Improving the data access control using blockchain for healthcare domain [version 1; peer review: awaiting peer review]

Olaosebikan Tahir Yinka¹, Su-Cheng Haw¹, Timothy Tzen Vun Yap¹, Samini Subramaniam²

¹Faculty of Computing & Informatics, Multimedia University, Cyberjaya, Selangor, 63100, Malaysia
²AirAsia Berhad, KLIA2, Selangor, 64000, Malaysia

Abstract
Introduction
Unauthorized access to data is one of the most significant privacy issues that hinder most industries from adopting big data technologies. Even though specific processes and structures have been put in place to deal with access authorization and identity management for large databases nonetheless, the scalability criteria are far beyond the capabilities of traditional databases. Hence, most researchers are looking into other solutions, such as big data management. Methods
In this paper, we firstly study the strengths and weaknesses of implementing cryptography and blockchain for identity management and authorization control in big data, focusing on the healthcare domain. Subsequently, we propose a decentralized data access and sharing system that preserves privacy to ensure adequate data access management under the blockchain. In addition, we designed a blockchain framework to resolve the decentralized data access and sharing system privacy issues, by implementing a public key infrastructure model, which utilizes a signature cryptography algorithm (elliptic curve and signcryption). Lastly, we compared the proposed blockchain model to previous techniques to see how well it performed.
Results
We evaluated the blockchain on four performance metrics which include throughput, latency, scalability, and security. The proposed blockchain model was tested using a sample of 5000 patients and 500,000 observations. The performance evaluation results further showed that the proposed model achieves higher throughput and lower latency compared to existing approaches when the workload varies up to 10,000 transactions.
Discussion
This research reviews the importance of blockchains as they provide infinite possibilities to individuals, companies, and governments.

**Keywords**
Blockchain, Healthcare datasets, Chaincode, Directed Acyclic Graph, Access Control.

This article is included in the Research Synergy Foundation gateway.


Introduction
The US social insurance system, such as healthcare, is gradually obtaining digital medical information, thanks to the fast-expanding availability of data which will considerably build up the number of medical information collected securely. Furthermore, a change in perspective in the medical services sector has seen the new trend of computerizing medical records. The medical services sector is therefore rapidly rising in data volume as far as randomness and simplicity are concerned. Although the public healthcare sector is struggling with the magnitude of big data, security and privacy concerns are converging as threats and vulnerabilities grow.

The modern and revolutionary technology to build safer, more private, and interoperable health systems, blockchain technology has proven to be efficient. The aim of this paper is to propose a decentralized model for sharing and storing medical information utilizing blockchain technology to ensure security, preserving complete privacy, and allowing the owner to be completely in control of their data. In this research, additional efforts were made to harness and itemize all blockchain technology technical tools and the current influence of this developing technology on healthcare and industry.

Recent studies in the healthcare sector dealing with issues of scalability have used blockchain. Nonetheless, the application of blockchain in these studies was limited to the healthcare dataset index and the storage of verified transaction by endorsing peers. In contrast to these approaches, the current blockchain model poses the storage of all medical datasets in blockchain and also improving data throughput limitations. In light of these proposed improvements, Yang et al. proposed the use of blockchain as an index of a medical dataset and a list of user’s information. Similarly, Daraghmi et al. introduced a data-sharing and access authentication scheme based on a private blockchain. Likewise, Genestier et al. offered a novel proposal for reshaping healthcare permission monitoring using blockchain technology and allow users to access their entire health record data. In their implementation, there is no permission settings and no access restriction. MedRec is a software system developed using blockchain technology by the MIT media lab to handle electronic health records. They created a hospital management system that responds to four major issues: disjointed, delayed access to health care information; process compatibility; respect for autonomy; and enhanced data quantity and quality for clinical research.

Medical Chain project began in 2016, with the launch of the first model in mid-2017. Later in 2017, a partnership with the Linux Foundation was created. In the early months of 2018, a beta version of the program was published. The primary objective is to develop a single, accurate version of the user's health data.

MedBlock, which is architecture based on a hybrid blockchain to protect Electronic Medical Records (EMRs). Their design nodes identify them as endorsers, orderers, and committers. Yet, the access control strategy to allow third-party researchers access to medical data is not specified precisely.

Xia et al. introduced the Blockchain-Based Data Sharing (BBDS) system allowing owners and participants to access EMR from a shared repository theory based on positive identity and key verification.

Diversely, other research projects related to adopting blockchain in the healthcare domain are summarized as follows.

Blockchain Health, ASTRI and Bloq allow users to use the integrated platform to share health data with researchers, which creates a tamper-proof knowledge custody chain. Similarly, HIE of One is a blockchain software initiative that provides resources for patients to access their own records. Hyperledger and IBM Blockchain is hyperledger fabric’s first regulated platform, allowing the development of company blockchain platforms that users can monitor and spread through various organizations.

All the principal functions of blockchain technology and some true blockchain applications in healthcare were discussed at this point. More concretely, issues addressed in this chapter include authentication management, identity management, and cryptography. In the next section we will clarify the model that helps to illustrate how the blockchain network communicates with the developed model.

The paper contributions are summarized as follows:

1. A file storage and sharing system for a pure decentralized network utilizing blockchain technology is proposed.
2. An extensive evaluation of the proposed system, which demonstrated that our proposed system achieves higher throughput and lower latency compared to some existing approaches at higher work-load varied up to 10,000 transactions.
Methods

The overall data storage workflow is displayed in Figure 1 based on the following steps:

1. A user joins through the graphical user interface (GUI) and the request for permission to access information can be inserted into the network when successfully authenticated.
2. The user's request is sent to the cloud server by the GUI.
3. The blockchain component, the server query enabled, or revoked access.
4. The blockchain component handles content verification, signing, and encryption via Public Key Infrastructure (PKI).
5. Finally, data updated/stored with the authenticated token takes place.

From Figure 1, steps (a) to (f) depict the procedures for accessing a data source:

a. A user authenticates using the GUI. Upon successful authentication, user input will be taken into the system.

b. Through the GUI, user input is forwarded to the cloud server.

c. The cloud server then run queries against the blockchain for the user's access token by running the proposed PKI algorithm.

d. The access token retrieved is been decrypted with the appropriate user keys.

e. Data access is granted and retrieved with the help of a database connector.

f. The server returns updates to display data in a format that is readable to the user.

Case study: implementing the proposed model prototype to healthcare

We first analyzed a case study concerning the healthcare domain. We will then describe each of the key components in the case studies: (i) join function, (ii) content authentication function, and (iii) secure content access function.

The whole scheme works as follows. Consider a healthcare scenario of file storing and sharing. For each transaction, the ‘patient’ provides the contents to be stored and accessed. The ‘hospital administrator’ and ‘doctor’ request access to these contents. We assume that ‘hospital administrator’ and ‘doctor’ use our proposed model (see Figure 1), acting as the search mechanism to engage in the process of searching for content.
The join function: Let us consider a contrary of the scenario described above, if the doctor has no clearance of access, the doctor is, therefore, unable to access the desired content. In this case, by initiating the join function (Algorithm 1), the content provider can update the doctor’s clearance or refuse the proposal.

As shown in Algorithm 1 below, the identity is made up of signature key-pairs marked as SK for Bob and Alice, with reference pointers to the keys represented by RPSK. A public key denoted as PK is used to encrypt (and decode) the data, ensuring that the data is secured from all other players in the system.

The content authentication function: In the same scenario described earlier in the join function, once the ‘user’ has access to the desired content, the ‘user’ must verify their authenticity with the content authentication function, this is done on the blockchain (Algorithm 2).

Parse(x), also known as xp, is an auxiliary function that de-serializes a transaction’s message, which includes the parameters. As seen in Algorithm 2, POLICYCHECK (PKK, xp) checks that the originator has the proper permissions. Memory on the blockchain, indicated by the letter “M”: We’ll call M the blockchain memory space, which can hold suitably big documents and is represented by the hashtable L: \{0, 1\}256 \rightarrow \{0, 1\} N, where N >> 256.

The secure content access function: Consider a situation where a ‘user’ wishing to use our model to access the desired content. The built model includes access chaincodes that record on the blockchain database all ‘user’ activities, such as, record of shared data or records of information access history. Similarly as proposed by, Algorithm 3 is executed when read/write transaction access is requested.

As described earlier in this section, this architecture was designed for secure, scalable storage and data sharing in healthcare. The hyperledger network system is a permissioned blockchain implementation, providing unique properties suitable for implementing our proposed model. It runs chaincodes written in Java and Go programming language. The proposed model also supports data transaction validation applications and a plug-in consensus validation protocol. It is also important to note that hyperledger fabric collaboration network utilized consensus validation entities of a different kind, such as clients, ordering service nodes, and peer nodes, which belong to various participating entities or organizations.

Experimental evaluations and results
In the evaluations, we observed the various experimental evaluations conducted for Hyperledger fabric. In the experiment, we considered scenarios where a client or user sends ‘N’ transactions of a certain type ‘f’ to the blockchain

---

Algorithm 1. Join function (creating identity).

```plaintext
1: procedure JOINFUNCTION (Alice, Bob)
2: Alice executes:
3:   SKAlice \rightarrow RPAlice
4:   EncRPSK_{Alice} = enc (PKBob, RPSK_{Alice})
5:   Alice shares EncRPSK_{Alice} with Bob
6: Bob executes:
7:   PKBob \rightarrow RPBob
8:   Bob shares PKBob with Alice
9: return EncRPSK_{Alice}
10: end procedure
```

Algorithm 2. Content authentication against blockchain.

```plaintext
1: procedure POLICYCHECK (PKk, xp)
2: Bob = False
3: a_{policy} = H (PKk)
4: if M \[a_{policy}\] \neq \text{null then}
5: PK_{Alice}, PK_{Bob}, POLICY_{Alice}, Parse(M \[a_{policy}\])
6: if PKk = PK_{Alice} or
7: (PKk = PK_{Bob} and xp \in POLICY_{Alice, Bob}) then
8: Bob = True
9: end if
10: end if
11: end procedure
```
in an asynchronous manner. The number of requests is set from 1000 to 10,000 transactions, with increments of 1000 transactions in-between them, a sample digitized data collection, namely OpenMRS that consists of 5000 patients and 500,000 observations is used for our evaluation (see Table 1). Our proposed approach was benchmarked against approaches proposed by4,5 for fair comparison.

Case study: implementing the proposed model prototype to healthcare

Figure 2 depict the average latency across specific block sizes, analyzing various datasets or arrival rates of transactions. From Figure 2, we made several observations. This include the average latency in our approach is almost two-times less than that of the average latency in both approaches by4,5 for all block sizes, except for when the transaction is at 1000 TX, we saw that latency of all approaches are lower. This is because the volume of pending transactions at validation stage grew on high count which affected commit latency.

Evaluating the impact of endorsement policy

Figure 3 depict the average latency time of endorsement policy with the various number of transactions per second (TPS) (for the number of transactions ranging from 1000 to 10000). From Figure 3, it can be observed that the number of sub-policies and the number of signature validation has caused high latency for the join, content authentication and secure content access functions in4,5 approaches.

Impact of state database

We study the throughput and latency over varying transaction arrival rates for database utilized in the three approaches with different transaction complexity.

From Figures 4 and 5, shows that as transaction arrival increased for read/write only complexity, the throughput increased and latency decreased. This was observed while utilizing CouchDB as the state database.

The result shows that GoLevelDB performance was better than CouchDB with respect to ledger database. The reason behind the relatively good performance is the existence of key-value state database embedded in the peer mechanism.

<table>
<thead>
<tr>
<th>Table 1. Experiment parameters.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evaluation parameters</strong></td>
</tr>
<tr>
<td>Transactions/Queries submitted</td>
</tr>
<tr>
<td>Block sizes</td>
</tr>
<tr>
<td>Transaction in byte</td>
</tr>
<tr>
<td>The stored health records</td>
</tr>
</tbody>
</table>
Figure 2. Average latency with block size of 200–400 on various transaction arrival rates.

Figure 3. Average latency time of 4–8 peers on endorsement policy.

Figure 4. Throughput of 5000–10000 transaction arrival rate with read/write transaction.
Discussion

The performance evaluation results further showed that the proposed model achieves higher throughput and lower latency compared to existing approaches when the workload varies up to 10,000 transactions.

It's also worth noting that the proposed model preserves confidentiality and security by controlling transactions with timed-based chaincodes. The use of sophisticated encryption maintains security and access control.

Security and access control are maintained by the adoption of advanced encryption (such as the proposed hybrid PKI) and authentication methods that defend against adversarial efforts to change unwanted entry when issuing encryption information to verify and validate transactions to network users.

Conclusions

We had presented a model, which describes the interaction between a blockchain network and the designed model. To ensure a safe and private environment to communicate and store health data, the designed model exploits the most significant elements of blockchain technology while suppressing features that are not significant. In future work, we expect to perform refined simulations so that our model is tested more rigorously. We could do this by downloading and testing a wider range of various blockchain frameworks in a verified setting, for instance, using the blockchain instance of Amazon Web Services' blockchain.

Author contributions

Olaosebikan Tahir Yinka constructed the prototype and conducted the experimental evaluations under the guidance of his supervisors, Su-Cheng Haw and Timothy Tzen Vun Yap. Samini Subramaniam is the external collaborator while Su-Cheng Haw is the corresponding author for this paper.

Data availability

No data are associated with this article.

Software availability

- Source code available from: https://github.com/captaintaheer/Solution_Code
- Archived source code at time of publication: https://doi.org/10.5281/zenodo.5226652
- License: Data are available under the terms of the Creative Commons Attribution 4.0 International license (CC-BY 4.0).

Ethics approval

Ethical approval was given by the ethical approval board of Multimedia University, with number: EA1762021.
<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>15. Distributed ledger technology and blockchain. World Bank. Reference Source</td>
</tr>
</tbody>
</table>
The benefits of publishing with F1000Research:

- Your article is published within days, with no editorial bias
- You can publish traditional articles, null/negative results, case reports, data notes and more
- The peer review process is transparent and collaborative
- Your article is indexed in PubMed after passing peer review
- Dedicated customer support at every stage

For pre-submission enquiries, contact research@f1000.com