Mobile-based Patient-centric EMR Sharing System Using Blockchain

Kanwar Muhammad Afaq
Department of Computer Science and Information Engineering
Asia University
Taichung, Taiwan
kmafaq786@gmail.com

Prayitno
Department of Computer Science and Information Engineering
Asia University
Taichung, Taiwan
prayitno@polines.ac.id

Yuan-Yu Tsai
Department of M-Commerce and Multimedia Applications
Asia University
Taichung, Taiwan
yytsai@asia.edu.tw

Yu-Ching Chen
Department of Bioinformatics and Medical Engineering
Asia University
Taichung, Taiwan
yuching@asia.edu.tw

Zon-Yin Shae*
Department of Computer Science and Information Engineering
Asia University
Taichung, Taiwan
zshae1@asia.edu.tw

2022 IEEE 4th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS) | 978-1-7281-9579-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ECBIOS54627.2022.9945017

***Abstract*—Nowadays, mobile devices are the most important components in human life. With the help of various apps, we interact with other people, play games to kill time, or perform online shopping activities. However, despite the convenience of mobile devices, most cross-institutional EMR sharing still needs written forms and waiting time for application. Although existing blockchain-based data exchange architectures have been proposed, the most frequently used mobile devices have never been considered. This study is carried out to integrate mobile devices to develop a blockchain-based patient-centric EMR sharing system considering data security, data integrity, and patient privacy. Under the patient's consent, the proposed system supports selective data sharing between different institutions through blockchain in real-time. Patients have the complete right to disclose what their EMR shares. Further, using mobile devices to scan the QR code provided by the doctor, patients easily employ this public key infrastructure to achieve enhanced data security. The proposed system provides necessary functionalities (authentication, integrity, and access control) for EMR data exchange. It shows how mobile features (camera, notification, bio-authentication) can be favorable to fulfill patient satisfaction.**

Keywords—blockchain, data sharing, EMR, mobile devices, patient-centric

I. Introduction

We are living in an age of invention and technological advancement. Globally, the use of mobile applications and wireless networks is expanding quickly across all sectors. We depend on smartphones to manage calendars, arrange work and business operations, remain updated and engaged through social networks, and book doctor visits and healthcare check-ups. Mobile health apps are becoming more popular, with functions such as self-monitoring chronic health issues, medication adherence reminders, scheduling, and direct contact with the health care system [1,2]. Healthcare innovation has raised app development to an essential and a pleasure. Mobile healthcare apps are being used excitedly by both healthcare organizations and patients. User-friendliness, dependability, time-efficiency, mobility, and other factors all contribute to the acceptance of mobile healthcare applications. Despite the increase in the number of mobile health applications, there are fewer studies about using mobile phones to share patients' sensitive medical data [3,4].

Patient-centric care coordination puts patients in control of their care and provides them with the information they need to achieve high-quality results. According to research on optimal chronic disease management, multi-component interventions are necessary to enhance patient-centric care. These interventions include organizational changes in how health provider teams work and communicate with patients, patient engagement methods, and both clinicians and patients having access to meaningful and relevant information. Mobile applications are thus seen as potentially valuable instruments for promoting patient-centric care coordination by providing new methods. They allow patients and clinicians to engage and give information in a personalized format that meets their requirements.

Mobile phones are suitable options for urgent decision-making with the patient's collaboration. Hence, there is an immediate need to digitize health records and build an effective communications system to share patient health records. New systems must be designed with secured electronic health records and an adequately authenticated retrieval mechanism [5]. In addition to the patient-provider relationship and access-sharing, this must also protect patients' privacy for the patient-centric health data sharing system [6].

Recent breakthroughs in blockchain technology have fundamentally altered the way of application development. Blockchain technology, which enables secured transactions between participants in the network, has been used in electronic health records (EHR) in recent years [7]. This technology's primary concepts include transparency, auditability, user sovereignty, and decentralized governance.

We propose a patient-centric secure mobile-based blockchain system for sharing electronic medical records (EMR) among legitimate participants. We employ a simple and effective access control, use of two-phase authentication, JSON web token, and encryption technique to protect the security and privacy of patient health data. Implementing these principles rebuilds patients' trust and provides them with a better sense of control over private data they can share with other parties.

II. Related Work

In recent years, blockchain technology has become a major central research topic in the development of secure

978-1-7281-9579-7/22/$31.00 ©2022 IEEE

healthcare systems. Hang et al. [8] designed a blockchain-based medical system that secures the maintenance of electronic medical records through smart contracts. It gave patients a complete, immutable log and simple access to their medical records across hospital departments. Jaiman and Urovi [9] developed a permission model for blockchain-based data exchange and access management over personal health records. They used smart contracts to represent an individual's consent to use health data dynamically. Kim et al. [10] introduced the blockchain-based Personal Health Record (PHR) application as a novel way to securely store and exchange medical information. An extensive questionnaire and usability evaluation indicate the high usability of the application. To make EHRs easier to use, Chelladurai and Pandian [11] came up with a blockchain-based model for healthcare. They talked about interoperability and data security. They also spoke about how important it is to have a patient-centric Electronic Health Record (EHR). Dubovitskaya et al. [12] developed a web-based system that facilitates the control, sharing, and reliability of medical data using cloud service. Their patient-centric solution permits individuals to maintain their medical records across various hospitals.

III. Proposed System

This article aims to introduce a mobile-based patient-centric EMR exchange via blockchain, a patient-centric access control mechanism for securely sharing EMRs with many stakeholders across healthcare systems. A private blockchain, commonly known as a "permissioned blockchain," restricts access to specific individuals. We set up a private Ethereum blockchain system with smart-contract functionality. One computer, denoted as the blockchain adapter for each hospital, serves as a bridge for communication between the blockchain network and the hospital database. The adapter deals with the data requests, validates them, retrieves the required data, and delivers the data to the doctor. A combination of JSON web token, asymmetric encryption, and blockchain technology makes the system more secure and reliable.

In our solution, we will build a mobile application where patients can use their daily mobile devices for a better medical experience. 'Patient,' 'Hospital,' and 'Doctor' are the main actors in this proposed system. In a high-level scenario, our system works as follows. 'Patient' receives the request for the medical test required by the 'Doctor' via scanning a quick response (QR) code. The 'Patient' then uses the JSON web token to request the necessary medical tests from the 'Hospital.' After all token verification has been completed, 'Hospital' fetches the patient medical records, encrypts them, and sends them to the Interplanetary File System (IPFS), a decentralized peer-to-peer file system. This system is a promising alternative for building a file-sharing platform in the blockchain network. Finally, Hospital transmits the received IPFS hash to the 'Doctor.' 'Doctor' uses a hash to access the patient's medical record on IPFS and decrypts it with their private key.

A. Blockchain (Smart Contract) Initialization

The suggested approach was implemented due to the sensitivity of healthcare data. A smart contract was built using private Ethereum blockchain technology. The smart contract primarily serves four main functions. The first function is "Transfer," which delivers the required test queries to the 'Hospital' via a transfer method. From the 'Patient' end, it helps store data on the blockchain. The second function is "Get." This function retrieves data from a blockchain. This is done from the 'Hospital' to retrieve test queries from the blockchain submitted by the Patient. The third function is "Send," used in the hospital. The 'Hospital' uses this function to transmit patient medical records to the appropriate 'Doctor' within a time constraint. The fourth function, "Retrieve," is employed in a doctor's application, as 'Doctor' retrieves a patient's health-record link from 'Hospital,' kept on a blockchain. The smart contract ensures that the 'Doctor' and 'Hospital' access the records on the blockchain without any form of barrier. As a result, the doctor will be able to diagnose the patient's condition better because he has access to accurate health records from a trusted source.

B. Patient/Doctor Registration

Fig. *1*1 illustrates the patient and doctor registration phase. Firstly, patients register themselves by using their social security number in the system, while doctors register by using their identity document (ID). The Resource Management System (RMS) checks the users based on a given number (social security number/doctor ID) with the hospital. If users have been registered in the hospital with the given number, the system retrieves the user's email from the hospital, generates a random code, and sends it to the users. After entering the code, the users become a part of the system. If the users have not been registered in the hospital with the given number, the system cannot fetch the information from the hospital. Thus, the users are not registered. The RMS tracks users' records and links to the hospital database (we use a temporary local database for a trial) to ensure that the users are adequately identified during the registration. The users create a blockchain wallet using a secret phrase that can be obtained when creating a wallet. If they already have a blockchain wallet, they can access their wallet back by entering the secret phrase or private key.

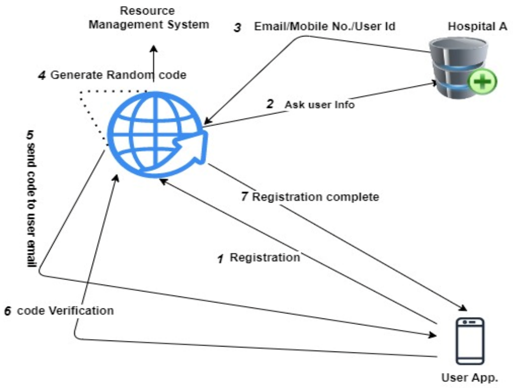

Fig. 1 User registration.

C. Data Inquiry

Fig. *2* illustrates the process of data inquiry. A data inquiry scenario requires tests result such as electrocardiogram (ECG), magnetic resonance imaging (MRI), and transesophageal echocardiogram (TEE), before diagnosing the patient's disease. The patient informed the doctor that they had already done tests (e.g., MRI) in the previous hospital. The doctor asked for the medical record of the patient.

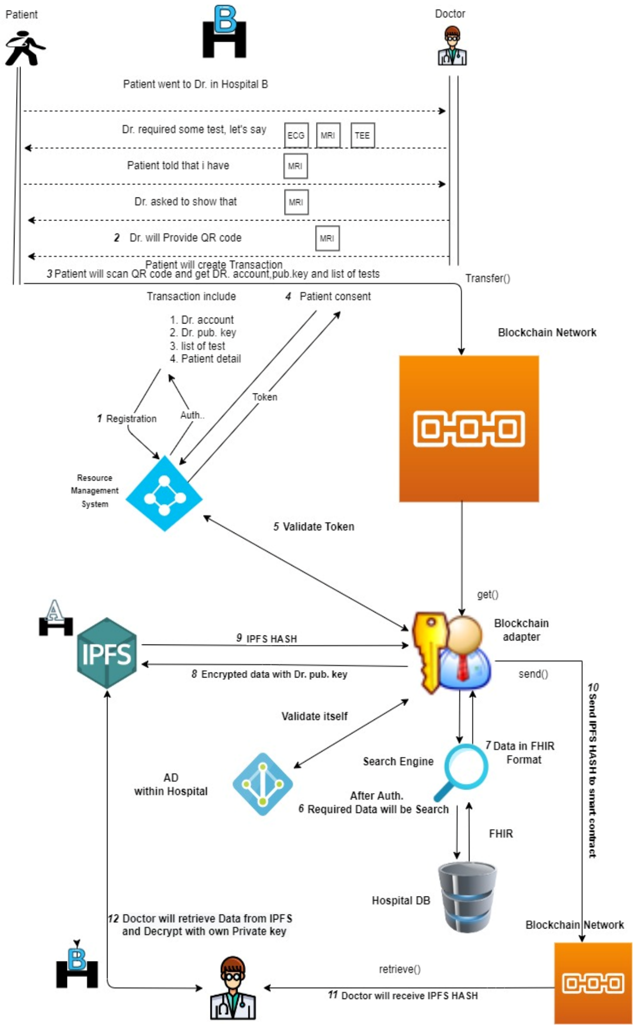
Patient
Doctor
Patient went to Dr. in Hospital B
Dr. required some test, let's say
ECG
MRI
TEE
Patient told that i have
MRI
Dr. asked to show that
MRI
2 Dr. will Provide QR code
MRI
Patient will create Transaction
3 Patient will scan QR code and get DR. account,pub.key and list of tests
Transfer()
Transaction include
4 Patient consent
1. Dr. account
2. Dr. pub. key
3. list of test
4. Patient detail
Blockchain Network
Token
1 Registration
Auth..
Resource Management System
5 Validate Token
get()
Blockchain adapter
9 IPFS HASH
IPFS
8 Encrypted data with Dr. pub. key
send()
10 Send IPFS HASH to smart contract
Validate itself
7 Data in FHIR Format
Search Engine
AD within Hospital
After Auth.
6 Required Data will be Search
FHIR
Hospital DB
12 Doctor will retrieve Data from IPFS and Decrypt with own Private key
Blockchain Network
retrieve()
11 Doctor will receive IPFS HASH

Fig. 2. Data inquiry and data sharing process.

Then the doctor provides a QR code, which contains the blockchain account, public key, and list of selected tests. To begin, patients use a two-phase authentication to access the system. The patient inputs an email address, and RMS generates a one-time password (OTP) and sends it to his email. By entering the OTP, the patient logs in to the system. The legitimate patient scans the QR code and obtains the blockchain account of the doctor, as well as the public key with the required tests. The patient consents to the selected medical tests provided by the doctor, and then sends the transaction to the hospital so that the hospital can send the patient's medical data to the specified doctor. When a patient initiates a transaction with consent, RMS generates a JSON web token (JWT) containing the patient's information, the doctor's information, the required tests, and token information (expiration time) in the ciphertext.

The transaction includes the doctor's account, doctor's public key, test name, and patient information in the form of a token. The blockchain adapter confirms the patient in the hospital where the transaction is forwarded. The blockchain adapter checks the token validity first for expiration time, and secondly, the hospital matches patient information with hospital records to confirm the patient's identity.

D. *Data Sharing*

The lower half of Fig. 2 shows the data sharing process. After the authentication and validation of the token, the blockchain adapter communicates with the hospital. The hospital searches for the requested medical record in its hospital database. On successful finding, the medical records are encrypted with a doctor's public key for authenticity and security of medical data. The blockchain adapter sends the encrypted medical record to the IPFS. All medical data stored in IPFS are encrypted by a doctor's public key to prevent unauthorized persons from accessing medical records. The returned hash from IPFS is sent to the doctor. The doctor receives the link to the IPFS server and hashes from the blockchain on the doctor application. The doctor of hospital B requests to retrieve data from IPFS using the IPFS hash within the specified time. The decryption technique is utilized when a doctor requests a patient's previous data. The doctor sees the patient's medical record, which is secure, authentic, and trustable because data is retrieved with the IPFS hash and decrypted with the doctor's private key.

In the patient application, patients can create or import the blockchain wallet, scan QR codes, agree/disagree with selected medical tests, send a transaction to the hospital, and save transaction ID for tracking. Doctors can create or import the blockchain wallet, select the required test, create QR codes, and retrieve and view patients' medical data in the doctor application.

IV. Discussion

This section shows how we achieve the required functionalities for a patient-centric EMR sharing system using blockchain. We also discuss the benefits of integrating mobile devices.

A. *Authentication*

The proposed system authenticates both patient and doctor during registration. The hospital helps to authenticate them during the process. The patient is verified with social security number while the doctor is confirmed with a doctor's ID. An unknown person cannot be a part of this system. Further, two-phase authentications increase confidentiality. A malicious attacker can intercept the information transferred between the patient and hospital A. He/she pretends to be a legitimate patient and then transmits the information to the targeted hospital after alteration. However, because the information is transferred between the patient and the hospital in the form of a token, the hospital identifies token modification during token validation if any change happens. The JSON web token provides additional verification while making the transaction from patient to hospital.

B. *Integrity*

Honesty and integrity are essential in the medical profession. To ensure the initiative's success, healthcare professionals must have confidence in the data integrity. Physicians may make critical decisions about the patient's survival. To guarantee the EMR's integrity, the returned hash from IPFS is safely exchanged with the doctor. This hash is generated by file content in the IPFS storage model, and any changes to IPFS data are immediately detectable. The doctor obtains the same EMR as the hospital share. Thus, the doctor can highly rely on retrieved EMR.

C. Access Control

Access control is one necessary security element for any organization, particularly in healthcare. This is especially true in healthcare clinics and hospitals where the data might be necessary for sustaining patients' health. The proposed method enables patients to have total control over their EMRs. Patients seeking treatment can choose the doctor they want to share their medical data with. Without the help of patients, other doctors cannot obtain patient medical data, and hospitals also only accept the data requests from the patients.

D. Integrating With Wearable Device

Quality care is more important than ever in the patient-centric world of today. Using health applications with wearable devices such as smartwatches provides many benefits. When a smartwatch is linked to a smartphone, the wearer reads and sends new messages without holding and looking at the phone. These devices are linked to a smartphone and see notifications right on the wrist. By connecting a wearable device to your mobile, notifications are checked and received updates about health such as heartbeat rate and health-related data with doctors for faster diagnosis and treatment.

E. Making use of Mobile Features

With the evolution of mobile devices and the increasing number of mobile users, new possibilities for the use of mobiles in patient care have been developed. Clinicians can quickly access patient records via a mobile-based EMR without sitting at a workstation. Mobile devices make it easy and quick for health care professionals to obtain evidence-based information, which helps them make clinical decisions at the point of care. Further, a mobile-based EMR sharing system has more extensive functionalities than previous systems, such as real-time notification, bio-authentication, camera, and auto-fill OTP.

Signup and login are the first two steps to use a health application because this is more related to personal information. The signup requires a two-phase authentication by sending a verification code using a mobile number or email. Patients benefit from the mobile application because the mobile app auto-fills the verification code. In contrast, there is no such option available on web apps to fill code automatically; patients need to fill it manually. More on, mobile apps offer more security protection with bio-authentication and fingerprints/face recognition than other web-based systems. Biometric authentication is incredibly simple and rapid from a user's perspective, despite its technical nature. Placing a finger on a scanner and instantly gaining access to an account.

Mobile applications have the functionality, including the contact list, GPS, phone calls, and accelerometer, of a mobile device. Such gadget characteristics make the patient's experience more participatory and convenient when utilized within an application. Additionally, these elements influence reduced effort. For instance, patients use the camera to complete a blockchain address by scanning the QR code rather than entering it manually. If you enter a blockchain address manually, it is time-consuming, and there is also a chance of a mistake. The integrated features of mobile apps significantly reduce the time required to complete certain processes in an app. Further, with notifications, users can remain updated about any unusual activity such as another user attempting to log in to your account, the mobile applications will alert you in real-time.

V. Conclusion

Mobile devices are used often in the medical field, and their capacity to provide access to services regardless of the user's time or location makes them ideal for providing healthcare to both patients and healthcare staff. While health-related apps are expanding, there is a significant gap in the availability of patient-centric apps. We proposed a mobile-based patient-centric medical data sharing system using blockchain. The system provides necessary functionalities for EMR data exchange and enables the patients to own, control, and share their health data quickly and securely. The mobile features can be effectively integrated to make the system more user-friendly.

Acknowledgment

This research is funded by the Ministry of Science and Technology (MOST) Taiwan under the grant numbers 110-2321-B-468-001 and 110-2511-H-468-005.

References

[1] B. Tofighi, A. Abrantes, and M. D. Stein, "The role of technology-based interventions for substance use disorders in primary care: A review of the literature," Med. Clin. North Am., vol. 102, no. 4, pp. 715–731, Jul. 2018.

[2] R. N. Moman et al., "A systematic review and meta-analysis of unguided electronic and mobile health technologies for chronic pain-is it time to start prescribing electronic health applications?" Pain Med. Malden Mass, vol. 20, no. 11, pp. 2238–2255, Nov. 2019.

[3] D. D. Taralunga and B. C. Florea, "A blockchain-enabled framework for mhealth systems," Sensors, vol. 21, no. 8, Art. no. 2828, Apr. 2021.

[4] Y. Petrakis, A. Kouroubali, and D. Katehakis, "A mobile app architecture for accessing EMRs using XDS and FHIR," in 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE), pp. 278–283, Oct. 2019.

[5] M. Engelhardt, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," Technol. Innov. Manag. Rev., vol. 7, no. 10, pp. 22–34, Oct. 2017.

[6] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: A blockchain-based platform for healthcare information exchange," in 2018 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 49–56, Jun. 2018.

[7] U. Chelladurai, S. Pandian, and K. Ramasamy, "A blockchain-based patient-centric electronic health record storage and integrity management for e-health systems," Health Policy Technol., vol. 10, no. 4, Art. no. 100513, Dec. 2021.

[8] L. Hang, E. Choi, and D.-H. Kim, "A novel EMR integrity management based on a medical blockchain platform in hospital," Electronics, vol. 8, no. 4, Art. no. 467, Apr. 2019.

[9] V. Jaiman and V. Urovi, "A consent model for blockchain-based health data sharing platforms," IEEE Access, vol. 8, pp. 143734–143745, Aug. 2020.

[10] J. W. Kim, S. J. Kim, W. C. Cha, and T. Kim, "A blockchain-applied personal health record application: Development and user experience," Appl. Sci., vol. 12, no. 4, Art. no. 1847, Jan. 2022.

[11] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," J. Ambient Intell. Humaniz. Comput., vol. 13, pp. 693–703 Jan. 2022.

[12] A. Dubovitskaya et al., "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," J. Med. Internet Res., vol. 22, no. 8, Art. no. e13598, Aug. 2020.