Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain

Richard Nuetey Nortey
Donghua University,
School of Computer Science and Technology
Shanghai, China
e-mail: rn.nortey@yahoo.com

Li Yue
Donghua University
School of Computer Science and Technology
Shanghai, China
e-mail: frankyueli@dhu.edu.cn

Promise Ricardo Agdedanu
Donghua University
School of Computer Science and Technology
Shanghai, China
e-mail: raptech2009@gmail.com

Michael Adjeisah
Donghua University
School of Computer Science and Technology
Shanghai, China
e-mail: madjeisah@yahoo.com

Abstract— **Currently, storing patient's sensitive data by medical healthcare into Electronic Healthcare Records (EHR) has evolved immensely. Specifically, distributed healthcare records have brought ease to how hospitals and other different third parties access the sensitive medical health information of patients for various uses leading to generation of big data. Big data in healthcare is important as it can be used in the prediction of outcome of diseases, prevention of co-morbidities fatality and saving the cost of medical treatment. However, this has also made it easy for security breaches and privacy violations during the data collection process. In this paper, we propose a platform which uses the blockchain technology for privacy preservation during collection, management and distribution of EHR data. The aim of this paper is to ensure the total privacy, integrity and access control of distributed electronic health records to the data owners during its distribution on the blockchain. Simulated results demonstrate our proposed system establishes total transparency and ensures perfect privacy within the distributed network of sharing EHRs in the medical setting using the blockchain.**

Keywords-component; privacy; EHR; blockchain; channel; certificate authority ; smart contract

I. Introduction

An electronic health record (EHR) is a digital version of an individual's medical data. It is collected and managed by multiple authorized healthcare providers, and can be exchanged electronically among them. It often includes demographic data, medical history and clinical information, such as laboratory, radiology and pharmacy data. The increasing uses of electronic health record (EHR) systems by different health institutions have led to huge collection of sensitive health data. Apart from patient treatments, patients' data can be used for various purposes that help to improve health outcomes and costs [1]. When it comes to patient health records the information stored using EHRs is highly sensitive therefore the parties or entities that can see it and share it must be limited. One of the main clinical aims of the Open EHR is to facilitate sharing of EHRs via interoperability at data and knowledge levels while reducing the incidence of patients being overlooked in the healthcare system due to information not being available or communicated [2]. However, the responsibility does not only lie on the medical health institution to ensure the safety and protect the privacy of these EHRs in transit but also there are some regulations that forces them to control how patient's sensitive health records can be accessed. HIPAA is a regulation that some governments imposes on medical institutions that collect information which goes into patient medical records [3]. It is essential to share these health records among other health institution and also to other parties such as the pharmaceutical industry and medical health research institutes, however the integrity of this data must be kept at all times and access to this information must be cleared. Tragically, as innovation has propelled, so excessively have the procedures utilized, making it impossible to abuse computerized protection and security. The medicinal services industry, specifically, has been a noteworthy focus for data robbery as well-being records regularly contain private data such as the names, biometric information, government managed savings numbers, and addresses of patients.

Much related work in the literature focuses on the use of blockchain together with various access control techniques and platforms to ensure the privacy of the patient's medical health Information. There have been many recent studies, which focuses combining different consensus algorithms in order to ensure perfect privacy of medical EHRs. The Blockchain is a secure transaction ledger database that is shared by all parties participating in an established, distributed network of computers. It records and stores every transaction that occurs in the network, essentially eliminating the need for "trusted" third parties such as payment processors. Many experts now believe that blockchain technology might be just the thing to get a patient's pertinent medical information from where it is stored to where it is needed, as well as to allow patients to easily view their own medical histories [4], [5].

978-1-7281-1282-4/19/$31.00 ©2019 IEEE

Our system proposes the use of blockchain to securely ensure that EHRs are only accessed by authorized parties through a technique known as channeling integrated with smart contract logic scripts within the network to ensure interoperability of EHRs and access control only through the authorization of the patient who is mainly the data owner. To achieve interoperability our proposed blockchain-based platform is able to interact with EHR platforms and other medical traditional platforms through the use of smart contracts and specified network configurations. All access control policies within the distributed network are instantiated through the uses of these smart contracts thereby creating a unique access to only authorized participants on the network fully managed by the patient. The rest of this paper consists of five sections. In section 2, research which are related to the privacy preserving of EHRs are discussed. The present EHR system within the medical system is discussed in section 3, section 4 will include our proposed model and implementation and section 5 includes a conclusion and some ideas for our future works.

II. Related Work

There are many ways in which cloud computing can deliver services to healthcare organizations, helping them to better serve their patients and to grow securely [6]. In Kaur et al [7] a model for healthcare data in blockchain-based architecture in the cloud computing environment is proposed to address privacy and security issues as the health data carries sensitive information and attackers are constantly trying new ways to enter the cloud storage system. The author combines the security and tamperproof nature of the blockchain with cloud computing for storing medical data. The author highlights the vulnerability of the cloud space and demonstrates how enabling blockchain can improve data privacy of medical health records.

Azaria et al [8] proposes a blockchain EHR platform that cryptographically incentivizes medical stakeholders to participate in the network as blockchain “miners” hence creating a cryptographically secured data access through the use of the blockchain technology. This provides the participants with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the privacy of EHRs on the network.

Realtime monitoring in medical health has revolutionized how patient health is monitored. Health monitoring from the patient’s home and other locations continues to gain importance as pressures comes from a variety of sources to reduce risks and costs of readmissions and hospitalizations nonetheless patient’s privacy must be ensured. An example of real-time patient data is the Patient Physiological Parameters (PPPs) in Patient Health Information (PHI). Masood et al [9] used data sets from various health institutions in Asia to investigate and analyze the sharing and exposure of PPPs by medical staff at various levels with regards to appropriate authorization rights without threatening the privacy of patients and concluded that patient privacy is being violated, yet suggested that with proper authorization access for PPPs the access can be managed.

Dagher et al [10] proposed a framework named Ancile which adopts specific Ethereum tools and develops and utilizes six smart contract types for operation: consensus, classification, service history, ownership, permissions, and re-encryption to maintain privacy of EHRs. In their Ethereum-based blockchain framework there is a heightened access control and obfuscation of data, and it employs advanced cryptographic techniques for further security. Their framework gives ownership and final control of EHRs to the patient, securely controlling who can access documents and track how records are used, allowing for secure transfer of records, and minimize ability for unauthorized actors to derive Patient Health Information.

Ouagne et al [11] proposed an EHR4CR Semantic Interoperability Framework for consistent interpretation of clinical data accessed from varying sources, and demonstrated the expressiveness and computability of the EHR4CR framework for eligibility determination hence providing a simplified information model for data sharing.

Yachana Kaur and sood [12] proposes a Trust based Access Control (TAC) system and privacy schemes which not only identifies authorized users for Patients centric big medical data but also defends Sensitive Personal Information (SPI) of a patient from insider attacks. The proposed system presents an approach to address security and privacy of patient’s medical health by using a trust-based access control system to fetch trust values of users and then calculates the trust values of access rights of users combined with various quantitative parameters such as medical evil process, patient centric models, satisfaction, resemblance and assessment reliability to grant access to only trustworthy users or participating parties within the medical setting. They concluded that the proposed system calculates accurate trust value of various users and provides secure access to data hence maintains privacy and security of EHRs.

Although many proposals to use the blockchain technology to secure and ensure privacy during the distribution of EHRs have proven very useful there is the need to have a more effective yet simple implementation procedures to do this. Since blockchain is a new and emerging technology there has been many complex and sophisticated approaches to ensure its usability. Our proposed system introduces the implementation of the blockchain in a simple yet very secured manner of appending and sharing EHR’s on a distributed network whiles ensuring the highest level of patient’s privacy. We propose a system the enables the hospital to be the administrator and creator of EHRs on a blockchain network after which the administrative rights are transferred to the patient who then can control access to their medical records on the network without any fear of interference from the hospital. These nodes contain ledgers on which every EHR is stored and automatically updated within all the nodes on the network to ensure trust and transparency. However, to maintain security on the network our system uses appropriate certificate authorities and network identification configuration to ensure the membership and cryptographically ensure the communication of network entities. Our main prerogative is to ensure true privacy and therefore we introduce the use of channels; which through the use of smart contracts on the blockchain creates a secure and private "pipe" like connection for a patient who is the owner of the EHR to grant and authorize other participating actors or shareholders on the network the access to their EHRs knowing that privacy is maintained.

III. Present Distributed EHRs

Electronic health information exchange allows doctors, nurses, pharmacists, other health care providers and patients to access and share essential medical information electronically[13]. This has the potential to improve the speed, quality, safety, and cost of patient care. Fig.1 shows the components of EHR such as immunization, dispensed medication, laboratory results, diagnostic reports and other relevant clinical information of a patient. It is important to use sharing techniques for distributing EHRs as it is used by providers to easily send patient information—such as laboratory orders and results, patient referrals, or discharge summaries—directly to other health care professionals. This information is sent over the internet amongst health care professionals and other parties who already know and trust each other [14]. Another important point to note is that EHR exchanges enables coordinated care, benefitting both providers and patient. Distributed EHR sharing provides patients with access to their health information, allowing them to manage their health care online in a similar fashion to how they might manage their finances through online banking. When in control of their own health information, patients can actively participate in their care coordination by providing other providers with their health information.

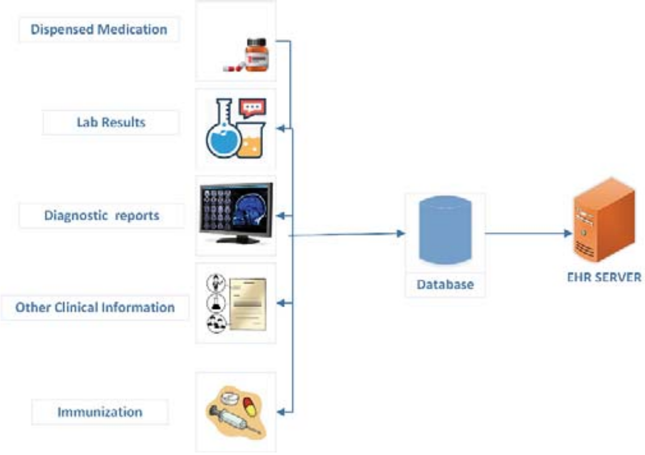

Figure 1. The components of an EHR

Fig. 2 shows how EHRs are shared and updated by parties involved within the EHR sharing eco system where the patient is a passive actor in the distributed EHR setting. In Fig. 3 A primary care provider such as the home doctor or a hospital can directly send electronic care summaries that include medications, problems, and lab results when referring their patients to the main EHR database which is accessible to the specialist, research institutions and other third parties like insurance companies and government bodies as well. This information helps to inform the visit and prevents the duplication of tests, redundant collection of information from the patient, wasted visits, and medication errors. Lab reports of patients are appended onto the EHR from laboratories. Through the distribution of EHRs immunization data of a patient can also be accessed through EHR by Medicare and Medicaid Services or public health organizations to report quality measures of health care's [15]. Through the distribution of EHRs, Fig. 3 continues to illustrate how physicians can access patient information—such as medications, recent radiology images, and problem lists—might adjust treatment plans to avoid adverse medication reactions or duplicative testing. However, the patient being the owner of the data is given the limited administrative rights to allow who has access to the EHRs thereby becoming a participant in the distribution process.

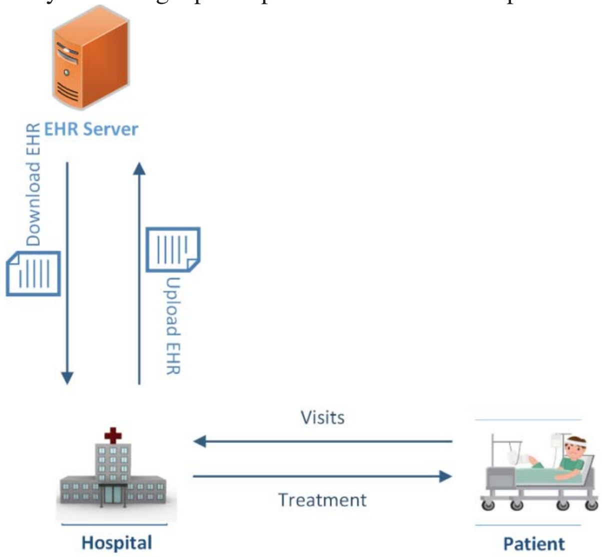

Figure 2. Current EHR network and the role of patient.

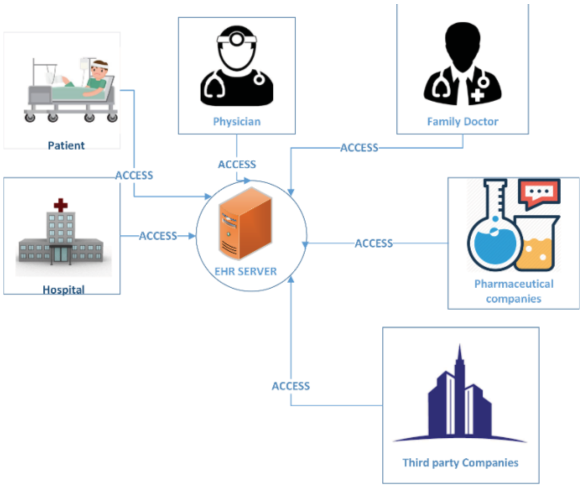

Figure 3. The Present EHR Distributed network

The flaw with the legacy way of distributing EHR is that the data owners who are the patients are only able to read

Identify applicable sponsor/s here. *(sponsors)* and most of the time have no say in how their EHR is viewed. However true privacy and confidentiality is when information of a patient is released to others only with the patient's permission or obligated by law. When a patient is unable to do so because of age or mental incapacity the decisions about information sharing should be made by the legal representative or legal guardian of the patient [16]. Information shared as a result of clinical interaction is considered confidential and its privacy must be protected.

IV. Proposed Model And Implementation

A. *Preliminary*

1) Blockchain:

A blockchain is a shared ledger distributed across a business network. Business transactions are permanently recorded in append-only blocks to the ledger. All the consensually confirmed and validated transaction blocks are linked from the genesis block to the most current block with each block linked to its previous block using the cryptographic hash of the previous block - hence the name blockchain [17]. The blockchain serves as a single source of truth for the network. Cryptography is used to ensure that network participants see only the parts of the ledger that are relevant to them, and that transactions are secure, authenticated and verifiable, in the context of permissioned business blockchains.

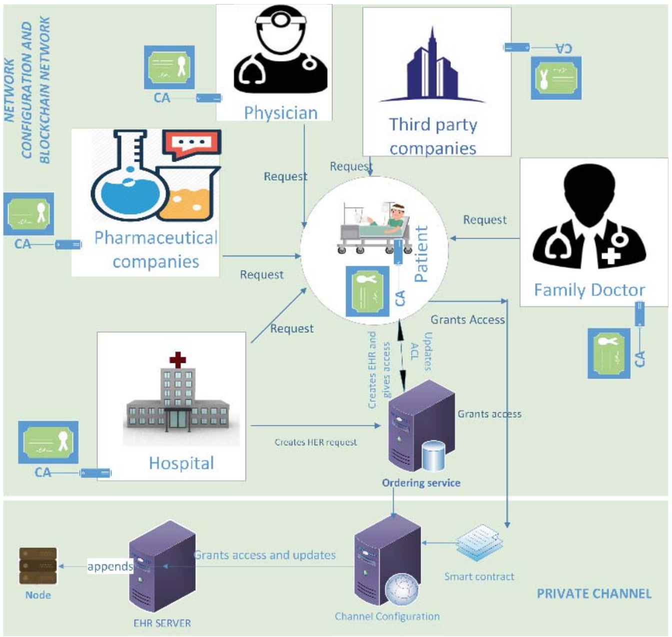

Figure 4. Proposed blockchain based EHR Platform

B. *Proposed Solution*

Our proposed system comprises of the following components within the network:

1) Ordering service: The ordering service is an administration point which provides all the entities with a controlled access to the network and resides on the data creator's infrastructure. It updates, validates and commits records to the ledger on the nodes on the blockchain.

2) Certificate Authority (CA): The certificate authority is used to uniquely identify every entity participating in the distribution of EHR on the blockchain network and it also binds together these entities cryptographically enabling secure communication between them.

*3) Blockchain Network Configuration***:** Network configurations interact directly with the blockchain maintaining all the distributions within the network.

4) Channel configuration: Channel configuration is detached from the network, it is created with smart contracts and it establishes privacy within the network and can be activated only by the authorized user to grant access to their data.

5) Smart Contracts: Smart contract is the executable software module which is developed and installed into the blockchain itself and enforced with pre-defined rules to ensure the channel configuration module is creating a unique access for authorized entities to access records through the channels.

6) Channel: Channel is the abstracted module from the blockchain which interacts with the applications access requests to create a unique private platform on which entities on the network can view and access records.

*7) Node***s**: Nodes are the network components where local copies of the ledger are hosted and stored on the blockchain network.

Our proposed approach in building our model is using blockchain technology as a solution to address EHR distribution's main challenge which is data privacy. First, it is infeasible and provokes very poor performance to store all the data on the blockchain, so the blockchain will be used as a tool to grant access to requests from other users before they are allowed access into the channel to update or view data on the EHR server. To achieve true interoperability and data sharing with the appropriate APIs our proposed system can integrate the blockchain system to existing EHR platforms by using its underlying technology which is a distributed ledger and coded smart contracts to ensure that all partakers in the distributed EHR sharing the network are governed by access control policies specified in the blockchain smart contract allowing only authorized parties to see and update records with the full permission and awareness of patients. our system employs modern cryptographic mechanisms to validate records which leaves a trail of access behind every data accessed or updated and this guarantees trust in the data distribution environment. We have explained each terminology to give an ample understanding to the fundamental operation of the network. We demonstrate a basic implementation of how our proposed model uses the blockchain to support health data distribution and access whiles maintaining privacy.

C. Implementation and Work Flow

To implement this model, the core of it is the blockchain. As already mentioned in Section 2, there exists multiple types of blockchains, but for reasons of ease of testing and further development, Hyperledger blockchain is used. Hyperledger Fabric is also a permissioned private blockchain which has its own characteristics and block parameters, but provides the capability of creating our own private blockchain for studying and testing purposes. As stated earlier, the EHR of a patient is accessed through a front-end client application, created by the hospital and used within the network. After the creation of the EHR, a certificate authority is issued to identify the patient on the blockchain network and all administrative privileges are automatically appended to the patient's account. As shown in Fig 4 the ordering is the administration point which provides all the entities-controlled access to the network, upon creation of EHR the hospital updates the network configuration to make the patients the administrator of their records. At this point the patient and hospital have equal rights over the network configuration on the network. Although the ordering service is running on the hospital's infrastructure, the patient has shared administrative rights over EHR records, as long as it can gain network access. In this way, even though the hospital is running the ordering service and the patient has full administrative rights over EHR, third parties have limited rights to access these records. The hospital who is the network administrator defines access of EHR through access requests from other parties with and only with the approval of the patient who is the owner of records. This distribution access policies or configuration are stored in the network configuration. The distribution configuration within the network configuration defines the set of entities in the network who wants to be a part of distribution in patients EHRs on the blockchain network with one another – with regards to this paper it is the patient, pharmaceutical, family doctor, physician and other third-party companies such as insurance and other interested governmental bodies. Once access is granted by patient a channel is created for a particular entity to access EHR records. However, access to EHRs is governed by channel configuration completely separate from the main network and can only be authorized by the patient. All records are accessed on the ledger through the nodes overseen by the ordering service. Before the data is stored on the blockchain it can be stored in a metadata using index files. On the blockchain we have the smart contract which defines all the common access patterns to the ledger; smart contract gives a well-defined set of ways by which the ledger can be queried or updated on the node. For the ease of distribution, the ledger is what holds the EHRs data or hashed EHR data pointing to the main data stored on respective EHR servers. In our experiment our blockchain platform's API is able to communicate with the client application on each device on the network node to have access to the server on which the EHR is stored.

V. Conclusion

In this paper, we propose a blockchain framework for EHR management on a distributed network that could ensure ultimate privacy to patient's health records giving patients the control over who accesses their EHRs through special means provided by our system. Collection and synchronization of this data into Big Data has a great potential of changing the healthcare outlook such as in drug discovery, patient's personalization care, treatment efficiency, improvement in clinical outcomes and patient's safety management. To ensure security a network configuration mechanism ensures that all participating entities are authorized to exchange and share this data. The blockchain provides the platform for which the patient's EHR can be stored without any attacks or tempering. Then to ensure ultimate privacy and access control to an EHR record on the blockchain a channeling mechanism ensures that patients authorize entities within the distributed network to exclusively access this information. In the future we will work on access control list and application programming interface issues with the blockchain in big data analysis.

Acknowledgements

This work is supported by National Key R&D Program of China, Grant No. 2017YFB0309800.

References

[1] V. A. IAVRUMOV, "Nabliudeniia nad izmenchivost'iu kishechnoi fekal'noi palochki.," *Gig. Sanit.*, vol. 9, pp. 52–53, 1953.

[2] M. A. Hailemichael, L. Marco-Ruiz, and J. G. Bellika, "Privacy-preserving Statistical Query and Processing on Distributed OpenEHR Data," *Stud. Health Technol. Inform.*, vol. 210, pp. 766–770, 2015.

[3] Y. H. Information and P. Rights, "Office Civil Rights for Your Health Information Privacy Rights," pp. 1–2, 1996.

[4] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm. Policy*, no. September, pp. 1–12, 2017.

[5] A. Sherriff, "Blockchain reaction," no. June, pp. 4–7, 2016.

[6] C. Standards and C. Council, "Impact of Cloud Computing on Healthcare," 2017.

[7] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment," *J. Med. Syst.*, vol. 42, no. 8, 2018.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016.

[9] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Privacy management of patient physiological parameters," *Telemat. Informatics*, vol. 35, no. 4, pp. 677–701, 2018.

[10] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, no. August 2017, pp. 283–297, 2018.

[11] D. Ouagne, S. Hussain, E. Sadou, M. C. Jaulent, and C. Daniel, "The Electronic Healthcare Record for Clinical Research (EHR4CR) information model and terminology," *Stud. Health* Technol. *Inform.*, vol. 180, pp. 534–538, 2012.

[12] Yachana, N. Kaur, and S. K. Sood, “A trustworthy system for secure access to patient centric sensitive information,” *Telemat. Informatics*, vol. 35, no. 4, pp. 790–800, 2018.

[13] N. Jamshed, F. Ozair, A. Sharma, and P. Aggarwal, “Ethical issues in electronic health records: A general overview,” *Perspect. Clin. Res.*, vol. 6, no. 2, p. 73, 2015.

[14] J. M. Madden, M. D. Lakoma, D. Rusinak, C. Y. Lu, and S. B. " Soumerai, “Missing Clinical and Behavioral Health Data in a Large Electronic Health Record (EHR) System,” 2015.

[15] C. Hew Hei and A. Ismail, “Indicators for Medical Mistrust in Healthcare–A Review and Standpoint from Southeast Asia,” Malaysian *J. Med. Sci.*, vol. 24, no. 6, pp. 5–20, Dec. 2017.

[16] L. B. Harman, “Ethical Challenges in the Management of Health Information,” *J. Healthc. Qual.*, vol. 23, no. 5, p. 49, Sep. 2001.

[17] “The IBM Advantage for Implementing the CSCC Cloud Customer Reference Architecture for Blockchain,” 2017.