



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

A futuristic digital interface with a glowing globe in the center. The background is dark blue with various data visualizations, including bar charts, line graphs, and network diagrams. Text elements like 'BUSINESS', 'NETWORK SEARCH', and 'LORDING 100%' are visible. A person's hand is seen at the bottom, interacting with the interface.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 11, November 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.569

9940 572 462

6381 907 438

ijrset@gmail.com

www.ijrset.com



A Methodology for Secure Sharing of Personal Health Records in Cloud

Snehal Somnath Ambre¹, Mansi Mukund Thigale², Rutuja Lalaso Bhosale³, Dhiraj Vinayak Surve⁴,
Prof. Chetan S. Pagar⁵

Department of Information Technology, Smt. Kashibai Navale Sinhgad Institute of Technology and Science,
Pune, India

ABSTRACT : Personal Health Records(PHR's) are a useful and supportive source for exchange of private data of patients in the healthcare arena. This is majorly achieved by storing the secret health information to cloud servers. Cloud Servers though secured can be exposed to the possibility of being misused for disclosure or theft by hackers. Thus they need new schemes to ensure the security of the PHR's. Here, we have used a methodology called PHR Sharing for secure sharing of the PHR's and enhanced it with a use of the lightweight algorithm and DROP algorithm for distribution of data over the replicated cloud. This method concentrates on patient-centric control on the PHR's. The patients store the encrypted form of PHR on the cloud servers and with help private key give access to different segments of PHR's to explicit people who need to know the information. A semi-trusted proxy called 'Setup and Reencryption Server' (SRS) is acquainted with setting up data users with a general/private key, which combines and delivers there encryption keys. The system data are stored in text or pdf file as part of PHR and then shared in the cloud.

KEYWORDS: Personal Health Records (PHRs),IoMT, Cloud Server, Healthcare Services.

I. INTRODUCTION

This Cloud computing and IoMT is transforming healthcare industry by providing large scale connectivity for medical devices, patients, physicians, clinical and nursing staff who use them and facilitate real-time monitoring based on the information gathered from the connected things. The cloud computing additionally incorporates different imperative elements such storage of vast data of healthcare domain. The security and privacy constraints for IoMT cloud includes confidentiality, integrity , authentication and accountability as prime key aspect. 'Privacy', guarantees that the health data is completely covered to the unsanctioned gatherings, while 'Integrity', manages to keep up the originality of the information. 'Authenticity' ensures that the health information is accessed by an authorized entity only, whereas 'Accountability' refers to the fact that the data access policies must comply with the agreed-upon procedures. Methodology called Secure Sharing of PHRs in the Cloud is enhanced with use of Advanced encryption algorithm (AES) which gives PHR more security and also as a control component managed by patients, limiting unauthorized users. PHR's are managed by patients such that they are be allowed to upload encoded form on the cloud. These PHR's can be used by patients themselves and by other people who are authorized by patient such as doctors , friends, family, insurance agent, etc. Access to these PHR depends on the role of user of PHR who are classified according to Access Control List(ACL) provided by patient himself for instance family might be given full access to the records whereas only Medclaim related records are shred with insurance agency. The system also includes the use of IoMT(Internet of Medical Things) to capture the live data of patient through WSN(Wireless Sensor Network).IoMT contains Temperature Sensor, Pulse Rate Sensor, Micro-controller. These sensors are embedded surface-mounted on the body of a patient which continuously monitor the vital physiological parameters of the patient such as body temperature, pulse rate. The values collected from these different sensors are stored in text or pdf file as part of PHR and then shared in the cloud. follow.

II. LITERATURE SURVEY

A. Abbas and S. U. Khan[7], This paper aimed to encompass the state-of-the-art privacy preserving approaches employed in the e-Health clouds. Automated PHRs are exposed to possible abuse and require security measures based on the identity management, access control, policy integration, and compliance management. 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. The cryptographic approaches to reduces the privacy risks by utilization of certain encryption schemes and cryptographic primitives. This includes Public key encryption, Symmetric key encryption, Alternative primitives such as Attribute based encryption, Identity based encryption, proxy-re encryption.

S. Yu, C. Wang, K. Ren, and W. Lou[14], addressed challenging open issue by, on one hand, characterizing and authorizing access policies dependent on information characteristics and then again enabling the data owner to assign a large portion of the task computation engaged with fine grained information access control to untrusted cloud servers without revealing the hidden information. It accomplished this objective by misusing and interestingly joining strategies of Attribute based encryption (ABE), proxy re-encryption, and sluggish re-encryption. This scheme likewise has notable properties of user access to benefit confidentiality and user secret key responsibility. Broad analysis demonstrates that this plan is exceptionally proficient and provably secures under existing security models.

M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang[3], gave a confirmed response to the issue by showing a general structure for secure sharing of PHRs. The presented framework empowers patients to safely store and share their PHR in the cloud server (for instance, to their careers), and moreover the treating doctors can refer the patients’ medical record to specialist for research purposes, at whatever point they are required, while guaranteeing that the patients’ data remain private. This framework additionally supports cross area activities (e.g., with various nations regulations).

P. V. Gorp and M. Comuzzi, present MyPHRMachines, a cloud-based PHR framework taking a profoundly new compositional answer for health record compactness. In MyPHRMachines, health related information and the application software to see and additionally analyze it are independently deployed in the PHR system. After uploading their medical information to MyPHRMachines, patients can get to them again from remote virtual machines that contain the correct software to visualize and analyze them with no requirement for transformation. Patients can share their remote virtual machine session with selected guardians, who will require just a Web browser to get to the pre-stacked sections of their long lasting PHR. There was a model of MyPHRMachines connected to two use cases, i.e., radiology picture sharing and customized medication[9].

D. Daglish and N. Archer[15], 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.

III. PROPOSED METHODOLOGY

The Proposed System shows an approach that grants patients to regulate the sharing of their own PHR’s in the cloud. The 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 overhead at the PHR owners end.

3.1 SYSTEM ARCHITECTURE

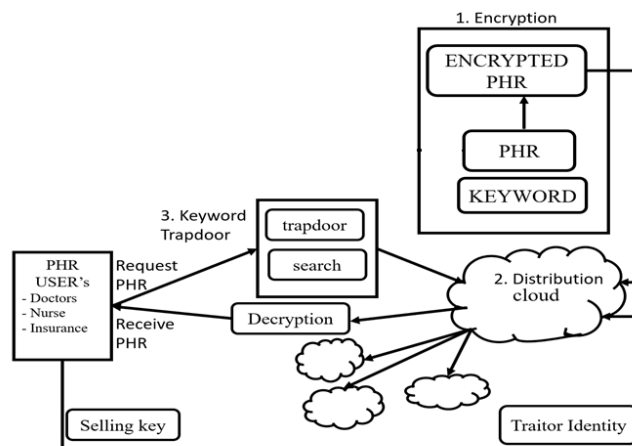


Fig 1: System Architecture



Fig 1. shows the architecture of proposed system for Secure Sharing of Personal Health Records in the Cloud using IoT.

1) Wireless Sensor Network (WSN) :

WSN includes small remote sensors that are inserted inside or surface-mounted on the body of a patient. These sensors constantly monitor the vital physiology parameters of the patient, for example, body temperature beat rate .Collected individual health information is aggregated and transmitted through a remote interface, for example, Bluetooth or WLAN. Keyword to delineate the health data is extricated from the health record. At that point, the keyword and PHR are encoded into a ciphertext under a particular access policy.

2) 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 system, 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 PHR documents are returned. At that point, the data user decrypts the PHR records and confirms the accuracy of decoding.

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 information 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

3.2 Algorithms

Algorithm 1: Advanced Encryption Standard (AES)

We made use of AES algorithm after comparing the same with DES algorithm in implementation. We used AES algorithm in Java .

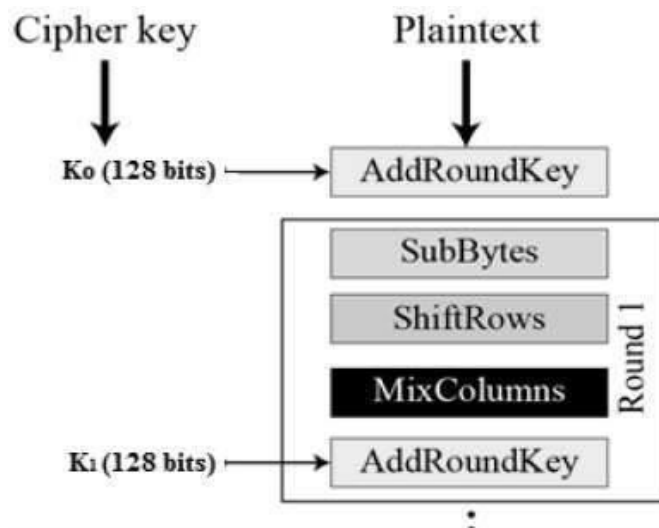


Fig 2: AES

Algorithm 2: Data in the Cloud for Optimal Performance and Security (DROPS)

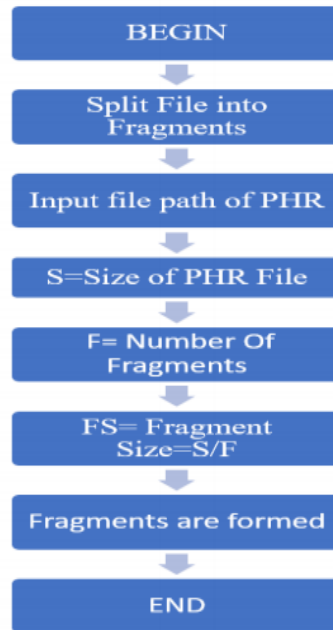


Fig 3: DROPS

is encrypted further it is used in before transferring data to cloud. Below figure shows steps used in algorithm.PHR is taken as input File which is then broken into fragments or chunks for level 2 of security.

IV. CONCLUSION

The enhanced methodology of securely stores data with help of Advanced Encryption Algorithm(AES) and transmits PHR's to the authorized users through use re encryption key issued by a semi-trusted authority. The activity of the semi-trusted authority is to deliver and store public/private key sets for the data-users in the framework. The technique preserves the security of the PHR's and authorizes a patient-driven access control. It is executing a fine-grained access control method so that even the valid system users can't access the fragments of the PHR for which they are not authorized. Future work can be done for PHR's in an advent towards machine learning and AI.

REFERENCES

[1] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multichannel 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] B. Qin, R. H. Deng, S. Liu, S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption", IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1384-1394, JULY 2015.

[6] J. Han, W. Susilo, Y. Mu. "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption", IEEE Transactions on Information Forensics and Security, 2015.

[7] A. Abbas, S. U. Khan, Senior Member, "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.

[8] M. S. Dohan, M. Abouzahra and J. Tan, Mobile Personal Health Records: Research Agenda for Applications in Global Health, Hawaii International Conference on System Science, 2014.



- [9] P. V. Gorp and M. Comuzzi, “Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud”, IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January 2014.
- [10] L. Guo, C. Zhang, J. Sun, Y. Fang, “A privacy-preserving attribute based authentication System for Mobile Health Networks”, IEEE Trans-actions on Mobile Computing, 2014.
- [11] J. Li, “Electronic personal health records and the question of privacy”, Computers, 2013.
- [12] A. Banerjee, P. Agrawal and R. Rajkumar, “Design of a Cloud Based Emergency Health-care Service Model”, Spvryan’s International Journal of Engineering Sciences & Technology (SEST) ISSN : 2394-0905, 2013.
- [13] 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.
- [14] 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.
- [15] D. Daglish and N. Archer, “Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues”, IEEE 2009



**Impact Factor:
7.569**



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details