International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 06, June 2022)

System for Electronic Health Records using Blockchain

Shiva Tiwari[1], Prof. Saurabh Sharma[2], Prof. Vishal Paranjape[3], Prof. Saurabh Kapoor[4]
[1,2,3,4]*Global Nature Care Sangathan Group of Institutions, Jabalpur (M.P), India*

Abstract: **The history of the patient's records is preserved using electronic health records (EHRs). But the hospitals have complete control over it. Patients must recover control over their own medical data and concentrate on the specifics of their own healthcare. Block chain technology's quick development encourages a safe healthcare system that protects patient data and medical records. This technology offers comprehensive, unedited records to patients and unrestricted access to EHRs from service providers and healthcare websites. We present an attribute-based signature scheme with multiple authorities to ensure the validity of EHRs encapsulated in block chains. In this scheme, a patient attests to the authenticity of a message based on an attribute while withholding all other information except for the proof that he has done so.**

Keywords: **Electronic Health Record System (EHRs), Blockchain, Multiple Authorities, Attribute Based Signature (ABS).**

I. INTRODUCTION

Electronic Health Records (EHRs) offer a service that is effective for maintaining health records, replacing the conventional paper-based patient medical records with digital ones that are available online. Patients currently scatter their electronic health records (EHRs) across many locations as a result of life events, which causes the EHRs to travel from one service provider database to another. Therefore, while the service provider often retains primary stewardship, the patient may lose custody of the current healthcare data. Patients often cannot easily access these data with researchers or clinicians since patient access permissions to EHRs are severely restricted. We provide Attribute-Based Signatures (ABS), which enable fine-grained control over identifying information when a party signs a message. A signer who owns a set of authority-issued attributes may sign a message in ABS with a predicate that is satisfied by those attributes. The signature shows that the message has been testified to by a single user who possesses a set of characteristics that satisfy the predicate. In particular, the signature conceals the predicate's properties and any personal data about the signer (that could link multiple signatures as being from the same signer). Additionally, users are unable to combine their attribute pools. After providing a generic framework for creating ABS schemes, we demonstrate various real-world examples based on groups with bilinear pairing operations while making the necessary presumptions.

In addition, we provide a structure whose security is demonstrated in the general group model, even in the presence of a malevolent attribute authority.

II. EXISTING SYSTEM

In the current system, the service provider typically retains primary stewardship while the patient may lose possession of the existing healthcare data. Patients generally find it difficult to share their data with academics or healthcare professionals since patient access permissions to EHRs are so restricted. High-performance data exchange is further hampered by interoperability issues between various hospitals, research institutions, providers, etc. The health records are dispersed rather than coherent if there isn't coordinated data management and exchange.

III. PROBLEM STATEMENT

To facilitate a more effective transmission of information between healthcare providers, and particularly to patients, problem lists must be standardised. Paper-based structures do not function in electronic contexts, and some methods of creating problem lists, such as auto-populating lists, raise serious issues with patient safety and compliance.

IV. 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. 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:

[1] Providing accurate, up-to-date, and complete information about patients at the point of care. [2] Enabling quick access to patient records for more coordinated, efficient care.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 06, June 2022)

[3]Securely sharing electronic information with patients and other clinicians. [4]Helping providers more effectively diagnose patients, reduce medical errors, and provide safer care. [5] Improving patient and provider interaction and communication, as well as health care convenience. [6] Enabling safer, more reliable prescribing.

V. IMPLEMENTATION

Multi-Authority Abs Scheme In Ehrs System

We now describe the EHRs system model 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.

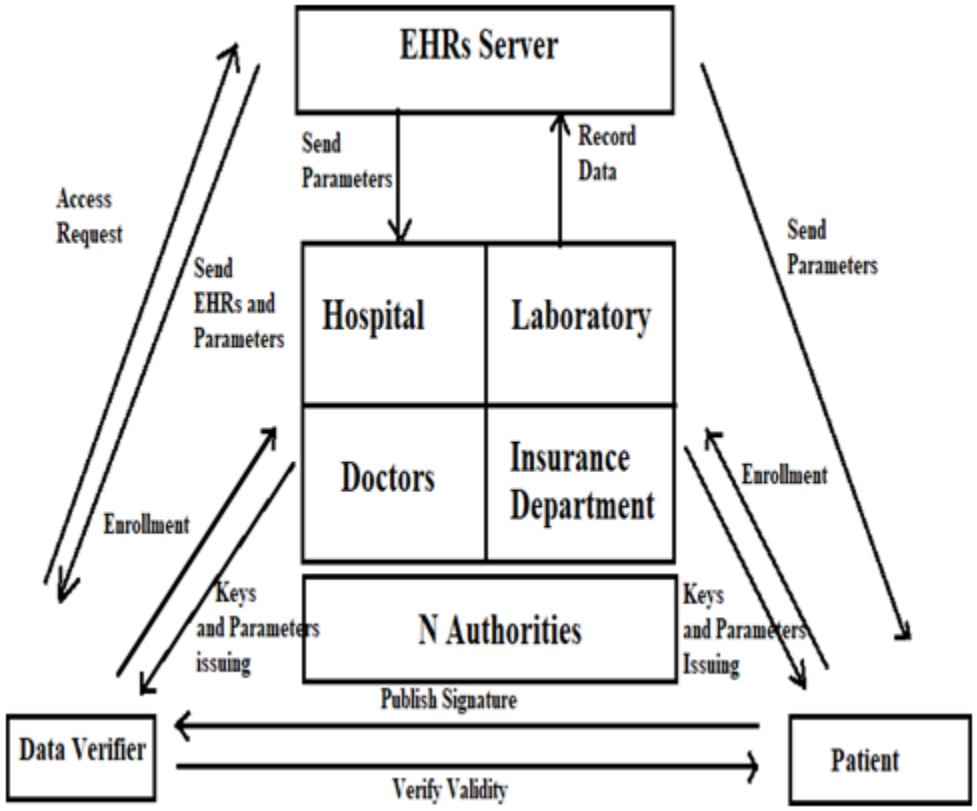

Fig 2.1. The EHRs system model.This model consisted of the four parties: EHRs Server, Authorities, Patient and DataVerifier.

MA-ABS For Healthcare In Blockchain Application

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 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 healthcare smarter.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 06, June 2022)

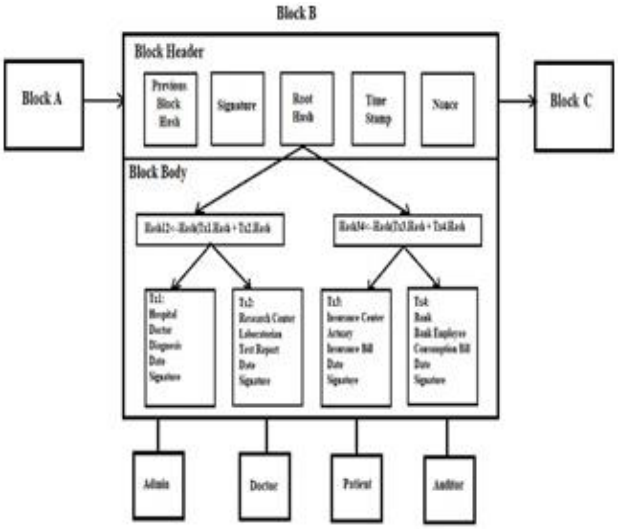

Fig 2.2 EHR System in Blockchain

VI. EHRs 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. 2.1, the EHRs server is just like a cloud storage server, which is responsible for storing and transmitting the EHRs. 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.

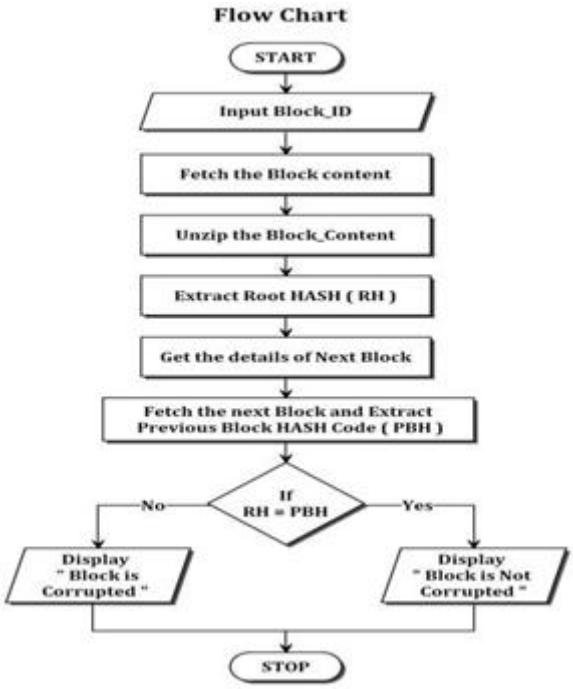

Fig 2.3 Flow Diagram of the working of model

VII. 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 and other important properties of the proposed and previous ABS schemes by considering the hash function.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 06, June 2022)

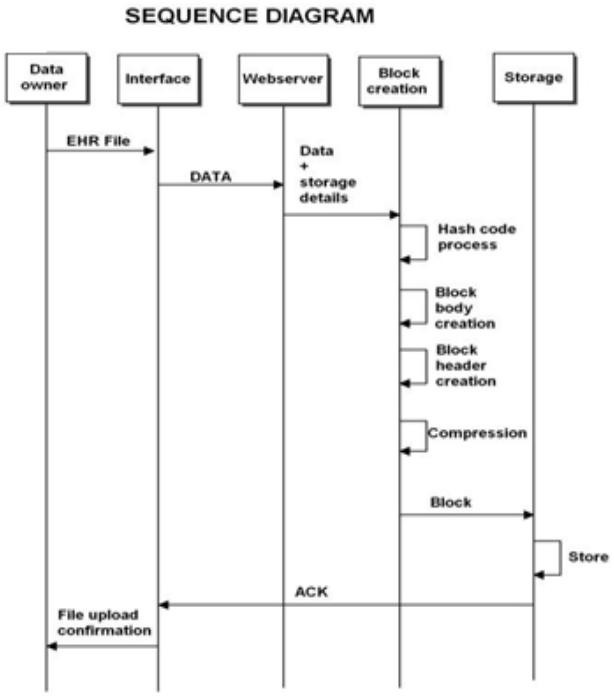

Fig 3.1 Performance analysis

VII. Conclusion And Future Enhancments

The main aim is preserving patient privacy in an EHRs 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 inblockchain technology is the direction of future work.

REFERENCES

[1] Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. (Aug. 20, 2015). Who Owns Medical Records: 50 State Comparison.[Online]..Available: http://www.healthinfolaw.org/comparative-analysis/who-owns-medicalrecords-50-state- comparison.

[2] K.D.Mandl,P.Szolovits,andI.S.Kohane,''Publicstandardsandpatients' control: How to keep electronic medical records accessible but private,'' BMJ, vol. 322, no. 7281, pp. 283–287, Feb. 2001.

[3] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: 2008. [Online]..Available:https://bitcoin.org/bitcoin.pdf

[4] World Economic Forum. (Sep. 9, 2015). Deep Shift: Technology Tipping Points and Societal Impact. [Online].. Available: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[5] (Dec. 12, 2016). Healthcare Rallies for Blockchains: Keeping Patients at the Center. [Online]..Available: http://www.ibm.biz/blockchainhealth

[6] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015, pp. 53–68.

[7] G.Prisco.(Apr.26,2016).TheBlockchainforHealthcare:GemLaunches Gem Health Network With Philips Blockchain Lab. [Online]..Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gemlaunches-gem-health-network-with-philips-blockchain-lab-1461674938

[8] U.S. White House. 104th Congress. (Aug. 21, 1996). Public Health Insurance Portability and Accountability Act. [Online].. Available:https://en.wikipedia.org/wiki/

[9] P. Taylor. (Apr. 27, 2016). Applying Blockchain Technology to Medicine Traceability. [Online]..Available: https://www.securingindustry.com/pharmaceuticals/applying-blockchain-technology-to-medicinetraceability

[10] P. B. Nichol. (Mar. 17, 2016). Blockchain Applications for Healthcare: Blockchain Opportunities are Changing Healthcare Globally-Innovative Leaders See the Change. [Online].. Available: http://www.cio.com/article/3042603/innovation/blockchain-applicationsfor-healthcare.html

[11] G. Irving and J. Holden, ''How blockchain-timestamped protocols could improve the trustworthiness of medical science,'' F1000Research, vol. 5, p. 222, May 2016.

[12] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, ''Searchain: Blockchainbased private keyword search in decentralized storage,'' Future Generat. Comput. Syst., 2017, doi: 10.1016/j.future.2017.08.036.

[13] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, ''Medical JPEG image steganography based on preserving inter-block dependencies,'' Computer Electrical Eng.,2017,doi:10.1016/j.compeleceng.2017.08.020.

[14] H. K. Maji, M. Prabhakaran, and M. Rosulek, ''Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,'' in Proc. IACR Cryptol. ePrint Arch., Apr. 2008, pp. 1–23. [Online] Available:https://eprint.iacr.org/2008/328.