ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940www.ijsem.org
Vol 14, Issuse.4 Dec 2023

Blockchain for securing Electronics Health Records, Sharing Mobile Cloud Based E-Health Sytem

R. RAVI[1], KATTOLLA PAVAN[2], JADHAV NAGAJYOTHI[3], SHENMALI PRANEETH[4], DEYYALA GOWTHAMNADH[5]

ABSTRACT:

Nowadays, electronic health records are an important system in cloud computing technology. Different types of algorithms are fostered various components by means of image based encryption for medical care applications. Although more security protocols werecreated among them without a doubt, not many procedures were proficient and hearty for the speedy recovery of reports from the cloud yet numerous conventions endure by reason of less security, privacy, and respectability. Existing techniques depended on encrypting the record in view of the key generation centre. To overcome the security issues a novel optimized Whale based Cryptographic Blockchain (WBCB) technique is proposed. Moreover, public cloud system is utilized to develop the technique efficiently. Here, the MATLAB platform is used for the implementation process. Furthermore, the developed technique is compared with conventional techniques such as encryption time, decryption time, etc.

Keywords: OpenCV, Face Detection, Face Recognition.

1. INTRODUCTION

Data in healthcare domain is highly sensitive in nature. Besides, there is need for maintaining integrity of such data. Blockchain technology has emerged to solve the problemof data integrity and non-repudiation with immutable storage in distributed repository. Thus secure data storage and retrieval in cloud environments is made possible using blockchain implementation. There are many existing healthcare systems with blockchain integration found in the literature. Blockchain technology is based on distributed network and it can be linked to cloud and distributed systems. Ngabo et al. [3] investigated on the possible integration of technologies such as IoT, fog computing and blockchain for seamless secure data storage of healthcare data in cloud. Blockchain can also be used in Mobile Cloud Computing (MCC) environments. Hguyen et al. [4] studied the possibilities of MCC linked to healthcare for integration with blockchain technology towards secure healthcare data sharing. There are many scenarios in which blockchain is integrated with healthcare applications for privacy and security of data besides efficient data sharing as discussed in [9] and [10]. From the literature, it is observed that there are many contributions in healthcare-blockchain integration. However, most of the works are conceptual and theoretical in nature. In this paper, we followed an empirical approach with healthcare application and smart contracts for secure storage and retrieval of electronic health records. Our contributions in this paper are as follows.

1Assistent Professor, Department of CSE-DS, Malla Reddy College of Engineering Hyderabad, TS, India.
2,3,4,5 UG students, Department of CSE-DS, Malla Reddy College of Engineering Hyderabad, TS, India.

1.We proposed a Blockchain based secure healthcare data storage and retrieval system known as HealthBlock for cloud computing environments.

2.We defined smart contract with underlying structures and functions using Solidity language for Ethereum blockchain platform.

3.We also proposed and implemented an algorithm known as Healthcare Transactions over Blockchain (HToB).

4.We developed an application to realize HealthBlock framework and the underlying algorithm besides evaluating the system.

2. LITERATURE SURVEY

Current related works based on securityand privacy of blockchain with cloud computing for medical data is summarizedbelow,Nowadays, wireless mobile technology, telemedicine systems, wearable technologies are rapidly turned up in the modern medicine world. Here, telemedicine information systems (TMIS) are very proficient healthcare management systems. Therefore, Salman shamshadet al.[21] has proposed a blockchain-based new e-health information sharing and storing system. This technology is only applicable to the telemedicine environment. Moreover, anonymity and security are controlled by safety desires.Nagasubramanianet al.[22] has introduced a keyless signature infrastructure-based blockchain technology. Here, the healthcare information is termed as resource standards of the interoperability system. Moreover, all type of healthcare information is managed by the seven international Medicare organization standards. This proposed technology is ensuring confirmation as well as offers more integrity to health information. Consequently, the validation of the proposed techniques is compared with traditional techniques.In modern years, cloud computing-based electronic healthcare record sharing strategies are having several conveniences. Nonetheless, centralization techniques are exposed to data privacy and security preservation. Thus Yonget al.[23] has proposed a blockchain-based security preserving protocol to secure electronic medical information from third parties. Here, data providers and data owners are the main contributors to the entire system's performance. Any one of the contributors can destroy the system the whole system is collapsed.Lately, cloud storage administration has generally drawn in the medical care industry and hospitalization. Moreover, health care managements are step by step rethinking the enormous scope of electronic medical care records on the cloud computing system. These specific cloud computing-based electronic medical care records are design works with high versatility, adaptability, minimal expense tasks, and accessibility to rethink the electronic medical care records.

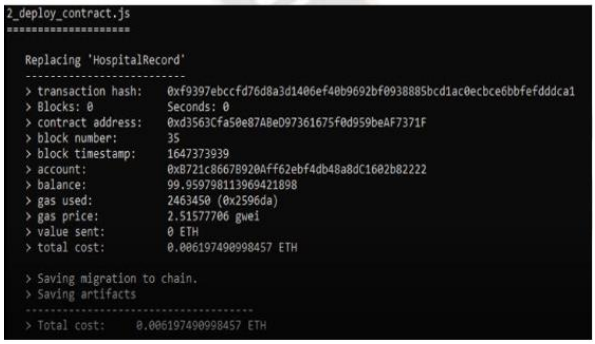
EXISTING SYSTEM:

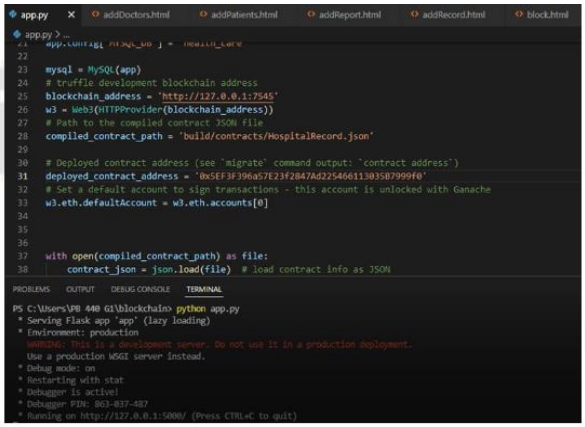
Data in healthcare domain is highly sensitive in nature. Besides, there is need for maintaining integrity of such data. Blockchain technology has emerged to solve the problem of data integrity and non-repudiation with immutable storage in distributed repository. Thus secure data storage and retrieval in cloud environments is made possible using blockchain implementation. There are many existing healthcare systems with blockchain integration found in the literature. However, there is need for a system that supports complete set of operations that are governed by smart contracts. Another important consideration is that end users should be able to operate healthcare system without the need for knowledge of blockchain technology. Towards this end, in this paper, we proposed a Blockchain based secure healthcare data storage and retrieval system known as HealthBlock for cloud computing environments. We defined smart contract with underlying structures and functions using Solidity language for Ethereum blockchain platform. We also proposed and implemented an algorithm known as Healthcare Transactions over Blockchain (HToB). This algorithm supports secure blockchain based data storage and retrieval governed by smart contracts. Our system is evaluated using user-friendly web based client application. The experimental results showed that our system is able to ensure data integrity and non-repudiation besides reaping all benefits of blockchain technology.

3. AN OVERVIEW OF PROPOSED SYSTEM

Nowadays, the digital performance of cloud computing-based blockchain technologies is the most important examination to enhance the security system during the data transmission periods.In the past lot of blockchain technologies are developed to achieve higher security. However, so many security issues are still now found in their cloud computing technology. To overcome such issues a novel whale-based Cryptographic Blockchain (WbCB) algorithm is developed to protect the cloud-based healthcare information during the data. transmission periods. Here, data owners of the cloud computing servers are only assessable for their cloud storage information. In addition, the proposed WbCB scheme was designed in the public cloud system. The proposed architecture is detailed in fig.3.Moreover, the proposed framework should guarantee the privacy and security of patient healthcare records. As a result, the framework needs to spread over the severe principles to ensure the healthcare information is honest and confidential also, the developed WbCB framework wants to predict the admittance of the healthcare records by any unapproved elements. Consequently, the framework has a higher ability to search the

files or patients despite the encryption process. However, the developed technique should offer the efficient capacity to confirm the records by any external related or third party substance. Here, the proposed strategy should accomplish elite execution and low expenses concerning price, storage, and latency to be appropriate reception in the clinical area.





4. CONCLUSION

The use of blockchain in healthcare systems plays a critical role in present health care industry, according to the study and the way the blockchain is embraced by different sectors. This may contribute to automated processes for data collection and reviewing, correcting and aggregating data from multiple sources that are permanent, tamper-resistant and provide safe data that have a lower risk of cybercrime. It supports distributed data with redundancy and device fault tolerance. In this research, the healthcare industry is addressing current issues. In order to achieve privacy and protection for patient information within the EHR program, we suggest a system architecture and access control policy algorithm based on blockchain based cryptographic method for participants & accessing the data securely. Implementation of a blockchain network-based EHR sharing framework. The research suggested removes the central authority and the system's inherent failure. System protection is accomplished by secure technology, as the ledger cannot be changed by any person as proposed system uses the keys for sharing and accessing the data. The caliper performance evaluations of the proposed system are completed with the configuration of block size, block build time, endorsement policies, and the proposed optimization of

REFERENCES

[1] Shuyun Shi, Debiao Hea,, Li Lia, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo "Applications of Blockchain in Ensuring the Security and Privacy of Electronic Health Record Systems: A Survey." Computers & Security (2020), doi:https://doi.org/10.1016/j.cose.2020.101966.

[2] AYESHA SHAHNAZ, USMAN QAMAR, AND AYESHA KHALID. "Using Blockchain for Electronic Health Records."

IEEE Access, vol. 7, pp. 147782–147795, 2019.

[3] Sabyasachi Dash, Sushil Kumar Shakyawar , Mohit Sharma and Sandeep Kaushik, "Big data in healthcare: management, analysis and future prospects", https://doi.org/10.1186/s40537-019-0217-0,springer 2019.

[4] Karim Abouelmehdi, Abderrahim BeniHessane and Hayat Khaloufi, "Big healthcare data: preserving security and privacy", https://doi.org/10.1186/s40537-017-0110-7,2018.

[5] Kashif Saleem, Xiaodong Yang, Abdelouahid Derhab, Mehmet A. Orgun, Waseem Iqbal, Imran Rashid, And Asif Yaseen "Privacy Preservation in eHealthcare Environments: State of the Art and Future Directions", October 30, 2017, 10.1109/ACCESS.2017.2767561.

[6] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba, "Blockchain Technology Innovations", 978-1-5090-1114- 8/17/$31.00 ©2017 IEEE.

[7] Pinyaphat Tasatanattakool, Chian Techapanupreeda, "Blockchain: Challenges and Applications", 978-1-5386-2290-2/18/$31.00 ©2018 IEEE.

[8] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 978-1-5386-1996-4/17 $31.00 © 2017 IEEE DOI 10.1109/BigDataCongress.2017.85.

[9] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Member, IEEE, Abdelouahid Derhab, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", 2327-4662 (c) 2018 IEEE.

[10] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," Futur. Gener. Comput. Syst., sep 2017.