A Survey on Auditing the Re-Encrypted Patients Health Records and Sharing with users on Cloud.

Prof. D. H. Patil [1], Atharv Potpelwar [2], Shital Kenjale [3], Pawan Pawar [4], Durgaprasad Mishra [5]

JSPM's Rajarshi Shahu College of Engineering, PUNE.

Abstract: The health care industry has a significant advantage of storing and exchanging of Patient's Health Records (PHRs) using cloud technology among various entities of the Health system. But still, to preserve the confidential records of patients on the cloud servers, it is permeable to afflatus and increment of request the event that methodologies make absolute privacy of the PHR. Therefore, we have the propensity to bend the proposed path mentioned as SeSPHR for the secure access of PHR's inside the cloud. The SeSPHR gives security to the patient-centered management of the PHR's and saves its furtiveness. Due to this, the patients can keep their encrypted data on an untrusted cloud server and share it with different selective users.

For encryption and Re-encryption, the Public, as well as Private access key, is used. Moreover, this security technique secures averse executive director bluster and keeps it together to apply for backward and forward access. In addition to this, we have the propensity to bend formally explore and verify the operation of the SeSPHR technique through the HLPN. The time consumption performance analysis for the SeSPHR technique has the potential to use for sturdily sharing of the PHR's on a different cloud. Put together, and we have the propensity to bend to implement as a contribution of this entire paper, time-bound and secure storage. In time-bound, the owner comes into the picture in starting and ending time after that attach and upload the encrypted files. And after all of that process, the TPA model is used to verify the PHR record, i.e., it checks if the data is hacked or corrupted. TPA also use to find out all details of a hacker if the PHR report is hacked, i.e. the contribution of TPA.

Keywords: *Access Control, Cloud Computing, Patients Health Records, Privacy, Proxy Server, Third Party Auditing*.

I. INTRODUCTION

Nowadays, cloud computing is in the emerging phase, and that is a vital computing example to give better output and on-demand facility of mixed resources at the different time-period the type software, hardware, storage, and infrastructure. Hence, cloud computing is one of the examples which gives a different facility to the organization so that they can decrease the extended job infrastructure development and have zinked them to believe in the third-part service. The cloud computing model has undeniable crucial potential to rise coordination diversely with several stakeholders and get a positive and continuous facility of the health knowledge and amount ability. To the addition of cloud computing and integrates diverse entities of aid domain like worker of a hospital, patients of the hospital And if we extend it, then it includes doctors, nursing workers, clinical laboratories, etc. therefore the mixed-up of all entities which are mention above are within the development of a price effective and cooperative well-being system where the owner can only manage and build our PHR. Due to the profitability of ascendable, price-efficient, and omnipresent features offered by the cloud's diverse privacy issues raised in PHR. The main apprehensions related to the furtiveness of PHR are by the patient's side is the nature of the cloud to share and store the PHR's. Saving private health data can be accessed by unauthorized users from third-parties. Especially, the privacy of the public cloud, which is managed by a business service provider, is very dangerous. Whenever the PHR is transferred from one user to another user on the cloud, it is at risk of unauthorized access. Also, the threat is that maybe an insider or an outsider can gain unauthorized access in the cloud server region resulting in the malicious behavior of external entities.

II. LITERATURE SURVEY

1. Secure Sharing of PHR's in the Cloud.

In recent times, the healthcare sector has accepted Cloud technology widely for storing and exchanging of Patients Health Records (PHR's). Although storing private health data on a cloud server is risky. Therefore, a technique is proposed for securely sharing the PHR's in the cloud called SeSPHR. It ensures patient-centered management of PHR's and maintains it's privacy. The patients store encrypted records on cloud servers and grant access to different users by selection. We have introduced a proxy server that is used for regeneration of the Patient's Health Record if the original file on the cloud gets corrupt. The proxy server adds more security while the re-generation of PHR's as the address of the proxy server is unknown. A dedicated server for key generation called Setup and Re-encryption Server (SRS) is introduced here for generating and sharing the key with patients and users. The re-encryption server makes sure the keys are safe and are shared with the authorized users only. One of the significant threats to store records on the cloud is to protect it from corporate executive threats. The methodology not only protects it from such threats but also enforces forward and backward access management — the performance analysis indicates that the SeSPHR method is capable and can be used for securely sharing the PHR's on the cloud [1].

2. Ciphertext Policy Attribute Based Signcryption.

Storing Patients Health Records on the cloud seems to be a trustful idea, but these non-public health records are sometimes outsourced to some third parties that may result in data leakage of Patients Health Records resulting in privacy issues and possibilities of unauthorized access of the Patients Health Records to individuals or organizations. So to eliminate this loophole, an approach is introduced called fine-grained access management and secure sharing of encrypted data(sign-then encrypt). The Patients Health records are first digitally signed and then stored on cloud in the encrypted format. It satisfies the previous issue of data leakage from cloud we were facing. This is known as Ciphertext Policy Attribute Based Encryption (Cp-ABSC). This methodology ensures genuineness, confidentiality, collision resistance, namelessness and unforgeability of the Patients Health Records. The security and correctness of the Patients Health Records are also covered using this method [2].

3. Cloud Incident Handling and Forensic by Design.

The information and cybersecurity or models unit area handling ways are essential to ensure the protection of organizations, mostly on cloud and large data environments. Nonetheless, current models or techniques are not satisfactory as the cloud is geographically distributed, virtualized, present in each territorial challenge and fleeting. And it comes with provincial and technical difficulties. Here, an integrated cloud handling and forensic by design model are introduced that focuses on validating the model and employs a set of control experiments on the cloud. Google Drive, Dropbox, and One Drive are the cloud storage applications where this methodology is deployed and implemented. This study undertakes the incident investigations and demonstrates the use of this model for cloud users (e.g., Collection and Analysis of residual information from these cloud storage applications) [3].

4. Blend Arithmetic Operations on Tensor based Fully Homomorphic Encryption Over Real Numbers.

Privacy and security of data are challenged every time with the vibrant growth and widespread acceptance of the cloud. These networking-based solutions bring various challenges to both outsider threats and corporate executives as well. A secure way of storing the data is in an encrypted format. But still, the process of storing data in encrypted form is facing a threat, and the process of encryption over data does not apply to cyphertexts. Fully harmonic encryption is a type of approach that permits computation over cyphertexts and can simultaneously deal with adversarial hazards. It uses tensor laws to perform calculations of arithmetic operations mixed with real numbers. In this analysis, a theoretical proof has demonstrated that impacts and adapts the planned approach [4].

5. Role Based Access Control.

In recent times the threat of data-stealing from the internal employees has been a risk to many organizations. It gets easy for them to access the data and leak it to outsiders. This may affect the organization severely. Also, as we are working on Patient's Health Records, they are one of the very personal and important documents of an individual. In cloud technology, as the data is stored distributedly, there is a major concern of data privacy and security, and various studies have proved that unauthorized access may cause massive losses, especially in the healthcare industry. Here, controlling the access of the PHR's becomes more and more crucial for the safety, security, and privacy of the PHR's. Among several access control methods such as DAC, MAC and RABC, The Remote Based Access Control (RBAC) model has come up with a way that meets the expectations of the access control needs. DAC is based on access matrix model. It allows to grant or revoke access privilege to the objects which belong to them. His is the main disadvantage of DAC. MAC is a better and stricter access control method than DAC. It is also called Latices-based access control. It assigns a special security attribute to subject and object. And, a subject can't change the security attributes of another subject. The RABC model states the rules to set up the process for granting or denying access to the users. Using this method we prevent unauthorized access to the PHRs stored on the cloud [5].

III. EXISTING SYSTEM

In the current million with no authority, the Insurance Movement and Responsibility Act rectify that health records must be protected from conditions of access and disclosure by suppliers to hold onto the integrity and confidentiality of electronic health data and with patients' permission. Besides, when a PHR organization owns third-party cloud storage, it must be encrypted in such a way that cloud server suppliers or unauthorized entities should not be able to use PHR. Besides, patients should provide the mechanism for providing access to the PHR so that any unauthorized alterations or misuse of knowledge can be avoided when forwarded to other stakeholders in the Health Cloud environment.

IV. PROBLEM STATEMENT

We are re-encrypting the PHRs and then store it on Cloud. The Third Party Auditing plays a great role in validating the PHRs' that are already stored on cloud. The Proxy Server is used to enhance the security of the PHRs' and regenerate them in case they are altered by someone when stored on cloud.

V. PROPOSED SYSTEM

Securely the PHR may remain in the cloud in the form of a re-encryption. Individual verified patients health records can also be sent to the user that is the doctor. A third-party auditor examines the PHR. With the use of dynamic time-bound, users can easily access the data for a certain amount of time. Suppose if the PHR data is being hacked, the third-party auditor can recover your data again. Suppose that every patient transfers their health records to the cloud. The Patient assession application creates random numbers for the user to divide the PHRs between different groups of access levels. In our given terms, assume that each of the four is graphical between units at an entirely different level of access. Here we are going to use a proxy server which is a proxy job type, but if any of these records get hacked then the proxy server sends the duplicate copy of the corresponding PHR data to the cloud.

VI. SYSTEM ARCHITECTURE

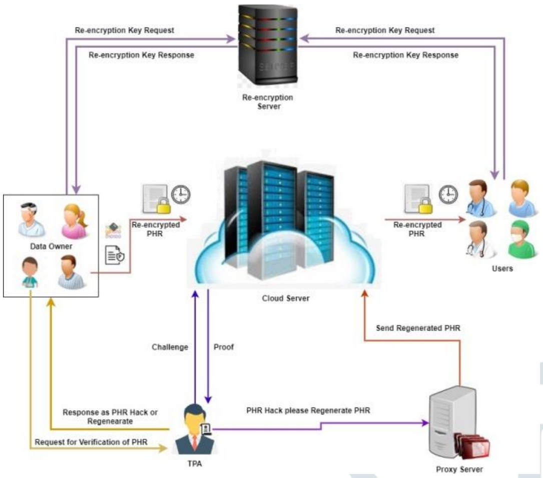
Re-encryption Key Request
Re-encryption Key Response
Re-encryption Server
Re-encryption Key Request
Re-encryption Key Response
Data Owner
Re-encrypted PHR
Cloud Server
Re-encrypted PHR
Users
Challenge
Proof
Send Regenerated PHR
Response as PHR Hack or Regenerate
Request for Verification of PHR
TPA
PHR Hack please Regenerate PHR
Proxy Server

Figure 1: System Architecture

VII. BLOCK DIAGRAM

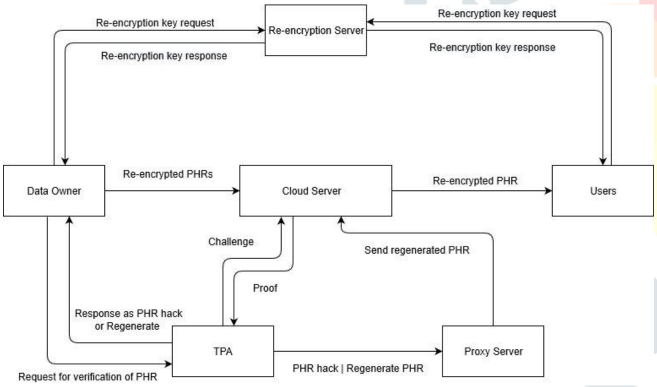
Re-encryption key request
Re-encryption Server
Re-encryption key request
Re-encryption key response
Re-encryption key response
Data Owner
Re-encrypted PHRs
Cloud Server
Re-encrypted PHR
Users
Challenge
Send regenerated PHR
Proof
Response as PHR hack or Regenerate
TPA
Proxy Server
Request for verification of PHR
PHR hack | Regenerate PHR

Figure 2 : Block Diagram

VIII. ALGORITHM

AES uses the Symmetric key in which the same key use for Encryption as well as Decryption. It has 128, 192, and 256 size bit key, and the number of rounds depends on key size selected.

A 128-bit key has ten rounds, the 192-bit key has twelve rounds, and the 256-bit key has fourteen rounds.

AES Encryption and Decryption Process: The given plaintext divides into 128-bit by considering the 4x4 matrix. It is called the state array.

- Encryption steps of AES:

  ➢ 1st Round: Add round key

  ➢ Repeat Nr-1 bound

1.Sub Byte 2. Shift Rows
3.Mix Columns 4. Add Round Key

- Final round:

  1.Sub Bytes 2.Shift Rows 3.Add round key

- Decryption Steps in AES

  - 1st Round: Add round key

  - Repeat Nr-1 round

    1.Inv Shift Rows 2.Inv Sub Bytes 3.Add Round Key 4.Inv Mix Columns

  - Final Round

    1.Inv Shift Rows 2.Inv Sub Bytes 3.Add Round Key

IX. ADVANTAGES

- Auditing operations performed on PHR's.
- PHR's data stored on the cloud in the re-encrypted format.
- We are securing as well as storing all the patients' data on the cloud.

X. DISADVANTAGES

- Dynamic operations not performed on the PHR's.
- Unable to remove duplicate PHR's from cloud.
- Memory wastage due to duplicate PHR's.

CONCLUSION

We have proposed a system to securely store the PHRs' along with the transmission of the PHRs to the authorized entities in the cloud. The methodology conserves the discretion in keeping secret information of the PHRs and enforces the patient centralized access management to entirely different parts of the patient's health records supported the access which is provided by patients. We tend to carry out a fine-grained accession management methodology in such a way that even the valid users cannot access the parts of the records or information that they're not approved. The homeowners of PHR's store the encrypted data cum records on the cloud, and only the authorized users can possess the valid re-encryption keys which are issued by a proxy unit to regenerate the PHR's. The function of the proxy is to provoke and store the public as well as private pairs of keys for the users inside the system. This also protects the confidentiality along with guaranteeing patient-centric accession management over the PHRs, forward as well as backward access management is achieved by the methodology along administers for outgoing of the new association users, independently. Furthermore, we inclined to tend to verify formally and analyzed the operation of secure sharing of patient's health records methodological analysis.

REFERENCES

[1] Mazhar Ali, Assad Abbas, Muhammad Usman Shahid Khan, and Samee U. Khan, *"SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud"*, 2018 IEEE, pp. 2168-7161.

[2] Jianghua Liu, Xinyi Huang, Joseph K. Liu, *"Scalable & Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Encryption"*, 2015 FGCS 52, pp. 67-76.

[3] Nurul Hidayah Ab Rahman, Niken Dwi Wahyu Cahyani and Kim-Kwang Raymond Choo, *"Cloud incident handling and forensic-by-design: cloud storage as a case study"*, 2016 Published on (wileyonlinelibrary.com).

[4] Keke Gai, Meikang Qiu, *"Blend Arithmetic Operations on Tensor-based Fully Homomorphic Encryption Over Real Numbers"*, 2017 IEEE, pp. 1551-3203.

[5] Dipmala Salunke and Anilkumar Upadhyay, "A survey paper on Role-Based Access Control", *IJARCCE*, Vol. *2, Issue 3, March 2013, pp. 1340-1342.*

[6] Mitash Sule and Dipmala Salunke, "Cost-Efficient Multi-Cloud Storage and Data Hosting with Cloud Computing Security Using AES Algorithm", *IJIRSET*, Vol. 5, Issue 5, May 2016, pp. 8725-8732.

[7] D.H. Patil, Rakesh R Bhavsar, Akshay S Thorve, "Data Security Over Cloud*", Emerging Trends in Computer Science and Information Technology -2012(ETCSIT2012), IJCA*, 2012, pp. 11-14.

[8] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, Atta ur Rehman Khan, "A Study of Incremental Cryptography for Security Schemes in Mobile Cloud Computing Environments*", IEEE Symposium on Wireless Technology and Applications (ISWTA)*, 2013.

[9] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud,"*Future Generation Computer Systems*, vol.35, 2014, pp. 102-113.
[10] Z. Xiao and Y. Xiao, "Security and privacy in cloud compu-ting," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 1–17, Jul. 2012.
[11] F. Xhafa, Fatos, J. Feng, Y. Zhang, X. Chen, and J. Li, "Privacy-aware attribute-based PHR sharing with user accountability in cloud computing,"*The Journal of Supercomputing*,2014, pp. 1-13.
[12] L. Ibraimi, M. Asim, and M. Petkovic, *Secure management of personal health records by applying attribute-based encryption*, Technical Report, University of Twente, 2009.