IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

Blockchain Technology in Electronic Health Record System

Malavika M.B[1], Richa Kumari[2], Nihara S.M[3]

Department of Information Science & Engineering, SJB Institute of Technology,

BGS Health and Education City, Kengeri, Bangalore, India[1,2,3]

Abstract: Electronic Health Records (EHRs) are used to maintain the history of the Patient's records. But 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 rapid development of block chain technology promotes a secure healthcare system, including medical records as well as patient-related data. This technology provides patients with an extensive, unaltered records and provides access to EHRs free from service providers and treatment websites. To guarantee the validity of EHRs 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 disclosing no information other than the evidence that he has attested to it.

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

INTRODUCTION

Electronic Health Records (EHRs) provides service which is efficient for health record storage, it overcomes the traditional patient medical records on paper to be electronically accessible on the web. However, in the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily access these data with researchers or providers. We introduce Attribute-Based Signatures (ABS) that allows a party to sign a message with fine-grained control over identifying information. In ABS, a signer, who possesses a set of attributes from the authority, can sign a message with a predicate that is satisfied by his attributes. The signature reveals that a single user with some set of attributes satisfying the predicate has attested to the message. In particular, the signature hides the attributes used to satisfy the predicate and any identifying information about the signer (that could link multiple signatures as being from the same signer). Furthermore, users cannot pool their attributes together. We give a general framework for constructing ABS schemes, and then show several practical instantiations based on groups with bilinear pairing operations, under standard assumptions. Further, we give a construction which is secure even against a malicious attribute authority, but the security for this scheme is proven in the generic group model.

II. 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. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals, research institutions, etc. add extra barriers to high-performance data sharing. Without coordinated data management and exchange, the health records are distributed instead of cohesive.

III. PROBLEM STATEMENT

Standardization 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 structures 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.

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

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019

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.[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.

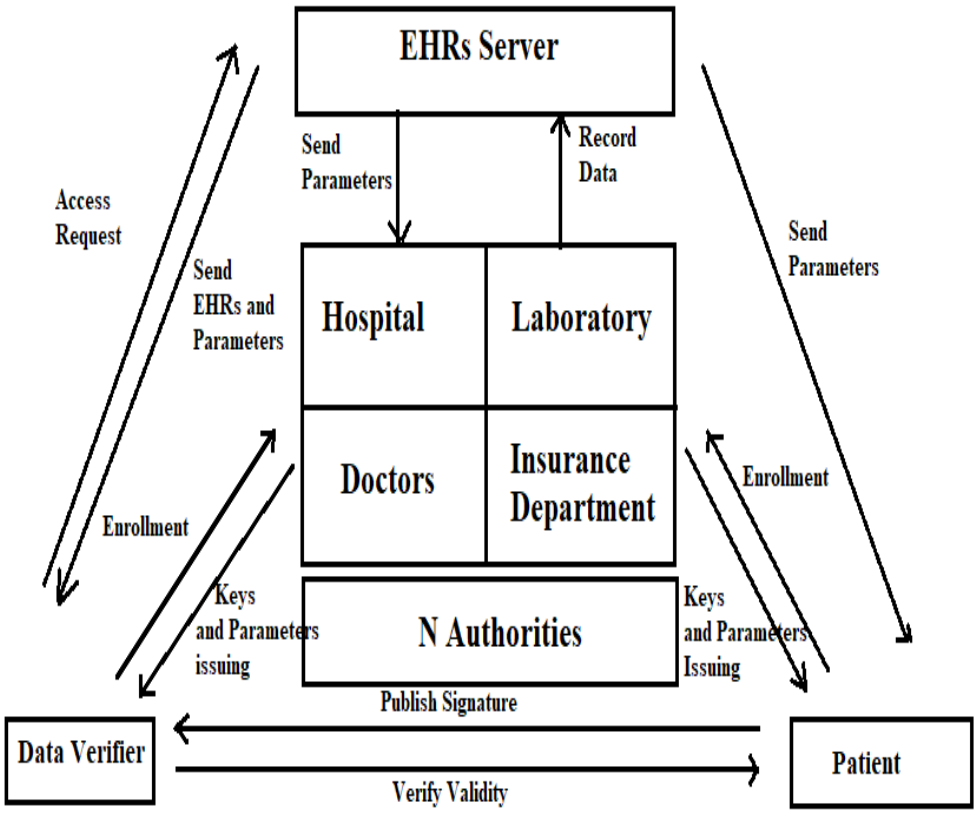

Fig 2.1. The EHRs system model.This model consisted of the four parties: EHRs Server, Authorities, Patient and Data Verifier.

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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019

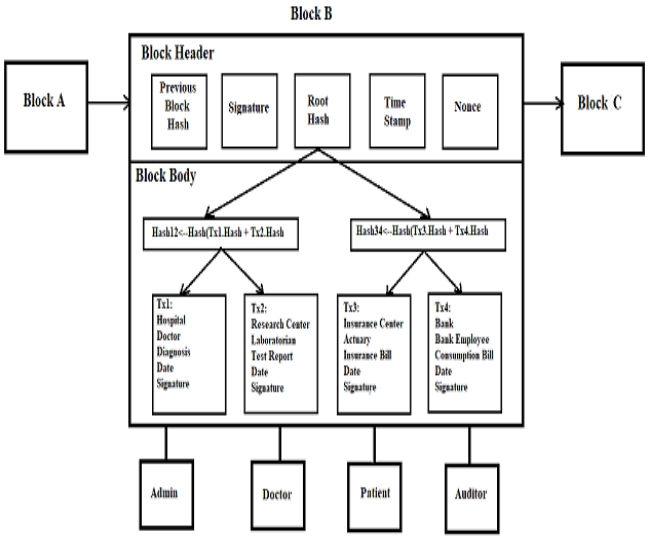

Fig 2.2 EHR System in Blockchain

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.

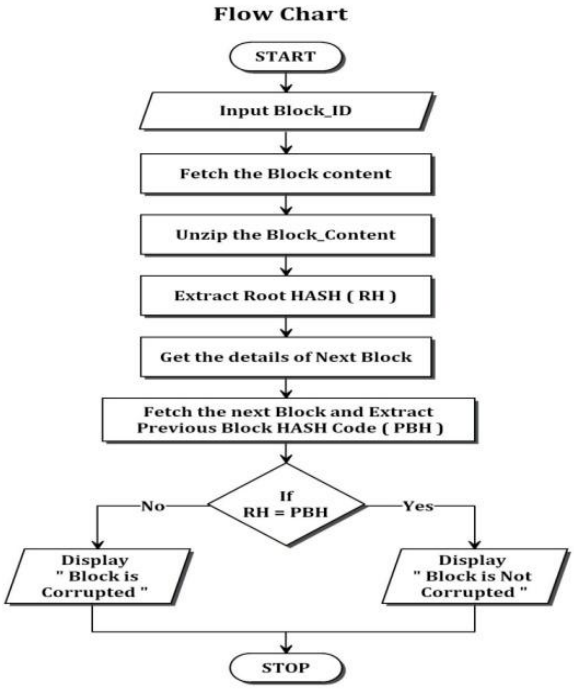

Fig 2.3 Flow Diagram of the working of model

3.1 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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019

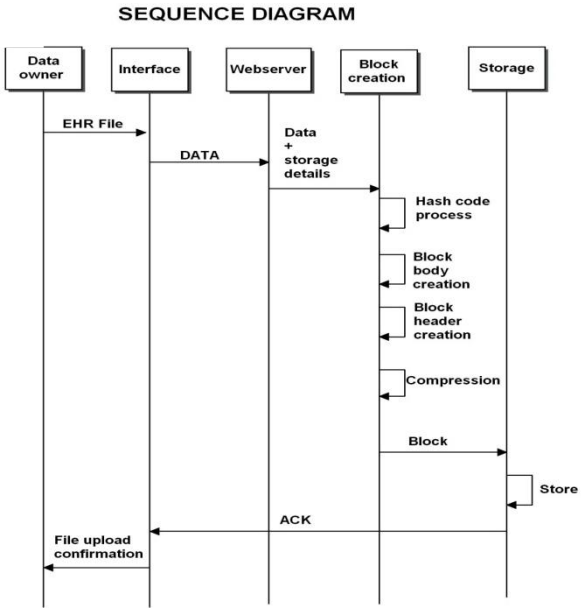

Fig 3.1 Performance analysis

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 in blockchain 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.