Blockchain Enabled Privacy Security Module for Sharing Electronic Health Records (EHRs)

Li Yue*, Richard Nuetey Nortey, Michael Adjeisah, Promise Ricardo Agbedanu, Xinyi Lui
College of Computer Science and Technology, Donghua University, Shanghai, China.

* Corresponding author. Tel.: 18621007839; email: rn.nortey@yahoo.com
Manuscript submitted May 15, 2019; accepted August 8, 2019.
doi: 10.17706/ijcce.2019.8.4.155-168

Abstract: Currently, storing sensitive data related to patient's medical healthcare into Electronic Health Records (EHRs) has developed rapidly. Specifically, the distribution of healthcare records has brought convenience to hospitals and other different third parties in accessing this sensitive medical health information of patients for various purposes, thus leading to the generation of big data. In the field of healthcare, big data plays a significant role as it can be employed in predicting outcomes of diseases, preventing co-morbidities fatality and saving the cost spent on medical treatment. However, it is most likely to lead to both security breaches and privacy violations in the process of data collection. In this paper, a platform employing the blockchain technology for privacy preservation during the process of collecting, managing and distributing EHR data is proposed. This paper aims to ensure the total privacy, integrity and access control of distributed electronic health records possessed by the data owners in the process of it being distributed on the blockchain. Simulated results demonstrate that the system proposed by us, which is totally transparent, is able to ensure perfect privacy within the distributed network of sharing EHRs in the medical setting by employing the blockchain.

Key words: Electronic health records, big data, privacy, blockchain, smart contract, ordering service.

1. Introduction

An electronic health record (EHR) is known as a repository of information concerning the health condition of a patient and it is usually stored in the processable form in computer. It is generally supposed that an EHR contains all the necessary information about a patient collected from several providers including evidence-based tools for the purpose of making intelligent decisions. In other words, EHR is able to maintain the health the patients from a macro perspective, because it can be both collected and managed by multiple authorized healthcare providers in addition to being exchanged electronically among the providers. EHR is often composed of demographic data, medical history and clinical information, such as laboratory, radiology and pharmacy data. The increasing employment of EHR systems by different health institutions have led to the collection of sensitive health data in large amount. Apart from treatments received by patients, patients' data can be adopted for various purposes in order to help to improve health outcomes and reduce relevant costs [1]. When it comes to patient's health records, the information stored by adopting EHRs is highly sensitive, and therefore the parties or entities which are entitled to see it and share it must be limited in certain amount. It is acknowledged that one of the main clinical aims of the Open EHR is facilitating the sharing of EHRs via interoperability at data and knowledge levels while reducing the

incidence of patients' being overlooked in the healthcare system because of the lack of information or unsmooth communication [2]. Apart from ensuring the safety and protecting the privacy of these EHRs in transit conducted by medical health institutions, some regulations should be established as well to control how patient's sensitive health records can be accessed. HIPAA is known as a regulation that some governments impose on medical institutions to offer guidance to the collection of information which goes into patient's medical records [3]. It is of great significance to share these health records among other health institutions and also to other parties such as the pharmaceutical industry and the institutes engaged in medical health research, however the integrity of such data must be kept at all times and access to such information must be cleared. Tragically, the procedures have been utilized excessively along with the progress of innovation, making it impossible to abuse computerized protection and security. Specifically, the industry of medicinal services has been known as a noteworthy focus for data robbery because well-being records regularly contain private data such as names, biometric information, savings numbers managed by the government, and addresses of patient.

In the literature, much related work focuses on the employment of blockchain together with various techniques on access control and platforms to ensure the privacy of information related to patient's medical health. Currently, many studies focus on the integration of different consensus algorithms for the purpose of ensuring perfect privacy of medical EHRs. In such circumstance, a new system is highly required to manage health data for the aim that all interested parties can monitor, access, and analyse consistent and updated information on electronic health records. For the purpose of removing information silos, this system must create a unifying backend that can be shared by the healthcare ecosystem. Blockchain distributed ledger, which is known as one emerging technology, is able to solve this problem by providing a decentralized backend that multiple parties can view and edit consistently without the demand to trust any of the other parties. In addition, the blockchain is a secure transaction ledger database that is shared by all parties engaged in an established and distributed network of computers. Moreover, it further records and stores every transaction occurring in the network, and essentially eliminates the need for "trusted" third parties such as payment processors [4]. Many experts now hold the view that the technology of blockchain might be just the thing to transfer a pertinent medical information possessed by patient from where it is stored to where it is needed, and it also allows patients to have easy access to their own medical histories [5], [6]. The use of blockchain proposed in our system aims to securely ensure that EHRs can only be accessed by authorized parties through the technique which is known as channeling by being integrated with the logic scripts of smart contract within the network for the purpose of ensuring interoperability of EHRs and access control only through the authorization of the patient who is actually the data owner. In order to achieve interoperability, the blockchain-based platform proposed by us is able to interact with EHR platforms and other medical traditional platforms through the adoption of smart contracts and specified network configurations. All policies of access control within the distributed network are instantiated through the employment of these smart contracts, which is able to create a unique access only to authorized participants on the network fully managed by the patient. The rest of this paper consists of five sections and the details of it is illustrated as follows. In section 2, research which are related to the privacy preserving of EHRs is discussed. As for the present EHR system within the medical system, it is explained in section 3. In addition, the workflow and implementation of the proposed system are illustrated in section 4 and section 5, which includes both the conclusion part and some ideas for our works in the future.

2. 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 [7]. In Kaur *et al*. [8] 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*. [9] 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*. [10] 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*. [11] proposed a framework named Ancile which adopts specific Ethereum tools and develops and utilizes six smart contracts 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*. [12] 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 [13] 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.

3. Present Distributed EHR

3.1. Electronic Health Record

EHR data is mainly composed of medical information like patient's basic information, clinical data, doctor's written notes, prescriptions and of patient's personal data of some other forms. Currently, new technologies are extensively employed in the medical domain in the aspects covering capturing devices, sensors, mobile applications and so on. Therefore, more amount of medical knowledge or discoveries are being accumulated in a constant flow. As a result, the costs spent on the collection of genomic information becomes lower. Consequently, results of medical images such as X-Rays, CT and MRI-scan, results from surgery and implants, laboratory records, genomic information, medication information, insurance details and other patient-related data are continuously being included in healthcare databases. Hence, the volume of healthcare database is witnessing an exponential growth. It is of great importance to note that EHR contains all the necessary information related to the patients that is collected from different providers. It can be further concluded that EHR contains the total health information of a patient, which enables it to be a valuable source of data which must be well protected. Fig. 1 shows the subordinate components of EHR and they are mainly composed of immunization, dispensed medication, laboratory results, diagnostic reports and other relevant clinical information that can be collected from a patient.

3.2. Distributed Electronic Health Records

It is of great significance to employ sharing techniques for the distribution of EHRs as the providers are able to easily send patient's information—such as laboratory orders and results, patient referrals, or discharge summaries—directly to other professionals engaged in the field of health care. As what has been stated above, EHRs plays a basic role of transforming physical records into digital records, which as a result is quite convenient in both recording and storing such data. However, it is quite necessary to share information of this kind among different entities or parties, more importantly, medical history, medication information, medical test results and all other relevant data about patient's health are all required to be shared from one hospital to another conveniently regardless of the time and location. It is sure that operating healthcare data and sharing the data over several locations may not be applicable by employing traditional DBMSs which is generally used in stand-alone system, and therefore the implementation of distributed EHRs is quite necessary. In the entire process, all information is sent over the internet amongst professionals engaged in health care and other parties who already know and trust each other [14]. It simply means that it is easy for medical services and data to be collected and analyzed in a distributed network of a medical setting. Another important point that is worth noting is that EHR exchanges results in

coordinated care, which consequently benefits not only providers but also patients. Moreover, distributed EHR sharing provides patients with easy access to their health information, and accordingly allows them to manage their health care online, which is quite similar to the management over their finances through online banking. During the process of controlling their own health information, patients are able to actively participate in their care coordination by providing other providers with health information of their own.

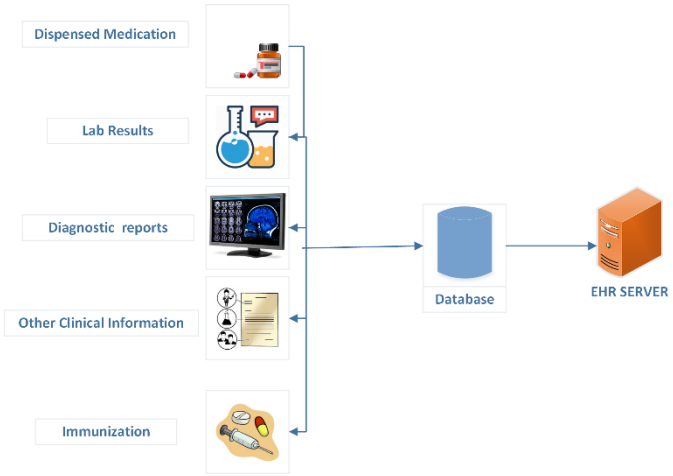

Fig. 1. The components of an HER.

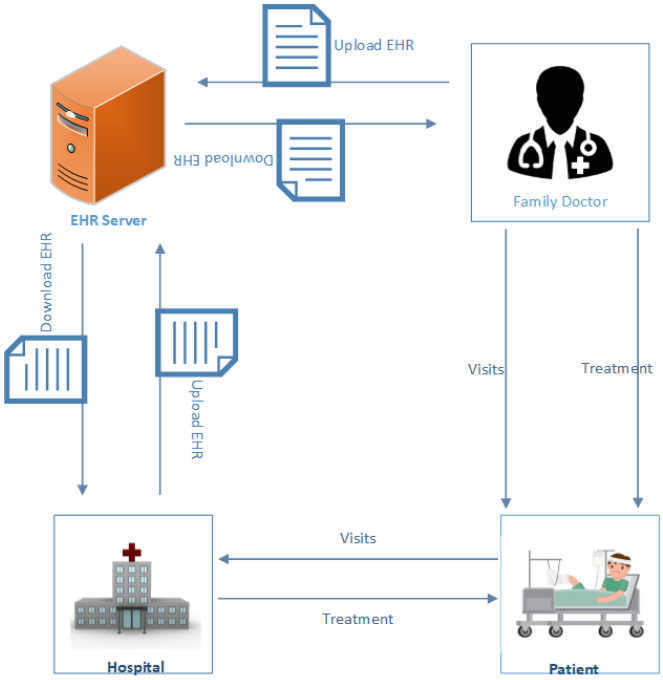

Fig. 2. Current EHR network and the role of patient.

Fig. 2 shows how EHRs are shared and updated among different parties engaged in the EHR sharing eco system where the patient is deemed as a passive actor in the distributed EHR setting. In the process, a primary care provider, such as the home doctor or a hospital, can directly send electronic care summaries including medications, problems, and lab results concerning their patients to the main EHR database which is available to the specialists, institutions involved in research and other third parties like insurance companies and government bodies as well. Such information obtained helps inform the visit and prevents the duplication of tests, redundantly collected information from patients, wasted visits, and errors in

medication. In addition, lab reports from patients are then appended onto the EHR from laboratories. Through the distribution of EHRs, data related to immunization of a patient can also be obtained through EHR via Medicare and Medicaid Services or public health organizations to report quality measures of health care [15]. Through the distribution of EHRs, Fig. 3 continues to illustrate in detail how physicians are able to access information obtained from patients—such as medications, recent radiology images, and problem lists—and consequently treatment plans might be adjusted for the purpose of avoiding adverse medication reactions or duplicative testing. However, the patient who is known as the owner of data is given limited administrative rights to determine who has access to the EHRs, and thereby the patient becomes a participant in the process of distribution.

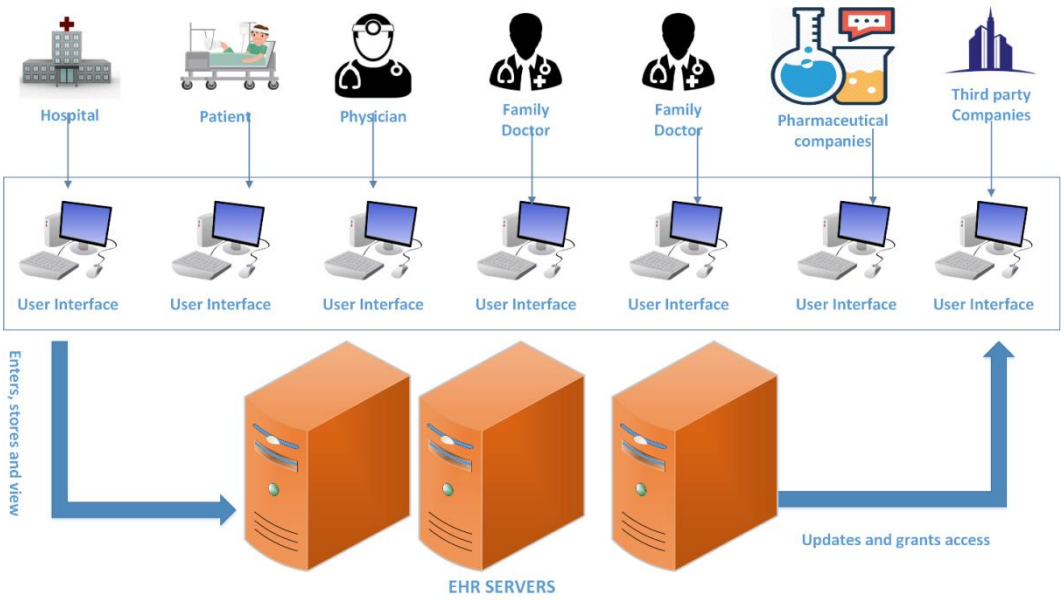

Fig. 3. The present EHR distributed network.

The flaw that is available in the traditional way of EHR distribution is that the data owners, who are the patients, are only able to read and they have no right in determining how their EHR is viewed most of the time. Distributed EHRs is able to ensure the interoperability and sharing of EHRs among healthcare providers, patients and practitioners and it also helps to conduct relevant analysis on patient's data so that right intervention can be provided to the right patient at the right time. However, the main limitation existing in this model is that its security is quite vulnerable to hackers. However, true privacy and confidentiality can be realized when information of a patient can only be released to others after being permitted by the patient or obligated by law. Moreover, when a patient fails 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]. Furthermore, information shared during the process of clinical interaction is considered confidential and its privacy must be well protected.

3.3. Security Issues with Electronic Health Record Distribution

Data breaches and attacks in the sector of healthcare generally occur in a variety of forms. They can include the cases where cyber criminals steal or modify health information that is well protected to commit medical identity theft, or instances that an employee views the records of one patient without being authorized. When such situation happens, hospitals or even insurers usually fail to take corresponding concrete measures to fix errors on someone's health record or help patients to cope with the other

consequences of identity theft. Unlike financial services in which credit card thefts can be dealt with and stolen transactions can be cancelled or recovered, healthcare information is usually non-recoverable. To this end, currently more and more healthcare providers are taking measures to enforce security practices such as implementing physical security controls, securing wireless networks, educating staff members and protecting the network such as upgrading the firewall and antivirus. However, these practices are only able to limit the danger during the process of cyber-attacks to certain extent and they are unable to fully eradicate or secure the privacy of data. Therefore, it is urgent to explore other alternative solutions and the use of the blockchain technology is deemed as the one among them. Fig. 3 shows some basic ideas on the logical architecture of an EHR system. The primary goal of the architecture is providing an interface between application and the users belonging to a hospital for easy access of data related to patient. The architecture includes a user interface (UI) which may have a user login system that can be employed to examine authentication of user (i.e. doctor, any third party and patient). However, UI is also adopted so as to provide input to update records and to retrieve and view records as well. Usually two security parameters, namely user-name and password, are available and they are essential in this purpose. It is quite obvious that if a user is authentic, then he or she is permitted to access his or her record stored in the server of patient EHR database, which is actually the digitized version of patient's information and known as EHR server. In particular, EHR is composed of medical and treatment history of patients such as patient name, address, mobile number, social security number, date of birth (DOB), medical information, surgery results, side effects, referred doctor information, etc. In addition, the information stored for each patient can be visualized as a single account and it is usually in the charge of the hospital. It is quite sure that EHR has several advantages compared with paper records. For instance, it allows clinicians to track data over time, to identify easily which patients should be treated with preventive screenings or check-ups, to check certain parameters of their patients, such as blood pressure readings or vaccinations, and to monitor and improve overall quality of care within the practice. It is possible for one to note that some important information owned by patient (named as sensitive data) may be blocked in the process of access (by applying appropriate encryption schemes) for the purpose of security. However, the problem of risk or threat existing in security of this architecture generally falls into two general categories, the software itself and failure to adopt good practices caused by human beings. It is from these two points that privacy violation and cyber-attacks come into being. However, a system is proposed and it can clearly enhance access control within the distributed network of EHRs at the same time of maintaining the highest form of privacy during the collection and management of patient's data irrespective of the velocity volume and speed of data by using the blockchain.

4. Proposed Model and Implementation

4.1. Preliminary

A blockchain is known as a shared ledger distributed across a business network. It is acknowledged that business transactions are permanently recorded in append-only blocks to the ledger. In the process, 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 by employing the cryptographic hash of the previous block, which leads to its name of blockchain [17]. The blockchain actually serves as a single source of truth that is available in the network. It can be obtained from a technical point of view that blockchain is a replicated and distributed ledger of transactions with ledger entries referencing other data stores for additional information related to ledger transactions. Actually, cryptography is a method employed to ensure that the participants of network see only the parts of the ledger that are relevant to them, and that transactions are secure, authenticated and verifiable under the background of permissioned business

blockchains. In general, a blockchain stores data through the employment of chained data structure, and it generates and updates data by using the consensus protocol between distributed nodes. In addition, it also uses the method of cryptography to ensure the security and automated scripting code to run intelligent contracts named smart contracts.

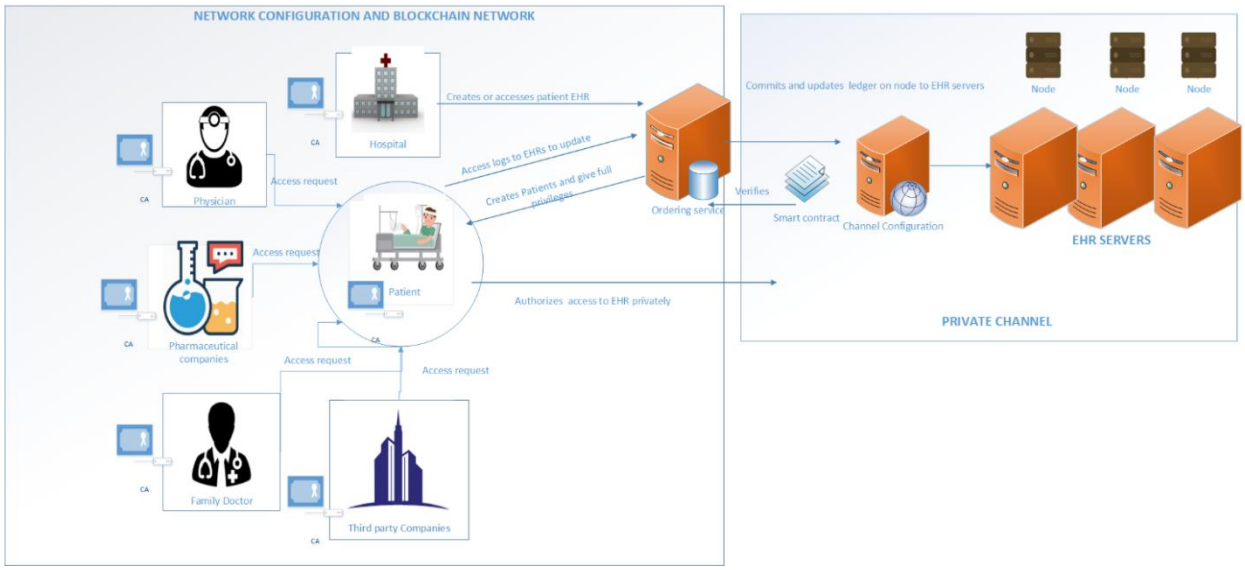

Fig. 4. Proposed blockchain based EHR platform.

4.2. Proposed Framework

4.2.1. Major components

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

1. Ordering service: It is known as an administration point where all the entities are provided with a controlled access to the network and they can reside on the data creator's infrastructure. In addition, it is able to update, validate and commit records to the ledger on the nodes of the blockchain.
2. Certificate Authority (CA): It is generally employed to uniquely identify every entity involved in the distribution of EHR on the blockchain network and it also binds together these entities cryptographically, which can consequently enable secure communication between them.
3. Blockchain Network Configuration**:** Its direct interaction with the blockchain can help to maintain all the distributions within the network.
4. Channel configuration: It is not only detached from the network, but also created with smart contracts. Besides, it can be activated only by the authorized user's granting access to their data in addition to establishing privacy within the network.
5. Smart Contracts: It is known as an executable software module which is developed and installed into the blockchain itself and further enforced with the pre-defined rules so that it can ensure that the channel configuration module is able to create a unique access for authorized entities to have access to records through the channels.
6. Channel: It 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 have the capability of not only viewing but accessing records.
7. Nodes: They are known as the network components where local copies of the ledger are hosted and stored on the network of blockchain.

8. Ledger**:** They are known as the individual EHRs of patient's histories and data that are connected together and stored on blocks which can never be altered or removed.

The approach proposed by us in building our model is making use of blockchain technology as a solution to address the main challenge, data privacy, existing in EHR distribution. Firstly, the method is infeasible and it provokes very poor performance for data storage on the blockchain, so the blockchain will be employed as a tool for the purpose of granting access to requests from other users before they are allowed to have access to the channel so as to update or view data on the EHR server. To achieve the aim of true interoperability and data sharing with appropriate APIs, our proposed system can integrate the blockchain system with existing EHR platforms by employing its underlying technology. Composed of a distributed ledger and coded smart contracts, the underlying technology is able to ensure that all partakers in the distributed EHR sharing network are governed by policies related to access control specified in the smart contract of blockchain, which consequently allows only the authorized parties to see and update records with full permission and awareness of the patients. It is of vital importance to note that a distributed ledger, which is essentially a database without a central authority that can be shared across a network of multiple institutions, is regarded as the core of the blockchain. In addition, all the participants of this network have their own identical copy of the ledger stored locally. Moreover, only when the authorization of the patient is obtained can the ledger be updated, which accordingly ensures that the patient can be fully engaged in the data distribution and management. In addition, another contribution made by this process in the correlation of data is that only accurate data will be collected and stored into the database, which surely guarantees high-quality profiles from patients. Thus, before data is committed the patient has the freedom to go over and at any point may modify an incorrect piece of information that is collected from a profile before it is committed into the ledger. Moreover, our system adopts the usage of modern cryptographic mechanisms in the validation of records, which as a result leaves a trail of access behind every data accessed or updated and it further guarantees the trust in the environment of data distribution. Furthermore, any change to this ledger must be verified by all participants and authorized by the patient before it is committed into the ledger. However, these changes can be clearly reflected in all copies within a few minutes. Besides, both the security and accuracy of the ledger can be maintained through the keys of cryptographic signatures and the certificate authority, which is able to control the level of access to the shared ledger. [18], [19] In addition, all the other parties engaged in this network can receive roles and permissions-based access based on rules agreed provided by the network configuration in advance. Each terminology has already been explained by us to give an ample understanding to the fundamental operation of the network. Besides, a basic implementation of how our proposed model uses the blockchain is demonstrated for the purpose of supporting health data distribution and access in the process of maintaining privacy.

4.2.2. Model attributes

The design components of the blockchain enabling electronic health records in a model of patient centric access is composed of links and keys, as well as front-end development and verifications.

4.2.3. Links and keys

Hosting data directly on the blockchain can make it to be bloated, thus increasing its size very quickly. To avoid the occasion from happening, only access-links are stored on the blockchain. As a consequence, it also limits who can access health information, with the electronic health record shared only between relevant interested parties or entities by the employment of these access links. Then, these links are shared as embedded and encrypted links within transactions to the blockchain. The links can only be activated and accessible to users who have appropriate private keys to match the public key hash, which in such case is granted to patients' accounts when EHR is created. In fact, actual data that is associated with the EHR is

then secured on the EHR server and it is only accessible to the user when access request, which can be placed through the same EHR user-interface, is granted by the patient.

4.2.4. Front-end development

Once a blockchain is employed for the management of EHRs, it then becomes the unified and common backbone for digital health. By expanding the consequences of this development to the specialized backend systems in the future, the implication of adopting this backbone is that each hospital or care provider no longer has the demand for a specific version of databases or software to have access to patient data. As all the data is stored in a decentralized manner, no single entity is required to store a specific portion of the data. In addition, there is no longer a demand for specific backend protocols or tools, and all interested parties just need an underlying protocol for the access to the blockchain for the purpose of sharing the same backend. In addition, the access-protocol creates distinct roles of users (administrators, maintainers, and patients) and permission groups that are entitled to varying levels of privileges. The other advantage lies in the fact that the development cycle of health data software is simplified significantly, because now the only importance is attached to the front-end software that has access to the blockchain. Even though different parties have various levels of access, all user-roles and permissions are built into the front-end managed by the network configuration, which as a result can reduce the costs spent on maintenance and development in the future.

4.2.5. Verification

One of the most significant features of the blockchain is reflected on the demand for verification and consensus from the entire network, and in this case, especially from the interested parties on the network. The thorough verification further guarantees that no edits can be made without accountability and visibility to other parties, which is known as the patient in such case. Therefore, without the authorization of the patient, the execution of account or node read or write is unable to take place, which as a consequence makes it a very secure and highly confidential framework. As the verification itself is automated and very rapid, all the parties can approve any change in about several minutes. Accordingly, it can become even more relevant to health records, because any update or additional information becomes instantly available to other members engaged in the blockchain.

4.3. Security Module Work Flow

For the purpose that entities engaged in the process can communicate with each other smoothly, they must be connected, have the same network configuration and be discoverable on the network. Besides, they are on the same channel only when the patient accepts a request to grant them the access to reading or writing their records. However, in order to ensure that security of relevant parameters can be realized, only the patient has the right to authorize requests coming from different entities on the distributed network. It is of vital significance to note that related requests can only be executed once the patient accepts and authorizes access to EHR data. In addition, once relevant access is granted for modifying or viewing EHR, the ordering service then is required to check the blockchain to ensure that all the connected entities on the network are in consensus before updating the EHR data on the blockchain. Firstly, the ordering service should verify the policies related to network from the angle of network configuration and then check the logic of smart contract before progressing to commit data to the ledger on a network node. Once access is granted for the ordering service to commit data onto the ledger, it firstly conducts verification on whether the cryptographic key of the patient who granted access is authentic and then hashes the modified data together with the patient's private key before committing it to the ledger. After that, all the individual nodes on the network will be updated accordingly in the meanwhile. The key is verifying that every request made has appropriate authorization granted by the patient to reading or writing data on the ledger. It is verified

by the ordering service that the policy for updating and viewing EHR record is satisfied. The feature shown by order security of the ordering service is for the purpose of ensuring that at all times the nodes or entities on the network are in sync and they have the same information at any given time. The network is distributed like this and therefore there could be multiple updates from different entities which the ordering service indexes all request and thus they can be executed sequentially before committing data onto the ledger which has the EHR records. This further ensures that no duplication of data is available and the nodes are always in sync. In the case that the compromised node on the network where data updated is rejected and a request is sent back to appropriate user who is the patient for authorization, one clear feature of the system is that the state of the ledger at any given time on every node must be the same. This model ensures that integrity, authenticity and privacy of EHR data is ensured efficiently at all times.

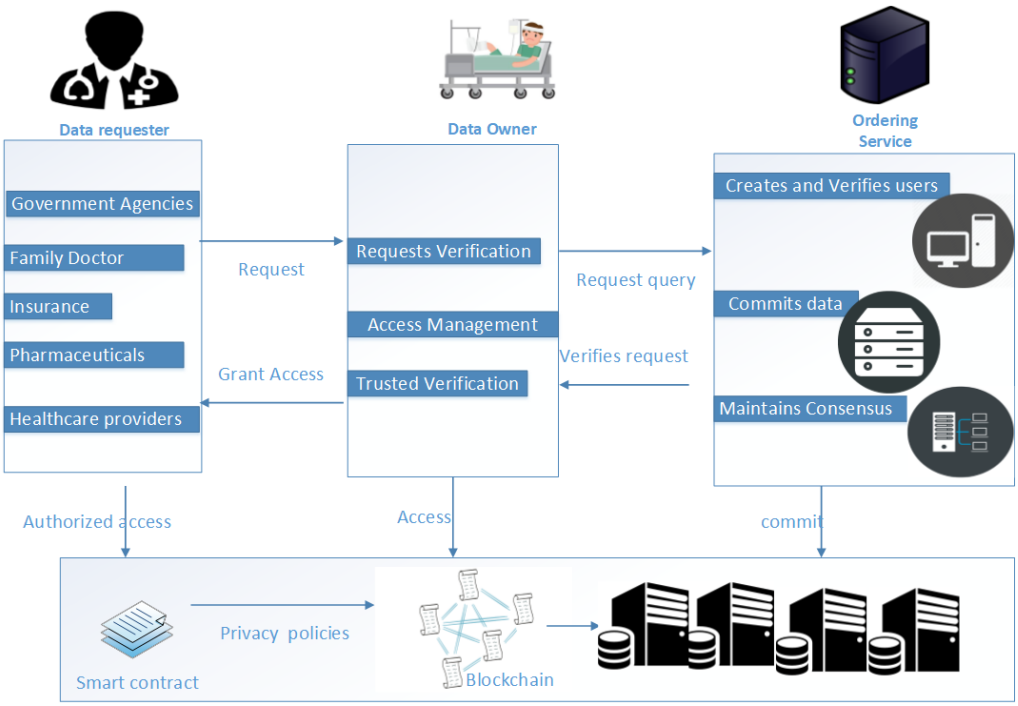

Fig. 5. Private data access control implementation.

4.4. Privacy Implementation

For the purpose of implementing this model, blockchain is known as the core of it. As what has already been mentioned in Section 2, multiple types of blockchains are available. However, for purpose of easing testing and further development, Hyperledger blockchain is employed in the process. With its own characteristics and block parameters, Hyperledger Fabric is deemed as a permissioned private blockchain that provides the capability of creating our own private blockchain for the purposes of studying and testing. As what has been stated above, the EHR of a patient can be accessed through a front-end client application, created by the hospital and employed within the network. After the EHR is created, a certificate authority is then issued to identify the patient on the blockchain network and then all administrative privileges will be automatically appended to the patient's account. Fig. 5 shows that the ordering is the administration point providing all the entities-controlled access to the network, and the hospital updates the network configuration to enable the patients to be the administrator of their records upon creation of EHR. After this point, both the patient and hospital possess equal rights over the network configuration on the network. Although the ordering service runs on the infrastructure of hospital, patient has shared administrative

rights over EHR records, as long as it has easy access to network. In such situation, even though the hospital runs the ordering service and the patient has full administrative rights over EHR, third parties have limited rights to have access to these records. After that, the hospital who is known as the network administrator is responsible for defining the 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 access policies or configuration of distribution are stored in the network configuration. As for the distribution configuration within the network configuration, it mainly defines the set of entities in the network which are willing to be a part of distribution in patients EHRs on the blockchain network with one another. With regards to this paper, it is regarded as the patient, pharmacy, 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 accordingly for a particular entity to have easy access to EHR records. Actually, the channel is known as a secure module for private communication created when a request by an entity within the network is granted by a patient for EHR to be accessed, which consequently creates the link of total privacy and exclusiveness to patient record through the distribution configuration. However, the access to EHRs is governed by channel configuration that is completely separated from the main network and it can be authorized by the patient only. All records are accessible on the ledger through the nodes, which is supervised by the ordering service. The smart contract is also available on the blockchain, and it is able to define all the common access patterns to the ledger [20]. Besides, smart contract gives a well-defined set of ways through which the ledger can be queried or updated on the node. For the purpose of easing the distribution, the ledger is what holds the EHRs data or hashed EHR data which points to the main data stored on respective EHR servers. In our experiment, API of our blockchain platform is able to communicate with the client application on each device on the network node for the aim of having access to the server where the EHR is stored.

5. 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 their EHRs through special means provided by our proposed 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 privacy security mechanism ensures that all participating entities are authorized to exchange and share patient's 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 channelling mechanism ensures that patients authorize entities within the distributed network to exclusively access this information. In the future we will work on blockchain integrated with machine learning issues in big data analysis.

Acknowledgment

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

References

[1] Iavrumov, V. A. (1953). Nabliudeniia nad izmenchivost'iu kishechnoi fekal'noi palochki. *Gig. Sanit.*, *9*, 52–53.

[2] Hailemichael, M. A., Marco-Ruiz, L., & Bellika, J. G. (2015). Privacy-preserving statistical query and processing on distributed openEHR data. *Stud. Health Technol. Inform.*, *210*, 766–770.

[3] Information, Y. H., & Rights, P. (1996). *Office Civil Rights for Your Health Information Privacy Rights* (pp. 1–2).
[4] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*.
[5] Kshetri, N. (2017, September). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecomm. Policy*, 1–12.
[6] Sherriff, A. (2016, June). *Blockchain Reaction*, 4–7.
[7] Standards, C. & Council, C. (2017). *Impact of Cloud Computing on Healthcare*.
[8] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst.*, *42(8)*.
[9] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *Proceedings of the 2016 2nd Int. Conf. Open Big Data, OBD 2016* (pp. 25–30).
[10] Masood, I., Wang, Y., Daud, A., Aljohani, N. R., & Dawood, H. (2018). Privacy management of patient physiological parameters. *Telemat. Informatics*, *35(4)*, 677–701.
[11] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018, August). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.*, *39*, 283–297.
[12] Ouagne, D., Hussain, S., Sadou, E., Jaulent, M. C., & Daniel, C. (2012). The electronic healthcare record for clinical research (EHR4CR) information model and terminology. *Stud. Health Technol. Inform.*, *80*, 534–538.
[13] Yachana, Kaur, N., & Sood, S. K. (2018). A trustworthy system for secure access to patient centric sensitive information. *Telemat. Informatics*, *35(4)*, 790–800.
[14] Madden, J. M., Lakoma, M. D., Rusinak, D., Lu, C. Y., & Soumerai, S. B. (2015). *Missing Clinical and Behavioral Health Data in a Large Electronic Health Record (EHR) System*.
[15] Hew-Hei, C., & Ismail, A. (2017, Dec.). Indicators for medical mistrust in healthcare – A review and standpoint from Southeast Asia. *Malaysian J. Med. Sci.*, *24(6)*, 5–20.
[16] Harman, L. B. (2001, Sep.). Ethical challenges in the management of health information. *J. Healthc. Qual.*, *23(5)*, 49.
[17] The IBM Advantage for Implementing the CSCC Cloud Customer Reference Architecture for Blockchain. (2017). Gartner Magic Quadrant Report. Retrieved from https://docplayer.net/81070877-The-ibm-advantage-for-implementing-the-cscc-cloud-customer-reference-architecture-for-blockchain.html
[18] Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology). *Journal of Financial Perspectives, 3(3)*.
[19] UK Government Chief Scientific Adviser. (2016). *Distributed Ledger Technology : Beyond Block Chain*.
[20] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303.

Li Yue received the B.Sc. degree in information technology and Ph.D. degrees in telecommunication engineering in 2005 and 2010, respectively, from University of Limerick, Ireland. He obtained the CISSP certificate in 2016. He is currently a lecturer in School of Computer Science and Technology, Donghua University, Shanghai, China. His current research includes privacy protection in blockchain and key agreement protocol for Internet of things.

Richard Nuetey Nortey is currently into research studies in machine and deep learning and the blockchain technology at Donghua University China (Shanghai). He received his bachelor's degree in information technology form the Methodist University, Ghana in 2013 and has 5 years of information security experience at telecom and digital certificate companies. He worked with United Nations Development Programme (UNDP) Ghana Technical Team two years and was part of the team to first develop the United Nations Country Team (UNCT) web database for project monitoring for all 20 UN agencies in Ghana which was launched in October 2013. His research interests include consensus protocols for distributed systems, blockchains, machine learning, big data and transactive energy systems.

Michael Adjeisah received his bachelor degree in 2011 and MSc in 2016. He is currently working toward the PhD degree at the School of Computer Science and Technology, Donghua University, Shanghai, China. His current and previous research interests include human computer interaction mainly somatosensory interaction system and human activity recognition, computer vision and machine learning. He is also interested in blockchain technology.

Promise Ricardo Agbedanu received his BSc degree in information and communications technology (2014) from the Presbyterian University College, Ghana and MPhil degree in information technology (2018) from the Kwame Nkrumah University of Science and Technology, Ghana. He is currently a master's student studying computer science and technology at Donghua University in Shanghai, China. His current research interests include computer security, network security and cloud security. He is also interested in using machine and deep learning to solve cyber-security problems.

Xinyi Lui is currently into research studies in computer science technology at Donghua University China (Shanghai). She received her bachelor's degree in information security from Donghua University China (Shanghai). Her research interests include big data, blockchains and machine learning.