A Novel Architecture for Tamper Proof Electronic Health Record Management System using Blockchain Wrapper

Mohammad Saidur Rahman
School of Science, RMIT University, Australia
Melbourne, Victoria
mohammadsaidur.rahman@rmit.edu.au

Ibrahim Khalil
School of Science, RMIT University, Australia
Melbourne, Victoria
ibrahim.khalil@rmit.edu.au

Pathum Chamikara Mahawaga Arachchige
School of Science, RMIT University, Australia
Melbourne, Victoria
pathumchamikara.mahawagaarachchige@rmit.edu.au

Abdelaziz Bouras
Qatar University
Qatar
abdelaziz.bouras@qu.edu.qa

Xun Yi
School of Science, RMIT University, Australia
Melbourne, Victoria
xun.yi@rmit.edu.au

ABSTRACT

In this paper, we present a novel architecture of blockchain-based tamper-proof electronic health record (EHR) management system. Recording electronic health data in cloud-based storage systems always pose a threat to information security. Intruders can delete or tamper EHR of patients, giving benefits to insurance companies or hiding medical malpractices (e.g. misdiagnosis and delayed diagnosis). A tamper-proof EHR management system is required that would essentially solve such issues. The blockchain is an emerging technology that can be adapted to develop a tamper-proof data management system. However, establishing a new blockchain based system replacing the existing system is expensive. In our proposed architecture, we introduce a wrapper layer integration mechanism, named as the blockchain handshaker, between the existing cloud-based EHR management system and public blockchain network to develop a tamper-proof health record management system. We implement a prototype to provide evidence on the feasibility of the proposed concept.

CCS CONCEPTS

• **Security and privacy → Systems security**; • **Computer systems organization → Distributed architectures**.

KEYWORDS

blockchain in healthcare, blockchain wrapper, tamper-proof record management, secured health record

ACM Reference Format:
Mohammad Saidur Rahman, Ibrahim Khalil, Pathum Chamikara Mahawaga Arachchige, Abdelaziz Bouras, and Xun Yi. 2019. A Novel Architecture for Tamper Proof Electronic Health Record Management System using Blockchain Wrapper. In *2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '19), July 8, 2019, Auckland, New Zealand.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3327960.3332392

1 INTRODUCTION

Implementation of Electronic Medical Record (EMR) Systems is considered to be a critical role in improving healthcare intelligence, quality, user experience and related costs. EMR system could eventually save more than billions of dollars annually [10]. Sharing of healthcare data will help to accommodate smarter, better understanding of patterns and trends in public health and diseases to ensure; better quality services [9], better recommendations for doctors [26], and plan services that make the best of limited national health service budgets for the health and wellbeing. For ease of discussion, we use healthcare data to represent patient data, and healthcare data systems to denote any system that generates, access and/or store patient data.

Cloud computing environments provide an excellent opportunity to accommodate e-Health services in different scenarios in effectively. The cloud-based environment can offer numerousbenefits by its scalability and mobility [6, 11, 14], but there are barriers that must be managed [3, 17]. A cloud-based Electronic Health Record (EHR) management system can provide two main advantages: 1) the ability to share patient records with other clinical centers, and 2) the integration of all the EHRs of a group of clinical centers in order to help medical staff perform their jobs efficiently [7, 8].

In spite of having several benefits of cloud-based EHR management systems, security is a critical concern. EHR in cloud-based management systems can be exposed to abuse, leakage, loss or theft [24]. For example, EHRs can be deleted or tampered by intruders to tamper treatments giving benefits to insurance companies or hiding medical malpractices (e.g. misdiagnosis and delayed diagnosis). EHRs are closely related to health insurances. Dishonest health

BSCI '19, July 8, 2019, Auckland, New Zealand

ACM ISBN 978-1-4503-6786-8/19/07…$15.00
https://doi.org/10.1145/3327960.3332392

insurance service providers may hire hackers to delete or tamper EHRs of patients to prove the existence of pre-existing health conditions. Medical malpractices such as misdiagnosis and delayed diagnosis, are few of the key reasons for medical insurance claims. In most cases, patients cannot prove the medical malpractices due to these issues. On the other hand, patients modify medical records to get financial advantages in spite of having some pre-existing medical conditions. Several countermeasures are proposed to provide security of EHRs using cryptographic techniques [1, 16, 22, 28]. Unfortunately, security threats still remain due to the centralized characteristics of cloud-based systems. Security risks on cloud-based healthcare system is presented in Figure 1.

Generally, a healthcare blockchain is treated as a distributed ledger to store health records for sharing, exchanging or other purposes among stakeholders [12]. In e-Health systems, data can be generated from different sources such as clinics, hospitals, and pathologies. In a blockchain-based EHR management system, all the data related to patients are stored in the distributed ledger offered by a blockchain network. The process of storing a set of related data is known as a transaction. Each transaction is evaluated by a group of participants, known as miners, before being stored in the distributed ledger. Blockchain networks are capable of rejecting an unauthorized transaction which try to modify the data in the distributed ledger. As a result, no unauthorized person can modify the data in a blockchain network. A key concept of blockchain, smart contract, empowers trustless features among different entities in the EHR management system. A smart contract involves a computer program that contains a set of agreements and principles. All of the participants in the network must follow the set of agreements and principles. Hence, no trusted third party is required to store data in the blockchain [19].

We identify two challenges for adopting blockchain in cloud-based EHR. *First*, the blockchain adoption should eliminate the control on data repository from a central authority. In other words, the data should be decartelized as much as possible. As a result, tampering data becomes difficult in the blockchain network. Therefore, it is important to choose appropriate blockchain network for the EHR management systems. *Second*, blockchain technology has a different platform other than traditional systems. Therefore, developing a blockchain-based system require a design from the scratch.

Designing a system from the scratch is time consuming, expensive and affects the existing stakeholders. As a summary, we try to answer the following questions related to designing blockchain-based EHR management systems:

(1) How to integrate blockchain network with the traditional cloud-based EHR management system such that current stakeholders are not affected?
(2) How to choose blockchain network so that the control on the data is fully decentralized?

In this paper, we propose blockchain-based system architecture to develop a tamper-proof EHR management system. There are three types of blockchain platforms exist so far [5]: public blockchain, consortium blockchain and private blockchain. In public blockchain, anyone can join in the consensus process. Hence, a particular organization joining the public blockchain has no control on the consensus tasks, i.e. the control is decentralized. Example of a public blockchain is Bitcoin. Contrarily, only a group of pre-selected nodes can perform the consensus tasks in the consortium blockchain. Giving an example of the consortium blockchain, each of a group of organizations building a blockchain network nominates one or multiple nodes as consensus nodes. In the private blockchain, only authorized nodes of an organization are capable of performing consensus tasks. Thus, all of the nodes that are responsible for consensus can be controlled by the organization. In order to build a tamper-proof EHR system we choose public blockchain network as our blockchain in this paper. Integrating the blockchain network to the traditional cloud-based EHR systems is a design challenge. A suitable design methodology needs to be selected that allows blockchain technology to be integrated and current stakeholders are not affected as well. In our system design, we would like to use bottom-up approach for integrating blockchain to the cloud-based EHR managements systems. We develop a prototype of blockchain based EHR management system using Ethereum [18], a public blockchain network, for showing the feasibility of blockchain integration to the traditional cloud-based EHR management systems. The main contributions of our work are as follows:

(1) A tamper-proof cloud-based EHR management system is proposed using blockchain technology.
(2) A novel architecture is proposed for integrating blockchain to an existing cloud-based EHR management systems.
(3) Introduces the concept of *blockchain handshaker* that works as a blockchain wrapper for supporting blockchain integration.
(4) The functionality of each component in the proposed architecture is discussed.
(5) A prototype is developed using Ethereum public blockchain to show the feasibility of blockchain integration to an existing cloud-based EHR management systems.

The rest of the paper is organized as follows. Section 2 presents an overview on blockchain technology and a summary of related work. Some preliminaries concepts are introduced in Section 3. Our proposed system architecture is described in Section 4. Section 5 presents the system workflow. An implementation of the system prototype is demonstrated in Section 6. Finally, Section 7 concludes the paper with some future directions.

2 RESEARCH BACKGROUND

2.1 Blockchain

A blockchain is a data structure which is composed of a collection of entities named blocks which are chronologically chained by a hash. Bitcoin (BC) is an example of a frequently buzzed platform which is based on the blockchain technologies. We consider the concepts used in a public BC architecture with publicly maintained nodes that allow anyone to join or quit the decision of creating a new block at any time. On the other hand, a permissioned blockchain would allow new block creation upon the decision of some trusted notes. Permissioned blockchains have applications in areas such as copyright management, authentication, and data storage services.

Both public (e.g. Bitcoin and Ethereum) and permissioned blockchains (e.g. Hyperledger) use consensus mechanisms to create

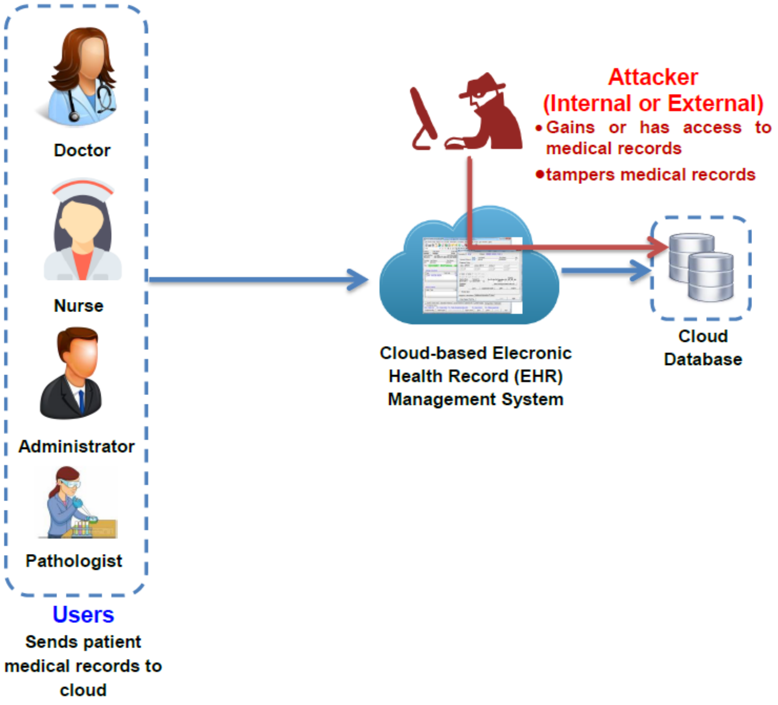

Doctor
Nurse
Administrator
Pathologist
Users
Sends patient medical records to cloud
Attacker
(Internal or External)
•Gains or has access to medical records
•tampers medical records
Cloud-based Elecronic Health Record (EHR) Management System
Cloud Database

Figure 1: Security Risks in Traditional Cloud-based Electronic Medical Record Management Systems.

a new block. A consensus mechanism involves an essential step of selecting/electing a minor to create a new block. Public blockchains conduct proof of work (PoW), proof of stake (PoS) and delegated proof of stake (DPoS) as the typical consensus mechanisms. Typical consensus mechanisms in permissioned blockchains include byzantine fault tolerance algorithm (PBFT).

We chose a public blockchain for our design which uses the PoW consensus mechanism as it is the widest deployed consensus mechanism in the existing blockchain technologies.

2.1.1 Proof of Work (PoW) Consensus Mechanism. PoW was introduced by the Bitcoin blockchain technology. PoW assumes that each peer uses computing power to solve the proof of work instances and construct the appropriate blocks for voting. Bitcoin uses a hash-based PoW which involves finding a nonce value. The value of the has to be smaller than the current target value when hashed with additional block parameters such as Merkle has and the previous block hash. After generating the nonce, a miner creates the block and forwards it to the peers of the network so that they can verify the PoW by computing the hash of the block and checking whether it satisfies the condition to be smaller than the current target value.

2.1.2 Smart Contracts. The business logic of a blockchain exists on a concept called a smart contract. Smart contracts are responsible for reading and writing data to the blockchain, as well as executing the business logic. Conventionally, smart contracts are written using a language called Solidity. We develop the decentralized portion of our app on a smart contract written using solidity. Solidity is a full-blown programming language that behaves like JavaScript. A smart contract is given its name as it represents an agreement that needs to be maintained within the blockchain system.

2.2 Blockchain in Healthcare

In this section, we discuss the latest research work on blockchain-based approaches in healthcare. Zhang et al. present a blockchain-based secure and privacy-preserving PHI sharing (BSPP) scheme for diagnosis improvements in e-Health systems [24]. Two kinds of blockchains, private and consortium, are constructed by devising their data structures, and consensus mechanisms. A private blockchain is responsible for storing the PHI while the consortium blockchain keeps records of the secure indexes of the PHI. To achieve data security, access control, privacy preservation, and secure search, all the data including the PHI, keywords and the patient identity are public key encrypted with a keyword search. Furthermore, the block generators are required to provide proof of conformance for adding new blocks to the blockchains, which guarantees the system availability.

The work in [21] proposes a blockchain-based health data sharing framework that sufficiently addresses the access control challenges associated with sensitive data stored in the cloud. The system is based on a permissioned blockchain which allows access to only invited, and hence verified users. Furthermore, in order to provide data provenance, auditing and secured data trailing on medical data, the authors employ smart contracts and an access control mechanism in their another work [20]. It effectively tracks the behavior of the data and revoke access to offending entities on detection of violation of permissions on data.

Yue et al. in [23] also propose a three-layered system: data usage layer, data management layer, and data storage layer. The cloud in this work is a storage infrastructure which is different from the aforementioned works. This work proposes that the private blockchain plays the role of the cloud. In [29], transactions are used to carry instructions, such as storing, querying and sharing data. The authors combine blockchain and off-blockchain storages to construct a personal data management platform focused on privacy. The work in [12] reviews the latest biomedical/health care applications of blockchain technologies. The work further discusses the potential challenges and proposes solutions of adopting blockchain technologies in biomedical/healthcare domains.

Authors in [4] constructed a smart contract to hold metadata about the record ownership, permissions, and data integrity. The contract's state-transition functions carry out the policies which enforce the data alternations only to legitimate transactions. Addresses of sensors and mobile devices are added to a healthcare blockchain for pervasive social network (PSN) nodes in [25] rather than storing the health records in the blocks. A PSN node can visit other nodes in the network and access the health data through the addresses stored in the blockchain. This work has the merit of reducing the storage overhead of devices while it did not consider the security of the addresses.

A Merkle tree-based structure is used for blocks in [13] which is similar to the Bitcoin approach. The leaf nodes represent patient record transactions and describe the addition of a resource to the official patient record. They referred Fast Healthcare Interoperability Resources (FHIR) via Uniform Resource Locators (URLs) instead of including the actual record document. A new consensus algorithm, proof of interoperability, is designed to facilitate data interoperability in this work.

The work in [15] proposes a blockchain architecture for clinical trials and precision medicine. This work investigates the suitability of the blockchain technologies particularly for the clinical trials and precision medicine. A key negotiation for key management schemes for blockchain is developed in [27]. It uses body sensor networks to design a lightweight backup and efficient recovery scheme for keys of health blockchain. This is a pioneering work in key management for blockchains while the hardware performance and environment greatly influence its performance.

Authors in [2] presents a patient-centric healthcare data management system by using blockchain as storage to enforce privacy. This work uses cryptographic functions to protect the patient data to ensure *pseudonymity.*

The existing works provide miscellaneous frameworks for healthcare data sharing in e-Health systems with blockchain. They take a blockchain as an assisted tool for data sharing instead of taking it as the main tool for data storage, data management, and data sharing. Furthermore, the works mentioned above do not discuss integrating blockchain to an existing healthcare system. We present a novel architecture for the integration of blockchain to the existing healthcare systems.

3 PRELIMINARIES

In this section, we discuss some of the key concepts that are used in our proposed architecture. Concepts include key setup, smart contract,transactions and transaction template.

3.1 Key setup

Assume that there are m users in our system. The set U of users can be denoted as, $U = \{u_1, u_2, \ldots, u_m\}$. In our system, we consider a human (e.g. doctors, nurse, etc.) or software component (e.g. cloud) as a user for the sake of simplicity. Each user generates a *public key-pair* containing a *public-key* and *private-key* using a secure public key cryptography algorithm (e.g. ElGamal). The public key-pair of a user u_i is denoted as (K_i^+, K_i^-) where K_i^+ is the public-key and K_i^+ is the private-key of u_i. K_i^- is kept secret by the user u_i, and K_i^+ is shared among all of the participants in the system using a key distribution center. Hence, the set K^+ of public-keys of m users in the system can be denoted as $K^+ = \{K_1^+, K_2^+, \ldots, K_m^+\}$. A secret-key $SK_{j,k}$ is established between two user, u_j and u_k, using a secure symmetric key encryption algorithm (e.g. Advanced Encryption Standard or AES). The key is established prior to any communication using a key distribution mechanism such as Diffie-Hellman key exchange mechanism. The secret-key $SK_{j,k}$ is only known to users u_j and u_k. Both of the public key-pair and secret keys are required during generations of transactions for security and authenticity of transaction. In our system, we mainly use three types of secret-keys: $SK_{user,BH}$, $SK_{BH,BC}$ and $SK_{BH,C}$. The $SK_{user,BH}$ is the secret-key between user and blockchain handshaker, $SK_{BH,BC}$ is the secret-key between blockchain handshaker and blockchain network, and $SK_{BH,C}$ is the secret-key between blockchain handshaker and cloud. Concepts of blockchain handshaker and cloud are discussed in later Section.

3.2 Smart Contract

In our system, smart contract is a set of instructions that validates data of one or more attributes value based on predefined conditions related to patient health condition. There can be single or multiple smart contracts in our system. The smart contract is created by a system administrator who decides which attributes of a patient health records need to be verified. Assume that there are t attributes in a complete patient health record. Among them, only r attributes (here, $r \leq t$) need to be verified. Then a smart contract should be created that receives r attributes as a transaction and validated. The set SC of smart contracts can be denoted as $SC = \{sc_1, sc_2, \ldots, sc_w\}$, where w is the number of smart contracts.

3.3 Transactions

In this system, a transaction is a set of attributes related to patient health records and sender's information encrypted with secret-key between sender u_j and receiver u_k. The main usage of a transaction is carrying patient health data. There are three types of transactions in our system as descried below:

3.3.1 Initial Transaction (T_I).

This transaction is generated by a user (e.g. doctors) for sending patient health record to blockchain handshaker for further processing such as validation by blockchain

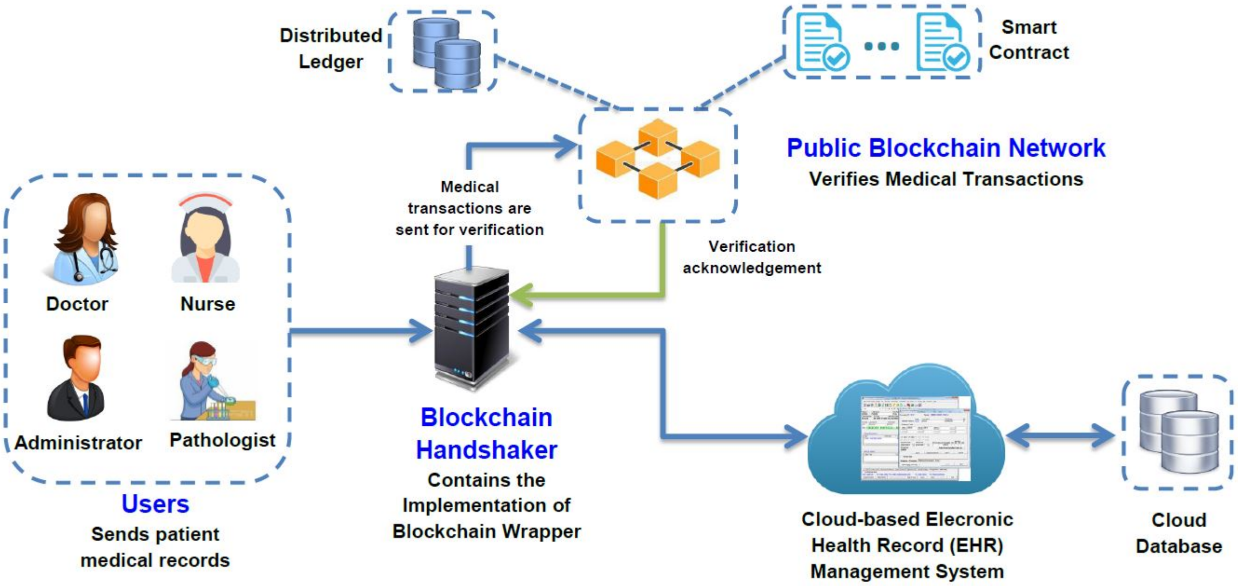

Distributed Ledger
Smart Contract
Public Blockchain Network
Verifies Medical Transactions
Medical transactions are sent for verification
Verification acknowledgement
Doctor
Nurse
Administrator
Pathologist
Users
Sends patient medical records
Blockchain Handshaker
Contains the Implementation of Blockchain Wrapper
Cloud-based Elecronic Health Record (EHR) Management System
Cloud Database

Figure 2: Proposed System Architecture of Blockchain-based Electronic Health Record Management Systems.

network. The initial transaction (T_I) can be represented as a tuple:

$$T_I = \mathcal{E}nc([tid, uid, pid, \mathcal{S}ign(\{a_1, a_2, \dots, a_t\}, K_i^-)], SK_{user,BH}),$$

where:

- tid is transaction ID.
- uid is user ID.
- pid is patient ID.
- $\mathcal{S}ign(\{a_1, a_2, \dots, a_t\}, K_i^-)$ is a signed message containing attributes in the set $A = \{a_1, a_2, \dots, a_t\}$ of t attributes related to patient health record. The signing is done by user's private-key K_i^-.
- $\mathcal{E}nc([tid, uid, pid, \mathcal{S}ign(\{a_1, a_2, \dots, a_t\}, K_i^-)], SK_{user,BH})$ is the encrypted transaction using secret key $SK_{user,BH}$.

3.3.2 Blockchain Transaction (T_C). This transaction is generated by blockchain handshakerfor sending patient health record to the blockchain network for validation and storing in the distributed ledger or blockchain. A blockchain transaction (T_C) can be represented as a tuple:

$$T_C = \mathcal{E}nc([tid, uid, pid, \mathcal{S}ign(\{a_1^{'}, a_2^{'}, \dots, a_r^{'}\}, K_{BH}^-)], SK_{BH,BC}),$$

where:

- tid is transaction ID.
- uid is user ID.
- pid is patient ID.
- $\mathcal{S}ign(\{a_1^{'}, a_2^{'}, \dots, a_r^{'}\}, K_{BH}^-)$ is signed attributes in the set $A^{'} = \{a_1^{'}, a_2^{'}, \dots, a_r^{'}\}(A^{'} \subseteq A)$ of r attributes related to patient health record that are required for validation. The signing is done by blockchain handshaker's private-key $K_B^- H$.
- $\mathcal{E}nc([tid, uid, pid, \mathcal{S}ign(\{a_1^{'}, a_2^{'}, \dots, a_r^{'}\}, K_{BH}^-)], SK_{BH,BC})$ is the encrypted transaction using secret key $SK_{BH,BC}$.

3.3.3 Validated transaction ($T_I^{'}$). This transaction is generated by blockchain network for blockchain handshaker as a result of validation. A blockchain transaction (T_C) can be represented as a tuple:

$$T_I^{'} = \mathcal{E}nc([T_I, ACK], SK_{BH,C}),$$

where:

- T_I is the initial transaction.
- ACK is validation status sent by blockchain network.
- $Enc([T_I, ACK], SK_{BH,C})$ is the encrypted transaction using secret key $SK_{BH,C}$.

3.4 Transaction Template

The transaction template is a formal specification for generating a blockchain transaction. In our system, the transaction template is generated by system administrator according to the transaction format of public blockchain network.

4 PROPOSED SYSTEM ARCHITECTURE

In this section, we discuss our proposed architecture based on blockchain for a tamper-proof cloud-based EHR management system. The architecture is depicted in Figure 2. There are four key components in our proposed architecture: *user application*, *blockchain handshaker*, *cloud*, and *public blockchain network*. Each component is explained as follows:

4.1 User Application

User application is a software module that provides two functionalities. Firstly, it provides application interfaces for users. In our system, there are several types of users such as doctors, nurses, system administrators, pathologists, etc. Each type of user has different role. Hence, the user application provides specific user interfaces based on a user role. Secondly, user application builds an initial transaction(T_I) based on data inserted by a user (e.g. patient blood pressure) and some system generated data (e.g. timestamp). T_I is sent to blockchain handshaker for verification purposes. In summary, user application establishes a link between users and blockchain handshaker.

4.2 Blockchain Handshaker

Blockchain handshaker (*BH*) is the key component of our proposed architecture. This component acts as a wrapper component that connects user application, cloud-based EHR system and public blockchain network in our proposed architecture. *BH* has three sub-components, namely transaction template manager (*TTM*), transaction generator (*TG*), and transaction validator (*TV*). The internal architecture of *BH* is illustrated in Figure 3. Description of each component of *BH* is described below:

- *Transaction template manager (TTM)*: contains a set of predefined transaction templates for blockchain network. Transaction templates are generated by the system administrator following specifications of the blockchain network platform and set of attributes in corresponding smart contracts.
- *Transaction generator (TG)*: builds a blockchain transaction (T_C) from an initial transaction (T_I) following one of the templates in *TTM*. *TG* does the mapping between T_I and a suitable template in *TTM*.
- *Transaction validator (TV)*: is the core component of *BH* that controls the overall interactions among international blocks of *BH* and handshaking user applications, blockchain network and cloud. *TV* receives an initial transaction T_I from user application, sends it to *TG* and waits for receiving a blockchain transaction *TC* from *TG*. Upon receiving a *TC*, *TV* sends it to blockchain network for validation.The blockchain network returns validated transaction $T_I^{'}$. If the validation is **true**, *ACK* is sent as **valid transaction** to the cloud for storing in cloud database. Otherwise, *ACK* is sent as **invalid transaction** and stored for future audit tasks.

4.3 Public Blockchain Network

We use a public blockchain network (e.g. Ethereum) in our proposed architecture. The public blockchain network comprises blockchain nodes, distributed ledger and smart contracts. Blockchain nodes are in fact miners that are responsible for maintaining blockchain according to the consensus mechanism. In other words, blockchain nodes receives transactions and validate based on smart contracts. If a transaction is found as valid, data are converted to blocks and added in the distributed ledger. Public blockchain network sends an acknowledgement as **true** or **false** to the transaction validator (*TV*) of the blockchain handshaker.

4.4 Cloud

The cloud provides two services in our proposed architecture that are similar to the traditional cloud-based EHR management system. The first service includes hosting the EHR management system. The second service is the storage service. The cloud provides a database for storing all health records. EHR management system receives transactions $T_I^{'}$ from *BH*, performs all tasks related to it and stores transaction data in the cloud database. The cloud responds with appropriate data in response to access requests from users.

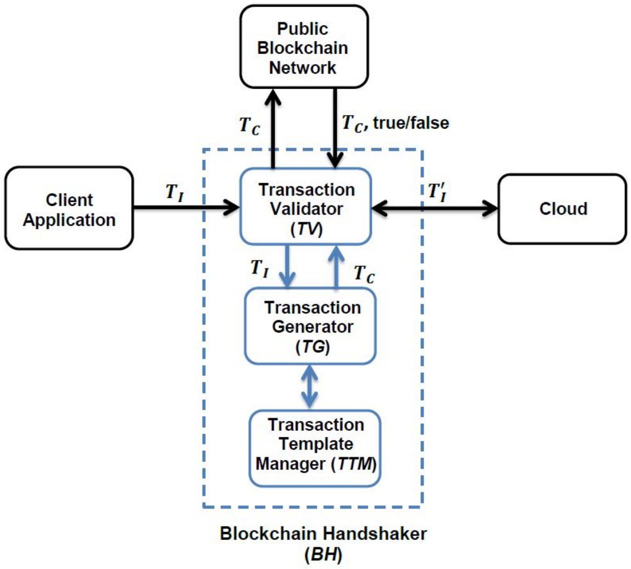

Public Blockchain Network
T_C
T_C, true/false
Client Application
T_I
Transaction Validator (TV)
T_I'
Cloud
T_I
T_C
Transaction Generator (TG)
Transaction Template Manager (TTM)
Blockchain Handshaker (BH)

Figure 3: Internal Architecture of Blockchain Handshaker (*BH*).

5 SYSTEM WORKFLOW

In this section, we discuss the system workflow of our blockchain and cloud-based EHR management system. Figure 4 shows an overview how the system components interact with each other. Initially, user application sends an initial transaction (T_I) that contains patient health data inserted by a user. Next, T_I is sent to Blockchain Handshaker (*BH*) for communicating with public blockchain network. *BH* generates a blockchain transaction (T_C) using its internal components transaction generator (*TG*) and transaction template manager (*TTM*). Another component of *BH*, transaction validator (*TV*), sends T_C to public blockchain network for validation. Further, the public blockchain network validates transaction using smart contracts and mines to add transaction data into the blockchain. Public blockchain network sends a validation acknowledgement to *BH* at the end of validation. *BH* sends the validated transaction $T_I^{'}$ to the cloud for further processing. Finally, the cloud stores data in the cloud database at the end of processing.

According to our proposed architecture, each and every record related to patient health is passed to Blockchain Handshaker (*BH*) first for validation. One or multiple smart contracts are created and distributed among public blockchain nodes. Whenever a transaction is sent to the public blockchain network, transactions are validated against smart contracts anonymously. At the end of validation, data of the transaction is stored in the blockchain or distributed ledger. As the blockchain nodes are anonymous, none of them can be compromised. Proof-of-Work (PoW) consensus mechanism ensures secure mining of blocks. Hence, our proposed system architecture ensures tamper-proof data ledger. Moreover, transactions are stored in cloud database as per validation of public blockchain network.

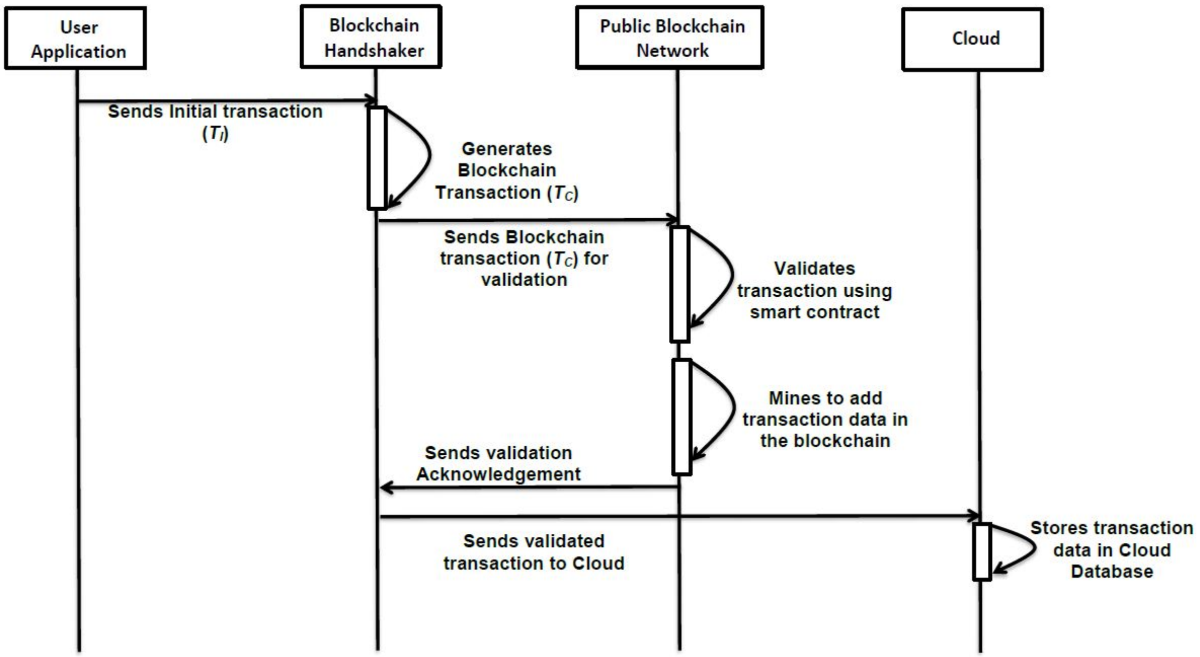

User Application
Blockchain Handshaker
Public Blockchain Network
Cloud
Sends Initial transaction (T_I)
Generates Blockchain Transaction (T_C)
Sends Blockchain transaction (T_C) for validation
Validates transaction using smart contract
Mines to add transaction data in the blockchain
Sends validation Acknowledgement
Sends validated transaction to Cloud
Stores transaction data in Cloud Database

Figure 4: Communication Among Components of Proposed Blockchain and Cloud-based EHR Management Systems.

The usage of *ACK* along with transaction data ensures which transaction are faulty and which are not. From there, data modification can be tracked and traced. Therefore, data accountability is ensured. As the system ensures tamper-proof data storage and accountability, it can be said as immutable system.

6 IMPLEMENTATION

In this section, we present an overview of the implementation of our proposed architecture using a case scenario. We discuss the scenario first. Later, we demonstrate the implementation.

6.1 Case Scenario

We consider a system, named as **MediBlock**, where healthcare staffs store patient health condition as comments after performing patient health assessment. Whenever a patient arrives, a new patient profile is created. Next, a thorough assessment is performed based on a pre-defined set of questionnaire. An assigned healthcare staff (e.g. a doctor) enters all of the patient health conditions as comments. Comments are sent to Blockchain Handshaker (*BH*). *BH* converts comments into blockchain transaction (T_C) and sends it to public blockchain network for validation. The comments are added as blocks in the blockchain. Once comments are added in the blockchain, they are sent to cloud-based system for further processing.

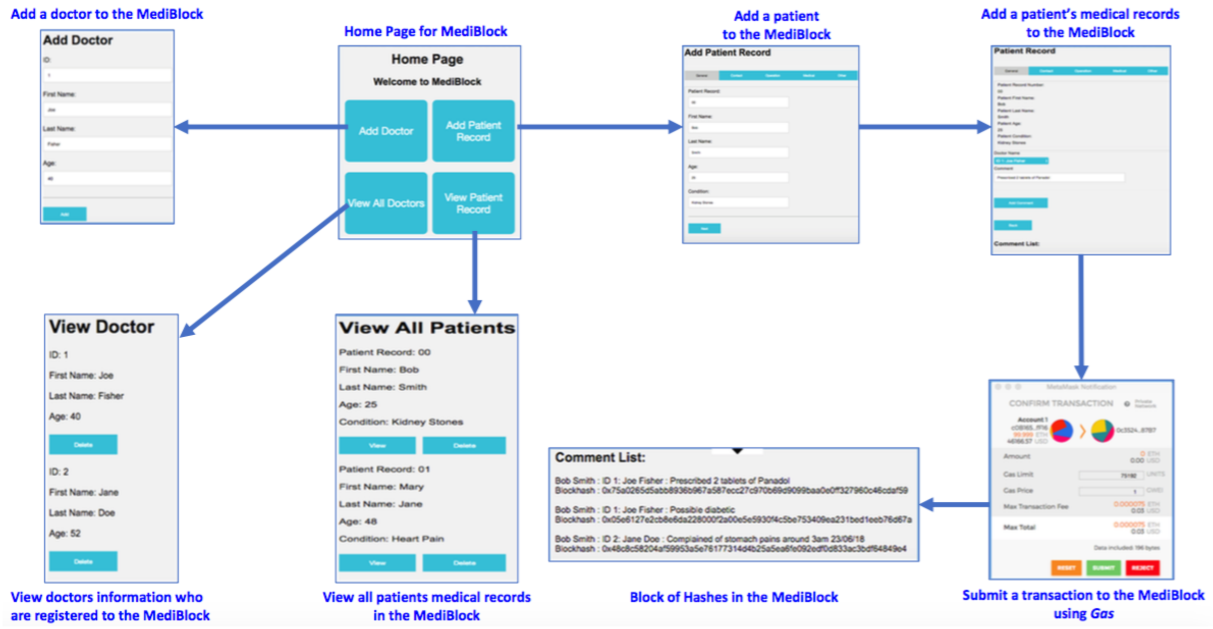
6.2 Implementation Details

Our prototype consists of three parts: client application, blockchain handshaker and cloud-based EHR management system. We use *Ethereum* as the public blockchain platform. We use a local version of Ethereum blockchain, called *Ganache*, in place of live blockchain. We use Ubuntu 16.04 for configuring Ganache. *NodeJS* is used to develop our blockchain wrapper, i.e. Blockchain Handshaker (*BH*). In order to interact with *BH* and Ganache, we use **web3js** which is a collection of libraries to interact with Ganache. The web3js uses a HTTP or IPC connection to communicate with Ganache. We have written our smart contracts using **solidity** that designed to support Ethereum platform. The Solidity is a JavaScript like programming language. Smart contracts are written and compiled using **Remix** which is an online text editor for Solidity. is used to write and compile codesfor smart contract. For simulating the Ethereumnetwork, we use **Metamask** which is a Google Chrome extension that should be enabled in the client system to communicate with Ethereum platform.

We develop client application using HTML5 and JavaScript. The cloud-based EHR management system is developed using Java and hosted in Amazon EC2. We have used Amazon Relational Database Service (Amazon RDS) for MySQL as our cloud database. An overall workflow of our developed prototype is presented in Figure 5.

7 CONCLUSIONS AND FUTURE WORK

We proposed a novel approach of tamperproof electronic medical record management using public blockchain technology. Compared to existing approaches, our method provides a more feasible mechanism that employs an abstraction service layer which we named as "blockchain handshaker". The existing approaches try to provide solutions based on blockchains from scratch, which can be infeasible and expensive as such procedures need drastic changes to the existing systems. We avoid such complexities by introducing independence between business logic and blockchain technologies.



View Doctor

ID: 1
First Name: Joe
Last Name: Fisher
Age: 40

ID: 2
First Name: Jane
Last Name: Doe
Age: 52

View All Patients

Patient Record: 00
First Name: Bob
Last Name: Smith
Age: 25
Condition: Kidney Stones

Patient Record: 01
First Name: Mary
Last Name: Jane
Age: 48
Condition: Heart Pain

Comment List:

Bob Smith : ID 1: Joe Fisher : Prescribed 2 tablets of Panadol
Blockhash : 0x75a0265d5abb8936b967a587ecc27c970b69d9099baa0e0ff327960c46cdaf59

Bob Smith : ID 1: Joe Fisher : Possible diabetic
Blockhash : 0x05e6127e2cb8e6da228000f2a00e5e5930f4c5be753409ea231bed1eeb76d67a

Bob Smith : ID 2: Jane Doe : Complained of stomach pains around 3am 23/06/18
Blockhash : 0x48c8c58204af59953a5e76177314d4b25a5ea6fe092edf0d833ac3bdf64849e4

Figure 5: Overview of the Developed Prototype using Ethereum Blockchain.

Our study confirms the effectiveness of the proposed approach towards tamperproof electronic health record management. Hence, the proposed mechanism allows an existing organization to utilize the capabilities of a public blockchain technology for protecting from modification the transactions of the current data management system with reduced complexity and increased efficiency and reliability.

The proposed work leads to many reach avenues for future work. Specifically, we would like to look at the possibility of using artificial intelligence to generate dynamic smart-contracts using the handshaker to address cross-domain diversities. Another research avenue is to compare the proposed method against existing from scratch approaches.

REFERENCES

[1] Assad Abbas and Samee U Khan. 2014. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics* 18, 4 (2014), 1431–1441.
[2] Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. 2017. Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 534–543.
[3] Nicholas R Anderson, E Sally Lee, J Scott Brockenbrough, Mark E Minie, Sherrilynne Fuller, James Brinkley, and Peter Tarczy-Hornoch. 2007. Issues in biomedical research data management and analysis: needs and barriers. *Journal of the American Medical Informatics Association* 14, 4 (2007), 478–488.
[4] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 25–30.
[5] Vitalik Buterin. 2015. On public and private blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
[6] Yu-Yi Chen, Jun-Chao Lu, and Jinn-Ke Jan. 2012. A secure EHR system based on hybrid clouds. *Journal of medical systems* 36, 5 (2012), 3375–3384.
[7] Gonzalo Fernández-Cardeñosa, Isabel de la Torre-Díez, Miguel López-Coronado, and Joel JPC Rodrigues. 2012. Analysis of cloud-based solutions on EHRs systems in different scenarios. *Journal of medical systems* 36, 6 (2012), 3777–3782.
[8] Gonzalo Fern'ndez, Isabel De La Torre-díez, and Joel JPC Rodrigues. 2012. Analysis of the cloud computing paradigm on mobile health records systems. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. IEEE, 927–932.
[9] Neesha Jothi, Wahidah Husain, et al. 2015. Data mining in healthcare–a review. *Procedia Computer Science* 72 (2015), 306–313.
[10] OS Kemkarl and DPB Dahikar. 2012. Can electronic medical record systems transform health care? potential health benefits, savings, and cost using latest advancements in ict for better interactive healthcare learning. *International Journal of Computer Science & Communication Networks* 2, 3/6 (2012), 453–455.
[11] Mu-Hsing Kuo. 2011. Opportunities and challenges of cloud computing to improve health care services. *Journal of medical Internet research* 13, 3 (2011), e67.
[12] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association* 24, 6 (2017), 1211–1220.
[13] Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles Mayo. 2016. A Blockchain-Based Approach to Health Information Exchange Networks. *Proceedings of NIST Workshop Blockchain Healthcare* (2016).
[14] M. Poulymenopoulou, Flora Malamateniou, and George Vassilacopoulos. 2012. Emergency Healthcare Process Automation Using Mobile Computing and Cloud Services. *J. Medical Systems* 36, 5 (2012), 3233–3241.
[15] Zonyin Shae and Jeffrey J. P. Tsai. 2017. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In *ICDCS*. IEEE Computer Society, 1972–1980.
[16] Qinghua Shen, Xiaohui Liang, Xuemin Shen, Xiaodong Lin, and Henry Y. Luo. 2014. Exploiting Geo-Distributed Clouds for a E-Health Monitoring System With Minimum Service Delay and Privacy Preservation. *IEEE J. Biomedical and Health Informatics* 18, 2 (2014), 430–439.
[17] & Clarke R. Svantesson, D. 2010. Privacy and consumer risks in cloud computing. *Computer law & security review* 26, 4 (2010), 391–397.
[18] G. Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151 (2014), 1–32.
[19] Craig S. Wright and Antoaneta Serguieva. 2017. Sustainable blockchain-enabled services: Smart contracts. In *BigData*. IEEE Computer Society, 4255–4264.
[20] Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. 2017. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access* 5 (2017), 14757–14767.
[21] Qi Xia, Emmanuel Boateng Sifah, Abla Smahi, Sandro Amofa, and Xiaosong Zhang. 2017. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information* 8, 2 (2017), 44.
[22] Yang Yang and Maode Ma. 2016. Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds. *IEEE Trans. Information Forensics and Security* 11, 4 (2016), 746–759.

[23] Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang. 2016. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Medical Systems* 40, 10 (2016), 218:1–218:8.

[24] Aiqing Zhang and Xiaodong Lin. 2018. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Medical Systems* 42, 8 (2018), 140:1–140:18.

[25] Jie Zhang, Nian Xue, and Xin Huang. 2016. A Secure System For Pervasive Social Network-Based Healthcare. *IEEE Access* 4 (2016), 9239–9250.

[26] Yin Zhang, Min Chen, Dijiang Huang, Di Wu, and Yong Li. 2017. iDoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization. *Future Generation Comp. Syst.* 66 (2017), 30–35.

[27] Huawei Zhao, Yong Zhang, Yun Peng, and Ruzhi Xu. 2017. Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys. In *ISADS*. IEEE Computer Society, 229–234.

[28] Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Xiaodong Lin. 2015. PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems. *J. Sel. Topics Signal Processing* 9, 7 (2015), 1332–1344.

[29] Guy Zyskind, Oz Nathan, and Alex Pentland. 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *IEEE Symposium on Security and Privacy Workshops*. IEEE Computer Society, 180–184.