Original Paper

Secure and Scalable mHealth Data Management Using Blockchain Combined With Client Hashchain: System Design and Validation

Tomomitsu Motohashi, MSc; Tomonobu Hirano, BSc; Kosuke Okumura, BSc; Makiko Kashiyama, MSc; Daisuke Ichikawa, MD, PhD; Taro Ueno, MD, PhD

SUSMED, Inc, Tokyo, Japan

Corresponding Author:
Taro Ueno, MD, PhD
SUSMED, Inc
Nihonbashi Life Science Bldg 2, 3-11-5, Honcho
Nihonbashi, Chuo-ku
Tokyo, 103-0023
Japan
Phone: 81 335273593
Email: t-ueno@umin.ac.jp

Abstract

Background: Blockchain is emerging as an innovative technology for secure data management in many areas, including medical practice. A distributed blockchain network is tolerant against network fault, and the registered data are resistant to tampering and revision. The technology has a high affinity with digital medicine like mobile health (mHealth) and provides reliability to the medical data without labor-intensive third-party contributions. On the other hand, the reliability of the medical data is not insured before registration to the blockchain network. Furthermore, there are issues with regard to how the clients' mobile devices should be dealt with and authenticated in the blockchain network in order to avoid impersonation.

Objective: The aim of the study was to design and validate an mHealth system that enables the compatibility of the security and scalability of the medical data using blockchain technology.

Methods: We designed an mHealth system that sends medical data to the blockchain network via relay servers. The architecture provides scalability and convenience of operation of the system. In order to ensure the reliability of the data from clients' mobile devices, hash values with chain structure (client hashchain) were calculated in the clients' devices and the results were registered on the blockchain network.

Results: The system was applied and deployed in mHealth for insomnia treatment. Clinical trials for mHealth were conducted with insomnia patients. Medical data of the recruited patients were successfully registered with the blockchain network via relay servers along with the hashchain calculated on the clients' mobile devices. The correctness of the data was validated by identifying illegal data, which were made by simulating fraudulent access.

Conclusions: Our proposed mHealth system, blockchain combined with client hashchain, ensures compatibility of security and scalability in the data management of mHealth medical practice.

Trial Registration: UMIN Clinical Trials Registry UMIN000032951; https://upload.umin.ac.jp/cgi-open-bin/ctr_e/ctr_view.cgi?recptno=R000037564 (Archived by WebCite at http://www.webcitation.org/78HP5iFIw)

(J Med Internet Res 2019;21(5):e13385) doi: 10.2196/13385

KEYWORDS

mobile health; electronic health records; blockchain; client hashchain; clinical trial

Introduction

Digital medicine, including the use of mHealth apps and internet of things (IoT) devices, has become popular in the everyday practice of medicine [1]. It has the potential to promote improved patient health outcomes, support care coordination, and improve communication with lower costs. While digital medicine has the potential for better practices to patients, we need to consider the security issues. Data tampering and impersonation are important security risks for digital medicine and clinical trials. Decision making in medical practice should be based on precise patient information. Data reliability is

compromised if data tampering and impersonation are used to attack the system. External cyberattacks, including ransomware attacks, which result in compromised medical records, are huge threats against the health care sector [2,3]. Data breaches can lead to privacy violations, embarrassment, and social stigma, as well as to fraud and medical identity theft.

In addition to cybersecurity, data governance and authenticity are also important issues in the health care sector, especially in data management in clinical trials [4,5]. Recently, Web-based clinical trials have been conducted to streamline and improve the convenience of clinical trial participation [6]. Since the results of the clinical trials are the basis of the approval of medicine or medical devices by regulatory agencies, the reliability and transparency of the data obtained by the clinical trial must be maintained [7]. However, there are reports that 17% of clinical drug trials were fabricated [8-10]. The ability to easily trace data back to the original source is indispensable.

Blockchain technology has recently garnered attention as a means for transferring data between participating parties based on a "distributed ledger" model that affords a fully transparent and immutable record of data transactions [11]. A blockchain consists of a continuously growing list of transactional records organized into blocks that are replicated on the nodes of a peer-to-peer network. Valid transactions stored in a blockchain are digitally signed and timestamped by their sender, providing cryptographically irrefutable evidence of both provenance and existence of a record at a given point in time. The technology provides a verifiable and tamper-proof history of the data in the blockchain network. Bitcoin is the first implementation of blockchain as a digital asset in widespread use [12]. It eliminates the need for trusted third parties in financial transactions by providing a secure and verifiable history for every transaction in the system.

Beyond digital currency, researchers have started to focus on using blockchain technology for building cryptographic proof in many areas including medical sectors [13]. Blockchain has already been proposed for use in various health care settings, with potential applications in health supply chain management [14-16], insurance claims processing [17-19], medical record management [20,21], and data management in clinical trials [22-26]. Drug counterfeiting is a global problem with significant risks to consumers and the general public. Blockchain has the potential for tracking and tracing drug products and reagents, and counterfeit detection through information verification of supply chain participants. Blockchain technology can also be applied to managing insurance claim policies by the insurance providers and the patients. It can provide authorized access of data to researchers to analyze diseases. Blockchain-based models for electronic medical records have been proposed to enhance ownership of their medical data and data sharing between platforms [17,27,28]. Since the blockchain can be used to establish a permanent record agreed on by all participating parties, it has the potential to mitigate some of the threats to data validity, so that some researchers have proposed to support or even replace the traditional data infrastructure used in clinical trials with blockchain systems [22,23,29,30]. Our previous study also demonstrated an mHealth system for insomnia using a mobile phone app together with a blockchain storage platform and evaluated resistance against tampering of the data collected with mobile phones [24].

Although medical data registered in a blockchain network have proved tamper-resistant, the vulnerability of the medical data lies before registration to the blockchain network. Impersonation of client devices or fabrication of data outside of the blockchain network can impair the reliability of the medical data. In addition, if the blockchain network is open to the Internet, the network is vulnerable to attack and to the theft of medical records. Client devices, such as mobile phones used by patients, should not be dealt with as nodes of the blockchain network in order to preserve the confidentiality of the personal medical data and to reduce the operational cost for the management of the private key. The trade-off must be recognized and overcome by technological improvements.

This study aims to describe and validate an mHealth system using a client management architecture along with a blockchain network. To overcome the remaining problems described above, we designed the whole system with relay servers, which connect client devices to the blockchain network. In order to ensure reliability and to prevent impersonation or fabrication, a hashchain was calculated in client devices and sent to the blockchain network along with the medical data. We further verified the proposed system in the actual clinical trial of mHealth for insomnia patients and evaluated the resistance to various fraud attacks.

Methods

Clinical Trial and mHealth Records

The proposed system was applied and deployed into the mHealth app, which treats chronic insomnia based on cognitive behavioral therapy for insomnia (CBTi) [31]. After a favorable formal review by the Japanese Pharmaceuticals and Medical Devices Agency, research on the mHealth app was conducted by the digital therapeutics company, SUSMED, Inc. (Tokyo, Japan). Informed consent was obtained from the patients for publication of this study. The study has received ethical approval from the Ethics Committee and registered to clinical trial registry (UMIN000032951). All the methods were performed in accordance with the relevant guidelines and regulations.

The mHealth records collected from patients were divided into subjective and objective data. The subjective data, which include clinical indicators, sleep status, and the review of daytime activities, were collected through a self-administered questionnaire. The objective data, which include the results of the Psychomotor Vigilance Test [32], were evaluated by measuring the touch response using the function of mobile phones. For clinical indicators, Athens Insomnia Scale [33], Epworth Sleepiness Scale [34], and Quick Inventory of Depressive Symptomatology [35] were collected. For sleep status, time to go to bed, time to fall asleep, time to wake up, and time to get out of bed were recorded. Along with the medical information, timestamps of the app operation were collected. These clinical indicators were collected using a mobile phone app. All data were stored in the JavaScript Object Notation (JSON) format in the database.

mHealth Data Transfer Via Relay Servers to Blockchain Network

The collected data from the patients' devices were sent to the blockchain network via relay servers. We used three relay servers, and the app randomly selected two relay servers to send the data after the authentication of the client device. By deploying the relay proxy and setting the blockchain software development kits (SDKs) to write-only mode, the relay server sent the received data to the blockchain network. The authentication of the relay server was conducted with a single common authentication server. By configuring the Internet Protocol (IP) address restriction to the listed relay servers, the blockchain network, which contains the medical data, was protected against external attack. The blockchain network was made up of three organizations that contain two validating peers. Each account for nodes of the blockchain network and the relay servers were managed by independent departments in SUSMED, Inc. The strictness of the governance of the data management can be adjusted by individually managing the accounts of different stakeholders, such as pharmaceutical companies, contract research organizations, and regulatory agencies.

mHealth Data Registration in the Blockchain Network

We used Hyperledger Fabric v1.0 to operate the blockchain network because Hyperledger is an open-source blockchain platform and has become widely used [36,37].

The blockchain network was administered by a collection of organizations. Each organization had multiple nodes. In this study, the network had three organizations and each organization had two nodes. As the state database, CouchDB was used to store the JSON document [38].

The nodes executed an installed chaincode and returned hash values generated from the execution result. The secure hash algorithm SHA-256 was used to compute the hash values encoded into the blocks of the blockchain [39]. To execute the transaction, each node followed the consensus algorithm, which was called endorsement policy [11], although the previous version of Hyperledger Fabric used Practical Byzantine Fault Tolerance as a consensus algorithm [40,41].

The endorsement policy was set in units of organizations, and the flexible set was available according to the needs of the app. Each organization issued one signature. The node that validated the transactions in each organization was called the endorser. In this study, the validation of each transaction required more than two signatures from three organizations.

Under the endorsement policy, transactions were validated and accepted in the following processes:

1. Proposal: The transaction was sent from the client app to the endorsers in each organization.
2. Endorse: Each endorser verified that (1) the transaction proposal was well formed, (2) it had not been already submitted in the past, (3) the signature was valid, and (4) the client was properly authorized to perform the proposed operation, which was described in the chaincode. If the transaction was validated, chaincode was executed and the result with the signature was returned to the client.
3. Submit: The client verified that the number of signatures from the organizations satisfied the endorsement policy. If it was satisfied, the transaction was sent to the ordering service, which ordered the series of transactions in chronological order and created the block of the transactions.
4. Broadcast: The block was delivered to all nodes.
5. Commit: If each block was validated to fulfill the endorsement policy and was to be well formed, the block was appended to the chain in each node.

All data, including the client hashchain, were registered in the blockchain network via relay servers to secure the tamper-resistance of the data. In contrast, the secure string for the calculation of the hash value was preserved in the client device. At the end of the study, the secure string was sent to the blockchain network to verify the hashchain. The client hash values were calculated on the mobile phone based on medical data, the secure string, and the previous hash value using the SHA-256 algorithm [39].

Test Scenarios

There are issues regarding cybersecurity (ie, concerning external actors) and governance/authenticity (eg, internal actors like researchers) in medical data management. The tamper-resistance of the data registered in the blockchain network against external attack has been proven in previous studies. The reliability of the data against internal actors in the blockchain network can also be guaranteed by managing the accounts for each node by different stakeholders, such as pharmaceutical companies, contract research organizations, and regulatory agencies. Here, we evaluated how the data manipulation before registration to the blockchain network can be detected and distinguished by simulating the following malicious access. The artificial data were created for each scenario and tested if the fraudulent access were detected and the original data can be distinguished from the illegal data. Since the results of the manipulation of the data are deterministic due to collision-resistant hash functions of SHA-256 [42], we verified the result of a single manipulation in each scenario. Since the accounts for nodes of the blockchain network and the relay servers were managed by independent departments, both internal and external actors can be simulated by hacking each server.

1. Attack on the relay server: To simulate an artificial attack on the relay server (ie, outside actors) or misconduct by the owner of the relay server (ie, inside actors) during the clinical trial, one of the relay servers was hacked. The data sent from a client device can be modified before registration to the blockchain network by the malicious access. In this case, the secure string for the calculation of a hash value in the client device was not stolen. Hence, the client hash value was calculated with the previous hash value, modified medical data, and the incorrect string.
2. Attack on the authentication server: To simulate an artificial attack on the authentication server (ie, outside actors) or misconduct by the owner of the authentication server (ie, inside actors) during the clinical trial, the authentication key of an existing account on the authentication server was stolen and the data of the hacked account was uploaded by

multiple devices. In this case, the secure string for the calculation of a hash value in the client device was not stolen. Hence, the client hash value was calculated with the previous hash value, modified medical data, and the incorrect string.

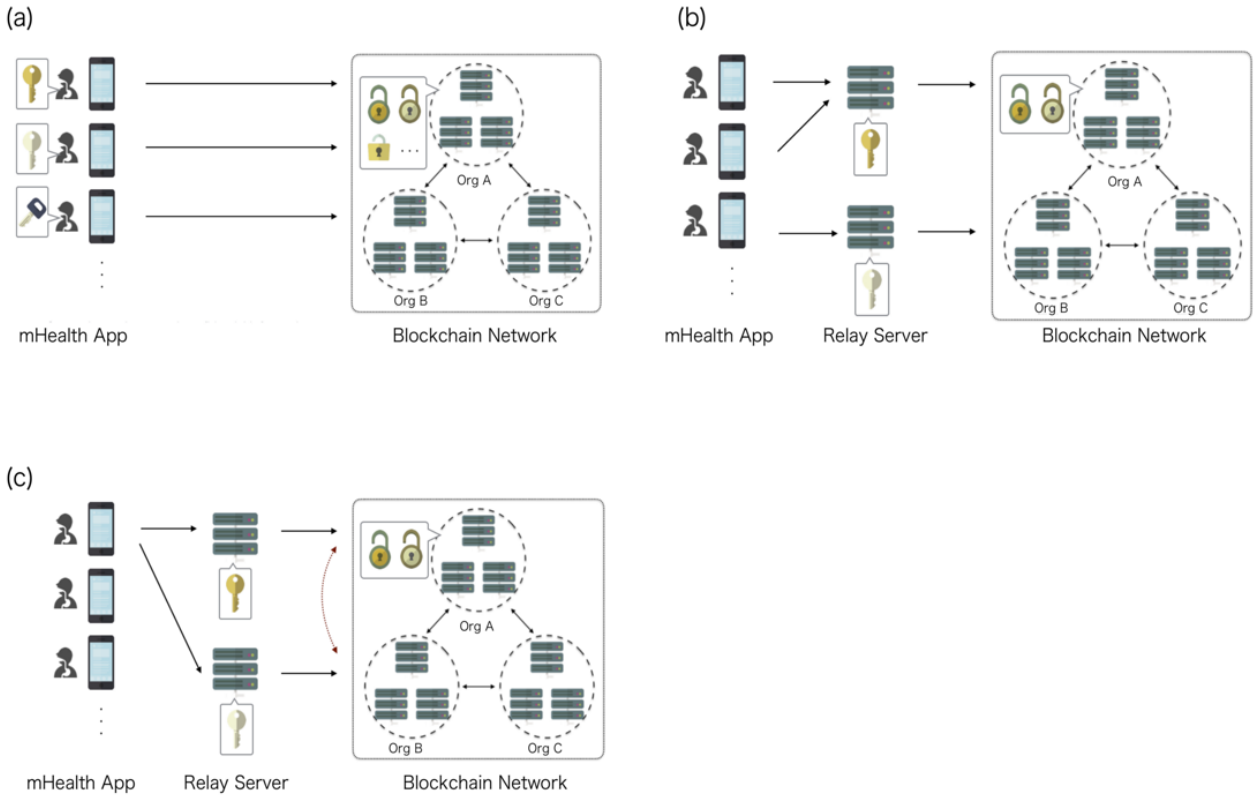
3. Attack on the client device: The secure string preserved in the client device was stolen by an attacker using a mobile malware root exploit. The authentication information to the relay servers was also stolen by the malicious infection. Hence, the client hash value was calculated by different devices with the previous hash value, modified medical data, and the correct secure string.

Results

Design of the Client for Blockchain Network in mHealth

In our previous study, the mHealth data obtained by a mobile phone were uploaded to the blockchain network. We then evaluated the robustness of the network and the tamper-resistance of the data in the blockchain network [24]. To advance further into the practical usage of blockchain in mHealth, it is necessary to design how the client devices, such as mobile phones, send medical data to the blockchain network. Client devices can send data to the blockchain network directly, but with this architecture, the mHealth app that patients installed to their mobile phone needs to have SDKs for blockchain. The blockchain network will also receive access from unspecified clients due to a lack of IP address restriction. In that situation, there are risks that unspecified clients can store medical information in the blockchain network using SDKs to read the data. The system is resistant against data tampering, but the operational costs increase since they must manage private keys for each client device (Figure 1). In order to overcome these obstacles, the usage of relay servers is one possible option. With the architecture using relay servers, the blockchain network can restrict the access by IP address selection and it is not necessary for the mHealth app to include SDKs for blockchain. With this architecture, blockchain networks were protected against unspecified access from the internet and the functions of SDKs in the relay server can be predetermined as write-only, resulting in the protection of the medical data stored in the blockchain network. On the other hand, there are risks that the hacking of the relay server will result in impersonation (Figure 1). To balance these trade-offs, we propose the following architecture of the client for the blockchain network in mHealth. The client devices, such as mobile phones, send their data to multiple relay servers and the data are compared between relay servers and verified. After verification, the relay server, which has permission to access by IP address restriction, sends the data to the blockchain network using write-only functions of SDKs. With this system, medical data stored in the blockchain network are protected against access from the internet and are resistant against the risks of server hacking (Figure 1).

Figure 1. mHealth system architecture, which sends the medical data to the blockchain network. Data sent to (a) the blockchain network without relay servers; client devices are dealt with as nodes of the blockchain network so that mHealth app needs to contain software development kits for blockchain; (b) the blockchain via a single relay server; public keys for each relay server should be managed; (c) the blockchain via multiple relay servers; public keys for each relay server should be managed. Data reliability can be verified by comparing the data to be registered (red line).



Authentication Between Clients and Relay Servers

For the usage of relay servers described above, it is indispensable to carefully design the authentication of client devices to send data to relay servers. It is possible that a single common server gives an authentication to client devices, but with this architecture, the system is vulnerable to server hacking. Malicious access to the single authentication server can result in impersonation (Figure 2). The alternative is to set an authentication server for each relay server. Although the risks of impersonation by server hacking can be reduced, the operational costs for authentication increase. In addition, it is not possible to verify the reliability of the original data if multiple authentication servers were maliciously accessed (Figure 2). In order to solve these problems, we implemented a single common authentication server with another method, using a hash value calculated on the client devices. As an initial setting, the client device generates and preserves a secure string. The client device calculates a hash value based on the medical data and the secure string, as well as the previous hash value using the SHA-256 hash algorithm. Thus, the hash value comprises the chain structure. The hash value was also registered in the blockchain network along with the medical data in order to guarantee tamper-resistance of the value, although the secure string was preserved in the client device. It is possible to verify the reliability of data using the secure string preserved in the client devices and to retrospectively reject impersonation after finishing the clinical trials. Even when a relay server was hacked by malicious access, we can verify the correct data based on the client hashchain and the secure string preserved in the client device. Since the hash value calculated in the client device makes up the chain structure, we called the technique “client hashchain” in contrast to blockchain (Figure 2). In the case of the device having been destroyed or disabled prior to the conclusion of the study, the secure string could be sent beforehand to the user’s personal storage, such as their email box.

Application of the Proposed System to mHealth and Data Management in a Clinical Trial

In order to validate the system proposed above, we have implemented the architecture into the mHealth app. The app was designed to treat insomnia patients based on CBTi and collects medical data using mobile phones. The app generates a secure string at login and stores it on the client device. The app also calculates a hash value based on the medical data, the previous hash value, and the secure string so that the hash values make up the chain structure. The medical data collected with the app, as well as the hash value, were sent to the blockchain network via relay servers. We used three relay servers and the app selected two relay servers at random to send the data to the blockchain network. The blockchain network comprised three organizations, which contain two validating peers.

With these systems, we conducted the clinical trial on the mHealth app for insomnia patients. Informed consent was obtained from the patients and the app account was provided by the medical doctor. mHealth data were collected with the mobile app and sent to the blockchain network via relay servers along with the client hash value (Figure 3). In the client devices, client hash values were calculated based on mHealth data, the previous client hash value, and the secure string stored on the client device. The client hash value constitutes the chain structure and proves the origin of the sequential data.

Both mHealth data and the client hash value were sent to the blockchain network to be registered in the ledger. The ledger is made up of the blockchain, sequenced records in blocks, and a state database. Each node of the blockchain maintains a copy of the ledger. If the transaction was validated under the endorsement policy, the chaincode was executed and the block of the transaction was appended in each node. The mHealth data and the client hash value were stored in CouchDB and the blockchain. The block includes a hash of the block’s transactions, as well as a hash of the prior block. In this way, it is not possible to tamper with the ledger data without breaking the hash links.

Although the block size is limited in blockchain, it is enough for our medical data since the clinical indicators are stored as JSON data. In addition, the transaction throughput in the Hyperledger Fabric platform that we used is 2250 transactions per second [27]. In contrast, in a permissionless network or public network, such as Bitcoin and Ethereum, it takes 600 seconds and 10 seconds respectively to write a transaction on the ledger [28]. Since the number of transactions in our mHealth system occur several times per day for every patient, the transaction performance of the blockchain will not be a bottleneck.

Figure 2. Authentication of client devices and relay servers. Client devices authenticated by (a) a single common authentication server; the system is vulnerable against server hacking; (b) multiple authentication servers for each relay servers; (c) a single common authentication server. In addition to authentication, client devices calculate a hash value based on data, secure string, and previous hash value, so the hash value consists of the chain structure (client hashchain).

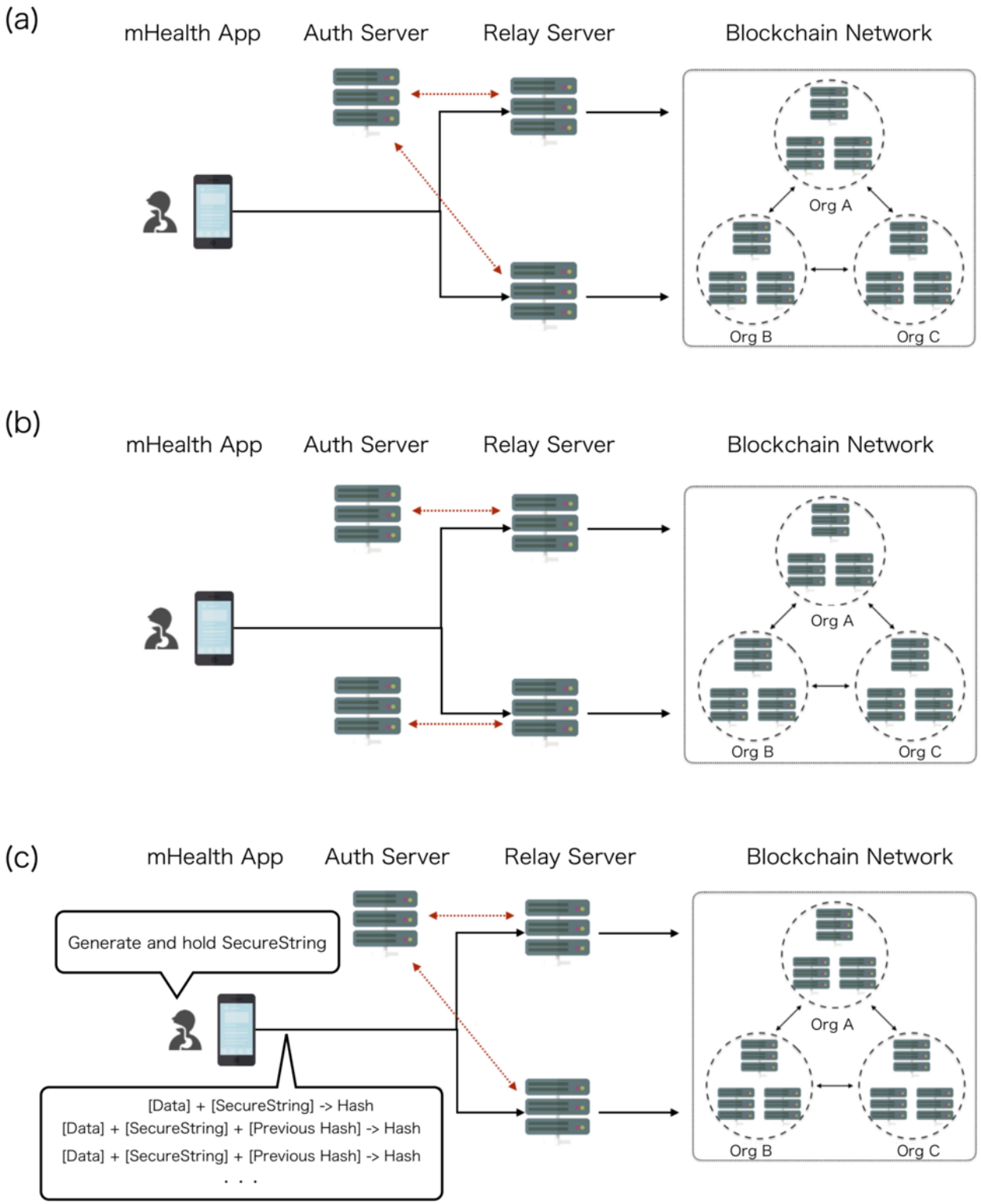


Figure 3. User data along with client hashchain registered to blockchain network.

user ID	Log ID	relay server	Data	ClientHash
112	1	1	{"arouseHour":5,"sleepHour":23,"arouseMinute":30,"baseDay":20180705,"sleepMinute":43,"startOn":1530752240}	5c1ae2dd2e09b87d06dd65259a5c680a054ee1aea50bb6649098d140867bac15
112	1	3	{"arouseHour":5,"sleepHour":23,"arouseMinute":30,"baseDay":20180705,"sleepMinute":43,"startOn":1530752240}	5c1ae2dd2e09b87d06dd65259a5c680a054ee1aea50bb6649098d140867bac15
112	2	2	{"usingMedicine":false,"stature":179,"id":"SY0105-17-112","deviceType":"iOS","initialAisScore":12,"startedBaseDay":20180705,"age":54,"weight":73,"gender":1,"medicineDescription":"","startedOn":1530752155}	51e9727ab04e0a7122e4d04ce99eed8d8bf056654f4b1cbb91e408b73c751528
112	2	3	{"usingMedicine":false,"stature":179,"id":"SY0105-17-112","deviceType":"iOS","initialAisScore":12,"startedBaseDay":20180705,"age":54,"weight":73,"gender":1,"medicineDescription":"","startedOn":1530752155}	51e9727ab04e0a7122e4d04ce99eed8d8bf056654f4b1cbb91e408b73c751528
112	3	1	{"mistakeCount":0,"msec":0,"day_activity_check_items":0,"reviewedMorning":false,"lapseCount":0,"baseDay":20180626,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1529951400,"reviewedEvening":false,"noSleep":false}	a014bb00ad6257b6bc12f061e613f7326a59183cb774fa449a26f41a45b26dae
112	3	2	{"mistakeCount":0,"msec":0,"day_activity_check_items":0,"reviewedMorning":false,"lapseCount":0,"baseDay":20180626,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1529951400,"reviewedEvening":false,"noSleep":false}	a014bb00ad6257b6bc12f061e613f7326a59183cb774fa449a26f41a45b26dae
…	…	…	…	…
112	374	1	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b
112	374	3	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b

Validation of the Resistance Against Attack on the Relay Server

To investigate the resistance of our proposed system, we first simulated an artificial attack on the relay server (ie, outside actors) or misconduct by the owner of the relay server (ie, inside actors) and evaluated if the malicious access was detected and if the original data are distinguishable from the illegal data. As described above, the client device sends the data to the blockchain network via multiple relay servers. We used three relay servers and the app selected two relay servers at random to send the data to the blockchain network. If one of the relay servers is hacked, the attacker can modify the data sent from the client device prior to blockchain submission and steal the authorization token. In this case, the secure string used in the calculation of the client hashchain was not stolen by the attacker.

As shown in Figure 4, an attacker hacked relay server #2 and modified some medical data as well as the client hash value. In this case, the client hash value was calculated with the previous hash value, modified medical data, and the incorrect string. The access fraud can be detected by the mismatch between the data sent from other relay servers. It is also possible to distinguish and reject illegal data from original data automatically using the client hashchain. At the end of the clinical trial, the device sent the secure string to the blockchain to make it possible to validate the uploaded data retrospectively. Since all the medical data and the client hash values were stored in the blockchain network, it is not possible to rewrite the hash value based on

the secure string, which was sent via the relay servers. Legal data can be guaranteed by combining the client hashchain, which rejects impersonation, with the blockchain, which provides tamper-proof history.

Validation of the Resistance Against Attack on the Authentication Server

We next simulated an artificial attack on the authentication server (ie, outside actors) or misconduct by the owner of the authentication server (ie, inside actors) during the clinical trial and evaluated whether the malicious access was detected if the original data are distinguishable from the illegal data. The authentication server possesses the authentication keys of every account. If the authentication key was stolen, the attacker can send illegal data from different devices. In this case, the secure string used in the calculation of the client hashchain was not stolen by the attacker.

Figure 4. Relay server hacked and data modified by access fraud (client hash value in red).

user ID	Log ID	relay server	Data	ClientHash
…	…	…	…	…
112	142	1	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":false,"noSleep":false}	401442e3815aecbf6a87ff58b1f20102cdfdd7dc7d93544a8edbcd808ac9f2ef
112	142	3	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":false,"noSleep":false}	401442e3815aecbf6a87ff58b1f20102cdfdd7dc7d93544a8edbcd808ac9f2ef
112	143	1	{"answer":4,"date":1532434656,"totalScore":4,"baseDay":20180724}	f1622ce6142870eb461dfcf09fe32785d350556841f08aee1916fbc26ab7b0a9
112	143	2	{"answer":8,"date":1532434656,"totalScore":8,"baseDay":20180724}	7d135f9fd3d99777d14e250ed8f6c900540071b2d1dbfd989a4c3bd85ed11f54
112	144	2	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":true,"noSleep":false}	ee5109a8ff2182dec4d50d4be29cb8c8399340007e28e9614d206860d707d60d
112	144	3	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":true,"noSleep":false}	ee5109a8ff2182dec4d50d4be29cb8c8399340007e28e9614d206860d707d60d
…	…	…	…	…
112	374	1	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b
112	374	3	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b

As shown in Figure 5, using the stolen authentication key, multiple data with the same log ID were generated and sent to the blockchain network via relay servers by the attacker. Fraud detection can be achieved by identifying branched data. Furthermore, it is also possible to distinguish and reject illegal data from original data automatically using the client hashchain.

At the end of the clinical trial, the device sent the secure string to the blockchain to enable the validation of the uploaded data retrospectively. Since all medical data and the client hash values were stored in the blockchain network, it is not possible to rewrite the hash value based on the secure string that was sent via relay servers.

Figure 5. Authentication server hacked and data generated from multiple devices using the authentication key (authentication key was stolen and the attacker created illegal data from different devices in red).

user ID	Log ID	relay server	Data	ClientHash
…	…	…	…	…
112	142	1	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":false,"noSleep":false}	401442e3815aecbf6a87ff58b1f20102cdfdd7dc7d93544a8edbcd808ac9f2ef
112	142	3	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":false,"noSleep":false}	401442e3815aecbf6a87ff58b1f20102cdfdd7dc7d93544a8edbcd808ac9f2ef
112	143	2	{"answer":4,"date":1532434656,"totalScore":4,"baseDay":20180724}	f1622ce6142870eb461dfcf09fe32785d350556841f08aee1916fbc26ab7b0a9
112	143	3	{"answer":4,"date":1532434656,"totalScore":4,"baseDay":20180724}	f1622ce6142870eb461dfcf09fe32785d350556841f08aee1916fbc26ab7b0a9
112	143	1	{"answer":8,"date":1532434656,"totalScore":8,"baseDay":20180724}	7d135f9fd3d99777d14e250ed8f6c900540071b2d1dbfd989a4c3bd85ed11f54
112	143	2	{"answer":8,"date":1532434656,"totalScore":8,"baseDay":20180724}	7d135f9fd3d99777d14e250ed8f6c900540071b2d1dbfd989a4c3bd85ed11f54
112	144	2	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":true,"noSleep":false}	ee5109a8ff2182dec4d50d4be29cb8c8399340007e28e9614d206860d707d60d
112	144	3	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":true,"noSleep":false}	ee5109a8ff2182dec4d50d4be29cb8c8399340007e28e9614d206860d707d60d
…	…	…	…	…
112	374	1	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b
112	374	3	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b

Validation of the Resistance Against Attack on the Client Device

To further investigate the resistance of our proposed system, we next simulated an artificial attack on the client device and evaluated if the malicious access was detected and if the original data are distinguishable from the illegal data. One of the most dangerous attacks is the malware root exploit, which enables the attacker to obtain the victim's private key. In this case, the authentication key as well as the secure string were stolen by the attacker, resulting in a more serious situation.

As shown in Figure 6, using the stolen authentication key, multiple data with the same log ID were generated and sent to the blockchain network. Fraud detection can be achieved by identifying the branched data. However, it is not possible to distinguish illegal data from original data automatically using the client hashchain because the attacker has stolen the secure string to calculate the client hash value. In this case, however, it is possible to judge which are the original data by checking the data in the patient's device offline, based on the fraud detection.

Figure 6. Client device washacked by malware root exploit and data generated from multiple devices using the authentication key (authentication key as well as the secure string for the client hash value were stolen by root exploit and the attacker created illegal data from different device in red).

user ID	Log ID	relay server	Data	ClientHash
…	…	…	…	…
112	142	1	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":false,"noSleep":false}	401442e3815aecbf6a87ff58b1f20102cdfdd7dc7d93544a8edbcd808ac9f2ef
112	142	3	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":false,"noSleep":false}	401442e3815aecbf6a87ff58b1f20102cdfdd7dc7d93544a8edbcd808ac9f2ef
112	143	2	{"answer":4,"date":1532434656,"totalScore":4,"baseDay":20180724}	f1622ce6142870eb461dfcf09fe32785d350556841f08aee1916fbc26ab7b0a9
112	143	3	{"answer":4,"date":1532434656,"totalScore":4,"baseDay":20180724}	f1622ce6142870eb461dfcf09fe32785d350556841f08aee1916fbc26ab7b0a9
112	143	1	{"answer":8,"date":1532434656,"totalScore":8,"baseDay":20180724}	14fea01f46f60cec11e61f2a25c38cf2d19a32ad38637c9fb5914bb65962c309
112	143	2	{"answer":8,"date":1532434656,"totalScore":8,"baseDay":20180724}	14fea01f46f60cec11e61f2a25c38cf2d19a32ad38637c9fb5914bb65962c309
112	144	2	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":true,"noSleep":false}	ee5109a8ff2182dec4d50d4be29cb8c8399340007e28e9614d206860d707d60d
112	144	3	{"mistakeCount":0,"msec":0,"day_activity_check_items":64775,"reviewedMorning":true,"lapseCount":0,"baseDay":20180724,"stimulation_restrict_items":0,"countOfTapAboutAnxiety":0,"timestamp":1532370600,"reviewedEvening":true,"noSleep":false}	ee5109a8ff2182dec4d50d4be29cb8c8399340007e28e9614d206860d707d60d
…	…	…	…	…
112	374	1	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b
112	374	3	{"key":"RMW9psVt7IDnHrNrIxol"}	93de64253446ae3c9bb045bb146226498258d4f5c2898ea7b9f8926498802e0b

Discussion

Principal Findings

In this study, we have developed a secure and scalable mHealth system using relay servers and blockchain combined with a client hashchain. Although blockchain technology provides tamper-resistance to medical data [24], the security was limited to the registered data and it cannot distinguish between original data and impersonated data. In addition, scalability will be compromised if the client devices were dealt with as a node of blockchain network. With our proposed system, we have shown that these problems can be resolved.

Bitcoin was the first implementation of blockchain as a digital asset in widespread use. Although bitcoin can be used as a platform for preventing data tampering, it is not appropriate since it is an open network and massive computing power is necessary for proof of work (PoW) to obtain consensus [43]. Private blockchain networks, such as Hyperledger Fabric, are more appropriate for the management of medical data since the node of stakeholders can be controlled. In addition, it is possible to process more transactions in a private blockchain without PoW. Using a private blockchain network, we used relay servers to send the data from authorized clients. With this architecture, it is not necessary to incorporate SDKs on client devices. To make the system robust against hacking of the relay server, the app sent data to the blockchain network via multiple relay servers. Even when one of the relay servers was hacked, we could detect access fraud and distinguish the original data from modified data. In our study, we used three relay servers and two were randomly selected to send the data. The robustness of the system against server attack can be increased if we use more relay servers, for instance, if three out of five relay servers are randomly selected to send the data.

To further clarify the origin of the data, we combined the client hashchain with the private blockchain. Hash values combined with the blockchain have been used as the metadata in a previous study for the management of rights for digital contents [44]. In contrast, we used hash values calculated on the client device to protect against impersonation and verify the origin of the data by chaining them. Hash values with chain structure (client hashchain) enable the identification of the original data sent from a specific client, which stores the secure string. In addition, in combination with the blockchain, the system also ensured tamper-resistance and the reliability of the hash values to prevent impersonation. We have shown that fraudulent data by compromised relay servers can be detected and distinguished from original data using the client hashchain. Even when the secure string used in calculating the client hash value was stolen by the attacker with root exploit [45], it is possible to detect the malformation in the branching of the chaincode. Based on the detection of the malformation, the researchers can ask the patients and check which are the original data. Therefore, the system is highly resistant against impersonation and tampering.

In this study, we designed the architecture for mHealth and verified the performance in a clinical study. Although mHealth is suitable for collecting medical data, such as patient reported outcomes [46], by changing the client device from patients' mobile phone to computers in medical institutions, the system can also be applied to clinical trials that use electronic data capture [47]. In addition, we could deploy smart contract, which is called chaincode in Hyperledger Fabric, to each node of the blockchain network to execute transactions. Since the smart contract may have the function to transform medical data into the determined format, it is possible to automatically complete the case report form of each patient if the app has access to additional medical data by deploying the smart contract for the clinical trial [25,48].

The system enables the verification of the accuracy of the medical data without confirmation by the third party, such as a contracted research organization, so that it is possible to reduce the cost of clinical trials as well as the possibility of human error. Thus, our system based on the blockchain technology combined with a client hashchain may enhance the development of drugs and medical devices.

Limitations

Further studies are needed to verify the scalability of the system for conducting multiple clinical trials simultaneously. In Hyperledger Fabric v1.0, it is possible to partition the network and define a communication channel using an ordering service, which enables multiple clinical trials to be conducted in the same system [49]. Although the transaction throughput in the Hyperledger Fabric platform that we used is much higher than public blockchain, one drawback of the private network described here is preventing 51% of attacks in networks that are composed of a limited number of nodes without public validation.

Although our system is resistant against impersonation and tampering, hacking of the client device is a great threat. Root exploit is a type of malware attackers use to modify the Android operating system kernel such that attackers are able to gain super-user privileges. When attackers gain root of the operating system kernel, they also gain access to full administrator privileges. Through this, attackers are able to install other malware types, such as botnets, worms, or Trojans into the system. Further studies like root exploit detection [45] may be beneficial for the improved security of the system.

Conclusion

In this study, we designed a secure and scalable mHealth system using blockchain. A client hashchain was combined with the blockchain network to protect against impersonation, enabling the usage of relay servers and reducing the complexity of authentication of client devices for mHealth. The system was validated in the clinical trial, and the resistance against various fraud attacks was evaluated.

Acknowledgments

This work was supported in part by the New Energy and Industrial Technology Development Organization and the Cabinet Office of Japan.

Authors' Contributions

TU designed the research; TH, KO, MK performed the research; TM, DI analyzed the data; and TM, TH, DI, and TU wrote the paper.

Conflicts of Interest

The authors are members of SUSMED, Inc.

References

1. Marzano L, Bardill A, Fields B, Herd K, Veale D, Grey N, et al. The application of mHealth to mental health: opportunities and challenges. Lancet Psychiatry 2015 Oct;2(10):942-948. [doi: 10.1016/S2215-0366(15)00268-0] [Medline: 26462228]
2. Kierkegaard P. Electronic health record: Wiring Europe's healthcare. Computer Law & Security Review 2011 Sep;27(5):503-515. [doi: 10.1016/j.clsr.2011.07.013]
3. Clarke R, Youngstein T. Cyberattack on Britain's National Health Service - A Wake-up Call for Modern Medicine. N Engl J Med 2017 Aug 03;377(5):409-411. [doi: 10.1056/NEJMp1706754] [Medline: 28591519]
4. Hao D, Patrick Y, Thomas D, Guannan G, Mingming K, Harlan K, et al. TrialChain: A Blockchain-Based Platform to Validate Data Integrity in Large, Biomedical Research Studies. arXiv 2018 Jul 10:03662 [FREE Full text]
5. Bekelman JE, Li Y, Gross CP. Scope and impact of financial conflicts of interest in biomedical research: a systematic review. JAMA 2003;289(4):454-465. [Medline: 12533125]
6. Orri M, Lipset CH, Jacobs BP, Costello AJ, Cummings SR. Web-based trial to evaluate the efficacy and safety of tolterodine ER 4 mg in participants with overactive bladder: REMOTE trial. Contemp Clin Trials 2014 Dec;38(2):190-197. [doi: 10.1016/j.cct.2014.04.009] [Medline: 24792229]
7. Pease AM, Krumholz HM, Downing NS, Aminawung JA, Shah ND, Ross JS. Postapproval studies of drugs initially approved by the FDA on the basis of limited evidence: systematic review. BMJ 2017 May 03;357:j1680 [FREE Full text] [doi: 10.1136/bmj.j1680] [Medline: 28468750]
8. Bhatt A. Quality of clinical trials: A moving target. Perspect Clin Res 2011 Oct;2(4):124-128 [FREE Full text] [doi: 10.4103/2229-3485.86880] [Medline: 22145122]
9. Sheehan JG. Fraud, conflict of interest, and other enforcement issues in clinical research. Cleve Clin J Med 2007 Mar;74 Suppl 2:S63-67; discussion S68. [Medline: 17471620]
10. Gupta A. Fraud and misconduct in clinical research: A concern. Perspect Clin Res 2013 Apr;4(2):144-147 [FREE Full text] [doi: 10.4103/2229-3485.111800] [Medline: 23833741]
11. Cai W, Wang Z, Ernst JB, Hong Z, Feng C, Leung VCM. Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access 2018;6:53019-53033 [FREE Full text] [doi: 10.1109/ACCESS.2018.2870644]
12. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. URL: https://bitcoin.org/bitcoin.pdf [accessed 2019-05-05] [WebCite Cache ID 78A7OLdwe]
13. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 2017 Nov 01;24(6):1211-1220 [FREE Full text] [doi: 10.1093/jamia/ocx068] [Medline: 29016974]
14. Sylim P, Liu F, Marcelo A, Fontelo P. Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. JMIR Res Protoc 2018 Sep 13;7(9):e10163 [FREE Full text] [doi: 10.2196/10163] [Medline: 30213780]
15. Mackey TK, Nayyar G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin Drug Saf 2017 May;16(5):587-602. [doi: 10.1080/14740338.2017.1313227] [Medline: 28349715]
16. Tseng J, Liao Y, Chong B, Liao S. Governance on the Drug Supply Chain via Gcoin Blockchain. Int J Environ Res Public Health 2018 Dec 23;15(6):E1055 [FREE Full text] [doi: 10.3390/ijerph15061055] [Medline: 29882861]
17. Mertz L. (Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution. IEEE Pulse 2018;9(3):4-7. [doi: 10.1109/MPUL.2018.2814879] [Medline: 29757744]
18. Zhou L, Wang L, Sun Y. MIStore: a Blockchain-Based Medical Insurance Storage System. J Med Syst 2018 Jul 02;42(8):149 [FREE Full text] [doi: 10.1007/s10916-018-0996-4] [Medline: 29968202]
19. Kaur H, Alam MA, Jameel R, Mourya AK, Chang V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. J Med Syst 2018 Jul 10;42(8):156. [doi: 10.1007/s10916-018-1007-5] [Medline: 29987560]
20. Mense A, Athanasiadis L. Concept for Sharing Distributed Personal Health Records with Blockchains. Stud Health Technol Inform 2018;251:7-10. [Medline: 29968588]
21. Wang H, Song Y. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. J Med Syst 2018 Jul 05;42(8):152. [doi: 10.1007/s10916-018-0994-6] [Medline: 29974270]
22. Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. Trials 2017 Dec 19;18(1):335 [FREE Full text] [doi: 10.1186/s13063-017-2035-z] [Medline: 28724395]

23. Maslove DM, Klein J, Brohman K, Martin P. Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study. JMIR Med Inform 2018 Dec 21;6(4):e11949 [FREE Full text] [doi: 10.2196/11949] [Medline: 30578196]
24. Ichikawa D, Kashiyama M, Ueno T. Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR Mhealth Uhealth 2017 Jul 26;5(7):e111 [FREE Full text] [doi: 10.2196/mhealth.7938] [Medline: 28747296]
25. Wong DR, Bhattacharya S, Butte AJ. Prototype of running clinical trials in an untrustworthy environment using blockchain. Nat Commun 2019 Dec 22;10(1):917 [FREE Full text] [doi: 10.1038/s41467-019-08874-y] [Medline: 30796226]
26. Zhuang Y, Sheets L, Shae Z, Tsai JJP, Shyu CR. Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials. AMIA Annu Symp Proc 2018;2018:1167-1175 [FREE Full text] [Medline: 30815159]
27. Angraal S, Krumholz HM, Schulz WL. Blockchain Technology: Applications in Health Care. Circ Cardiovasc Qual Outcomes 2017 Dec;10(9):E003800. [doi: 10.1161/CIRCOUTCOMES.117.003800] [Medline: 28912202]
28. Roehrs A, da Costa CA, da Rosa Righi R. OmniPHR: A distributed architecture model to integrate personal health records. J Biomed Inform 2017 Dec;71:70-81 [FREE Full text] [doi: 10.1016/j.jbi.2017.05.012] [Medline: 28545835]
29. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput Struct Biotechnol J 2018;16:267-278 [FREE Full text] [doi: 10.1016/j.csbj.2018.07.004] [Medline: 30108685]
30. Zhang A, Lin X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst 2018 Jun 28;42(8):140. [doi: 10.1007/s10916-018-0995-5] [Medline: 29956061]
31. Jacobs GD, Pace-Schott EF, Stickgold R, Otto MW. Cognitive behavior therapy and pharmacotherapy for insomnia: a randomized controlled trial and direct comparison. Arch Intern Med 2004 Sep 27;164(17):1888-1896. [doi: 10.1001/archinte.164.17.1888] [Medline: 15451764]
32. Basner M, Dinges DF. Maximizing sensitivity of the psychomotor vigilance test (PVT) to sleep loss. Sleep 2011 May 01;34(5):581-591 [FREE Full text] [Medline: 21532951]
33. Soldatos CR, Dikeos DG, Paparrigopoulos TJ. Athens Insomnia Scale: validation of an instrument based on ICD-10 criteria. J Psychosom Res 2000 Jun;48(6):555-560. [Medline: 11033374]
34. Johns MW. A new method for measuring daytime sleepiness: the Epworth sleepiness scale. Sleep 1991 Dec;14(6):540-545. [Medline: 1798888]
35. Biggs MM, Shores-Wilson K, Rush AJ, Carmody TJ, Trivedi MH, Crismon ML, et al. A comparison of alternative assessments of depressive symptom severity: a pilot study. Psychiatry Res 2000 Nov 20;96(3):269-279. [Medline: 11084222]
36. Christian C. IBM research. Architecture of the Hyperledger Blockchain Fabric URL: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf [accessed 2019-05-06] [WebCite Cache ID 78A8lYPTB]
37. Hossein K. Lexology. The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies URL: https://www.lexology.com/library/detail.aspx?g=5adaf528-b9ad-4575-8933-4cb033a2536d [accessed 2019-05-05] [WebCite Cache ID 78A91hLdN]
38. Abiteboul S. Web Data Management. London, UK: Cambridge University Press; 2012.
39. Shay G. Speeding Up SHA-1, SHA-256 and SHA-512 on the 2nd Generation Intel® Core™ Processors. In: Ninth International Conference on Information Technology - New Generations. 2012 Presented at: International Conference on Information Technology - New Generations; April 16-18, 2012; Las Vegas, NV URL: https://ieeexplore.ieee.org/document/6209073 [doi: 10.1109/ITNG.2012.62]
40. Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst 2002;20(4):398-461 [FREE Full text] [doi: 10.1145/571637.571640]
41. Castro M, Liskov B. 3rd Symposium on Operating Systems Design and Implementation (OSDI) Proceedings. Berkeley, CA: USENIX Association; 1999.
42. Gilbert H, Handschuh H. Security Analysis of SHA-256 and Sisters. In: International Workshop on Selected Areas in Cryptography.: Springer; 2003 Presented at: International Workshop on Selected Areas in Cryptography; Aug. 14-15, 2003; Ottawa, ON, Canada p. 175-193 URL: https://link.springer.com/chapter/10.1007/978-3-540-24654-1_13
43. Michael C. Applied Innovation Review. 2016. BlockChain Technology: Beyond Bitcoin URL: http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf [accessed 2019-05-06] [WebCite Cache ID 78AAoBhUS]
44. Shigeru F, Hiroki W, Atsushi N, Tomokazu Y, Akihito A, Junichi K. BRIGHT: A concept for a decentralized rights management system based on blockchain. In: IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin). 2015 Presented at: IEEE 5th International Conference on Consumer Electronics; Sept. 6-9, 2015; Berlin, Germany URL: https://ieeexplore.ieee.org/document/7391275 [doi: 10.1109/ICCE-Berlin.2015.7391275]
45. Firdaus A, Anuar NB, Razak MFA, Hashem IAT, Bachok S, Sangaiah AK. Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management. J Med Syst 2018 May 04;42(6):112. [doi: 10.1007/s10916-018-0966-x] [Medline: 29728780]
46. Basch E. The missing voice of patients in drug-safety reporting. N Engl J Med 2010 Mar 11;362(10):865-869 [FREE Full text] [doi: 10.1056/NEJMp0911494] [Medline: 20220181]

47. Rorie DA, Flynn RWV, Grieve K, Doney A, Mackenzie I, MacDonald TM, et al. Electronic case report forms and electronic data capture within clinical trials and pharmacoepidemiology. Br J Clin Pharmacol 2017 Sep;83(9):1880-1895 [FREE Full text] [doi: 10.1111/bcp.13285] [Medline: 28276585]
48. Ene-Iordache B, Carminati S, Antiga L, Rubis N, Ruggenenti P, Remuzzi G, et al. Developing regulatory-compliant electronic case report forms for clinical trials: experience with the demand trial. J Am Med Inform Assoc 2009;16(3):404-408 [FREE Full text] [doi: 10.1197/jamia.M2787] [Medline: 19261946]
49. Fabrice B, Shai H, Tzipora H. Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation. In: 2018 IEEE International Conference on Cloud Engineering (IC2E). 2018 Presented at: 2018 IEEE International Conference on Cloud Engineering (IC2E); April 17-20, 2018; Orlando, FL URL: http://paperpile.com/b/1Cd2iA/77nZK [doi: 10.1109/IC2E.2018.00069]

Abbreviations

CBTi: cognitive behavioral therapy for insomnia
IoT: internet of things
IP: Internet Protocol
JSON: JavaScript Object Notation
PoW: proof of work
SDK: software development kit
SHA: secure hash algorithm

Edited by P Zhang, K Clauson; submitted 24.01.19; peer-reviewed by YC Lin, W Schulz, MS Aslam; comments to author 25.02.19; revised version received 23.03.19; accepted 27.04.19; published 16.05.19

Please cite as:
Motohashi T, Hirano T, Okumura K, Kashiyama M, Ichikawa D, Ueno T
Secure and Scalable mHealth Data Management Using Blockchain Combined With Client Hashchain: System Design and Validation
J Med Internet Res 2019;21(5):e13385
URL: http://www.jmir.org/2019/5/e13385/
doi: 10.2196/13385
PMID: 31099337