ISSN PRINT 2319 1775 Online 2320 7876
Research paper , UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

BLOCK CHAIN WITH SECURITY ANALYSIS PERFORMANCE IMPROVEMENTSIN LIGHTWEIGHT ACCESS CONTROL FOR EHRS SHARING

[1]J.Praveen Kumar , [2]Ganji Preetham, [3]Bhukya Ram Priya Das , [4]Durvasula Sri Gayathri

[1] Associate Professor, Department of Information Technology, Teegala Krishna Reddy Engineering College Hyderabad, Telangana, India.

[1] praveentkrecit@gmail.com

[2,3,4] UG Scholars Department of Information Technology, Teegala Krishna Reddy Engineering College , Hyderabad, Telangana, India.

[2] ganjipreetham2@gmail.com , [3] tinkulufeas@gmail.com ,[4] srigayathri224@gmail.com

Abstract

Recent years have witnessed a paradigm shift in storage of Electronic Health Records (EHRs) on mobile cloud environments where mobile devices are integrated with cloud computing to facilitate medical data exchanges among patients and healthcare providers. This advanced model enables healthcare services with low operational cost, high flexibility and EHRs availability. However, this new paradigm also raises concerns about data privacy and network security for e-health systems.. In this paper, we propose a novel EHRs sharing framework that combines blockchain and the decentralized interplanetary file system (IPFS) on a mobile cloud platform. Particularly, we design a trustworthy access control mechanism using smart contracts to achieve secure EHRs sharing among different patients and medical providers. We present a prototype implementation using Ethereum block chain in a real data sharingscenario on a mobile app with Amazon cloud computing. Empirical results show that our proposal provides an effective solution for reliable data exchanges on mobile clouds while preserving sensitive health information against potential threats. The system evaluation and security analysis also demonstrate performance improvements in lightweight access control design, minimum network latency with high security anddata privacy levels, compared to existing data sharing models.

I .INTRODUCTION

Recently, there has been a growing interest in employing the blockchain technologyto promote medical and e-health Services Blockchain with its decentralized and trustworthy nature has demonstrated

immense potentials in various e-health sectors such as secure sharing of Electronic Health Records (EHRs) and data access management among multiple medical entities Therefore, the adoption of block chain can provide promising solutions to facilitate health care delivery and thus revolutionize the healthcare industry. With the emergence of innovative technologies, including Mobile Cloud Computing (MCC) and Internet of Medical Things (IoMT), the healthcare industry has witnessed significant changes in e-health operations . Patients now can collect their personal health information at homebased on mobile devices (such as smart phones and wearable sensors) and share on cloud environments where health care providers can access instantly to analyze medical records and provide timely medical supports. This smart e-health service allows healthcare providers remotely monitor patients and offer ambulatory care at home, which not only facilitates healthcare delivery but also brings economic benefits to patients. Further, the availability of complete EHRs on clouds also helps healthcare providers track patient health and offers proper medical services during diagnosis and treatment processes .Besides all these great advantages, however, the trend of EHRs storage on clouds also poses security challenges which hinder the deployment of e- health applications on clouds . Among such security issues is secure EHRs sharing between patients and healthcare providers onmobile cloud environments. Unauthorized entities may gain malicious access to EHRs without consent of patients, which has detrimental impacts on data integrity, privacy and security of cloud e-health systems . Moreover, patients may find it difficult to track and manage their health records shared among healthcare providers on clouds. It therefore is necessary to propose efficient access control solutions for mobile cloud EHRs sharingsystems.Meanwhile, blockchain-based access control provides various new security features for e-health with great advantages over conventional access control solutions.

II.LITERATURE SURVEY

An energy-efficient transaction model for the blockchain-enabled Internet of Vehicles (IoV),"

The blockchain is a safe, reliable and innovative mechanism for managing numerous vehicles seeking connectivity. However, following the principles of the blockchain, the number of transactions required to update ledgers pose serious issues for vehicles as these may consume the maximum available energy. To resolve this, an efficient model is presented in this letter which is capable of handling the energy demands of the blockchainenabled Internet of Vehicles (IoV) by optimally controlling the number of transactions through distributed clustering. Numerical results suggest that the proposed approach is 40.16% better in terms of energy conservation and 82.06% better in terms of th e number of transactions required to share the entire blockchaindata compared with the traditional blockchain

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

"On scaling decentralized blockchains,"

The increasing popularity of block chain-based crypto currencies has made scalability a primary and urgent concern. We analyze how fundamental and circumstantial bottlenecks in Bit coin limit the ability of its current peer-to-peer overlay network to support substantially higher throughputs and lower latencies. Our results suggest thatreparameterization of block size and intervals should be viewed only as a first increment toward achieving next-generation, high-load block chain protocols, and major advances will additionally require a basic rethinking of technical approaches. We offer a structured perspective on the design space for such approaches. Within this perspective, we enumerate and briefly discuss a number of recently proposed protocolideas and offer several new ideas and open challenges.

"A low storage room requirement framework for distributed ledger inblock chain,

Block chain systems establish a cryptographically secure data structure for storing datain the form of a hash chain. We use a novel combination of distributed storage, private key encryption, and Shamirs secret sharing scheme to distribute transaction data, without significant loss in data integrity. Additionally, using Shamirs secret sharing scheme on the hash values and dynamic zone allocation, we further enhance the integrity. We highlight the tradeoff in storage cost and data loss probability with varying zone size choices. We also study the tradeoff between recovery cost and security from adversarial corruption with varying recovery mechanisms. Then, we formulate code design, given a probability of data recovery and targeted corruption, as an integer program. Using the coding scheme we establish a mechanism to insure data, for instance in block chain-based cloud storage systems, based on the value of the data, by understanding the costs involved for the service provider.

III.EXISTING SYSTEM

Block chain is a paradigm-shifting technology that has emerged over the past decade, which is based on peer-to-peer communication technology, network theory, and cryptography. However, there are still some limitations in the existing block chain frameworkthat prevents its wide spread adoption in the commercial world. One important limitation is the storage requirement, wherein each block chain node has to store a copy of the distributed ledger. us, as the number of transactions increases, this storage requirement grows quadratic ally, eventually limiting the scalability of a block chain

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

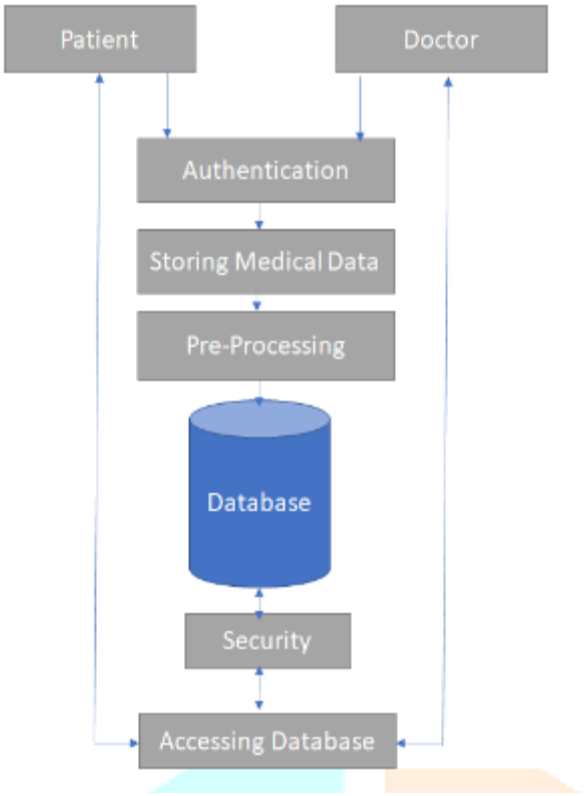
IV PROBLEM STATEMENT

Recent years have witnessed a paradigm shift in the storage of Electronic Health Records (EHRs) on mobile cloud environments, where mobile devices are integrated with cloud computing to facilitate medical data exchanges among patients and healthcare providers. This advanced model enables health care services with low operational cost, high flexibility, and EHRs availability. However, this new paradigm also raises concerns about data privacy and network security for e-health systems. How to reliably share EHRs among mobile users while guaranteeing high-security levels in the mobile cloud is a challenging issue. In this paper, we propose a novel EHRs sharing framework that combines block chain and the decentralized interplanetary file system (IPFS) on a mobile cloud platform. Particularly, we design a trustworthy access control mechanism using smart contracts to achieve secure EHRs sharing among different patients and medical providers. We present a prototype implementation using Ethereum block chain in areal data sharing scenario on a mobile app with Amazon cloud computing. The empirical results show that our proposal provides an effective solution for reliable data exchanges on mobile clouds while preserving sensitive health information against potential threats. The system evaluation and security analysis also demonstrate the performance improvements in lightweight access control design, minimum network latency with high security and data privacy levels, compared to the existing data sharing models.

IV PROPOSED SYSTEM

In this paper, instead of saving entire transaction of blocks we are saving only one block. To provide security to block author converting that block in to SHAMIR share and then all SHAMIR share will be distributed between all available nodes. While reconstruction application will obtain all shares from nodes and then apply SHAMIR SECRET to recover original block data. If any share missed or return incorrect value then reconstruction will be failed. SHAMIR secret will work based on random polynomial and prime number while generating secret polynomial will be applied onblock data and while getting original value will perform reverse polynomial

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023



This research work proposes different modules for providing security and privacy to electronic healthcare data using blockchain technology.

 Healthcare database is accessible for patients as well as medicos from anywhere for patients' diagnosis.

 For both patient and medico staffauthentication and validitation step is required.

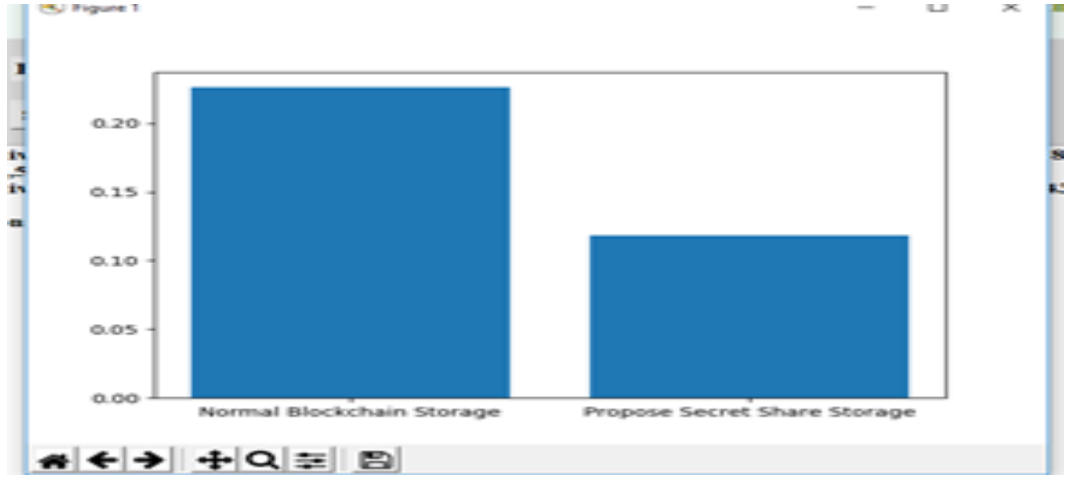
 Electronic healthcare data such as details oftreatment with all proofs of X- rays scan repots, subscription, images etc. with date and time wise detail as preprocessing will be required to store data into database.

 Data Preparation is required. Data pre- processing is the most important step that helps in building model more accurately

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

V RESULTS

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023



VI .CONCLUSION

This paper proposes a novel EHRs sharing scheme enabled by mobile cloud computingand block chain. We identify critical challenges of current EHRs sharing systems and propose efficient solutions to address these issues through a real prototype implementation. In this work, our focus is on designing a trust worthy accesscontrol mechanism based on a single smart contract to manage user access for ensuring efficient and secure EHRs sharing. To investigate the performance of the proposed approach, we deploy an Ethereum block chain on the Amazon cloud, where medical entities can interact with theEHRs sharing system via a developed mobile Android application. We also integrate the peer-to-peer IPFS storage system with block chain to achieve a decentralized data storage and data sharing. The implementation results show that our framework can allow medical users to share medical data over mobile cloud environments in a reliable and quick manner, in comparison to conventional schemes. In particular, our access control can identify and prevent effectively unauthorized access to the e-healthsystem, aiming for achieving a desired level of patient privacy and network security. We also provide security analysis and extensive evaluations on various technical aspects of the proposed system, showing advantages of our proposal over existing solutions. Based on the merits of our model, we believe that our block chain enabled solution is a step towards efficient management of e-health records on mobile clouds, which is promising in many healthcare applications.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

REFERENCES

[1] V. Sharma, "An energy-efficient transaction model for the blockchain-enabled Internet of Vehicles (IoV)," IEEE Communications Letters, vol. 23, no. 2, pp. 246– 249, 2019.

[2] K. Croman, C. Decker, I. Eyal et al., "On scaling decentralized blockchains," in Financial Cryptography and Data Security, pp. 106–125, Springer, Berlin, Germany,2016.

[3] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," IEEE Access, vol. 6, pp. 22970– 22975, 2018.

[4] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: a memory optimized and flexible blockchain for large scale networks," Future Generation Computer Systems, vol. 92, pp. 357–373, 2019.

[5] R. K. Raman and L. R. Varshney, "Distributed storage meets secret sharing on the blockchain," in Proceedings of Information -eory and Applications Workshop (ITA), San Diego, CA, USA, February 2018.

[6] Y. Kim, R. K. Raman, Y.-S. Kim, L. R. Varshney, and N. R. Shanbhag, "Efficient local secret sharing for distributed blockchain systems," IEEE Communications Letters, vol. 23, no. 2, pp. 282–285, 2018.

[7] S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in E-voting," Electronic Notes in -eoretical Computer Science, vol. 186, pp. 67–84, 2007.

[8] C. Guo, N. Luo, M. Z. A. Bhuiyan et al., "Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage," Future Generation Computer Systems, vol. 84, pp. 190–199, 2018.