Joint Framework for Access Control and Authentication using Blockchain over Cloud Environment

S.Sai Satyanarayana Reddy
Professor, Department of Computer Science & Engineering
Sreyas Institute of Engineering and Technology, Hyderabad, India
saisn90@gmail.com

Abstract. There is an increasing adoption of blockchain technology over different environment for leveraging security features. After reviewing existing blockchain-based approaches, it is noticed that there is still a large scope of improvement towards data security using blockchain. Therefore, this paper considers a case study of healthcare facilities, where the sensitive information of patient are required to be accessed as well as stored using a novel blockchain-based approach. The proposed system contributes towards developing a novel access control policy as well as a cost-effective authentication policy using a simplified hashing scheme. The prime contribution of the study is to prove that without using sophisticated encryption, it is feasible to integrate blockchain with hashing method for offering higher degree of threat mitigation measures by proposed system.

Keywords: Attack, Secure Access, Authentication, Blockchain, Cloud Computing, Hashing, Security

1 Introduction

The evolution of the blockchain is due to the modernization in the area of artificial intelligence and Internet-of-Things [1]. This is one of the most unique decentralized technology where the data can be subjected to authentication, storing, and synchronizing over multiple users without any dependencies towards third-party. It is claimed to offer highest degree of data security as once the data is secured using blockchain that cannot be subjected to any form of data alteration process without legitimate permission from the ledger. Blockchain technology is increasingly reported to be used in cloud computing environment [2]. However, various reported security problems has been discussed in recent times. Not all the research work towards blockchain is claimed to offer fairness or accountable. It doesn't even guarantee regular update policies towards its block structure according to existing studies [2]. Irrespective of dif-

ferent levels of application of blockchain in cloud, there are many number of challenges too [3]. Existing approaches doesn't ensure scalability with less consideration of network performance. Apart from this, privacy aspect and its success factor after implementing blockchain over large scale of data remains unknown. Not all the security issues has been studied and still it is under development stages of research work. Apart from this, its mechanism is quite complex to model for simplified data security applications.Therefore, this paper introduces a simplified access control and authentication policy in blockchain deployed over cloud environment considering healthcare as a case study. The organization of the paper is as follow: Section 2 discusses about the existing research work followed by problem identification in Section 3. Section 4 discusses about proposed methodology followed by elaborated discussion of algorithm implementation in Section 5. Comparative analysis of accomplished result is discussed under Section 6 followed by conclusion in Section 7.

2 Related Work

There has been various existing approaches where blockchain has been used for securing cloud system. The recent work of Huang et al. [4] have used an auditing mechanism towards assessing integrity of cloud data over consensus node.An incentive based scheme for secure sharing of data has been discussed in study of Shen et al. [5]. Secure and fair approach towards payment system has been reported in study of Yang et al. [6] where multi-keywords has been used towards facilitating public variability. Current work is also carried out towards privacy protection where access control is designed to protect the data using blockchain as seen in work of Yang et al. [7]. Audition scheme towards multi-cloud data with multi-replica using blockchain is studied by Yang et al. [8]. Adoption of Signcryption scheme is considered in study of Yang et al. [9] which was used for securing the healthcare data along with blockchain. Apart from this, there are various other associated blockchain based approaches e.g. cloud manufacturing scheme (Kaynak et al. [10]), resource trading scheme (Yao et al. [11]), game-based service management (Xiong et al. [12]), blockchain in the form of services (Zheng et al. [13]), fog computing with blockchain (Memon et al. [14]), forensics using elliptical curve and software defined network (Pourvahab and Ekbatanifard [15]), game-based monitoring of service quality (Taghavi et al. [16]), deduplication based fair payment (Wang et al. [17]), cipher-

text-policy attribute based encryption and blockchain (Wang et al. [18]), resource management (Xiong et al. [19]). The next section briefs about research problem. (Kumar et al. [20-22]) proposed an object detection method for blind people to locate objects from a scene. They have used machine learning based methods along with single SSMD detector algorithm to develop the model.

3 Problem Description

The core problems of existing studies are as follows: i) majority of existing studies has used high-end encryption, ii) the user is not endowed with any scheme to have complete ownership of data, iii) data addresses and scheme of managing blockchain is not much emphasized, iv) not all approaches are completely cloud-based and hence there is always an access-related problems, v) there are lesser occurrences of any scheme where simplified encryption is implement, and vi) less focus on computational complexity observed in existing blockchain approaches.

4 Proposed Methodology

The prime purpose of the proposed system is to offer an extensive level of security for the transacted information in healthcare facility using blockchain technology. Fig.1 highlights the link among all the essential actors involved in proposed system.

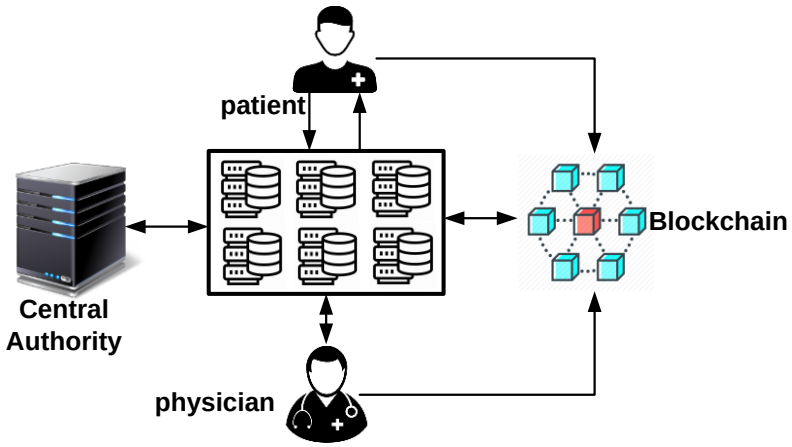


Figure 1 Schematic Architecture of AEOC

The central authority is responsible for generating master secret key for all users in healthcare facility. The storage unit is meant for repositing all clinical information where there is a possibility of suspected attacks. After the data is stored, the storage unit forward the access tree of data, hash, and address to blockchain. Blockchain is further used by

patient / physician to ensure that data is not tampered illegitimately. Patient is required to first enroll itself prior to use this system. It has to get itself authenticated prior data uploading. Along with this, patient can configure its data access tree, encrypt them, and forward it to storage unit. The blockchain can be accessed by physician along with retrieval of hash value and data access tree in order to verify the data.

5 System Implementation

The proposed system mainly presents a novel access-based policy with an aid of blockchain mechanism. It is carried out in sequential phases of operation to ensure that there is a higher degree of secrecy maintained by all the parties of healthcare section.

i) Algorithm for Secure Enrollment

This algorithm is responsible for carrying out secure enrollment operation for patient and storage unit. The input to the algorithm is C_{auth} (central authority) while the output is Pub_{key} (public key). The algorithmic steps are as follows:

Algorithm for Secure Enrollment

Input: C_{auth} (central authority)

Output: Pub_{key} (public key)

Start

1. $C_{auth} \rightarrow (\Phi_2, scal, gen, hash)$
2. $C_{auth} \rightarrow (pub_{key}, \theta)$
3. $C_{auth} \rightarrow (aux_{key})Ph_k$
4. $Ph_k \leftarrow (Pub_{key})h_s$
5. $n_i \rightarrow (Sec_{tok})C_{auth}$
6. $C_{auth} \rightarrow (\gamma_i|\lambda_i)n_i$
7. $SU \rightarrow (\mu_{su}, \beta_{su})C_{auth}$
8. $Pub_{key}(SU)=m_{su}.\eta$

End

In the above mentioned algorithm, the central authority C_{auth} generates a cyclic group $\Phi_2 \leftarrow \Phi_1$ x $\Phi_1$along with the generation of scalar attributes*scal*along with a random generator *gen*which belongs to Φ_1 group, and hash function *hash* (Line-1). Further, a public key pub_{key} is generated using dot product of *scal* and *gen* (Line-2), The central authority c_{auth} further constructs a secret key as *scal* and random number of prime order. The variable θ is meant for generating feature key calculated as prime number divided by *scal* (Line-2). The next process of the algorithm is to generate auxiliary key aux_{key} by the central authority C_{auth} and

forwards them to *k* number of physician Ph_k (Line-3). The study considers that j^{th} healthcare unit forwards a message as a request to the central authority C_{auth} for generating the key. For this, j^{th} node forwards information associated about identity of physician and patient with auxiliary features of doctor to C_{auth}. Upon obtaining this message, C_{auth} computes a secret key by hashing identity of doctor with *gen* as well as it also generates auxiliary key as follows,

$$aux_{key}=\theta(q \mid r_k) \quad (1)$$

According to the expression(1), the variable *q* and r_k represents natural number and random *k* numbers respectively. The central authority c_{auth} then forwards the private key of the doctor which it has carried out in prior steps by hashing identity and gen (Line-4). Apart from this, a set of auxiliary keys are forwarded to the j^{th} healthcare unit which is computed by multiplying r_k with prime number. Further, a public key is calculatedby the j^{th} healthcare unit and is forwarded to the physician Ph_k (Line-4). Once, this operation is carried out, the next set of operation is about forwarding three modalities of information to the blockchain i.e. identity of patient and doctor, public key, and auxiliary key. The next phase of implementation is about enrolling the patient and the storage unit carried out by central authority in two important steps. In the first step, enrollment of patient is carried out by transmitting their security token to the c_{auth} securely (Line-5). The computation of security token $sec_{tok}$is carried out by hashing identity of the patient with a random number. Further, a secured identity λ_i is computed by product of security token sec_{tok}, *scal*, and public key issued by the central authority. The information associated with secured identity λ_i associated with γ_i is forwarded to patient n_i securely (Line-6). Further, the patient n_i generates a random natural number which is required in further process. This natural number is XORed with hashed value of identity information and primary random natural number. The patient n_i also generates enrollment attribute τ_i which is again a hash value of primary-secondary natural number, hashed value of identity and primary natural number and secured identity. The next process is about enrolling storage unit where μ_{su} is computed by XORing identity of storage unit and random number $\beta_{su}$and this information is stored in c_{auth}(Line-7). Further C_{auth} computes identity of the storage units μ_{su} and secure key of storage units m_{su}. This information are stored in secure memory system within C_{auth}, while the information of secured key of storage unit and security token $sec_{tok.}$ Finally, an identity of the storage unique is computed by hashing the security

token sec_{tok} with secure key of storage unit followed by computing a public key Pub_{key} (Line-8). This completes the process of initialization, generation of key till enrollment of patients and storage unit.

ii) Algorithm for Authentication

This algorithm is the continuation of the prior algorithm which carry out authentication of all the prominent actors in order to prove their legitimacy. The algorithm takes input of w (multi-modal security attributes) to give outcome of Sec_{data} (Secured data). The steps of the algorithm are as follows:

Algorithm for Authentication

Input: w (multi-modal security attributes)

Output: Sec_{data} (Secure authentication and data storage)

Start

1. **If** $\tau_i=w$
2. n_i is given access to SU_i
3. $\gamma_i \rightarrow (T_i, r_i, Pub_{key,} \sigma_1, \sigma_2, \sigma_3, \mu_i)$
4. **If** $|T_1-T_2|<T_{thresh}$
5. Declare T_1 as valid timestamp
6. **If** $f(e_1)=f(e_2)$
7. ni is authenticated
8. sec_{data}: $n_i \rightarrow f_2$(data)
9. **End**
10. **End**
11. **End**

End

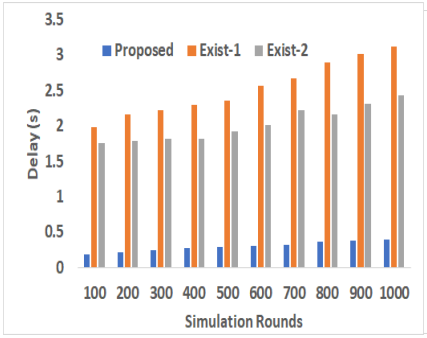
In this operation, the authentication is carried out for patient n_i and storage unit *su* in order to establish a session key. First the identity as well as credentials of the patient n_i is fed to the hardware device (e.g. smart card) which is capable of computing βi by XORing random number with hash valued of identity and credential. The next operation is about assessing a logical condition stated in Line-1 where the variable τ_i is compared with a variable *w* for its equivalency. The variable *w* represents hashed value of primary-secondary natural number along with hashed credential and secure identity (Line-1). If this equivalency holds good, then the storage unit permits the patient to have an access (Line-2). In the next process, an arbitrary number r_k is generated by the storage unit along with time stamp T_1. Further, computation of the public key is carried out by obtaining a product of primary natural number, random number, and prime number. It then carry out computation of three more

parameters σ_1(product of β_i, r_i, $pub_{key}(su)$), σ_2(XORed operation of security token and hash of σ_1), σ_3(hashed value of σ_1, security token, time stamp, and identity of storage unit) (Line-3). The system also computes μ_{su} as product of secured identity and $\sigma_{2.}$ followed by transmission of the message by patient n_i to storage unit *su* using public channel. Upon receiving this information, the storage unit assess the validity of the obtained information about the timestamp using the logical condition stated in Line-4. According to this condition, if the difference of two timestamp T_1 and T_2(receiving timestamp) is found less than a threshold time T_{thresh} (Line-4) than the primary timestamp T_1 is declared as valid (Line-5). The study considers T_{thresh} as delay caused due to transmission to highest extent linked with message transmission. If the above-mentioned condition of equivalency (Line-4) is found valid than the storage unit computes σ1 using public key pub_{key} and secret key of storage unit, it also computes security token sec_{tok} and matches of hashed value of the security token and secret key of storage unit matches with identity of the storage unit. Once, it is found valid than the system enrolls the patient n_i.

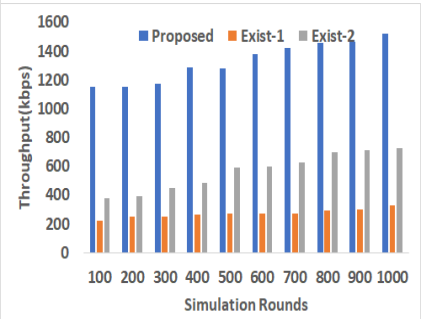
In the next stage of authentication, the storage unit computes the third parameter σ_3 obtained by hashing of $\sigma_{1,}$ security token, timestamp, and identity of storage unit. The system further formulates another conditional logic stated in Line-6. The left side of expression in Line-6 is about a function *f*(x) considering a set e_1 with μ_i and public key. The right side consists of using same function with security token sec_{tok}, σ_3, and public key of central authority. The storage unit further computes verification parameters with respect to current timestamp as well as identity-related parameters. Then the storage unit forwards a message to patient. Upon receiving the message, the timestamp T2 validity is checked and once it finds to be valid, the secured data is transmitted by the patient to storage unit (Line-8). The data are stored in secured manner considering a tree-based logic. The function in Line-8 is used to further carry out encryption on the data where the encrypted data is stored over the tree structure. The structure and positional information of the data over the tree is further hashed with respect to identity of the storage unit, public key, and maximum timestamp. This record is uploaded by the storage unit to the blockchain. The identity of the request by the user is further retrieved from blockchain in case of retrieval. Further the algorithms offers extensive security owing to multiple assessment in blockchain.

6 Results Discussion

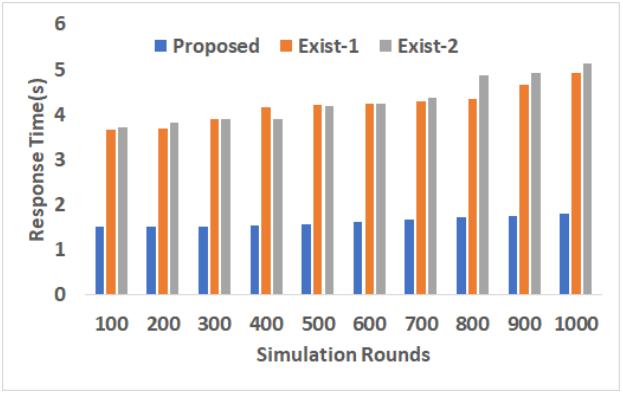
The implementation of the proposed system is carried out considering 500 nodes representing patient and 250 nodes representing physician. The analysis is proposed outcome is compared with existing studies carried out by Tang et al. [20] and Wang et al. [21]. Both these existing scheme focuses on using blockchain for similar purpose and hence compared over similar test environment with respect to delay, throughput, and response time. It cam be seen from Fig.2 that proposed system offer considerably better performance compared to existing approaches. The proposed system offers approximately 82% reduction in delay (Fig.2(a)), 75% improvement in throughput (Fig.2.(b)), and 57% of speedy response time (Fig.2(c)); thereby exhibiting that proposed blockchain-based authentication is better than existing approach.



(a) Delay Analysis



(b) Throughput Analysis



(c) Response Time

Figure 2 Comparative Analysis

Apart from this, it can be also said that proposed system offers resistivity against any form of attacks related to identity theft, data tampering, distributed denial-of-service mainly. Any form of attacker with any scale of threat is required to break multiple dependencies to have an access to the original data. As the proposed system offers multiple layers of hashing in incorporation of multiple dependable parameters, therefore, it is im-

possible for the attacker to introduce attack in simpler attempt. Moreover, it is less likely for an attacker to introduce an attack on proposed blockchain as it would require massive resources to obtain data blocks and data access tree just from any one user. Therefore, a higher degree of protection is offered in proposed blockchain.

7 Conclusion

This paper has introduced a scheme towards effective authentication followed by secure access policy in healthcare facilities. Following are the contribution/novelties: i) the blockchain is designed with both access control and authentication scheme storing data access tree, address, hash, ii) proposed system offers data integrity and scalability, iii) it offers resistivity from multiple forms of attack, iv) without using any sophisticated encryption, it offers simple and cost effective data security over cloud.

References

[1] O. Ali, A. Jaradat, A. Kulakli and A. Abuhalimeh, "A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities," in IEEE Access, vol. 9, pp. 12730-12749, 2021,

[2] K. Gai, J. Guo, L. Zhu and S. Yu, "Blockchain Meets Cloud Computing: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2009-2030, thirdquarter 2020, doi: 10.1109/COMST.2020.2989392.

[3] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2521-2549, Fourthquarter 2020, doi: 10.1109/COMST.2020.3020092.

[4] P. Huang, K. Fan, H. Yang, K. Zhang, H. Li and Y. Yang, "A Collaborative Auditing Blockchain for Trustworthy Data Integrity in Cloud Storage System," in IEEE Access, vol. 8, pp. 94780-94794, 2020.

[5] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du and M. Guizani, "Blockchain-Based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1229-1241, June 2020, doi: 10.1109/JSAC.2020.2986619.

[6] Y. Yang, H. Lin, X. Liu, W. Guo, X. Zheng and Z. Liu, "Blockchain-Based Verifiable Multi-Keyword Ranked Search on Encrypted Cloud

With Fair Payment," in IEEE Access, vol. 7, pp. 140818-140832, 2019, doi: 10.1109/ACCESS.2019.2943356.

[7] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao and K. Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud," in IEEE Access, vol. 8, pp. 70604-70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[8] X. Yang, X. Pei, M. Wang, T. Li and C. Wang, "Multi-Replica and Multi-Cloud Data Public Audit Scheme Based on Blockchain," in IEEE Access, vol. 8, pp. 144809-144822, 2020, doi: 10.1109/ACCESS.2020.3014510.

[9] X. Yang, T. Li, W. Xi, A. Chen and C. Wang, "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud," in IEEE Access, vol. 8, pp. 170713-170731, 2020, doi: 10.1109/ACCESS.2020.3025060.

[10] B. Kaynak, S. Kaynak and Ö. Uygun, "Cloud Manufacturing Architecture Based on Public Blockchain Technology," in IEEE Access, vol. 8, pp. 2163-2177, 2020,

[11] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang and Y. Qian, "Resource Trading in Blockchain-Based Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3602-3609, June 2019, doi: 10.1109/TII.2019.2902563.

[12] Z. Xiong, J. Kang, D. Niyato, P. Wang and H. V. Poor, "Cloud/Edge Computing Service Management in Blockchain Networks: Multi-Leader Multi-Follower Game-Based ADMM for Pricing," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 356-367, 1 March-April 2020,

[13] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in IEEE Access, vol. 7, pp. 134422-134433, 2019, doi: 10.1109/ACCESS.2019.2941905.

[14] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan and J. Ahmed, "DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things," in IEEE Access, vol. 7, pp. 169073-169093, 2019, doi: 10.1109/ACCESS.2019.2952472.

[15] M. Pourvahab and G. Ekbatanifard, "Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology," in IEEE Access, vol. 7, pp. 153349-153364, 2019, doi: 10.1109/ACCESS.2019.2946978.

[16] M. Taghavi, J. Bentahar, H. Otrok and K. Bakhtiyari, "A Blockchain-Based Model for Cloud Service Quality Monitoring," in IEEE

Transactions on Services Computing, vol. 13, no. 2, pp. 276-288, 1 2020,

[17] S. Wang, Y. Wang and Y. Zhang, "Blockchain-Based Fair Payment Protocol for Deduplication Cloud Storage System," in IEEE Access, vol. 7, pp. 127652-127668, 2019,

[18] S. Wang, X. Wang and Y. Zhang, "A Secure Cloud Storage Framework With Access Control Based on Blockchain," in IEEE Access, vol. 7, pp. 112713-112725, 2019,

[19] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang and Z. Han, "Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4585-4600, June 2019.

[20] Kumar, Ashwani. "Design of Secure Image Fusion Technique Using Cloud for Privacy-Preserving and Copyright Protection." International Journal of Cloud Applications and Computing (IJCAC) 9.3 (2019): 22-36.

[21] Ashwani Kumar, Sonam Srivastava, “Object Detection System Based on Convolution Neural Networks Using Single Shot Multi-Box Detector”, Procedia Computer Science, Volume 171, 2020, Pages 2610-2617.

[22] Ashwani Kumar, S. S. S. S. Reddy and V. Kulkarni, "An Object Detection Technique For Blind People in Real-Time Using Deep Neural Network," 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India, 2019, pp. 292-297, doi: 10.1109/ICIIP47207.2019.8985965.

[23] F. Tang, S. Ma, Y. Xiang and C. Lin, "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records," in IEEE Access, vol. 7, pp. 41678-41689, 2019,

[24] J. Wang, L. Wu, K. R. Choo and D. He, "Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1984-1992, March 2020, doi: 10.1109/TII.2019.2936278.