Check for updates

RESEARCH ARTICLE

REVISED Improving the data access control using blockchain for healthcare domain [version 3; peer review: 2 approved]Olaosebikan Tahir Yinka¹, Su-Cheng Haw¹, Timothy Tzen Vun Yap¹, Samini Subramaniam²¹Faculty of Computing & Informatics, Multimedia University, Cyberjaya, Selangor, 63100, Malaysia²AirAsia Berhad, KLIA2, Selangor, 64000, Malaysia

v3 First published: 08 Sep 2021, 10:901
<https://doi.org/10.12688/f1000research.72890.1>
 Second version: 27 Oct 2021, 10:901
<https://doi.org/10.12688/f1000research.72890.2>
 Latest published: 19 Nov 2021, 10:901
<https://doi.org/10.12688/f1000research.72890.3>

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.

Open Peer Review**Approval Status** ✓ ✓

	1	2
version 3		
(revision)		
19 Nov 2021		
version 2		
(revision)	✓	✓
27 Oct 2021	view	view
	↑	
version 1	?	
08 Sep 2021	view	

1. **Huo Chong Ling**, Curtin University Malaysia, Miri, Malaysia

2. **Heru Agus Santoso** , Dian Nuswantoro University, Semarang, Indonesia

Any reports and responses or comments on the article can be found at the end of the article.

Keywords

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

This article is included in the **Research Synergy Foundation** gateway.

This article is included in the **Health Services** gateway.

Corresponding author: Su-Cheng Haw (sucheng@mmu.edu.my)

Author roles: **Tahir Yinka O:** Conceptualization, Formal Analysis, Investigation, Methodology, Validation, Writing – Original Draft Preparation; **Haw SC:** Project Administration, Supervision, Writing – Review & Editing; **Yap TTV:** Supervision, Writing – Review & Editing; **Subramaniam S:** Writing – Review & Editing

Competing interests: No competing interests were disclosed.

Grant information: The author(s) declared that no grants were involved in supporting this work.

Copyright: © 2021 Tahir Yinka O *et al.* This is an open access article distributed under the terms of the **Creative Commons Attribution License**, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

How to cite this article: Tahir Yinka O, Haw SC, Yap TTV and Subramaniam S. **Improving the data access control using blockchain for healthcare domain [version 3; peer review: 2 approved]** F1000Research 2021, 10:901 <https://doi.org/10.12688/f1000research.72890.3>

First published: 08 Sep 2021, 10:901 <https://doi.org/10.12688/f1000research.72890.1>

REVISED Amendments from Version 2

In the version 3, we have re-organised the algorithms (Algorithm 3 and 4) to ensure clearer description. In addition, we have also restructured and elaborated on the analysis of the impact of block sizes and transaction arrival rate. As the number of transactions and block size increases, the average latency for all approaches go higher, and the difference in average latency in all approaches are more noticeable. It can be seen most obviously especially as the block size increases, the number of transaction arrival rate increases from 5,000 to 10,000 transactions. This is because the volume of pending transactions at validation stage grew on high count which affected commit latency. Lastly, we have elaborated further on the role of blockchain framework to resolve decentralised access and authentication control in the discussions section.

Any further responses from the reviewers can be found at the end of the article

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.¹ 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.^{2,3}

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 transactions by endorsing peers. In contrast to these approaches, the current blockchain model proposes the storage of all medical datasets in blockchain and also improving data throughput limitations. In light of these proposed improvements, Yang *et al.*⁴ proposed the use of blockchain as an index of a medical dataset and a list of user's information. Similarly, Daraghmi *et al.*⁵ introduced a data-sharing and access authentication scheme based on a private blockchain. Likewise, Genestier *et al.*⁶ 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. MedRec⁷ 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 Chain⁸ 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,⁹ 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.*¹⁰ 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,¹¹ ASTRI¹² and Bloq¹³ allow users to use the integrated platform to share health data with researchers, which creates a tamper-proof knowledge custody chain. Similarly, HIE of One¹⁴⁻¹⁶ is a blockchain software initiative that provides resources for patients to access their own records. Hyperledger¹⁷ and IBM Blockchain¹⁸ 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 workload 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.

Figure 1. Overall framework of proposed system.

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 $N \gg 256$.

The secure content access function: Consider a situation where a ‘user’ wishes to use our model to access the desired content. The built model includes access chaincodes that record all ‘user’ activities on the blockchain server, such as records of shared data or records of information access history. Similarly as proposed by,¹⁹ [Algorithm 3](#) is executed when read/write transaction access is requested. We utilized the regular expression to access the distributed hash like a standard hashtable in lines 4 - 5 and 9 - 12 of [Algorithm 3](#). By doing this, we were able to establish an off-blockchain read and write interactions for transactions sent to the distributed hash.

Algorithm 1. Join function (creating identity).

```

1: procedure JOINFUNCTION (Alice, Bob)
2:   Alice executes:
3:      $SK^{Alice} \leftarrow RP^{Alice}$ 
4:      $EncRPSK^{Alice} = enc(PK^{Bob}, RPSK^{Alice})$ 
5:     Alice shares  $EncRPSK^{Alice}$  with Bob
6:   Bob executes:
7:      $PK^{Bob} \leftarrow RP^{Bob}$ 
8:     Bob shares  $PK^{Bob}$  with Alice
9:   return  $EncRPSK^{Alice}$ 
10: end procedure
```

Algorithm 2. Content authentication against blockchain.

```

1: procedure POLICYCHECK ( $PK^K, x_p$ )
2:   Bob  $\leftarrow$  False
3:    $a_{policy} = H(PK^K)$ 
4:   if  $M[a_{policy}] \neq \text{null}$  then
5:      $PK^{Alice}, PK^{Bob}, POLICY^{Alice}, Parse(M[a_{policy}])$ 
6:     if  $PK^K = PK^{Alice}$  or
7:      $(PK^K = PK^{Bob} \text{ and } x_p \in POLICY^{Alice, Bob})$  then
8:       Bob  $\leftarrow$  True
9:     end if
10:  end if
11: end procedure
```

Algorithm 3. Content access function (read/write function).

```

1: procedure RWTX ( $PK^K$ ,  $m$ )
2:    $c, x_p, rw = \text{Parse}(m)$ 
3:   if PolicyCheck ( $PK^K, x_p$ ) = 1 then
4:      $PK^{Alice}, PK^{Bob}, \text{POLICY}^{Alice, Bob} \leftarrow \text{Parse}(M[H() PK^{Alice}])$ 
5:      $a_{xp} = H(PK^{Alice} || x_p)$ 
6:     if  $rw = 0$  then
7:        $hc = H(c)$ 
8:        $M[a_{xp}] \leftarrow M[a_{xp}] \cup hc$ 
9:       (DHT)  $ds[h_c] \leftarrow c$ 
10:      return  $h_c$ 
11:     else if  $c \in M[a_{xp}]$  then
12:       (DHT) return  $ds[h_c]$ 
13:     end if
14:   end if
15:   return 0
16: end procedure

```

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. Similar to Shadab et al., 2021²⁰ 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, all algorithms run on the same PC, 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 in an asynchronous manner. Between 1000 to 10,000 transactions were asynchronously sent to the blockchain server. The number of run transaction requests is set from 1000 to 10,000 transactions, with increments of 1000 transactions for every run a sample digitized data collection, namely OpenMRS that consists of 5000 patients and 500,000 observations is used for our evaluation. We have study latency and throughput up to 600blocks in the thesis presented for the work (see Table 1). We benchmarked the proposed model against approaches proposed.^{4,5} Also, all algorithms run on the same evaluation PC for a 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 average latency in both approaches by^{4,5} for all block sizes, except for when the transaction is at 1000 TX, we saw that latency of all approaches are lower. Further observations shows that, as the number of transactions and block size increases, the average latency for all approaches go higher, and the difference in average latency in all approaches are more noticeable. It can be most obvious especially as the block size increases, the number of transaction arrival rate increases from 5,000 to 10,000 transactions. 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

Table 1. Experiment parameters.

Evaluation parameters	Evaluation values
Transactions/Queries submitted	1000, 2000, 300, 4000, 5000, 6000, 7000, 8000, 9000 and 10,000
Block sizes	200, 400, 600
Transaction in byte	1,000–10,000
The stored health records	10,000–100,000

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.

Figure 5. Latency of 5000–10000 transaction arrival rate with read/write transaction.

sub-policies and the number of signature validation has caused high latency for the join, content authentication and secure content access functions in ^{4,5} 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.

Discussion

By implementing the proposed model and incorporating it with blockchain technologies, the proposed model makes tough reference pointers for heterogeneous databases and trades these pointers rather than real information by means of the blockchain part. This approach can overcome service provider limitations for medical imaging centers or hospitals in rural areas in particular by enabling scalable data sharing without requiring data to be uploaded to some other centralized repository, whereby other parties may share and retrieve data.

The proposed model also ensures exhaustive attention is given to efficiency and effectiveness. In addition, the proposed model creates authentication tokens that are linked to each participating care agency (service manager or organization) as electronic health identities.

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>²¹
- **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.

References

1. Zyskind G, Nathan O, Pentland A: *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. IEEE Security and Privacy Workshops; 2015.
2. Aljawarneh S, Yassein MB, Talafha WA: **A resource-efficient encryption algorithm for multimedia big data**. *Multimedia Tools and Applications*. 2015; **76**(21): 22703–22724.
[Publisher Full Text](#)
3. Hilbert M: **Big Data for Development: A Review of Promises and Challenges** Development Policy Review. 2015; **34**(1), pp. 135–174.
[Publisher Full Text](#)
4. Yang J, Onik M, Lee N, et al.: **Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making**. *Appl. Sci.* 2019; **13**70.
[Publisher Full Text](#)
5. Daraghmi E-Y, Daraghmi Y-A, Yuan SM: **MedChain: A Design of Blockchain-based System for Medical Records Access and Permissions Management**. *IEEE Access*. 2019; 1–1.
[Publisher Full Text](#)
6. Genestier P: **Blockchain for consent management in the eHealth environment: A nugget for privacy and security challenges**. *J. Int. Soc. Telemedicine eHealth*. 2017, April; **5**: 1–4.
7. Azaria A, Ekblaw A, Vieira T, et al.: **MedRec: Using blockchain for medical data access and permission management**. *2nd Int. Conf. Open Big Data*. Aug. 2016; (p. 2530).
8. Albeyatti A, Tayeb M, Yin A, et al.: **Medicalchain (Whitepaper)**. 2018; pp. 1–42.
9. Chen M, Qian Y, Chen J, et al.: **Privacy Protection and Intrusion Avoidance for Cloudlet based Medical Data Sharing**. *IEEE Transactions on Cloud Computing*. 2016; **1**(1).
[Publisher Full Text](#)
10. Amofa S, Sifah EB, Agyekum KO-B, et al.: **A blockchain-based architecture framework for secure sharing of personal health data**. *IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*. 2018; **16**.
[Publisher Full Text](#)
11. ASTRI: **Whitepaper on Distributed Ledger Technology**. 2016.
[Reference Source](#)
12. Culver K: *Blockchain technologies: A whitepaper discussing how the claims process can be improved*. Workshop: ONC/NIST Use Blockchain Healthcare Res; 2016.
13. Genestier P: **Blockchain for consent management in the eHealth environment: A nugget for privacy and security challenges**. *J. Int. Soc. Telemedicine eHealth*; 2017, April; **5**: 1–4.
14. Gropper A, MD: **Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT**. H N, S K, H G2017.
15. **Distributed ledger technology and blockchain**. *World Bank*.
[Reference Source](#)
16. T L: **Foundation Hyperledger Overview**. 2018.
17. Dagher GG, Mohler J, Milojkovic M, et al.: **Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology**. *Sustain. Cities Soc.* 2018, May; **39**: 283297.
[Publisher Full Text](#)
18. Guo R, Shi H, Zhao Q, et al.: **Secure attribute-based signature scheme with multiple authorities for blockchain in electronic healthrecords systems**. *IEEE Access*. 2018; **6**: 1167611686.
[Publisher Full Text](#)
19. Aazam M, Zeadally S, Harras KA: **Health fog for smart healthcare**. *IEEE Consum Electron Maga*. 2020; **9**(2): 96–102.
[Publisher Full Text](#)
20. Shadab A, F AR, S MZHKKR, et al.: **Towards Trustworthiness of Electronic Health Record system using Blockchain**. *Annals of the Romanian Society for Cell Biology*. 2021; **25**(6): 2425–2434.
[Reference Source](#)
21. Olaosebikan, Tahir Y, Su-Cheng H, et al.: **Improving the data access control using blockchain for healthcare domain (Version v1) [Data set]**. *Zenodo*. 2021.
[Publisher Full Text](#)

Open Peer Review

Current Peer Review Status:

Version 2

Reviewer Report 09 November 2021

<https://doi.org/10.5256/f1000research.78587.r97373>

© 2021 Santoso H. This is an open access peer review report distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Heru Agus Santoso

¹ Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia

² Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia

The paper intended to show the advantage of blockchain to improve data access control for the healthcare domain. The goal is to provide a blockchain framework to resolve decentralised access and authentication control. However, in my opinion, the paper needs some clarifications in regards to data analysis and text:

1. You said Algorithm 3 and 4 run on the same evaluation PC, but I didn't find Algorithm 4 in the text.
2. Algorithm 3 hasn't been explained adequately, especially in lines 4-5; and returned values in lines 10 and 12, what is the difference between the two?
3. In the sense of statistical analysis and interpretation, you said the latency was getting lower because the volume of pending transactions grew high? This needs a clear explanation.
4. Add the point of blockchain framework to resolve decentralised access and authentication control in the discussions.

Is the work clearly and accurately presented and does it cite the current literature?

Yes

Is the study design appropriate and is the work technically sound?

Yes

Are sufficient details of methods and analysis provided to allow replication by others?

Yes

If applicable, is the statistical analysis and its interpretation appropriate?

Partly

Are all the source data underlying the results available to ensure full reproducibility?

Yes

Are the conclusions drawn adequately supported by the results?

Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Database, ontology, information retrieval

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.

Author Response 17 Nov 2021

Haw Su Cheng .

The paper intended to show the advantage of blockchain to improve data access control for the healthcare domain. The goal is to provide a blockchain framework to resolve decentralised access and authentication control. However, in my opinion, the paper needs some clarifications in regards to data analysis and text:

- You said Algorithm 3 and 4 run on the same evaluation PC, but I didn't find Algorithm 4 in the text.

Response: *Corrected. We have re-organised the algorithms (Algorithms 3 and 4) to ensure a clearer description.*

-
- Algorithm 3 hasn't been explained adequately, especially in lines 4-5; and returned values in lines 10 and 12, what is the difference between the two?

Response: *Corrected. We have elaborated further in the description.*

-
- In the sense of statistical analysis and interpretation, you said the latency was getting lower because the volume of pending transactions grew high? This needs a clear explanation.

Response: *Corrected. This analysis has been restructured and explained in detail in the revised version.*

-
- Add the point of blockchain framework to resolve decentralised access and authentication control in the discussions.

Response: *Corrected. This has been addressed in the revised version.*

Competing Interests: No competing interests were disclosed.

Reviewer Report 02 November 2021

<https://doi.org/10.5256/f1000research.78587.r98039>

© 2021 Ling H. This is an open access peer review report distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Huo Chong Ling

¹ Department of Electrical and Computer Engineering, Curtin University Malaysia, Miri, Malaysia

² Department of Electrical and Computer Engineering, Curtin University Malaysia, Miri, Malaysia

The authors have addressed all the comments. I have no further comments.

Is the work clearly and accurately presented and does it cite the current literature?

Partly

Is the study design appropriate and is the work technically sound?

Partly

Are sufficient details of methods and analysis provided to allow replication by others?

Partly

If applicable, is the statistical analysis and its interpretation appropriate?

Partly

Are all the source data underlying the results available to ensure full reproducibility?

Partly

Are the conclusions drawn adequately supported by the results?

Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Security

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.

Version 1

Reviewer Report 08 October 2021

<https://doi.org/10.5256/f1000research.76499.r94763>

© 2021 Ling H. This is an open access peer review report distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Huo Chong Ling

¹ Department of Electrical and Computer Engineering, Curtin University Malaysia, Miri, Malaysia

² Department of Electrical and Computer Engineering, Curtin University Malaysia, Miri, Malaysia

³ Department of Electrical and Computer Engineering, Curtin University Malaysia, Miri, Malaysia

The authors proposed a decentralized network using blockchain technology to store and share health data securely by adopting a PKI model in their blockchain framework. The PKI model consists of content verification and authentication and secure access. Experiments were conducted to evaluate the performance of the proposed blockchain framework in terms of throughput, latency, scalability, and security, and compared to existing approaches in the literature. The experiments showed promising results, which indicate the feasibility of the framework to be used in the healthcare domain.

However, there are a few doubts regarding the statistical analysis of the experimental results as follows:

1. Do the results obtained consist of the average of several runs or just one run?
2. Are the algorithms used in [4] and [5] implemented as well on the same PC that is used for the proposed approach? This is to ensure fair performance evaluation.
3. The latency results showed the average for the block size of 200-400. How about the latency results for the block size of 400 and above?

Other comments on the article are as follows:

- The year of publication for Yang *et al.* is 2019, but in your figures, it is shown as 2018.
- It's better to write "Proposed approach" instead of "My approach" in the figures.
- Reference 20 is not cited in the text.

Is the work clearly and accurately presented and does it cite the current literature?

Yes

Is the study design appropriate and is the work technically sound?

Yes

Are sufficient details of methods and analysis provided to allow replication by others?

Yes

If applicable, is the statistical analysis and its interpretation appropriate?

Partly

Are all the source data underlying the results available to ensure full reproducibility?

Yes

Are the conclusions drawn adequately supported by the results?

Yes

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Security

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.

Author Response 22 Oct 2021

Haw Su Cheng .

- Do the results obtained consist of the average of several runs or just one run?

Author response: Yes, between 1000 to 10,000 transactions were asynchronously sent to the blockchain server. The number of requests is set from 1000 to 10,000 transactions, with increments of 1000 transactions for every run.

- Are the algorithms used in [4] and [5] implemented as well on the same PC that is used for the proposed approach? This is to ensure fair performance evaluation.

Author response: Yes, this was included in the proposed model access chaincodes, which record all 'user' activities, such as the record of shared data or information access history on the blockchain. Algorithm 3 is executed when transaction access is requested, and similarly, Algorithm 4 is executed for read/write transactions.

- The latency results showed the average for the block size of 200-400. How about the latency results for the block size of 400 and above?

Author response We have studied latency and throughput up to 600 blocks in the thesis presented for the work. Also, as stated in observations for all block sizes as for all block sizes, except for when the transaction is at 1000, we saw that latency of all approaches are lower.

Other comments on the article are as follows:

- The year of publication for Yang *et al.* is 2019, but in your figures, it is shown as 2018.

Author response: This has been adjusted in figures

- It's better to write "Proposed approach" instead of "My approach" in the figures.

Author response: This has been adjusted in figures as advised

- Reference 20 is not cited in the text.

Author response: Citation added.

Competing Interests: No competing interests were disclosed.

Comments on this article

Version 2

Reader Comment 01 Nov 2021

Getachew Gobena Amesgeha, Ambo University, Ambo, Ethiopia

I found this article valuable and believe it will contribute to data science use in health care. I recommend practitioners and academics for making use of this scholarly article. I also appreciate the Authors.

Getachew Gobena (Assistant Professor)

Competing Interests: I consent for the peer review, if any.

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

F1000Research