Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2022.024714
Article

Tech Science Press

Fog-based Self-Sovereign Identity with RSA in Securing IoMT Data

A. Jameer Basha[1], N. Rajkumar[2], Mohammed A. AlZain[3], Mehedi Masud[4] and Mohamed Abouhawwash[5,6,*]

[1]Department of Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore, 641032, India
[2]Department of Computer Science and Engineering, School of Engineering, Presidency University, Bangalore, 560064, India
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[5]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[6]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI, 48824, USA
*Corresponding Author: Mohamed Abouhawwash. Email: abouhaww@msu.edu

Received: 28 October 2021; Accepted: 05 February 2022

Abstract: In the healthcare applications, Internet of Medical Things (IoMT) comforts the communication processes between the medical devices and the humans *via* wireless network. Moreover, this communication helps both the physicians and the patients to contact remotely for the diagnosis of the disease's wearable devices sensor signals. However, IoMT system violates the privacy preserving of Patient's Health Record (PHR) as well as self-sovereign identity of patient. In this regard, security action should be taken. Previous techniques used in IoMT are in lack of data consistency, confidentiality, and inaccessible of data. To overcome these issues, the fog computing-based technology is used in order to handle the health data of the patient for digital identity management. Self-Sovereign Identity empowers the patient to handle and control their own data. This paper proposes Fog Computing based Self-Sovereign Identity with Rivest, Shamir, Adleman (RSA) for IoMT (FCSSI+RSA-IoMT). For that, it keeps the Patient Health Record (PHR) securely and effectively using RSA to make the identification and authentication procedures at ease. Besides, PHR is used to store the sensitive information regarding identity and privacy of the patient. Additionally, it records the diagnosis history of patient by the doctors and radiology images. Therefore, the result evaluation proves that, for 100 users, the proposed technique takes only 631 secs and also the throughput performance is better when compared to the existing techniques.

Keywords: Fog computing; self-sovereign identity; PHR; privacy; security; IoMT

1 Introduction

Fog computing is based on the decentralized model of security. Users in the decentralized model use the edge network for verifying the transaction of the network. In the network, all the transactions are stored in an open ledger for visibility of all participants. By this way fault transactions can be detected. In particular, the decentralized model security of data is high because the unauthorized users cannot interfere in the access of the database. Only authorized users can create, distribute and control PHR to health care providers [1]. IoMT is used in the medical field which interconnects multiple medical devices and its applications to provide medical service to the end user [2]. IoMT architecture connects the hardware devices and healthcare software devices that form the health IoMT system through nodes in the network. By the way, it can help the user in the means of decreasing the hospital appointments and get the service of e-health care by connecting the doctors to their patients and diagnosis the diseases [3].

IoMT based fog-based technology has provided many services such as managing diseases in the network, improving the health care services, analytics of health care data, and minimum cost of services. Based upon the survey of research on economics, IoMT domain in healthcare has raised to 120 billion $ by 2020 [4]. This paper [5] proposed the challenges in the identity management system in terms of IoMT, privacy preserving, access control of healthcare data. It also compares traditional identity management system regarding domain name service, authentication in decentralized, infrastructure of fog server, privacy and security. However, it does not cover the challenges in PHR which denotes IoHT [6]. By using Self-Sovereign Identities (SSI) concept, data ownership of dilemma can be overcome and allows the users grant permission in accessing the data, data control and revoking the access of data at any time [7]. The benefits of Decentralized Ledger Technologies (DLT) using fog server may face a problem in sharing the sensitive health information in a secured manner. Therefore, SSI ensures the healthcare parties of patient health data that it has their own control [8,9].

In order to overcome the issues such as insecure transmission of data in a high speed of processing, the proposed work based on fog computing driven Self-Sovereign Identity with RSA for IoMT (FCSSI+RSA-IoMT) is implemented. The benefits of the proposed work include accessing of patient data from various health centres which minimizes the diagnosis time, accessing of physicians in a faster pace, getting rapid treatment for the illness. PHR data is stored in the fog node with patient identity, name, health details, and radiology images. In addition to that, the privacy of patient is also be protected and distributed with other IoMT devices using fog server in a protected way. The main contributions of this work are:

1. Designing architecture of Self-Sovereign Identity of patient ID is presented with the details such as patient name, identity of patient, diagnosis of treatment, and radiology images.

2. Identity of doctor in SSI is also presented with the name of the physician with ID, details of specialists for particular details and by using the fog server, all PHR data are encrypted.

3. RSA is implemented in the verification of PHR data to facilitate the identification and authorization process.

4. IoMT based fog computing is used to evaluate the FCSSI+RSA-IoMT in terms of latency, throughput, fog node propagation time, consumption time using RSA.

The paper has been organized as follows: Section 2 describes the review of literature, Section 3 introduces the fog computing self-sovereign identity with RSA for IoMT (FCSSI+RSA-IoMT), Section 4 discusses the experimented results and Section 5 concludes the paper with future directions.

2 Review of Literature

The Internet of Medical Things (IoMT) is a system which connects the multiple nodes and each node is linked with IoMT wearable devices. Also, it enhances both the response time for medical treatment and the treatment quality of the particular patient [10]. Digital transformation of medical data in IoMT is connected to various devices and applications through wireless communication of the network, actuators, analysis of big data, sensors, and cloud-based computing. In the healthcare field, digital transformation has improved the delivery of medicine to the patient by continuous monitoring of the patient [11]. In recent years, several research works have been concerned with the challenges in sharing of medical data. In such case, managing the medical data using fog computing technology with fully functioned prototype is called “MedRec” [12]. The author Yue et al. analyzed the solution to get the medical records from health entities and act as a gateway to enable the patients as the owner of the medical record and grant privileges to choose their desired physicians and hospitals.

In PHR, patients have rights to access their medical and health data on the basis of demand. Exchanging of medical information between healthcare institutions requires consent from the patient. The features of Distributed Ledger Technology (DLT) are used in PHR [13]. Instead of using DLT as the decentralized structure, medical data can be stored in encrypted form by enhancing privacy and security of the users. However, in DLT, data accessing of the patient through any structure of the network is quite difficult. Moreover, the foundation of Internet of Healthcare Things (IoHT) is dependent on PHR. In the decentralized structure nodes of the network, RSA is implemented using fog server. Also, various fog computing technology has multiple procedures to run code in the structure of peer-to-peer network. Hyper-ledger fabric uses the similar concept of RSA which is termed as chain code. This chain code can be executed in the peer-to-peer network that process both internally and externally controlled by Docker container called as System Chain Code. The distributed software is run by the lightweight technology of Docker container. This Docker container allows to communicate with System Chain Code using `interfaces of “Get State” and Put State [14].

Preserving the medical data in a secured way using fog computing and encryption technique is implemented. For accessing the data, it needs decryption format only then the owner of the data can retrieve it from PHR [15]. Besides, the user can download the encrypted data and at the receiving side, the decryption key is used to receive the data *via* gateway architecture [16]. The sensitive medical information of the patient is encrypted and stored it in cloud storage; sharing is based on fog server. Moreover, only authorized users can have rights to access it [17]. RSA can run the fog nodes in the network and sharing of medical data can be carried out only with secret key. In accessing the data, it can be compared with the secret key only if it matches and then, the data will be retrieved from the storage area [18].

Aggregate signature is needed for providing high security of data, in which the individual signature of the patient is combined and forms a single length aggregate signature and only then the data will be accessed by the third party [19]. Likewise, the sequential aggregate signature was implemented using trapdoor permutations in the random oracle model [20]. Ontological scenario-based security is provided for IoMT framework [21]. The IoMT system provides fog-cloud storage of data and implements preserving the details in terms of privacy of the particular patient, authentication of the data. The main aim of saving data is from tamper-proof [22]. The decrypted data is stored in the IoMT nodes with different locations and fog server is used for transmitting the data in secure, and also maintains the integrity of data in file storage protocol. For example, the consensus algorithm is used in the PoW model for the distribution of power [23,24]. Tab. 1 shows the survey of the existing methods using fog server based IoMT.

Table 1: Survey of existing algorithms

Author Name	Description
Shamshad, S. et al. [25]	e-health records storage and sharing scheme
Bodkhe, et al. [26]	Blockchain for industry 4.0
Attaran, M. [27]	Personal healthcare-associated problems using block chain
Abu-Elezz, I. et al. [28]	security in blockchain
Liu, Y. et al. [29]	Blockchain-based identity management systems
Gorkhali, A. et al. [30]	Identity management based on a blockchain-supported association service

(Continued)

Table 1 (continued).

Author Name	Description
Cilliers, L. [31]	Mobile appliance created to gather medical information from body sensor nodes and also coordinates data for the cloud
McGhin, T. et al. [32]	Management of individual EHR using blockchain and provide authentication to the users.
Nguyen, D. C. et al. [33]	Security of EHR data and share through the mobile based cloud system.
Ismail, L. et al. [34]	Lightweight technology in blockchain of healthcare
Wang, S. et al. [35]	Sharing of PHR using Blockchain-based with data integrity verifiable
Balasubramanian, K. et al. [36]	Identity based encryption and decryption.
Sun, J. et al. [37]	Attribute-based encryption scheme for cloud storage using multi keyword search
Wagh, S. B. et al. [38]	Blockchain technology in securing health care data for medical research.
Ramani, V. et al. [39]	Accessing of data in a secured way using blockchain technology
Ying, Z. et al [40]	Preserving EHR data and sharing in the cloud.
Wang, H. et al. [41]	Attribute based crypto used for secured cloud based EHR system
Khan, K. M. et al. [42]	Digital voting system based on blockchain technology for securing data.
Es-Samaali, H. et al. [43]	Handling Big data using Blockchain-based access control.
Fan, K. et al. [44]	Sharing of medical data in MedShare system using blockchain technology.
D. Baars [45]	Self-Sovereign Identity using blockchain technology
N. Rifi et al. [46]	Accessing of medical data and granting permission using blockchain technology

The major drawbacks of the above techniques are in terms of high storage requirement, not addressing the unknown data access, high transaction time and high cost. The paper [47–66] describes more techniques on efficient and secured IoT data storage and transactions. Further, the proposed model overcomes all hitches of previous technologies and new fog computing methodology is suggested.

3 Proposed FCSSI+RSA-IoMT Methodology

Fog computing technology is based on decentralized security model. The medical data transfer between the healthcare institutions and the patient as per the need of patient. In such case, the patient has the ownership controls to access their health record on the basis of their demand. So, this patient-driven accessibility of health record is called as PHR. This proposed work is based on fog computing self-sovereign identity with Real Application Cluster (RAC) for IoMT in (FCSSI-IoMT). Fig. 1 shows the workflow of FCSSI+RSA-IoMT. Besides, this proposed work contains three phases.

Phase 1: Creation of patient self-sovereign identity in fog server.

Phase 2: Creation of doctor’s self-sovereign identity in fog server

Phase 3: validation using RSA

The characteristics of self-sovereign identity is given in the Fig. 2. For the ownerships, the individual user/patient’s identities are described below:

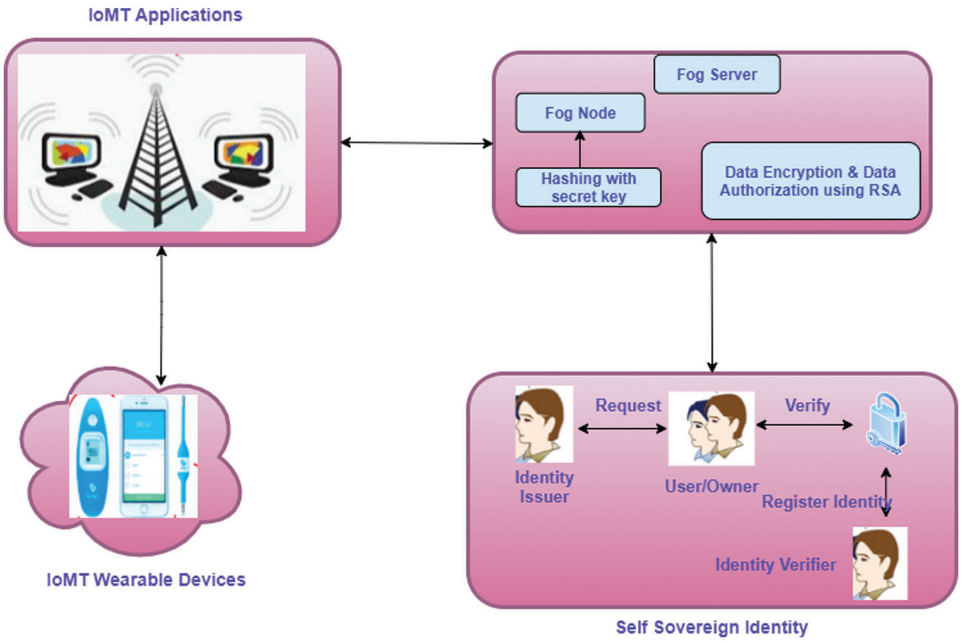

Figure 1: Workflow of FCSSI+RSA-IoMT

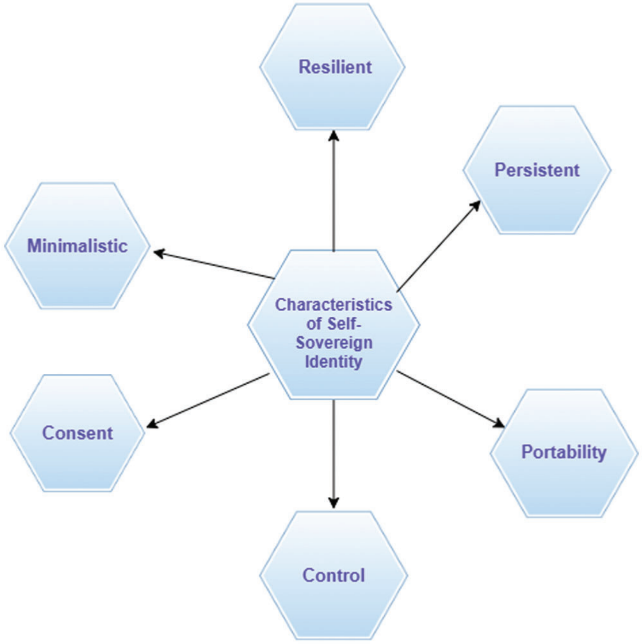

Figure 2: Characteristics of self-sovereign identity

Resilient : Verify the patient identity and accept if not remove the identity of the user
Persistent : Identity of the patient cannot be taken away from the user.
Portability : Services and information about the identities must be interoperability.
Control : Users control the identity of the patient.

Consent : User is ready to use patient's identity only if the user agrees to use the identities.

Minimalistic : Discloses the claims and identities which is needed as minimum for the task.

Security : Maintain confidentiality and privacy.

In this paper, Distributed Ledger Technology-based fog computing is focused, in which the patient identity with diagnosis treatment and radiology images are stored in fog node and added to the distributed ledger after the verification process [67]. Algorithm 2 implements the adding of fog node which contains patient identity in PHR.

```
Algorithm 1: RSA Algorithm
Input: $m, n$
Output: $j, e, k$
Step 1: Randomly select two large prime numbers $m$ and $n$.
Step 2: $j = m \times n$
Step 3: Compute $\varnothing(j) = (m - 1) \times (n - 1)$
Step 4: Select $1 < e < j$ such that $p$ is prime number to $\varnothing(j)$
Step 5: Evaluate $k = e^{-1} mod \varnothing$ (j)
Phase 1: Creation of patient Self-Sovereign Identity in fog server information
```

```
Algorithm 2: FCSSI+RSA-IoMT Patient identity and add fog node
Input: PHR Readings for a $patient(IoMT\_patient1)$
Output: Creation of $patient1$ identity and add information in the fog node
Step 1: Read $PHR \leftarrow Patient(IoMT\_patient1)$
Step 2: Use of Algorithm 1 generates Public Key and Private Key.
Step 3: For the encryption process $patient(IoMT\_patient1)$identity uses the public key. For the decryption process, use the private key and it is shared to the doctor's identity.
Step 4: Use of public key encrypts the $encrypt\_PHR \leftarrow PHR(IoMT\_patient1)$
Step 5: Generate the hash function for $encrypt\_PHR$.
Step 6: Generate Bilinear Map for $encrypt\_PHR$ with patient identity ($patient\_ID$)
Step 7: Generate a fog node for $patient(IoMT\_patient1)$ in the fog server using the patient's name, patient identity ($patient\_ID$) and password.
Step 8: $fognode \leftarrow encrypt\_PHR$ and hash value with Bilinear Map
Step 9: Add this fog node to $Patient(IoMT\_patient1)$ in the fog server.
```

For improving the security in PHR, the bilinear map is used in FCSSI+RSA-IoMT. The function of the bilinear map merges the two vector space elements and produce third elements of vector space with linear argument values. See Eq. (1).

$$P \times Q \rightarrow Y \tag{1}$$

Where, P is the first vector space, Q is the second vector space and Y is the third vector space. The implement of Algorithm 2 encrypts PHR as vector space P. The vector space Q is the identity of patient $patient\_ID$. The self-sovereign identity-based encryption technique is used to generate the bilinear map Y.

Phase 2: Creation of Doctor's Self-Sovereign Identity in fog server

Algorithm 3: FCSSI+RSA-IoMT doctor's identity into the fog server

```
Input: patient1 fog node from the patient fog server
Output: doctor_id fog node is added to the fog server.
Step 1: $fognode \leftarrow IoMT\_doctor\_id$ is able to access the $IoMT\_patient1$ health details from the patient fog node using private key.
Step 2: Retrieve $Block \rightarrow encrypt\_PHR$, and Hash value with BilinearMap from fog node
Step 3: Decrypt $encrypt\_PHR$ based on $PrivateKey \rightarrow PHR$
Step 4: Generate fog node for $Doctor(IoMT\_doctor\_id)$ fog server using doctor name, identity $(IoMT\_doctor\_id)$, and password.
Step 6: Place $fognode \leftarrow encrypt\_PHR$, and hash value with Bilinear Map
Step 7: Add this fog node to $Doctor(IoMT\_doctor\_id)$ in the fog server
Phase 3: Fog server verification using RSA (Algorithm 1)
```

In the fog server verification, check the identity of the patient in the fog node that is safe or not. Algorithm 4 explains the FCSSI+RSA-IoMT fog server verification algorithm using RSA. In the decentralized security model, which is based on fog server with RSA for IoMT contains the identity of the patient along with details of them, doctor, details of prescription, and radiology images. In the fog server, it creates one fog node for each patient.

Algorithm 4: FCSSI+RSA-IoMT fog server verification algorithm using RSA

```
Input: $Patient(IoMT\_patient1)$fog server
Output: Safe or not
Step 1: Access the fog server $fs$ of $Patient(IoMT\_patient1)$ from patient's fog node.
Step 2: if $sender\_ID == patient\_ID$ then
Step 3: $fs\_Status = "Safe"$
Step 4: FOR each fog node $fn$ from $fs$
Step 5: Retrieve $fognode \rightarrow encrypt\_PHR$, hash value with Bilinear Map from the patient's fog node
Step 6: Generate new hash value $new\_Hash \leftarrow encrypt\_PHR$.
Step 7: Generate new bilinear map value $new\_BilinearMap \leftarrow encrypt\_PHR$ with patient identity $patient\_ID$.
Step 8: IF $((hash == new\_Hash)\&(BilinearMap = new\_BilinearMap))$
Step 9: patient fog node is safe
Step 10: Data transmitted with fog-based RSA for IoMT in PHR
Step 11: ELSE
Step 12: patient fog node is not safe
Step 13: $fs\_Status = "NotSafe"$
Step 14: Break
Step 15: END FOR
Step 16: End
```

4 Result Analysis

This fog computing based Self-Sovereign Identity of PHR in the framework of IoMT is used to secure the sensitive information of the patient with confidentiality and maintaining consistency of PHR. In the fog server technology, a set of fog nodes contains the sensitive information of the patient, and it is identified by hash value. Each fog node is hashed and connected with another fog node so as to form a fog server. Tab. 2 shows the comparison of FCSSI+RSA-IoMT with several other related works.

Table 2: Comparison of FCSSI+RSA-IoMT in terms of characteristics

Characteristics	Ying, Z. et al. [30]	Ramani V. et al. [29]	Xia Q. I. et al. [34]	Liang X. et al. [47]	FCSSI+RSA-IoMT
Data Privacy	Yes	Yes	Yes	Yes	Yes
Data Availability	No	No	Yes	Yes	Yes
Data Integrity	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	No	Yes
Access in Decentralized	No	Yes	Yes	Yes	Yes
Flexibility	No	No	No	Yes	Yes

From Tab. 2, it is observed that the proposed work BCSSI-IoMT has performed better than the other existing works and it offers promising better solution in PHR application. The fog node with the decentralized security model using RSA enables the patients to manage and maintain their identity in a protected way. This allows user/owner to decide and share medical information in a secured means [48]. Self-Sovereign Identity needs no central control and leads to disclosure of identities. This FCSSI+RSA-IoMT work is evaluated using the following performance parameter.

4.1 Latency

Latency in FCSSI+RSA-IoMT has been calculated by analyzing the time taken to access a patient identity. The latency for FCSSI+RSA-IoMT is represented in Tab. 3.

Table 3: Latency for DVASE

Number of users request	Latency (Sec)
10	89.43
20	124.54
40	240.76
60	324.89
80	489.12
100	631.98

In the observation of latency in Tab. 3. If the request of the user gets increased to access the patient identity, the latency time also gets increased.

4.2 Throughput

In this parameter of performance, it is the rate at which valid transactions of IoMT medical data are committed by the fog server.

This throughput parameter is compared with fig server of centralized storage, and FCSSI+RSA-IoMT. Fig. 3 shows the comparison of throughput in the fog server with centralized using RSA and FCSSI+RSA-IoMT using RSA. See Eqs. (2)–(4),

$$transaction\,per\,node = (node\,size)/(average\,transaction\,size) \tag{2}$$

$$fraction\,of\,fog\,node\,per\,second = 1/(fog\,time\,in\,seconds) \tag{3}$$

$$transaction\,per\,fog\,node = transcation\ per\ node * fraction\ of\ node\,per\,second \tag{4}$$

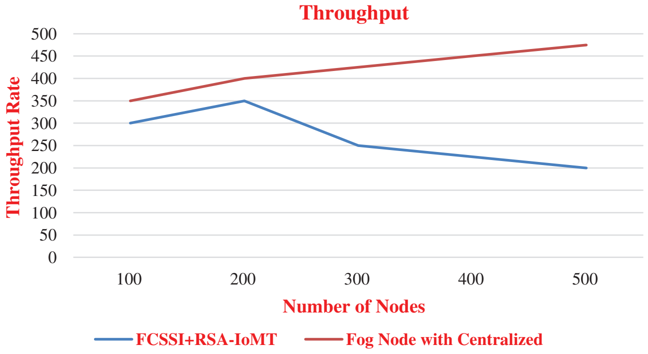

Figure 3: Throughput

This throughput parameter is compared with the fog server with centralized storage, and FCSSI+RSA-IoMT. Fig. 3 shows the comparison of throughput in the fog server with centralized using RSA and FCSSI +RSA-IoMT using RSA.

4.3 Fog Node Propagation Time (FPT)

It is the time taken for the distribution of new fog node with the majority set of nodes in the network. After the verification process using algorithm 4, each fog server from all nodes in the network calculates the propagation time of each node which is given in Fig. 4. FPT is the time required for a node to be distributed to most of the nodes in the network.

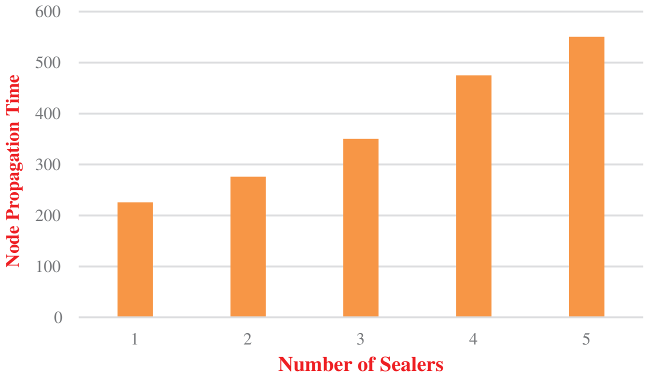

Figure 4: Performance of fog node propagation time

It can be observed from the Fig. 4 that the FPT is calculated by the number of sealers in the network. If a greater number of sealers available in the network, it increases the synchronization issues. It leads to higher propagation delay in the network. Fig. 5 shows the consumption of time for accessing PHR in FCSSI+RSA-IoMT using RSA *versus* centralized storage using RSA.

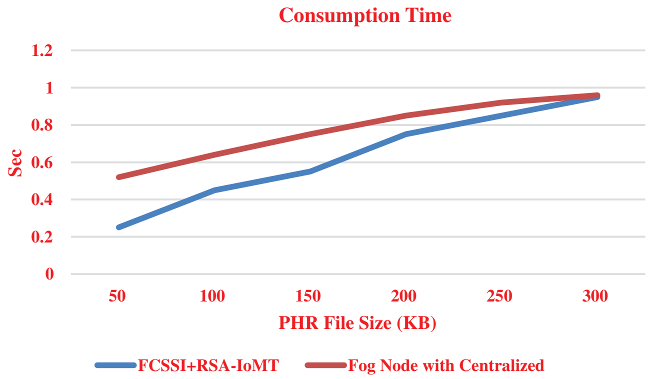

Figure 5: Consumption time of FCSSI+RSA-IoMT using RSA

It can be observed from Fig. 5 that the time consumption of accessing the data of PHR from requesting to receive the medical data. In centralized storage, PHR data are stored. If a patient wants to access PHR, it creates identity for the patient (patient_ID) and the time taken to create the identity is T1, then the request is sent to the centralized server. After receiving the request of PHR from patient ID centralized server, it transmits to the corresponding patient identity at time T2. Time consumption for accessing PHR data is T2-T1 seconds. Depending upon the PHR size consumption, the time gets varied. If PHR file size is large, the time consumption for accessing the request is also high. In FCSSI+RSA-IoMT using RSA, PHR data is stored in the fog server. This FCSSI+RSA-IoMT contains PHR data in the encrypted format. In the distributed storage of FCSSI+RSA-IoMT, PHR data after decryption takes less in time.

5 Conclusion

This paper proposes FCSSI+RSA-IoMT using RSA in PHR data to store in distributed format securely and effectively. The experimental results show that FCSSI+RSA-IoMT achieves in sharing the data between owner/user. This FCSSI+RSA-IoMT of PHR access control system protects the patient identity details in PHR from external attacks. It requires minimum time consumption compared to the existing centralized storage of PHR data. This FCSSI+RSA-IoMT is the decentralized identity of PHR which preserves data privacy and access control over the patient identity of information. In order to get the optimized solution (FCSSI+RSA-IoMT), the number of sealers should be less than the nodes in the network. In addition to that, it minimizes the delay in synchronization and propagation. In future, this FCSSI+RSA-IoMT using RSA is applicable for various domain such as agriculture, logistics, education. Also, it can be extended for solving the privacy and preserving issues in the fog computing-based health care system.

Acknowledgement: We would like to give special thanks to Taif University Research supporting project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project Number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] B. Houtan, A. S. Hafid and D. Makrakis, “A survey on blockchain-based self-sovereign patient identity in healthcare,” *IEEE Access*, vol. 8, no. 3, pp. 90478–90494, 2020.

[2] P. Dudhe, N. Kadam, R. Hushangabade and M. Deshmukh, “Internet of Things (IOT): An overview and its applications,” in *Proc. 2017 Int. Conf. on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, pp. 2650–2653, 2017.

[3] F. Alsubaei, A. Abuhussein, V. Shandilya and S. Shiva, “IoMT-SAF: Internet of medical things security assessment framework,” *Internet of Things*, vol. 8, no. 2, pp. 100123, 2019.

[4] A. Mavrogiorgou, A. Kiourtis, M. Touloupou, E. Kapassa and D. Kyriazis, “Internet of medical things (IoMT) acquiring and transforming data into HL7 FHIR through 5G network slicing,” *Emerging Science Journal*, vol. 3, no. 2, pp. 64–77, 2019.

[5] X. Zhu and Y. Badr, “A survey on blockchain based identity management systems for the internet of things,” in *Proc. IEEE Int. Conf. on Internet of Things (iThings)*, Chengdu, China, pp. 1568–1573, 2018.

[6] D. V. Dimitrov, “Blockchain applications for healthcare data management,” *Healthcare Informatics Research*, vol. 25, no. 3, pp. 51–56, 2019.

[7] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, “In search of self-sovereign identity leveraging blockchain technology,” *IEEE Access*, vol. 7, no. 3, pp. 103059–103079, 2019.

[8] M. Kassab, J. Franco, T. Malas, V. V. G. Neto and G. Destefanis, “Blockchain: A panacea for electronic health records?” in *Proc. 2019 IEEE ACM 1st Int. Workshop on Software Engineering for Healthcare (SEH)*, QC, Canada, pp. 21–24, 2019.

[9] A. Siqueira, A. F. Da Conceição and V. Rocha, “Blockchains and self sovereign identities applied to healthcare solutions: A systematic review,” *Arxiv Preprint Arxiv: 2104.12298*, 2021.

[10] W. O. B. Stein and M. Boswell, “The current ethical and regulatory status of the internet of medical thing (IoMT) and the need of a new IoMT law,” *Journal of Healthcare Ethics & Administration*, vol. 4, no. 2, pp. 32–38, 2018.

[11] A. A. Mawgoud, A. I. Karadawy and B. S. Tawfik, “A secure authentication technique in internet of medical things through machine learning,” *Arxiv Preprint Arxiv:1912.12143,* 2019.

[12] A. Azaria, A. Ekblaw, T. Vieira and A. L. ippman, “Medrec: Using blockchain for medical data access and permission management,” in *Proc. 2nd Int. Conf. on Open and Big Data (OBD)*, Vienna, Austria, IEEE, pp. 25–30, 2016.

[13] D. Ivan, “Moving toward a blockchain-based method for the secure storage of patient records,” in *Proc. ONC/ NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States, pp. 1–11, 2016.

[14] M. Graf, R. Küsters and D. Rausch, “Accountability in a permissioned blockchain: Formal analysis of hyperledger fabric,” in *Proc. 2020 IEEE European Sym. on Security and Privacy (EuroS&P)*, Genoa, Italy, IEEE, pp. 236–255, 2020.

[15] A. A. Omar, M. S. Rahman, A. Basu and S. Kiyomoto, “Medibchain: A blockchain based privacy preserving platform for healthcare data,” in *Proc. Int. conf. on Security, Privacy and Anonymity in Computation, Communication and Storage*, Guangzhou, China, pp. 534–543, 2017.

[16] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” *Journal of Medical Systems*, vol. 40, no. 10, pp. 1–8, 2016.

[17] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher and F. Wang, “Secure and trustable electronic medical records sharing using blockchain,” in *Proc. AMIA annual sym. proc. American Medical Informatics Association*, Washington, DC, USA, pp. 650, 2017.

[18] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du *et al.,* “Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, no. 12, pp. 14757–14767, 2017.

[19] D. Boneh, B. Lynn C.Gentry and H. Shacham, “Aggregate and verifiably encrypted signatures from bilinear maps,” in *Proc. Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Warsaw, Poland, Springer, pp. 416–432, 2003.

[20] A. Lysyanskaya, S. Micali, L. Reyzin and H. Shacham, “Sequential aggregate signatures from trapdoor permutations,” in *Proc. Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Interlaken, Switzerland, pp. 74–90, 2004.

[21] G. J. Joyia, R. M. Liaqat, A. Farooq and S. Rehman, “Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain,” *Journal of Communications*, vol. 12, no. 4, pp. 240–247, 2017.

[22] F. H. Khoso, A. Lakhan, A. A. Arain, M. A. Soomro, S. Z. Nizamani *et al.,* “A microservice based system for industrial internet of things in fog cloud assisted network,” *Engineering, Technology & Applied Science Research*, vol. 11, no. 2, pp. 7029–7032, 2021.

[23] L. Wu, X. Du, W. Wang and B. Lin, “An out-of-band authentication scheme for internet of things using blockchain technology,” in *Proc. 2018 Int. Conf. on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, IEEE, pp. 769–773, 2018.

[24] A. Ouaddah, A. Abou Elkalam and A. A. Ouahman, “Towards a novel privacy preserving access control model based on blockchain technology in IoT,” in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, Saidia, Oujda, Morocco, pp. 523–533, 2017.

[25] S. Shamshad, K. Mahmood, S. Kumari and C. M. Chen, “A secure blockchain-based e-health records storage and sharing scheme,” *Journal of Information Security and Applications*, vol. 55, no. 4, pp. 102590, 2020.

[26] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi *et al.,* “Blockchain for industry 4.0: A comprehensive review,” *IEEE Access*, vol. 8, no. 4, pp. 79764–79800, 2020.

[27] M. Attaran, “Blockchain technology in healthcare: Challenges and opportunities,” *International Journal of Healthcare Management*, vol. 12, no. 6, pp. 1–14, 2020.

[28] I. Abu Elezz, A. Hassan, A. Nazeemudeen, M. Househ and A. Abd Alrazaq, “The benefits and threats of blockchain technology in healthcare: A scoping review,” *International Journal of Medical Informatics*, vol. 12, no. 3, pp. 104246, 2020.

[29] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan *et al.,* “Blockchain based identity management systems: A review,” *Journal of Network and Computer Applications*, vol. 166, no. 7, pp. 102731, 2020.

[30] A. Gorkhali, L. Li and A. Shrestha, “Blockchain: A literature review,” *Journal of Management Analytics*, vol. 7, no. 3, pp. 321–343, 2020.

[31] L. Cilliers, “Wearable devices in healthcare: Privacy and information security issues,” *Health Information Management Journal*, vol. 49, no. 3, pp. 150–156, 2020.

[32] T. McGhin, K. K. R. Choo, C. Z. Liu and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” *Journal of Network and Computer Applications*, vol. 135, no. 6, pp. 62–75, 2019.

[33] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, “Blockchain for secure ehrs sharing of mobile cloud based e-health systems,” *IEEE Access*, vol. 7, no. 11, pp. 66792–66806, 2019.

[34] L. Ismail, H. Materwala and S. Zeadally, “Lightweight blockchain for healthcare,” *IEEE Access*, vol. 7, no. 13, pp. 149935–149951, 2019.

[35] S. Wang, D. Zhang and Y. Zhang, “Blockchain-based personal health records sharing scheme with data integrity verifiable,” *IEEE Access*, vol. 7, no. 4, pp. 102887–102901, 2019.

[36] K. Balasubramanian and M. Rajakani, “Implementation of algorithms for identity based encryption and decryption,” in *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government: IGI Global*, California, USA, pp. 320–332, 2021.

[37] J. Sun, L. Ren, S. Wang and X. Yao, “Multi-keyword searchable and data verifiable attribute-based encryption scheme for cloud storage,” *IEEE Access*, vol. 7, no. 4, pp. 66655–66667, 2019.

[38] S. B. Wagh and J. K. Murthy, “Securing health care data for medical research using blockchain technology,” *Journal of Advancement in Electronics Design*, vol. 1, no. 3, pp. 17–23, 2018.

[39] V. Ramani, T. Kumar, A. Bracken, M. Liyanage and M. Ylianttila, “Secure and efficient data accessibility in blockchain based healthcare systems,” in *Proc.2018 IEEE Global Communications Conf. (GLOBECOM)* , Abu Dhabi, UAE, IEEE, pp. 206–212, 2018.

[40] Z. Ying, L. Wei, Q. Li, X. Liu and J. Cui, “A lightweight policy preserving EHR sharing scheme in the cloud,” *IEEE Access*, vol. 6, no. 14, pp. 53698–53708, 2018.

[41] H. Wang and Y. Song, “Secure cloud-based EHR system using attribute-based cryptosystem and blockchain,” *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–9, 2018.

[42] K. M. Khan, J. Arshad and M. M. Khan, “Secure digital voting system based on blockchain technology,” *International Journal of Electronic Government Research (IJEGR)*, vol. 14, no. 1, pp. 53–62, 2018.

[43] H. Es-Samaali, A. Outchakoucht and J. P. Leroy, “A blockchain-based access control for big data,” *International Journal of Computer Networks and Communications Security*, vol. 5, no. 7, pp. 137, 2017.

[44] K. Fan, S. Wang, Y. Ren, H. Li and Y. Yang, “Medblock: Efficient and secure medical data sharing via blockchain,” *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018.

[45] D. Baars, *Towards self-sovereign identity using blockchain technology.* University of Twente, Drienerlolaan, Netherlands, pp. 1–81, 2016.

[46] N. Rifi, E. Rachkidi, N. Agoulmine and N. C. Taher, “Towards using blockchain technology for IoT data access protection,” in *Proc. 17th Int. Conf. on Ubiquitous Wireless Broadband (ICUWB)*, Salamanca, Spain, IEEE, pp. 1–5, 2017.

[47] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in *Proc. IEEE 28th Annual Int. Sym. on Personal, Indoor, and mobile radio communications (PIMRC)*, Montreal, QC, Canada, IEEE, pp. 1–5, 2017.

[48] M. Shanmugam and R. Asokan, “A machine-vision-based real-time sensor system to control weeds in agricultural fields,” *Sensor Letters*, vol. 13, no. 6, pp. 489–495, 2015.

[49] A. A. Mutlag, M. K. A. Ghani, M. A. Mohammed and A. Lakhan, “Multi-agent systems in fog-cloud computing for critical healthcare task management model (CHTM) used for ECG monitoring,” *Sensors*, vol. 21, no. 20, pp. 6923, 2021.

[50] A. Lakhan, M. A. Mohammed, S. Kozlov and J. J. Rodrigues, “Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows,” *Transactions on Emerging Telecommunications Technologies*, vol. 3, no. 6, pp. e4363, 2021.

[51] A. Mutlag, M. Ghani and M. Mohammed, “A healthcare resource management optimization framework for ECG biomedical sensors,” *Proc. Efficient Data Handling for Massive Internet of Medical Things Springer*, vol. 12, no. 5, pp. 229–244, 2021.

[52] M. Kumar, K. Venkatachalam, P. Prabu, A. Almutairi and M. Abouhawwash, “Secure biometric authentication with de-duplication on distributed cloud storage,” *PeerJ Computer Science*, vol. 14, no. 4, pp. e569, 2021.

[53] M. Abdel Basset, N. Moustafa, R. Mohamed, M. Osama and M. Abouhawwash, “Multi-objective task scheduling approach for fog computing,” *IEEE Access*, vol. 9, no. 6, pp. 126988–127009, 2021.

[54] M. Masud, G. S. Gaba, K. Choudhary, M. Hossain, M. F. Alhamid *et al.,* “Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare,” *IEEE Internet of Things Journal*, vol. 2, no. 4, pp. 1–14, 2021.

[55] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou *et al.,* “Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps,” *IEEE Access*, vol. 8, no. 13, pp. 160433–160449, 2020.

[56] M. Rawashdeh, M. Zamil, S. M. Samarah, M. Obaidat and M. Masud, “IOT-based service migration for connected communities,” *Computers & Electrical Engineering*, vol. 96, no. 6, pp. 1–10, 2021.

[57] Y. Wang, J. Ma, A. Sharma, P. K. Singh, G. Singh *et al.,* “An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks,” *Journal of Sensors*, vol. 2021, no. 12, pp. 1–11, 2021.

[58] M. Abouhawwash and K. Deb, “Karush-kuhn-tucker proximity measure for multi-objective optimization based on numerical gradients,” in *Proc. of the 2016 on Genetic and Evolutionary Computation Conf. Companion*, Denver, USA, pp. 525–532, 2016.

[59] M. Abouhawwash and A. Alessio, “Develop a multi-objective evolutionary algorithm for pet image reconstruction: concept,” *IEEE Transactions on Medical Imaging*, vol. 40, no. 8, pp. 2142–2151, 2021.

[60] M. Abouhawwash, “Hybrid evolutionary multi-objective optimization algorithm for helping multi-criterion decision makers,” *International Journal of Management Science and Engineering Management*, vol. 16, no. 2, pp. 94–106, 2021.

[61] M. Abdel-Basset, R. Mohamed, M. Abouhawwash, R. K. Chakrabortty and M. J. Ryan, “EA-MSCA: An effective energy-aware multi-objective modified sine-cosine algorithm for real-time task scheduling in multiprocessor systems: Methods and analysis,” *Expert Systems with Applications*, vol. 173, no. 4, pp. 114699, 2021.

[62] M. Masud, M. Alazab, K. Choudhary and G. S. Gaba, “3P-SAKE: Privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks,” *Computer Communications*, vol. 175, no. 4, pp. 82–90, 2021.

[63] M. Abouhawwash, K. Deb and A. Alessio, “Exploration of multi-objective optimization with genetic algorithms for PET image reconstruction,” *Journal of Nuclear Medicine*, vol. 61, no. 3, pp. 572, 2020.

[64] P. Singh, M. Masud, M. S. Hossain and A. Kaur, “Cross-domain secure data sharing using blockchain for industrial IoT,” *Journal of Parallel and Distributed Computing*, vol. 156, no. 7, pp. 176–184, 2021.

[65] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea and M. S. Hossain, “A robust and lightweight secure access scheme for cloud based E-healthcare services,” *Peer-to-peer Networking and Applications*, vol. 14, no. 5, pp. 3043–3057, 2021.

[66] M. Abdel-Basset, R. Mohamed, M. Abouhawwash, R. K. Chakrabortty and M. J. Ryan, “A simple and effective approach for tackling the permutation flow shop scheduling problem,” *Mathematics*, vol. 9, no. 3, pp. 270–282, 2021.

[67] S. Maheswaran, B. K. Paul, M. A. Khalek, S. Chakma, K. Ahmed *et al.,* “Design of tellurite glass based quasi photonic crystal fiber with high nonlinearity,” *Optik*, vol. 181, no. 4, pp. 185–190, 2019.