio Code is an editor for Windows, Linux, and macOS. Troubleshooting, Git management, GitHub, syntax underlining, smart code completion, samples, and bug fixes are all available.

vi. Languages. The front-end design of the webpage was created using HTML (Hypertext Markup Language), CSS (Cascading Style Sheets), and React.js, and the server and back-end using the Solidity programming language and Node.js.

4. Results

Tools for building local Ethereum, Ganache, and Truffle were used in building this system. The Solidity programming language and Node.js were used to control the system's server and back end. To create a blockchain and access the system, the Ethereum virtual interface, MetaMask, Truffle, Ganache, and Local Web3 (web interface) were used. The interface in Figure 3 shows how the patient or medical professional provides information for registration to the blockchain-based system. After a user signs in to an application, the application sends a JSON Web Token (Jwt) to the user with NodeJS. Jwt is mainly used for Authentication. Once registration is done, the user profile is created and can be updated as depicted in Figure 4 below. In the diagram shown in Figure 5 below, the patient grants access to the doctor to the blockchain system, uploads a medical file to the node, and the file is encrypted on the IPFS network then returns and saves the Hash file back to the blockchain. IPFS allows transactions to be completed with minimal resources and time. A content address is generated after a file is uploaded to the IPFS network

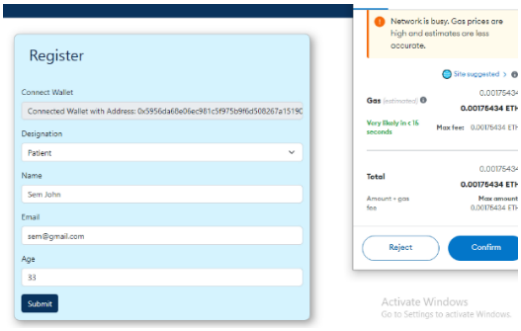

Figure 3. User Registration Interface

5. Conclusion

EHR is the digital record of the medical history of the patient. It has solved many issues related to data handling and its security. The system developed aimed at bridging the gap between data security and data privacy thereby reducing the risk of hackers gaining unauthorized access to a patient record, and unauthorized usage of records, ensuring the integrity of records, and improving interoperability of the systems via system event tracking.

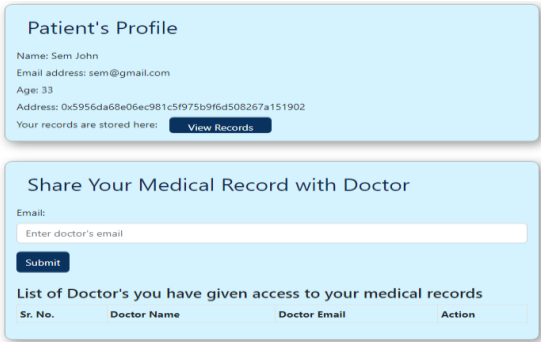

Figure 4. Interface showing User Profile

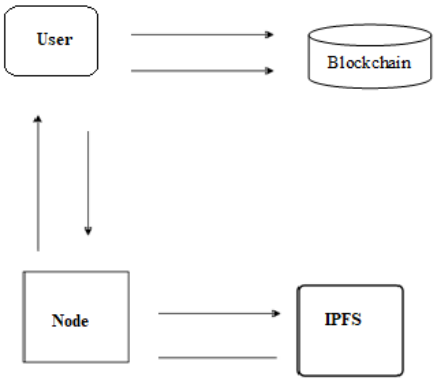

Figure 5. Flow of file Upload to Blockchain

The integration of Blockchain technology into the EHR marks a significant leap forward in enhancing data security, preserving patient privacy, and fortifying trust within the healthcare sector. Through rigorous implementation and testing, this system has demonstrated its potential to revolutionize healthcare data management. The system allows the patient to grant and revoke any record-specific authorization to the authorities when needed. The research objectives were successfully implemented.

References

[1] Ismail, L., and Materwala, H. (2020). Blockchain Paradigm for Healthcare: Performance Evaluation. Symmetry, 12(8), 1200.

[2] Sharma, Y., and Balamurugan, B. (2020). Preserving the

 | DOI: 10.20533/ijehis.2046.3332.2023.0029

Privacy of Electronic health records using blockchain. Procedia Computer Science, 173, 171-180.

[3] Shahnaz, A., Qamar, U., and Khalid, A. (2019). Using Blockchain for Electronic Health Records. IEEE Access, 7, 147782-147795.

[4] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., and Zhang, X. (2017). BBDS: Blockchain-based Data Sharing for Electronic Medical Records in Cloud Environments. Information, 8(2), 44.

[5] Wang, S., Zhang, D., and Zhang, Y. (2019). Blockchain-based Personal Health Records Sharing Scheme with Data Integrity Verifiable. IEEE Access, 7, 102887-102901.

[6] Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using Blockchain for Medical Data Access and Permission Management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

[7] Mahore, V., Aggarwal, P., Andola, N., and Venkatesan, S. (2019). Secure and Privacy focused electronic health record management system using Permissioned Blockchain. In 2019 IEEE Conference on Information and Communication Technology (pp. 1-6). IEEE.

[8] Sun, J., Yao, X., Wang, S., and Wu, Y. (2020). Blockchain-based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. IEEE Access, 8, 59389-59401.

[9] Uddin, M., Memon, M. S., Memon, I., Ali, I., Memon, J., Abdelhaq, M., and Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. Comput. Mater. Contin, 68(2), 2377-2397.

[10] Chelladurai, U., and Pandian, S. (2022). A novel Blockchain-based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing, 1-11.

 | DOI: 10.20533/ijehis.2046.3332.2023.0029