Industrial Engineering Journal
ISSN: 0970-2555
Volume: 54, Issue 1, January:2025

Access Control Frame Work Based a Smart Healthcare System

D. LEELA DHARANI Assistant professor Department of Information Technology P.V.P Siddhartha Institute of Technology,

Vijayawada, A.P., India

JAMPANA LEELA DEEPAK, GUNTAGANI ABHILASH, SAI SUREKHA KARRI, B.SAI SRINIVAS RAJU, Students of Department of Information Technology P.V.P Siddhartha Institute of Technology,

Vijayawada, A.P., India

ABSTRACT:

In current healthcare systems, electronic medical records (EMRs) are always located in different hospitals and controlled by a centralized cloud provider. However, it leads to single point of failure as patients being the real owner lose track of their private and sensitive EMRs. Hence, this paper aims to build an access control framework based on smart contract, which is built on the top of distributed ledger (blockchain), to secure the sharing of EMRs among different entities involved in the smart healthcare system. For this, we propose four forms of smart contracts for user verification, access authorization, misbehavior detection, and access revocation respectively. In this framework, considering the block size of ledger and huge amount of patient data, the EMRs are stored in cloud after being encrypted through the cryptographic functions of Elliptic Curve Cryptography (ECC) and Edwards-Curve Digital Signature Algorithm (EdDSA), while their corresponding hashes are packed into blockchain. The performance evaluation based on a private Ethereum system is used to verify the efficiency of proposed access control framework in the real-time smart healthcare system.

INTRODUCTION

Due to the rapid advancement of Internet of Things (IoT) technologies, an increasing number of smart healthcare gadgets provide greater access to electronic medical records (EMRs) than before for monitoring patient's regular health and recommending treatments. Although this IoT-enabled approach to eHealth is useful in the medical field, there are

a lot of concerns about the confidentiality and integrity of accessing smart healthcare data [1], [2]. In addition, although the EMRs are conventionally recorded in centralized cloud health registries of a healthcare provider, they are managed by third-party authorities, which constitutes a high risk for a security breach to occur. Furthermore, there is a fundamental issue of interoperability among different healthcare providers such as the sharing of healthcare records [3]. The delegation, verification, and revocation of access rights to another healthcare provider is a critical concern while sharing confidential patient data. More challenging, the access should be restricted to authorized entities by keeping it highly confidential and patient-centric [4].

An analysis in [5] shows that the traditional IoT access control models which are predominantly based on established access control models, such as discretionary access control model (DAC) [6], role-based access control model (RBAC) [7], attribute-based access control model (ABAC) [8], and capability-based access control model (CaBAC) [9] validate the access rights through a centralized entity, which is prone to a single point of failure. Thus, decentralized access control has been a key research topic for years. However, current decentralized access control techniques, due to storage of access policies in the cloud, are unable to make the access control policies transparent and secure. To deal with this issue, the concept of distributed IoT has been proposed recently [10], where access authorization is performed at the end devices. However, it is very difficult to enforce as these IoT devices are computationally restrained.

EXISTING SYSTEM

In existing cloud or network servers all user's data will be stored at centralized single server. In addition, although the EMRs are conventionally recorded in centralized cloud health registries of a healthcare provider, they are managed by third-party authorities

Disadvantages of Existing system

- If one node corrupted then user can recover data from other node.
- If that server hacked or corrupted then data will be lost.

PROPOSED SYSTEM

In this we are using Blockchain tool called Ethereum which contains Blockchain implementation and it store data in the form of blocks and this block contains encrypted and hash data. Each hash verification will be done with the help of PROOFOF WORK technique. The performance evaluation based on this private Ethereum system is used to verify the efficiency of proposed access control

frame work in there al-time smart health care system

Advantages of Proposed System

- In blockchain each party data will be encrypted and then hashed and then store in blocks and each block will have chain of hash code of one and other and each block hash code will be verify before storing new block.
- If attacker modify any block then that block hash code verification will be failed and due to this technique no attacker can be able to alter block data.

LITERATURE SURVEY

Cross-organization or cross-domain cooper ation takes place from time to time in Elect ronic Health Record (EHR) system for nec essary and high-quality patient treatment. Cautious design of delegation mechanism must be in place as a building block of cro ss-domain cooperation, since the cooperati on inevitably involves exchanging and sha ring relevant patient data that are considere d highly private and confidential. The dele gation mechanism grants permission to an d restricts access rights of a cooperating pa rtner. Patients are unwilling to accept the E HR system unless their health data are gua ranteed proper use and disclosure, which c annot be easily achieved without cross-do main authentication and fine-grained acces s control. In addition, revocation of the del egated rights should be possible at any tim e during the cooperation. In this paper, we propose a secure EHR system, based on cr yptographic constructions, to enable secure sharing of sensitive patient data during coo peration and preserve patient data privacy. Our EHR system further incorporates adva nced mechanisms for fine-grained access c ontrol, and on-demand revocation, as enha ncements to the basic access control offere d by the delegation mechanism, and the ba sic revocation mechanism, respectively. Th e proposed EHR system is demonstrated to fulfill objectives specific to the cross-doma in delegation scenario of interest.

The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bit coin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we describe a decentralized personal data management system that

ensures users own and control their data. We implement a protocol that turns a block chain into an automated access-control manager that does not require trust in a third party. Unlike Bit coin, transactions in our system are not strictly financial -- they are used to carry instructions, such as storing, querying and sharing data. Finally, we discuss possible future extensions to block chains that could harness them into a well-rounded solution for trusted computing problems in society.

RELATED WORK

Blockchain

In this project we are using Blockchain too l called Ethereum which contains Blockch ain implementation and it store data in the form of blocks and this block contains encr ypted and hash data.

Admin

Admin will store patient records and then s hare this patient records with either researc hers or doctors. In this work with patient d ata we can store patient medical image als o but block chain cannot store huge patient image data so we are using IPFS server to store patient image and patient data will be store in block chain Ethereum tool. Blockc hain will send uploaded patient image to I PFS server and then IPFS server will store that image and then the address of stored i mage will be sent back to blockchain and l ater blockchain can obtained that image fro m IPFS server by giving that image addres s.

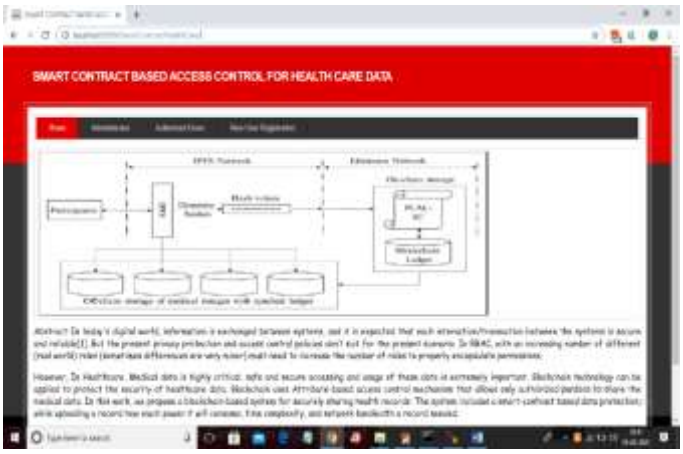
Doctor

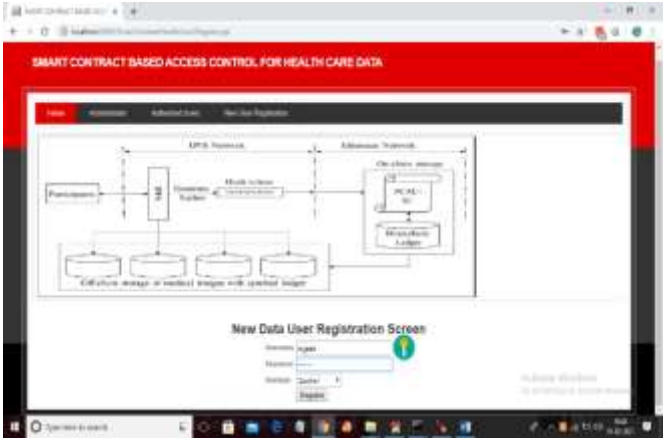
Doctor can ‘Access Patient Data’ link to vi ew all those patient details added by admin . Doctor can view all patient data and get a ccess to patient image.

Researcher

Researcher can ‘Access Patient Data’ link t o view patient details

SAMPLE RESULTS





CONCLUSION

This paper proposed and developed an access control model for IoT enabled smart healthcare devices and the medical system through blockchain-based smart contract. We have achieved our goal of patient-centricity and accessibility of medical records across the system. Cloud is used as a storage to avoid the congestion in the blockchain network. EMR is securely registered and retrieved through the cryptographic functions of ECC and EdDSA. The proposed scheme has been implemented on the Ethereum private blockchain network. The performance evaluation and efficiency analysis demonstrate the feasibility of the proposed scheme in the real-time smart healthcare system for a secure, decentralized, distributed, and patient-centric access control.While the proposed scheme has demonstrated attractive features, the integration of blockchain and cloud to provide decentralized access control incurs challenges of scalability and performance. By using edge computing, the latency that occurs in processing and fetching the EMR can be greatly reduced. Therefore, further research is required to address this issue. Furthermore, in order to enhance the liveliness and fairness of the system, another future research work is to develop an incentive mechanism for EMR owners in the proposed scheme

REFERENCES

[1] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, “Access control in the internet of things: Big challenges and new opportunities,” Computer Networks, vol. 112, pp. 237–262, 2017.

[2] N. Fatema and R. Brad, “Security requirements, counterattacks and projects in healthcare applications using wsns-a review,” arXiv preprint arXiv:1406.1795, 2014.

[3] J. Sun and Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, 2009.

[4] L. J. Kish and E. J. Topol, “Unpatients-why patients should own their medical

data," Nature biotechnology, vol. 33, no. 9, p. 921, 2015.

[5] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in internet-of-things: A survey," Journal of Network and Computer Applications, vol. 144, pp. 79–101, 2019.

[6] S. Osborn, R. Sandhu, and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," ACM Transactions on Information and System Security (TISSEC), vol. 3, no. 2, pp. 85–106, 2000.

[7] R. S. Sandhu, "Role-based access control," in Advances in computers. Elsevier, 1998, vol. 46, pp. 237–286.

[8] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," Computer, vol. 48, no. 2, pp. 85–88, 2015.

[9] R. S. Sandhu and P. Samarati, "Access control: principle and practice," IEEE communications magazine, vol. 32, no. 9, pp. 40–48, 1994.