Secure E-Healthcare System Using Block chain Technology

[1]Ms. Disha Kalbhor, [2]Mr. Vaibhav Deshpande, [3]Ms. Saishree Gole, [4]Mr. Shubham Deshmukh, [5]Mr. Umesh Nanavare

Department of Information Technology
Zeal College of Engineering and Research, Pune, India
Affiliated to Savitribai Phule Pune University

***Abstract*: in today's life healthcare security is most important issue. In block-chain technology, each page in a ledger of medical data forms a block. That block has an effect on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or block-chain. In proposed system data will be of Medical data need to secure. This work is designed using block chain concept and key-based cryptographic technique. Stores the hash tables of raw data and files on the block-chain, validates other copies by running a hashing technique, and then compares the data stored in the block-chain, any interfere with the data will be quickly found, because the original hash Tables are stored on millions of nodes. Proposed system work on storing data of healthcare data. This system will work on consensus mechanism while adding data in block chain. This system will find malicious user's and inform to owner.**

***Keywords*: Block chain, Data Encryption, Healthcare system, Security.**

I. INTRODUCTION

Block-chain is an emerging technology for distributed and healthcare data sharing across a large network of un-trusted participants. In today's day in healthcare system is growing fast also as well as the medical data need to store securely[5]. It allows new forms of distributed software architectures. Although the technology was mainly accepted in digital currency in initial days, but it is a promising technology for other areas too. This work is designed using block chain concept and key-based cryptographic technique.

Electronic health has become one of the main research topics. Because of the sensitivity of patient data, preserving patient privacy seems to be a challenge. In healthcare applications, patient data is generally stored in the cloud, making it difficult for users to have sufficient control over their data. However, due to the general data protection regulation, it is the data subject's right to know where and how their data was stored, who can access it and to what extent. In this article, we propose a block chain-based architecture for electronic healthcare applications that provides an efficient access control mechanism that preserves privacy. We take advantage of the special features of the block chain, namely the immutability and anonymity of users, while modifying the classical structure of the block chain to overcome their challenges in existing applications (for example low performance, high overload and latency). For this purpose, we group the miners of the block chain, store and process the data in the group closest to the patient

II. RELATED WORK

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.
In this section, we briefly review the related work on Health care Systems and their different techniques.

Luming Wan et al. examines [1] the effect of network latency on blockchain forking activity and potential breaches of the above six transaction acceptance confirmations. Authors simplify the data structure of the blockchain and stop large calculations in order to speed up our simulations proof-of-work (PoW) via simulation, authors demonstrate that the six confirmation agreement is vulnerable to peer-to-peer latency and also show how rapidly PoW mining is broken. It is not shocking that the latency of the underlying Peer to Peer network is severely impacted by the speed at which all nodes converge on the blockchain. It is also seen to what an unfair benefit in proof-of-work mining incentives will come from nodes with higher internet access.

WEILIN ZHENG et al. creates [2] a BaaS(blockchain as a service) framework called NutBaaS, which offers cloud computing environment blockchain services, for instance network integration and device management, intelligent contract analysis and checking based on such services, developers should concentrate their efforts on the market codes and find out, without bothering to manage and track the system, how blockchain technology can be applied more appropriately to their business situation.

Wenbin Zhang et al. suggest [3] a local blockchain voting protocol to help people vote on their native blockchain network with the need of any trustworthy or third party to promote decision making in a decentralised and safe way. This protocol safeguards complete secrecy and valuable properties such as detectability and cheating correction. An implementation of Hyperledger Fabric Protocol is also given which demonstrates the validity and functional application of our Protocol.

Sidra Malik et al propose [4] TrustChain as a trust management system that uses the blockchain consortium to monitor and dynamically delegate trust-related and reputation-based interactions among supply chain participants. Trustchain's innovation comes from: (a) a credibility model that assesses product consistency and the trustworthiness of individuals based on a number of supply chain case findings, (b) supporting the reputation ratings separating a supply chain participant and products, enabling the assignment for the same participant of product-specific reputation, (c) using intelligent contracts for transparent, effective, safe and automated calculation of reputation ratings and (d) minimum latency and output overhead, in comparison to a single blockchain.

Jinglin Qiu et al. propose [5] convergence of hospitals and intelligent cities has contributed to the use of information and technology in the field of healthcare and medical practise. The incorporation increased the quality of life and health of smart city residents. However, convergence has also opened the healthcare sector to safety issues, including patient protection and safety of nearby mobile health consumers. Blockchain is nonetheless a promising tool that enables health care to tackle safety issues in intelligent communities.

Anton Hasselgren et al. This research [6] demonstrates an unprecedented increase in efforts to employ blockchain technologies in the health sector. There are places in the health area where blockchain technologies may possibly be heavily affected.

AYESHA SHAHNAZ et al. explore [7] how blockchain technologies can be used to transform and solve EHR processes. We are presenting a platform that could be used in the EHR health sector for the application of blockchain technologies. The objective of our proposed structure is, first of all, to incorporate EHR's blockchain technologies and secondly, to ensure safe preservation of electronic documents by granular access regulations. In addition, the scalability issue of blockchain technologies generally by the use of documents off-chain storage, is discussed in this context.

DINH C. NGUYEN et al. propose [8] a new architecture for EHR sharing which combines the interplanetary decentralized (IPFS) blockchain on mobile cloud platforms. In order to achieve safe EHRs sharing among patients and health care providers, authors especially design a confident access control framework using intelligent contracts. In a real data sharing situation, authors introduce a prototyping implementation using Ethereum blockchain in Amazon's cloud computing smartphone app. Empirical findings suggest that our proposal offers an efficient alternative to secure mobile cloud data exchanges and preserves critical health data against future risks.

III. PROPOSED SYSTEM:-

1. In proposed system, we implement a block chain healthcare system, in which each patient upload a data files and encrypts these data with corresponding key.
2. To implement both privacy preservation and efficiency searches, we propose an efficient search scheme.
3. In this system, the cloud server is allowed to effectively merge multiple encrypted indexes, and securely perform the search without revealing the Patients' sensitive information, neither data files nor the queries.

System Architecture:

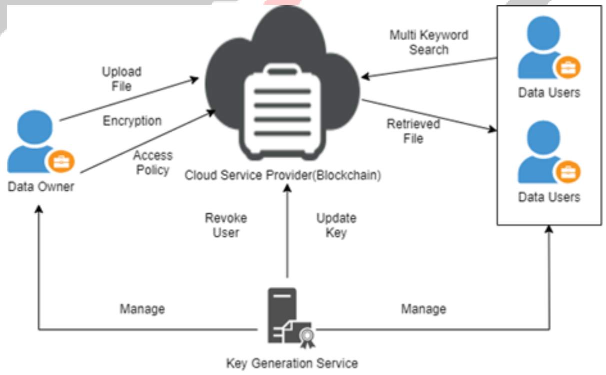


Figure 1. System Architecture

Algorithms:
1. AES Algorithm
It is symmetric algorithm. It used to convert plain text into cipher text .
The need for coming with this algorithm is weakness in DES/RSA.
The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak.
AES was to be used 128-bit block with 128-bit keys. **Input:**
Send an input file.
128 bit /192 bit/256 bit input (0, 1) Secret key (128 bit) +plain text (128 bit).
Process:

10/12/14-rounds for-128 bit /192 bit/256 bit input Xor state block (i/p) Final round:10,12,14 Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

Cipher text(128 bit)

IV. Results and Discussion:-

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel Pentium 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the various encryption algorithms such as AES, RSA. In our experiments, System first Install required Software.

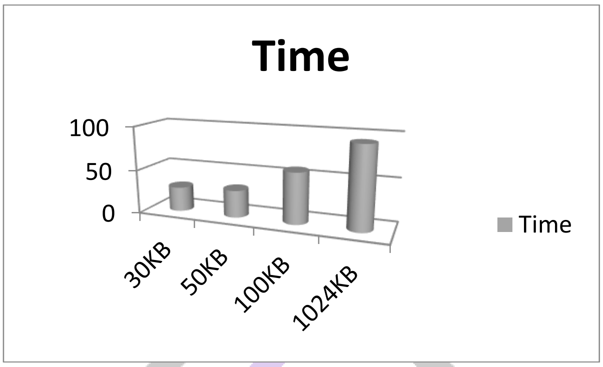
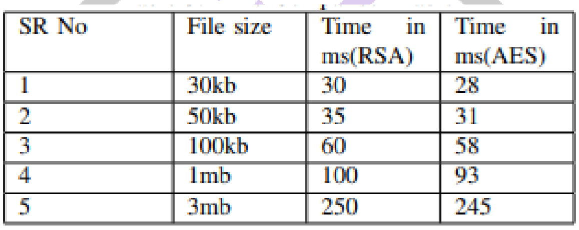


Figure 2 Show File Size and Time to Upload



SR No	File size	Time in ms(RSA)	Time in ms(AES)
1	30kb	30	28
2	50kb	35	31
3	100kb	60	58
4	1mb	100	93
5	3mb	250	245

Table 1Time Comparison Table

Conclusion

In work is designed using block chain concept and cryptography technique which estimate the security of block-chains specifically using hashing. Proposed system work to security on healthcare data. Block-chain technology is not just an application technology for new-generation data storage. It creates trust, responsibility and transparency while simplifying business processes. This approach allows users to authenticate the data access through the key of user sources, while improving network access performance by locally authenticating keys based on block-chain copies and its hash values. This work is designed using block chain concept and key-based cryptography technology to provide the security to healthcare data. It maintains the reliability and anonymity of the messages simultaneously.

References

[1] Luming Wan, David Eyers, Haibo Zhang” Evaluating The Impact of Network Latency on The Safety of Blockchain Transactions”IEEE international conference on blockchain 2019.

[2] WEILIN ZHENG , ZIBIN ZHENG , XIANGPING CHEN , KEMIAN DAI ,PEISHAN LI , AND RENFEI CHEN “NutBaaS: A Blockchain-as-a-Service Platform” IEEE Access 2019.

[3] Wenbin Zhang, Sheng Huang, Yuan Yuan□, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra” A Privacy-Preserving Voting Protocol on Blockchain” 2018 IEEE 11th International Conference on Cloud Computing.

[4] Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains. 2019 IEEE International Conference on Blockchain.

[5] Qiu, J., Liang, X., Shetty, S., & Bowden, D. (2018). Towards Secure and Smart Healthcare in Smart Cities Using Blockchain. 2018 IEEE International Smart Cities Conference (ISC2).

[6] Anton Hasselgren, Katina Kralevskab, Danilo Gligoroski, Sindre A. Pedersenc, Arild Faxvaag” Blockchain in healthcare and health sciences—A scoping review” science direct 2020.

[7] AYESHA SHAHNAZ, USMAN QAMAR, AND AYESHA KHALID" Using Blockchain for Electronic Health Records" IEEE Access 2019.

[8] DINH C. NGUYEN, PUBUDU N. PATHIRANA, MING DING AND ARUNA SENEVIRATNE" Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems" IEEE Access 2019