ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 12, December 2019**

# Survey on Securing Data with Blockchain and AI

Ravi Kajale[1], Aniket Raskar[2], Kiran Choudhari[3], Supriya Jagtap[4], Bharati R. Patil[5]

U.G. Student, Department of Computer Engineering, SEC, Someshwarnagar, Maharashtra, India[1,2,3,4]

Associate Professor, Department of Computer Engineering, SEC, Someshwarnagar, Maharashtra, India[5]

**ABSTRACT**: The broad acknowledgment of cloud based services in the healthcare sector has brought about practical and helpful trade of Personal Health Records (PHRs) among a few taking part elements of the e-Health systems. Nevertheless, putting away the secret health data to cloud servers is susceptible to revelation or theft and requires the improvement of approaches that guarantee the protection of the PHRs. Along these lines; we propose an approach called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the classification of the PHRs. The patients store the encrypted PHRs on the un-trusted in cloud servers and specifically grant access to various kinds of clients on various parts of the PHRs. A semi-trusted in proxy called Setup and Re-encryption Server (SRS) is acquainted with set up people in general/private key combines and to deliver the re-encryption keys. Besides, the strategy is secure against insider threats and furthermore authorizes a forward and in reverse access control. Moreover, we formally examine and check the working of SeSPHR strategy through the High Level Petri Nets (HLPN). Execution assessment in regards to time utilization demonstrates that the SeSPHR strategy can possibly be utilized for safely sharing the PHRs in the cloud. Here we are securing data by using blockchain.

**KEYWORDS**: Cyber space, Cloud security, data sharing, Private Data Center (PDC), EHR.

## I. INTRODUCTION

Image Cloud computing has emerged as an important computing paradigm to offer pervasive and on demand availability of various resources in the form of hardware, software, infrastructure, and storage. The cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service providers. Numerous methods have been employed to ensure the privacy of the PHRs stored on the cloud servers. The privacy preserving approaches make sure confidentiality, integrity, authenticity, accountability, and audit trial. Confidentiality ensures that the health information is entirely concealed to the unsanctioned parties, whereas integrity deals with maintaining the originality of the data, whether in transit or in cloud storage.

The broad acknowledgment of cloud based services in the healthcare sector has brought about practical and helpful trade of Personal Health Records (PHRs) among a few taking part elements of the e-Health systems. We propose an approach called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the classification of the PHRs. SeSPHR strategy can possibly be utilized for safely sharing the PHRs in the cloud.

## II. RELATED WORK

1. **A Review on the State of-the-Art Privacy Preserving Approaches in the e-Health Clouds,** 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 12, December 2019**

2. **A general framework for secure sharing of personal health records in cloud system,** This system enables patients to securely store and share their PHR in the cloud server (for example, to their carers), and furthermore the treating doctors can refer the patient's medical record to specialists for research purposes, whenever they are required, while ensuring that the patients information remain private. This system also supports cross domain operations (e.g., with different countries regulations).

3. **Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues,** This paper addressed design and architectural issues of PHR systems, and focused on privacy and security issues which must be addressed carefully if PHRs are to become generally acceptable to consumers.

4. **Achieving secure, scalable and fine-grained data access control in cloud computing,** This paper addressed challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. It achieved this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. This scheme also has salient properties.

5. **On the Resilience of a QKD Key Synchronization Protocol for IPsec,** In this paper, an authorization scheme was proposed for collaborative healthcare system to address the problem of information sharing and information security. The proposed scheme provides an efficient solution to security challenges related to authorization. The security analysis has showed that our proposed scheme is unforgettable, coalition resistant, and traceable as well as it providers confidentiality and anonymity.

6. **A hybrid solution for privacy preserving medical data sharing in the cloud environment**, This paper propose a practical solution for privacy preserving medical record sharing for cloud computing. Based on the classification of the attributes of medical records, we use vertical partition of medical dataset to achieve the consideration of different parts of medical data with different privacy concerns.

7. **A privacy-preserving attribute based authentication System for Mobile Health Networks**, paper proposed a decentralized system that leverages users' verifiable attributes to authenticate each other while preserving attribute and identity privacy. Moreover, we design authentication strategies with progressive privacy requirements in different interactions among participating entities. Finally, we have thoroughly evaluated the security and computational overheads for our propose schemes via extensive simulations and experiments.

8. **Secure Sharing of Medical Records Using Cryptographic Methods in Cloud,**In this paper, The personal health records are now considered as the emerging trend in the personal health information exchange field. So cloud computing storage and sharing service is highly utilized by the users. We can provide good security to our data's using encryption technique in cloud the data security is the main privacy issue.

9. **A review on the state-of- the-art privacy preserving approaches in e-health clouds, This** survey aims 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.

10. **Improving privacy and security in decentralized ciphertext-policy attribute-based encryption,**In this paper, a privacy-preserving decentralized CP-ABE (PPDCPABE) is propose to reduce the trust on the central authority and protect users' privacy. In our collaboration to initial the system and issue secret keys to users.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 12, December 2019**

11. **Scalable and secure sharing of personal health records in cloud computing using attribute based encryption**, In the propose distributed attribute based encryption scheme PMR can be accessed from any hospital using a single key thereby reducing the complexity of key management.

12. **Attribute-based encryption for fine-grained access control of encrypted data,** develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute Based Encryption (KPABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption.

## III. DISADVANTAGES

- Does not cover all the aspects and applications.
- Integrity of the rank order in the search result assuming the cloud server is untrusted.
- Privacy and security to safeguard sensitive and personal digital information.

## IV. PROBLEM DEFINITION

To solve the problem of data exchange between medical units, we propose system which helps to improve patient safety and quality care, but also reduce time and resources.

## V. 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. 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.

## 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, Computers, 2013.
[7] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable and finegrained data access control in cloud computing, in Proceedings of the IEEE INFOCOM, March 2010.
[8] David Daglish and Norm Archer, Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues, IEEE 2009.
[9] Assad Abbas, Samee U. Khan, Senior Member, "A Review on the State-oftheArt Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.
[10] J. Li, "Electronic personal health records and the question of privacy", Computers, 2013.
[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and finegrained data access control in cloud computing", in Proceedings of the IEEE INFOCOM, March 2010.
[12] David Daglish and Norm Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues", IEEE 2009.
[13] Stefan Marksteiner, Benjamin Rainer, "On the Resilience of a QKD Key Synchronization Protocol for IPsec" 2016

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 12, December 2019**

[14] J. Yang, J. Li, Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, 2015, vol. 43-44, pp. 74-86.
[15] L. Guo, C. Zhang, J. Sun, Y. Fang. "A privacy-preserving attribute based authentication System for Mobile Health Networks," IEEE Transactions on Mobile Computing, 2014, vol. 13, no. 9, pp. 1927- 1941.
[16] M.P. Radhini, P. Ananthaprabha, "Secure Sharing of Medical Records Using Cryptographic Methods in Cloud. 2014
[17] A. Abbas, S. Khan, "A review on the state-of- the-art privacy preserving approaches in e-health clouds," IEEE Journal of Biomedical Health Informatics, 2014, vol. 18, pp. 1431-1441.
[18] J. Han, W. Susilo, Y. Mu. "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption" 2013
[19] M. Li, S. Yu, Y. Zheng, K. Ren,W. Lou. "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE transactions on parallel and distributed systems, 2013, 24(1): 131-143.
[20] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for finegrained access control of encrypted data," Proc. 13 th ACM Conf. Computer and Comm. Security (CCS'06), pp. 89-98,2006