|| Volume 6 || Issue 3 || March 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

AN APPROACH TOWARDS SECURE SHARING OF HEALTHCARE RECORDS WITH BLOCKCHAIN

Prajakta P. Kadam[1] , Prof. Prathamesh Powar[2]

Dept. of Computer Science and Engg. Ashokrao Mane Group of Institutions, Kolhapur Maharashtra, India[1]

Dept. of Computer Science and Engg. Ashokrao Mane Group of Institutions, Kolhapur, Maharashtra, India[2]

pariatthebest@gmail.com[1], pgcse@amgoi.edu[2]

Abstract: - The broad acknowledgement of cloud-based services in the healthcare area has achieved useful and supportive exchange of Healthcare Records among a couple of components of the e-Health frameworks. In any case, storing the secret health information to cloud servers is vulnerable to disclosure or burglary and requires the enhancement of methodologies that ensure the security of the PHRs. Hence analysed a methodology for secure sharing of the records in the cloud. The pro- posed system guarantees patient-centric control on the records and preserves the grouping of the records. The patients store the encoded records on the cloud servers and explicitly give access to different segments of records to dif- ferent sorts of people. A semi-trusted proxy called 'Setup and Re-encryption Server' (SRS) is acquainted with setting up data users with a general/private key, which combines and delivers there encryption keys. In addition, it uses Blockchain technology to share these records and secure privacy

Keywords: *Healthcare, Blockchain, Security, Encryption, Safety, Medical.*

I INTRODUCTION

In the medical system, the verification, preservation and synchronization of electronic medical records has always been a difficult problem, and the random dissemination of patient records will bring various risks to patient privacy. Therefore, how to achieve secure data sharing on the basis of ensuring users' personal privacy becomes the key. In recent years, blockchain has been proposed to be a promising solution to achieve data sharing with security and privacy preservation due to its advantages of immutability.

Problem Definition:

To solve the problem of data exchange between medical units and users, this proposed system will help to improve patient safety and quality care, but also reduce time and resources.

List of Modules:

1)Data Owner

2)Data User

3)Blockchain

Current Market Survey:

With growing people and growing technology trends nothing is private these days, But health records must be maintained securely so that no misuse can be done with health records

Scope of The Project:

- The proposed system is able to resist internal and external attacks.
- The generation of blocks and the algorithms are simple.
- The proposed system overcomes the dynamic access control problems.

II LITERATURE SURVEY

1.Pieter Van Gorp Marco Comuzzi,"Lifelong Personal Health Data and Ap- plication Software via Virtual Machines in the Cloud",IEEE Journal of Biomedical and Health Informatics (Volume: 18 , Issue: 1 , Jan. 2014).

In this paper, authors presented My PHR Machines, a novel PHR system. Leveraging virtualization techniques, My P HR Machines allows patients to build lifelong PHRs. The records can be shared by the patient with any stakeholder interested in those. MyPHR Machines allows also the controlled sharing of application software that is required to view and/or analyze health records. Patients seeking care by caregivers in different geographical areas will be able to reproduce their original health records, no matter the limitations imposed by the heterogeneity of local health care information systems.

2.Michael S. Dohan ,Mohamed Abouzahra and Joseph Tan,"

Mobile Personal Health Records: Research Agenda for Applications in Global Health",IEEE,47th Hawaii International Conference on System Science,2014.

This paper discusses six research areas in which mPHRs are applied to global health issues. These research areas are: applications that are disease specific and otherwise; ensuring local relevance of initiatives; using mPHRs for the collection of data for epidemic intelligence; innovative de- vices and infrastructures; integration with other technologies; and issues with global health initiatives that can apply these technologies. Despite the challenges with mPHRs, they remain a viable option for addressing the various global health concerns of today.

3.M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang," A general framework for secure sharing of personal health records in cloud system", Journal of Computer and System Sciences, 2017.

In this paper, authors proposed a general framework of secure sharing of PHRs. The system enables patients to securely store and share their PHR in the cloud server to their carers or family members. Treating doctors can further refer the patient's medical record to specialists for research purposes, while the patient's personal information remain private. In addition, cross domains operations can be supported. They provided a concrete instantiation of system. They also gave a simulation result for it.

4.Assad Abbas, Samee U. Khan,," A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.

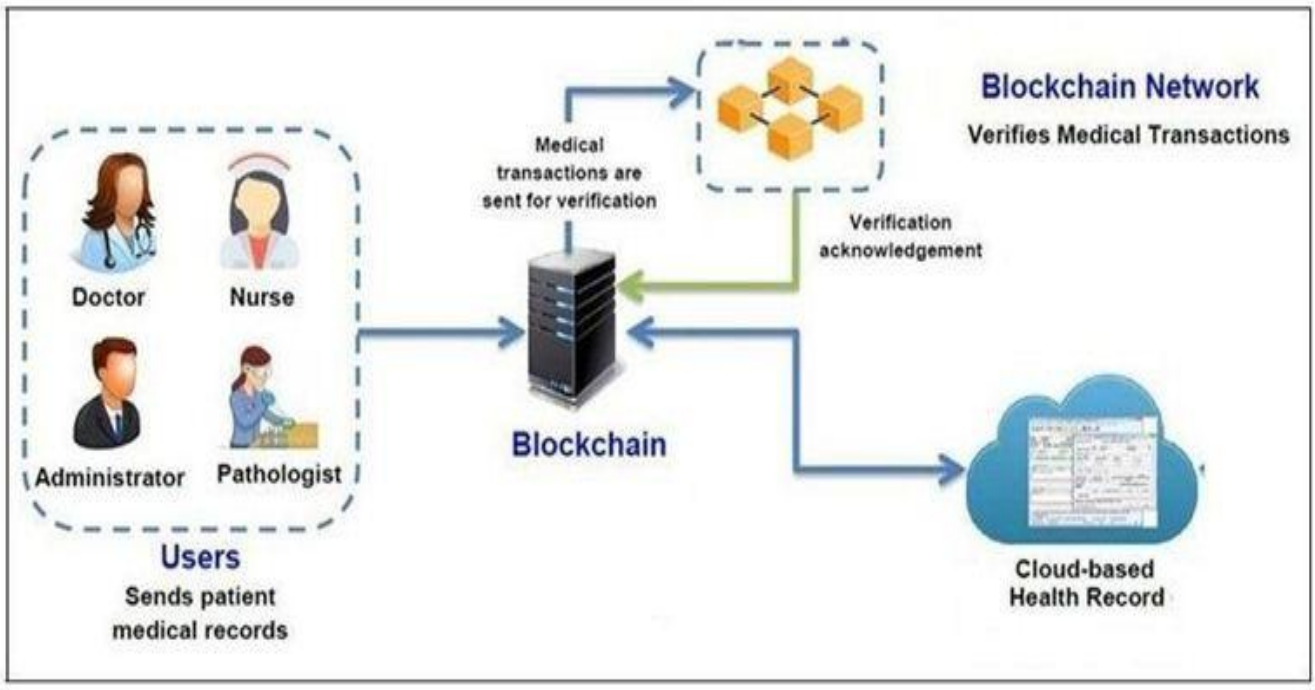
This paper aimed to encompass the state-of-the-art privacy preserving approaches employed in the e-Health clouds.

Moreover, the privacy preserving approaches are classified into cryptographic and non-cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted.

Securities to health records and secure sharing of records. Privacy of health records is maintained. The person can share his /her records with only concerned person. No other people can get access to these records and misuse it.

The design for fruit recognition includes the capture the image, extract features to classify the fruit and then recongnize it to determine whether it is infected

III SYSTEM ARCHITECTURE



IV PROPOSED METHODOLOGY

Methodology proposes an approach that grants patients to regulate the sharing of their own PHR's. The methodology utilizes the Blockchain methods to guarantee the PHR security.

Proposed System shows an approach called SeSPHR that grants patients to regulate the sharing of their own PHR's in the cloud.

The SeSPHR methodology utilizes the encryption and decryption to guarantee the PHR confidentiality. The approach enables the PHR owners to specifically allow access of their PHR to users over the segments based on the access level determined in the ACL for various groups of users. KGC produces the re-encryption keys , for various groups of PHR users in this manner , eliminating the key management

Verification of the proposed approach are performed to approve its working as indicated by the determinations.

V MODULES

1.Personal Health Record (PHR):

Doctors, nursing staff, pharmacies, clinical lab workers, insurance suppliers, and the service providers are the information users in Health network. Every data user has a lot of characteristics, for example, alliance, office, and sort of hospital services staff, and is approved to look on encoded PHR's dependent on his set of properties. In SeSPHR, a data utilizes asset constrained terminals to create secret keys and direct the data recovery activity. The secret keys are sent to the general public cloud by remote channel and recovered PHRdocuments are returned. At that point, the data user decrypts the PHR records and confirms the accuracy of decoding.

2.Blockchain:

The Blockcain guarantees the security of PHR

3.Public Cloud:

The Public Cloud has practically boundless storage and computing capacity. This is to embrace the PHR remote storage assignment and react on informa- tion recovery request. Lightweight test algorithm is structured in this proposed framework to enhance performance.

4.Key Generation Center(KGC):

KGC creates open parameters for the whole system and distributes secret keys to data users. A data users, set of qualities is inserted in his secret key to acknowledge access control. If the traitor sells his secret key for financial profit, the KGC can trace the character of the malicious user and revoke his secret key.

VI MATHEMATICAL MODEL

Let S be the whole System,

•S = {I, P, O}

I = Input

P = Procedure O = Output

- users U =Doctors, Nurse,Medical Officer , Insurance
- Keywords K = K0,K1,K2.. Kn
- PHR = Personal Health Record
- trapdoor generation T =t1,t2,..tn
- I = {I0, I1,I2 }
- I0 = U
- I1 = K
- I2 = PHR
- P = {P0, P1, P2, P3}
- P0 = Block Chain PHR
- P1 = K
- P2 = T
- P3 = key Generate
- P4 = Sell Secret key
- O = {O0, O1, O2}
- O0 = PHR
- O1 = User revocation
- O2 = Traitors identify

VII CONCLUSION

We proposed a procedure to safely store and transmission of the PHRs to the authorized elements in the cloud. The strategy preserves the security of the PHRs and authorizes a patient-driven access control to various segments of the PHRs on the access provided by the patients. We executed a fine-grained access control tech- nique so that even the valid system clients can't get to those segments of the PHR for which they are not authorized. The PHR owners store the encrypted information on the cloud and just the approved users having valid re-encryption keys issued by a semi-trusted authority can decrypt the PHRs. The job of the semi-trusted authority is to produce and store the public/private key sets for the clients in the system. The performance Evaluation was done on the based on time required to generate keys, encryption and decryption tasks, and turnaround time. The trial results display the reasonability of the SeSPHR system to secure share the PHRs in the cloud environ- ment.

REFERENCES

1.K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things", Future Generation Computer Systems, 2018.

2.K. Gai, M. Qiu, and X. Sun, "A survey on FinTech", Journal of Network and Computer Applications, 2017.

3.M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system", Journal of Computer and System Sciences, 2017.

4.A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, Future Generation Computer Systems, 2015.

5.Assad Abbas, Samee U. Khan, Senior Member, "A Review on the State of- the-Art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.

6.J. Li, "Electronic personal health records and the question of privacy", Com- puters, 2013.

7.S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine- grained data access control in cloud computing", in Proceedings of the IEEE INFOCOM, March 2010.

8.David Daglish and Norm Archer, "Electronic Personal Health Record Sys- tems: A Brief Review of Privacy, Security, and Architectural Issues", IEEE 2009.