ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

A Methodology for Secure Sharing of Personal Health Records in Cloud Environment

Supriya Patil[1], Prof. Sandip D. Satav[2]

P. G Student, Dept of IT, JSPM College of Engg, Pune, Maharashtra, India[1]

Associate. Prof. Dept of IT, JSPM College of Engg. Pune, Pune, Maharashtra, India[2]

ABSTRACT: The Personal Health Record (PHR) is an emerging framework of health information exchange, which is often stored at cloud servers. But there are still various privacy problems as personal health information could be discovered to unauthorized people. To guarantee the patients control over to their own PHRs, it is a method to encrypt the PHRs before storing on cloud. But still issues such as risks of privacy, efficiency in key administration, flexible access and efficient user administration, have still remained the important challenges toward achieving better, cryptographically imposed data access control. ABE. This paper we proposes a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High Level Petri Nets (HLPN).

KEYWORDS : Access control, cloud computing, Personal Health Records, privacy

I. INTRODUCTION

In the proposed research work to design and implement a system that can provide the security to Personnel Health Records (PHR) files using semi trusted proxy re-encryption services, and eliminate the insider attacks like collusion attack, bruited force attack as well as SQL injection attack. In this research work to design and implement a security and privacy mechanism health care system such as, data confidentiality, data integrity and fine grained access control. The privacy and security are most affected issue in the cloud environment. In this architecture used clouds with some advantages like as a huge storage capacity and high scalability. The used attribute encryption based (ABE) algorithm for the fine grained access control. The attribute based encryption algorithm first encrypt data before storing on the cloud server. In ABE there are two variants based on placing attributes and access attribute policy. Here in this research paper, we develop a model and mechanism for control of data access to PHRs stored in cloud servers. To achieve efficient and modular data access control for PHRs, we provide ABE encryption approach to encrypt each PHR file. In this system we try to focus on the multiple data owner scheme, and divide the users into security domains that highly reduce the key management complication for owners and users. In this system patient privacy is guaranteed by exploiting multi-authority

II. LITERATURE SURVEY

In [1], Hamid et al. target the confidentiality of healthcare patient's multimedia data in the cloud by proposing a tri-party one-round authenticated key agreement protocol based on bilinear pairing cryptography. The proposed protocol can generate a session key among the participants to communicate securely. Finally, the private healthcare data is accessed and stored securely by implementing a decoy technique with a fog computing facility. Nonetheless, the proposed approach incurs a computational overhead cost in communication in sacrifice for strong security.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

In [2], Marwan et al. propose a novel method based on Shamir's Secret Share Scheme (SSS) and multi-cloud concept to enhance the reliability of cloud storage in order to meet security requirements to avoid loss of data, unauthorized access, and privacy disclosure. The proposed technique divides the secret data into many small shares so that one does not reveal any information about medical records. Besides, mutli-cloud architecture, data are spread across different cloud storage systems. In such a scenario, cloud consumers encrypt their data using SSS technique to ensure confidentiality and privacy. Therefore, the healthcare data are split into various shares so that data confidentiality is guaranteed. On contrary, the paper does not discuss any aspects of the optimal number of shares for the incurred trade-off between efficiency and security. It does not discuss the quality analysis of recovered healthcare data.

In [3], Galletta et al. present a system developed at Instituto di Ricovero e Cura a Carattere Scientifico (IRCCS) that is claimed to address the patient's data security and privacy. The presented system is based on two software components the anonymizer and splitter. The first collects anonymize clinical data, whereas the second obfuscates and stores data in multiple cloud storage providers. Thus, only authorized clinical operators can access data over the Cloud. They present a case study that uses Magnetic Resonance Imaging (MRI) data to assess the performance of the implemented system.

The paper [4] discusses important concepts related to EHRs sharing and integration in healthcare clouds and analyze the arising security and privacy issues in access and management of EHRs. The paper presents several basic security and privacy requirements for application clouds: ownership, authenticity, non-repudiation, patient consent and authorization, integrity and confidentiality and availability, archiving and auditing. Then they present an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud: secure collection and integration, secure storage and access management, and secure usage model. Finally, they illustrate the development of the proposed EHR security reference model through a use-case scenario and describe the corresponding security countermeasures and possible security techniques

The paper [5] lists various methods of encryption and also addresses security and privacy challenges in healthcare cloud by deploying a novel framework with Cloud-based Privacy aware Role Based Access Control (CPRBAC) model. The side goal is to reduce computational complexity and communication overhead. However, there is no qualitative analysis discussion on the efficiency of the approach and its mitigation to security and privacy attacks.

In [6], Padaki et al. survey several healthcare security lapses pertaining to non-repudiation, CIA model, and what it means to stakeholders in the healthcare industry. They also discuss few proven operational strategies, risk management methodologies and discern what the industry can do to mitigate such security risks and privacy threats. The paper classifies the security threats posed on healthcare clouds into three high level categories including: network, system care and protection, and compliance with standard acts and rules.

Ibrahim et al. [7] propose a framework which allows secure sharing of EHRs over the Cloud among different healthcare providers. In the proposed framework, Public Key Infrastructure (PKI) is used to maintain authentication between participating healthcare providers and the EHR sharing cloud. The proposed framework claims that it ensures the confidentiality, integrity, authenticity, availability and auditability. It also claims that it meets the security standards defined in the technical safeguards of the HIPAA Security Rule.

In general, the owner is defined as the creator of the information. Establishing information ownership is necessary for protection against unauthorized access or misuse of patient's medical information. Ownership of healthcare information can be protected through a combination of encryption and watermarking techniques that results in secured healthcare information that cannot be transmitted, accessed, or released without the mutual acceptance of all entities involved in the ownership/creation of the healthcare information. Patients can allow or deny the sharing of their information with other healthcare practitioners [8]. To implement patient data sharing in a healthcare system, patient may grant rights to users based on a role or attributes held by the respective user to share specific healthcare data with that user.

Authenticity in general refers to the truthfulness of origins, attributions, commitments, and intentions. It ensures that the entity requesting access is authentic. In healthcare systems, the information provided by the healthcare providers and the identities of the entities using such information must be verified via the Authentication Act [9]. The authentication of information can pose special problems, like man-in-the middle attacks, and is often mitigated with a combination of usernames and passwords. Most cryptographic protocols include some form of endpoint authentication specifically to prevent man-in-the-middle attacks. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at every access.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Confidentiality is the act of ensuring that patients health data is kept completely undisclosed to unauthorized entities. Delegating data control to the cloud, leads to an increase in the risk of data compromises, as the data becomes accessible to an augmented number of parties. Due to the increased number of parties, devices and applications involved, there is an increase in data compromise threats. To make the patient/doctor relationship work effectively, it is necessary for the patient to trust the healthcare system to protect the confidentiality of his data. If the patient feels that the information he gives to his doctor is not protected, and that his privacy is threatened, he can be more selective about the information he will provide to his doctor in the future. The threat of data compromise can harm the patient/doctor relationship and hamper the proper medical diagnosis and treatment [10]. For example, an employer may refuse a job if the patient's medical data are disclosed. Confidentiality can be achieved by access control and using encryption techniques.

III. SYSTEM OVERVIEW

In the proposed research work to design and implement a system that can provide the security to Personnel Health Records (PHR) files using encryption as well as proxy re-encryption services, in cloud environment and provide the security from insider attacks like collusion attack, bruited force attack as well as SQL injection attack.

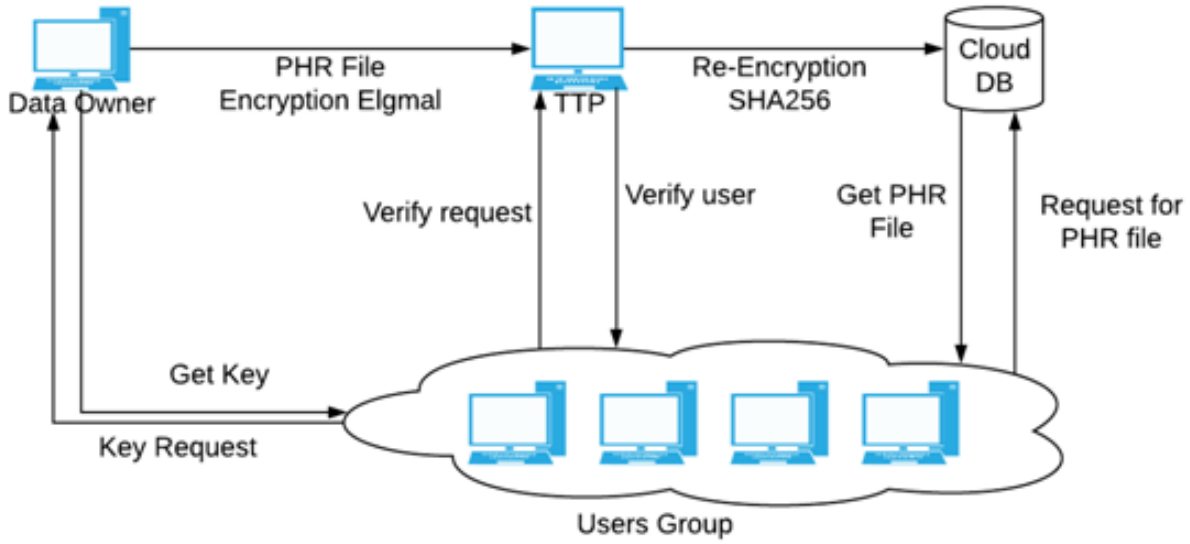

Figure 1 : Proposed System Architecture

In this architecture the will give some security and privacy mechanism such as, confidentiality, data integrity and fine grained access control. The privacy and security are most affected issue in the cloud environment. In this architecture used clouds with some advantages like as a huge storage capacity and high scalability. The used attribute encryption based (ABE) algorithm for the fine grained access control. The attribute based encryption algorithm first encrypt data before storing on the cloud server. In ABE there are two variants based on placing attributes and access attribute policy.

- The system first upload the own PHR file on cloud using Elgamal encryption scheme.
- This file first received by TTP and generate the proxy re-encryption using SHA-256 algorithm and store the file into the cloud server.
- Data owner can share the file to individual user as well as whole group using RBAC algorithm.
- When end user's give request to CSP, then authentication has done by TTP.
- In the proposed work we have written web service for owner that can 24*7 available for private key distribution.
- When data owner revoke any user system automatically expired the existing keys and generate new keys.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

Our Contribution

To define the a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamically to end user. Provide a secure way for key distribution with secure communication channels. The users can securely obtain their private keys from data owner. Scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

IV. RESULTS AND DISCUSSION

According to proposed survey system provide the highest security of personnel; heath care data in cloud environment.

Advantages

- System can work any kind of encrypted data without any third party dependency.
- Minimum time complexity.
- System can work on big data.
- It can be applicable for structured as well semi structured data.
- Can be achieve RBAC for end user.

Disadvantages

- There is only single disadvantages for system, searching depends on keyword trapdoor generation, if the some words has generate wrong trapdoor when no background knowledge, then system generate false positive ratio.

Applications

- Cloud base encrypted document search system for health care systems on PHR data.
- Encrypted document verification system for banking applications.
- Role base access control applications on public cloud system.
- Document search on encrypted with multi keyword search applications.

V. CONCLUSION

Data security is the major problem in cloud storage. Before outsourcing PHR into the third party server different attribute based encryption schemes are used for secure storage. ABE is used to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliation. Using Enhance MA ABE scheme, better on demand revocation is possible. In practical case some more problems will arise. The main issue in this case is trying to implement work flow based conditions. For solving these need attribute-based broadcast encryption (ABBE). Work flow Based situation is implement using ABBE and analyze security and computation cost. From analysis show that this work flow based scheme is both scalable and efficient. It gives better on demand user revocation also.

VI. FUTURE WORK

In future it would be interesting to consider Attribute Based Broadcast Encryption system with different types of impressibility. If consider different credential are equal then Distributed ABE scheme is needed.

REFERENCES

[1] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a
Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," IEEE Access, 2017.
[2] M. Marwan, A. Kartit, and H. Ouahmane, "Protecting medical data in cloud storage using faulttolerance mechanism," in Proceedings of the 2017 International Conference on Smart Digital Environment, 2017, pp. 214–219.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 11, November 2018

[3] A. Galletta, L. Bonanno, A. Celesti, S. Marino, P. Bramanti, and M. Villari, "An approach to share MRI data over the Cloud preserving patients' privacy," in Computers and Communications (ISCC), 2017 IEEE Symposium on, 2017, pp. 94–99.
[4] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010, pp. 268–275.
[5] K. Shah and V. Prasad, "Security for Healthcare Data on Cloud," 2017.
[6] S. Supriya and S. Padaki, "Data Security and Privacy Challenges in Adopting Solutions for IOT," in Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on, 2016, pp. 410–415.
[7] A. Ibrahim, B. Mahmood, and M. Singhal, "A secure framework for sharing Electronic Health Records over Clouds," in Serious Games and Applications for Health (SeGAH), 2016 IEEE International Conference on, 2016, pp. 1–8.
[8] P. Metri and G. Sarote, "Privacy issues and challenges in cloud computing," Int. J. Adv. Eng. Sci. Technol., vol. 5, no. 1, pp. 5–6, 2011.
[9] Washington Electronic Authentication Act, "Revised Code of Washington," Vol RCW, vol. 70, no. 10, 1992.
[10] P. Duquenoy, N. M. Mekawie, and M. Springett, "Patients, trust and ethics in information privacy in eHealth," in eHealth: Legal, Ethical and Governance Challenges, Springer, 2013, pp. 275–295.