An Efficient Authentication Scheme for Block chain-Based Electronic Health Records

K.Venu Madhava Reddy
B.Tech, Department of Computer science and engineering, Narayana Engineering College Gudur

N.Koteswara Rao
Asso. Professor, Department of Computer science and engineering, Narayana Engineering College Gudur

A.Sasi Kumar Reddy
B.Tech Department of Computer science and engineering, Narayana Engineering College Gudur

K.Guru Teja
B.Tech Department of Computer science and engineering, Narayana Engineering College Gudur

ABSTRACT:

Electronic Health Records (EHR) are used to maintain the history of the Patient's health records. But now it is entirely controlled by the hospitals Patients face a critical need to focus on the details of their own healthcare and restore management of their own medical data. The fastest development of block chain technology promotes a secure healthcare system , that including medical records and patient-related data. This technology provides patients with an extensive, unmodified records and provides access to EHR for free of cost from service providers and treatment website. To warranty the endorsement of EHR encapsulated in block chain , we present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosed no information other than the evidence that he has attested to it.

.**Keywords:** Electronic health records, block chain, identity-based signatures, multiple authorities.

1. INTRODUCTION:

In today's digital world, different systems connect with each other for data and information transformation. Blockchain is a new technology that promises an efficient ,cost-effective, reliable and secure system for conducting and recording any transactions without the need of middleman[1]. The block chain network will be assigned a secret public and private key pairs. Public key acts as public address which is visible is all participants. A message can be encrypted using a private key. By using public key we can only read the data we cannot modify it.

2. EXISTING SYSTEM:

In the existing system the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship[2]. Patient access permissions to EHR are very limited, and patients are typically unable to easily share these data with researchers or providers. compatibility challenges between different providers, hospitals, research institutions, etc. add extra fence to high-performance data sharing. Without coordinated data management and exchange, the health records are distributed instead of cohesive.

3. PROBLEM STATEMENT

Similarity of problem lists in the healthcare industry is needed to enable more efficient exchange of information between health providers and especially to patients. Paper-based shapes do not work in electronic environments and some forms of problem list preparation, such as auto-population of lists, represent significant compliance and patient safety concerns.

4.PROPOSED SYSTEM

Block chain is considered as a new technological revolution that was introduced. It is a peer-to-peer distributed ledger technology to record transactions, agreements, and sales[3]. The benefits of the block chain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti- tamper and undeniable data security. Taking advantage of these distinguishing features above in an EHRs system, block chain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population.

Advantage of Proposed System:

I. Providing correct, up-to-date, and complete information about patients at the point of care.

II. license quick access to patient records for morecoordinated, efficient care.

III. Securely sharing electronic information with patients and other clinicians.

IV. Helping providers more effectively diagnose patients, reduce medical errors, and provide safer care

V. Improving patient and provider connection and communication, as well as health care convenience.

VI. Enabling safer, more reliable prescribing.

5.IMPLEMENTATION

MULTI-AUTHORITY ABS SCHEME IN EHRs SYSTEM

As described in the EHRs system model shown in Fig 1 and detailed ABS construction in this section. The proposal is an ABS scheme with multiple authorities which can be applied in the healthcare with blockchain technology[4].

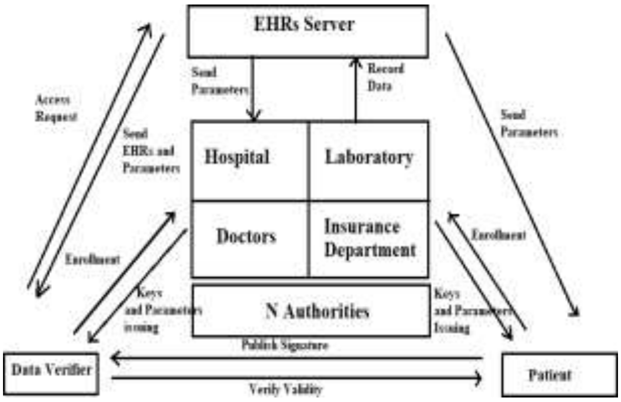

FIG .1 EHR SYSTEM MODELMA-ABS FOR HEALTHCARE IN BLOCKCHAINAPPLICATION

Blockchain is considered as a new technological revolution that was introduced as the backbone of the Bitcoin cryptocurrency. It is a peer-to-peer distributed ledger technology to record transactions, agreements and sales. The benefits of the block chain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security Taking advantage of the distinguishing features shown in Fig 2. Of EHR system, block chain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population health care smarter.

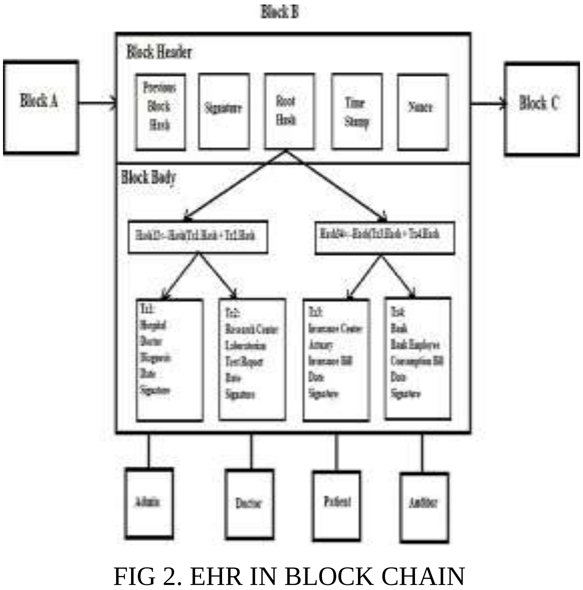

FIG 2. EHR IN BLOCK CHAIN

6.EHR SYSTEM MODEL

This EHRs system model consisted of the following four parties: an EHRs server, N authorities, patients and data verifiers. As shown in Fig. 3, the EHR server is just like a cloud storage server, which is responsible for storing and transmitting the EHR. N authorities are various different organizations, such as hospitals, medical insurance organizations, medical research institutes, etc., which are responsible for accepting the enrollment and exchange of patient information. Patients may create, manage, control and sign their own EHRs and define the predicate while the data verifier is allowed to access this signature and verify the correctness.

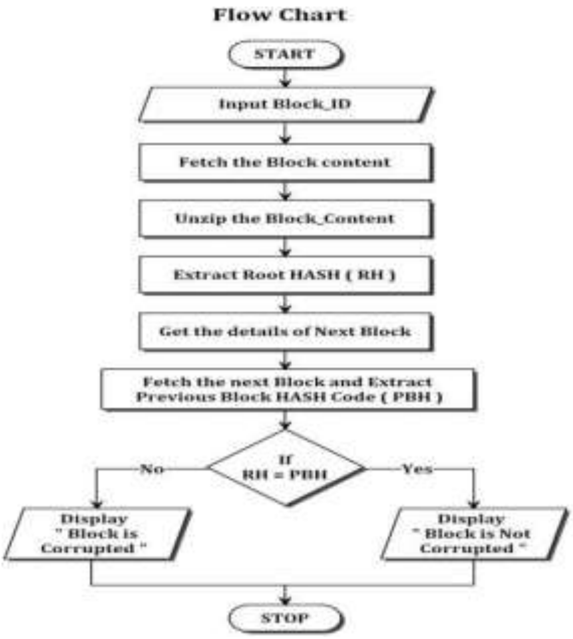
Flow Chart
START
Input Block_ID
Fetch the Block content
Unzip the Block_Content
Extract Root HASH (RH)
Get the details of Next Block
Fetch the next Block and Extract Previous Block HASH Code (PBH)
If RH = PBH
No
Yes
Display " Block is Corrupted "
Display " Block is Not Corrupted "
STOP

FIG 3 Flow Chart

7. RESULTS AND DISCUSSION

The result of this paper is mainly focused on preserving the data of the patients by providing security through blockchain and multiple ABS schemes. This subsection compares the efficiency as shown in Fig. 4 and other important properties of the proposed and previous ABS schemes by considering the hash function.

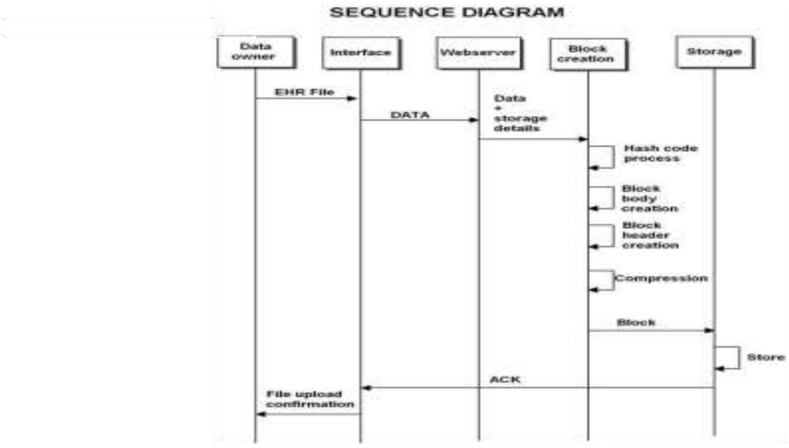

FIG 4 PERFORMANCE ANALYSIS

8. CONCLUSION AND FUTURE ENHANCMENTS

The main aim is preserving patient privacy in an EHR system on block chain, multiple authorities are introduced into ABS and a MA-ABS scheme is used, which meets the requirement of the structure of block chain, as well as guaranteeing the anonymity and immutability of the information. PRF seeds are needed among authorities and the patient private keys need to be constructed.

The comparison analysis demonstrates the performance and the cost of this protocol increases linearly with the number of authorities and patient attributes as well. A non-monotone predicate could be used in many distributed system applications, which enriches the representation of the predicate. Supporting general non-monotone predicates in blockchain technology is the direction of future work.

9.REFERENCES

[1] J. C. Cha, J. H. Cheon, “An identity-based signature from Diffie- Hellman groups,” PKC 2003, LNCS 25s7, 2003, pp.18–30.

[2] M. Bellare, J. A. Garay, T. Rabin, “Fast batch verification for modular exponentiation and digital signatures,” EUROCRYPT 1998, LNCS 1403, 1998, pp. 236–250.

[3] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, “Secure distributed key generation for discrete-log based cryptosystems,” EUROCRYPT 1999, LNCS 1592, 1999, pp.295–310.

[4] R. Guo, H. Shi, Q. Zhao, D Zheng, “Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,” IEEE Access, PP 99, 2018, pp.11676–11686.