ELECTRONIC HEALTH RECORD MANAGEMENT WITH SECURE ATTRIBUTE BASED TECHNIQUE USING BLOCKCHAIN

[1]Vaishnavi Bijalpure, [2]Aishwarya Gawale, [3]Abhishek Gavande, [4]Pratiksha Agawane, [5]M. V. Shinde

Dept. of Computer Engineering
MET Bhujbal knowledge City Nashik, Maharashtra

***Abstract*- Electronic Health Records (EHRs) are entirely controlled by hospitals instead of patients, which complicates seeking medical advice from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore managementof their own medical data. The rapid development of blockchain technology promotes population healthcare, including medical records as well as patient-related data. This technology provides patients with comprehensive, immutable records and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in blockchain, we present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the at- tribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attacks out of N from N 1 corrupted authorities. Under the assumption of the computational bilinear Diffie Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies**

***Key Words*: Hospital, Blockchain, Encryption, Detection, Patient, records.**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 3, May-June 2023

INTRODUCTION

Electronic Health Records (EHRs) provide a convenient health record storage ser- vice, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such services access these EHRs across-the board, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across 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 [1]. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers.

PROBLEM DEFINITION

Patients face a critical need to focus on the details of their own healthcare records and management of their own medical data. Our system provides patients with comprehensive,immutable records and access to EHRs free from doctors**.**

OBJECTIVE OF SYSTEM

- Providing accurate, up-to-date, and complete information about patients at thepoint of care.
- Securely sharing electronic information with patients and other clinicians.
- Enhancing privacy and secure patient data.
- Increase Data Security and Privacy
- Helping providers more effectively diagnose patients, reduce medical errors, and providesafer care.

Functional Requirements

- The System should be able to retrieve the results stored on the database by using aquick retrieved process.
- The system application of modules must able to encrypt the data and decrypt itwhenever needed

Nonfunctional Requirement

- There should be minimal lag between taking of the processing and result
- The processing should be as efficient with maximum accuracy.
- The system should give valid results for positive as well as negative test cases.
- **Usability**: The ease with which the system can be learned, managed or used.Usability gives the measure of how user friendly the system is. •

Reliability: The degree to which the system must work for users. It also refers to themean time between failures, means what can be the maximum down time

- **Performance**: Performance specifications typically refer to response time, trans- action throughput, and capacity. They deal with response time, which means the timetaken by the system to load, reload, screen open and refresh times etc.
- **Scalability**: It refers to the ability of the proposed software application to increase thenumber of users or applications associated with the product.
- **Open standard**: t ensures the viability and future expansion of the system, all offereddevelopment tools, server software, as well as, the application are based on open templates and are available under the terms of the General Public License

Hardware Requirements

• AMD/Intel i3 Processor or above Processor • 4GB RAM for applicationdevelopment • 80 GB or above Hard Disk

Software Requirements

- Windows 7 or above
- Vscode, Xampp

SYSTEM ARCHITECTURE

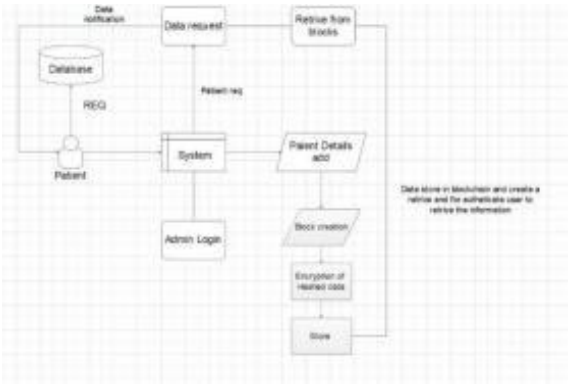

Fig -1: System Architecture Diagram

Project Scope

Blockchain is considered as a new technological revolution that was introduced as the backbone of the Bitcoin crypto currency. It is a peer-to-peer distributed ledger technology to record transactions, agreements, and sales. The benefits of the blockchain 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, blockchain enables the management of authentication, confidentiality, accountability and data sharing while handling information related to privacy, medical resource saving and facilitating for the patient, and making population healthcare smarter.

ADVANTAGES:

• Providing accurate, up-to-date, and complete information about patients at the point ofcare. • Securely sharing electronic information with patient and other clinicians.

• Enhancing privacy and secure patient data. • Increase Data Security and Privacy

• Helping providers more effectively diagnose patients, reduce medical errors, and providesafer care.

APPLICATION

• In Hospitals

• In Organizations

• Research

RESULT

CONCLUSION

Hence our system will overcome the drawback of the existing system , we are alsoproviding a better solution as compared to the existing system at an affordable price. Weare also planning to guarantee the validity of EHRs encapsulated in blockchain, we presentan attribute-based signature scheme with multiple authorities, in which a patient endorsesa message according to the attribute while disclosing no information other than theevidence that he has attested to it. Furthermore, there are multiple authorities without atrusted single or central one to generate and distribute public/private keys of the patient,which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain.

REFERENCES:

1. Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. (2015, Aug, 20). Who owns medical records: 50 state compar- ison. [Online]. Available: http://www.healthinfolaw.org/comparative analysis/who- ownsmedical-records-50-state comparison
2. K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' 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 cashsystem,"[Online].Available:https://bitcoin.org/bitcoin.pdf .
4. IBM, "Healthcare rallies for blockchains: Keeping patients at the center," Dec. 12, 2016. [Online].Available:http://www.ibm.biz/blockchainh ealth. [Online.]
5. "Blockchain Consensus Mechanisms", The buzz around,[online]Available:https://medium.com/datadr iveninvestor/blockchain-consensus- mechanisms 7aa0176d488a..
6. G. Sabarmathi and R. Chinnaiyan, "Big Data Analytics Framework for Opinion Min- ing of Patient HealthCare Experience", 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 352-357, 2020
7. G. Sabarmathi and R. Chinnaiyan, "Investigations on big data features research chal- lenges and applications", 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 782-786, 2017