ISSN 2395-1621

Identity Based Authentication Of Health Records Using Blockchain

[1]Prof. D.S. Zingade, [2]Abhijeet Shedge, [3]Aishwarya Borate, [4]Sharayu Sawant, [5]Ajinkya Hole
deeplakshmissch@gmail.com[1] , abhijeet5424@gmail.com[2] ,
borateaishu@gmail.com[3] , sharayu6340@gmail.com[4] ,
holeajinkya118@gmail.com[5]
Department of Computer Engineering
AISSMS Institute of Information Technology
Kennedy Road, Near R.T.O. Pune 411001 Maharashtra (India)
Savitribai Phule Pune University

ABSTRACT

The Development of the internet has made a significant and important progress in recent few years. Protecting and making storage of these huge volume of data has become a big issue to handle. Traditionally, cloud based structure were used but they lead to high computation and storage demands on the cloud servers. Due to centralized servers there were many trust issues. To solve these problems, we have proposed in our paper a distributed data storage scheme which uses the Blockchain. Blockchain is an unchangeable distributed ledger which allows transactions take place in a Decentralized manner.

Keywords: Data Security, Encryption, Healthcare Information Management, Proxy Re-Encryption.

ARTICLE INFO

Article History

Received: 8th March 2020

Received in revised form :

8th March 2020

Accepted: 10th March 2020

Published online :

11th March 2020

I. INTRODUCTION

Traditional paper-based health records apparently are inconvenient for information interchange or sharing [1]. The technology of Electronic Health Records provides a novel way to collect and manage health-related information. It is more convenient than traditional paper-based health records for information storage and retrieval. Cloud is an open and shared environment for storage resources and computing resources. It provides end-users with a one-stop service of Anytime, Anywhere, Anything over the Internet [2]. However, the incidents that the cloud computing platform leaks user data continue to emerge. How to ensure the security of the cloud computing system has become a problem that cannot be ignored from the perspective of user data security requirements, research on security-critical technologies in cloud computing mainly focuses on data privacy protection, cipher text based data retrieval, cipher text-based proof of possession, and access control and other fields [4]. As access control is the first line of defence to prevent unauthorized users from accessing sensitive data in the cloud, it has attracted much attention and has become a hot topic of current research. In order to solve the problem of information sharing in the traditional Electronic Health Records, the cloud-based framework can be seen as an application of the could computing technology [2]. In cloud-based systems, there still needs a cloud service provider who plays the role of authority. As many sectors such as, all medical-related data, from doctor, pharmacy, diagnostic laboratory, insurance centre, and so on, will be uploaded to the cloud server [7]. Then, users can search and download useful information from the could server. In order to solve the problem of information sharing in the traditional Electronic Health Records, the cloud-based framework can be seen as an application of the could computing technology [8]. In cloud-based systems, there still needs a cloud service provider who plays the role of authority [3]. As many sectors such as, all medical-related data, from doctor, pharmacy, diagnostic laboratory, insurance centre, and so on, will be uploaded to the cloud server [7]. Then, users can search and download useful information from the could server.

II. LITERATURE SURVEY

Electronic records, produced in production and living activities, have shown rapid growth all over the world, and have gradually become the primary source of recording human activities and an essential source of information resources [1], [5], [6], [9]. Electronic records as a memory of social activities not only has the function of saving data but also has the evidence value [9]. Our findings show that academic research in this area has only just started and issues discussed in the selected literatures are still very limited [10]. Consequently, more intensive research in this area is still necessary to advance the maturity of this field of research. Particularly, empirical studies using rigorous research protocols should be enforced in government context to study the various potential benefits of block chain adoption [8]. Because of the excellent nature of blockchain-based solutions and the urgency of using blockchain as a trusted preservation solution to electronic records, there is a need for professionals to be more confident about the credibility of the technology of electronic records [1], [4], [7]. Block chain Technology is that the advance info technology in medical sector which require excellent knowledge sharing among connected parties within the network [9]. In the end, this thought of blockchain was being utilized in different fields of life. Social insurance part moreover being one of them plans to utilize it [9]. Various specialists have completed the exploration on this territory, these examination works centre around the way that whether utilizing blockchain for social insurance area is plausible or not [9]. They too distinguish the focal points, dangers, issues, or difficulties related by the use of this innovation [6].

III. Proposed system

In our proposed system we use Proof of work algorithm and RSA algorithm. We store the Medical data on cloud server and the data is maintained by cloud service provider. Our system solves the problem information sharing as it is stored on the cloud.

IV. system architecture

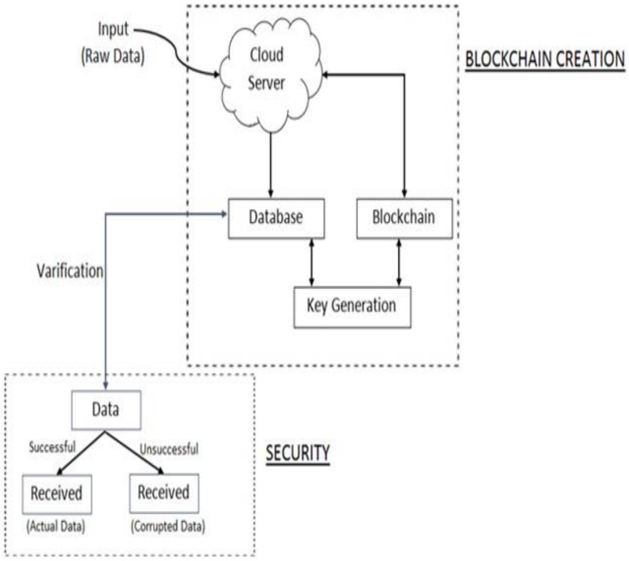


Fig 1: System architecture

Blockchain is considered as a new technological revolution that was introduced as the backbone of the bitcoin cryptocurrency. Assuming that there is a health record file system in a cloud storage platform, which consists of raw data(input). Thus, a file system with a blockchain structure is designed. All the information is encapsulated in one block and at different times will be generated in different blocks. Then, a series of blocks generated. Every block contains one file which located with unique key. Taking advantage of this technique, it achieves a perfect privacy-preserving for patient. Hence, it constructs a secure and controllable mechanism in files to confirm the validity of the data.

V. Algorithms

RSA Algorithm

RSA uses the arithmetic operations using modulo-n (mod *n*) arithmetic. x mod n means the remainder of x when divided by n [1].
For example,
22 mod 5 = 2.

In general, RSA constitutes of three important parts
1.Generate the public key and the private key
2.Encrypt data using generated public key
3.Decrypt data using generated private key

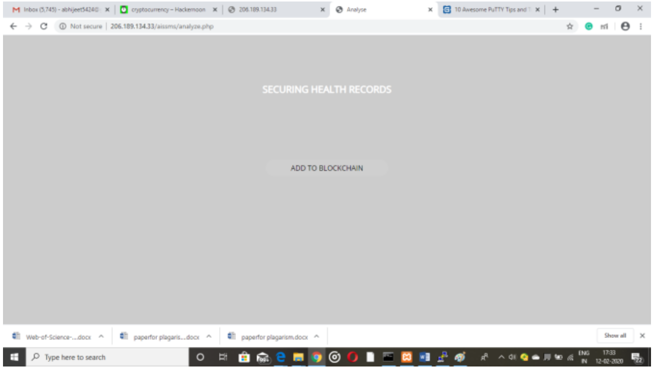
VI. Mathematical function

Our MA-IBS for blockchain-based Health records contains the following seven algorithms:
System Setup: The system setup algorithm is run by cloud server who takes as input a raw data file. Then it outputs system a filter data.
Authority Setup: The authority setup algorithm is interactively executed by all authorities who take as inputs filtered data and convert it into the blocks.
Key Generation: The key generation algorithm is also interactively executed by all authorities who take as inputs as filtered blocks of the data and generate unique keys ID1,ID2,…….IDn.
User-Sign: This sign algorithm is run by signer IDi who want to request particular record file from cloud server.
User-Verify: This verification algorithm can be publicly executed by all users who take as inputs the signer's identity *IDi*. Then it outputs *Accept* if it is valid; Else, outputs *Reject*.
Authority-Sign: This sign algorithm is run by user *IDi* who takes as inputs user requested file.
Authority-Verify: This verification algorithm can be publicly executed by anyone who takes as inputs identity *IDi*. Then it outputs *Accept* if it is valid; Else, outputs *Reject*.

VII. Experimental Results

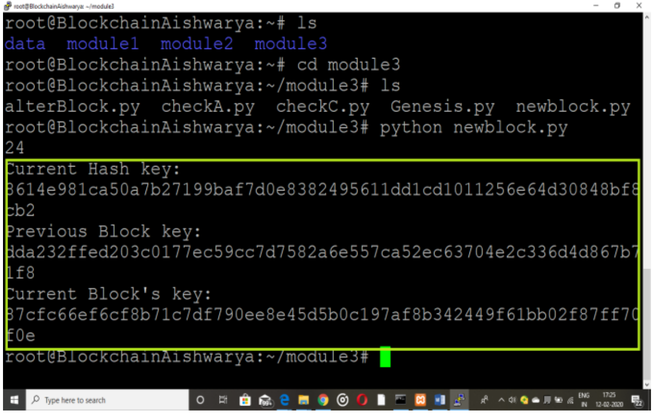
Experimental results are obtained from the raw medical data set. These results were used to verify our approach and compare it with existing ones.

1.Experiments on data uploading:-
Firstly, the raw data is captured from medical data set and is filtered according to need. Filtered data is uploaded on the cloud for securing that file.



2.Experiments on key Generation:-

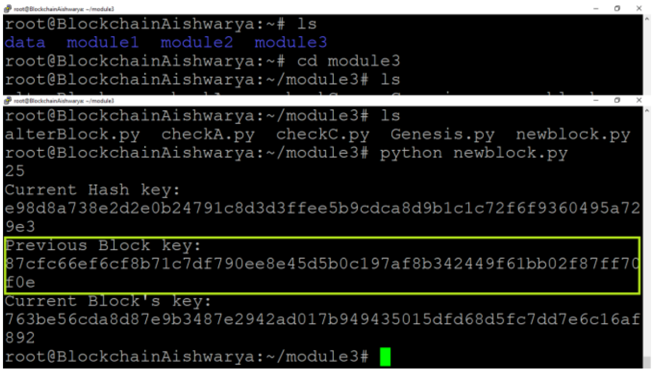
Filtered data uploaded on the cloud is taken as input and unique keys are generated using SHA256 key generation algorithm according to our approach



```
root@BlockchainAishwarya:~# ls
data  module1  module2  module3
root@BlockchainAishwarya:~# cd module3
root@BlockchainAishwarya:~/module3# ls
alterBlock.py  checkA.py  checkC.py  Genesis.py  newblock.py
root@BlockchainAishwarya:~/module3# python newblock.py
24
Current Hash key:
3614e981ca50a7b27199baf7d0e8382495611dd1cd1011256e64d30848bf8
cb2
Previous Block key:
dda232ffed203c0177ec59cc7d7582a6e557ca52ec63704e2c336d4d867b7
1f8
Current Block's key:
87cfc66ef6cf8b71c7df790ee8e45d5b0c197af8b342449f61bb02f87ff70
f0e
root@BlockchainAishwarya:~/module3#
```

3.Experiments on Blockchain creation:-

It is growing list of records called blocks. Firstly, the initial block that is Genesis block is created. Then the subsequent blocks follow as the new files are uploaded and the blocks are chained.


root@BlockchainAishwarya: ~/module3
root@BlockchainAishwarya: ~/module3

```
root@BlockchainAishwarya:~# ls
data  module1  module2  module3
root@BlockchainAishwarya:~# cd module3
root@BlockchainAishwarya:~/module3# ls
```

```
root@BlockchainAishwarya:~/module3# ls
alterBlock.py  checkA.py  checkC.py  Genesis.py  newblock.py
root@BlockchainAishwarya:~/module3# python newblock.py
25
Current Hash key:
e98d8a738e2d2e0b24791c8d3d3ffee5b9cdca8d9b1c1c72f6f9360495a72
9e3
Previous Block key:
87cfc66ef6cf8b71c7df790ee8e45d5b0c197af8b342449f61bb02f87ff70
f0e
Current Block's key:
763be56cda8d87e9b3487e2942ad017b949435015dfd68d5fc7dd7e6c16af
892
root@BlockchainAishwarya:~/module3#
```

VIII. Conclusion

It is known that Blockchain offers no of opportunities for usage in the healthcare sector, e.g. In public health management, user-oriented medical research based on personal patient data as well as drug counterfeiting. Blockchain shows enormous potential in the healthcare domain because it resolves issues related to medical records while providing security, privacy, validation, interoperability, and authentication. With help of innovative character, Blockchain technology will strongly affect the balance of power between existing market players in healthcare.

REFRENCES

[1] Fei Tang, Shuai Ma, Yong Xiang, (Senior Member, IEEE), And Changlu Lin, "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records", IEEE Access, 2018.

[2] Qi Xia Emmanuel Boateng Sifah2, Kwame Omono Asamoah, Jianbin GAO, Xiaojiang Du, (Senior Member, IEEE), And Mohsen Guizani, (Fellow, IEEE), "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain", IEEE Access, 2017.

[3] Rui Guo, Huixian Shi, Qinglan Zhao, And Dong Zheng, "Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems", IEEE Access, 2018.

[4] Dinh C. Nguyen, Pubudu N. Pathirana, (Senior Member, IEEE),
Ming Ding, (Senior Member, IEEE), And
Aruna Seneviratne, (Senior Member, IEEE), "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems", IEEE Access, 2019.

[5] Xiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen Li, (Member, IEEE), And Gaoping Li, "A Blockchain-Based Medical Data
Sharing and Protection Scheme", IEEE Access, 2019.

[6] Yong Wang, Aiqing Zhang, (Member, IEEE), Peiyun Zhang, (Senior Member, IEEE),
And Huaqun Wang, (Member, IEEE) "Cloud-Assisted EHR Sharing with Security and
Privacy Preservation via Consortium Blockchain", IEEE Aceess.

[7] Ayesha Shahnaz, Usman Qamar, And Ayesha Khalid, (Member, IEEE) "Using Blockchain for Electronic Health Records", IEEE Access, 2019.

[8] Zhiliang Deng, Yongjun Ren, Yepeng Liu, Xiang Yin, Zixuan Shen, and Hye-Jin Kim, "Blockchain-Based Trusted Electronic Records Preservation in Cloud Storage", IEEE Aceess,
CMC, vol.58, no.1, pp.135-151, 2019

[9] B. Narendra Kumar Rao, B. Bhaskar Kumar Rao, Vellingiri J, "Block chain Based Implementation of Electronic Medical Health Record", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue, 2019

[10] Haider Dhia Zubaydi, Yung-Wey Chong, Kwangman Ko, Sabri M. Hanshi and
Shankar Karuppayah, "A Review on the Role of Blockchain Technology in the Healthcare Domain". MDPI, 2019.