IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 86-88

An Empirical Study of Securing Electronic Health Record through Access Policies Generation by Usage of Attribute Based Encryption Techniques and Automatic Revocation Techniques in the Cloud

G.Abarna 1, S.Dhanalakshmi 2
1(Research Scholar, Department of Computer Science, Sri Krishna Arts and Science College, India)
2(Assistant Professor, Department of BCA & SS, Sri Krishna Arts and Science College, India)

Abstract: *Now a days data outsourcing to the cloud is getting accustomed by the data owners due to enormous benefits of the scalable data storage paradigms. In these paradigms, privacy and confidentiality is the primary concerns on the outsourced data .Because it contains more sensitive information. With the emergence of sharing confidential data, several existing technique has employed using attribute based encryption and fine grained access control model with external authorities to achieve the above requirement. In addition it leads to key management issue and key escrow attacks. An empirical study of securing electronic health record through generation of access policies and automatic revocation principles is carried out in this work. Revocation becomes important due to expiration or change of user membership or user credentials so it has to be addressed properly. In order to handle revocation properly, efficient access policies in terms of many constraints has to be employed effectively on the encrypted data with periodic updates on the cloud server. In case of feasibility analysis, it incurs additional cost due to frequent updating. To resolve the issue, an outline of a novel technique to be proposed through incorporation of proxy is highlighted. On extensive experiment analysis of each state of art approaches considered in this study, it is possible to evaluate the performance of the system on various aspects which bring more conceptual strength to build a proposed model.*

Keywords: *Cloud Computing, Electronic Health Record, Access policies, Attribute Based Encryption, Multi Authority ABE*

I. INTRODUCTION

Cloud offers patients centric model as service towards exchange of the health information between the entities. Nowadays many patients planning to host their data into the cloud for ease of usage and convenience. Especially patient health records has enabled with control to share the information wide variety of user groups [1]. Due to security and privacy violation, insider attacks impede the wide adaptation. A feasible and promising approach against the insider treats would be to encrypt the data before outsourcing. Electronic health Record should only be available to the users containing corresponding decryption key. Encryption and decryption is provided using public key cryptosystem [2]. The data owner retains the rights to grand and also to revoke access privileges [3]. The Data owner may overwhelm in managing all data user by key management overhead [4]. On other hand, Personal Health record (PHR) has been administrated by multiowner scenario, each owner encrypts the records according to their constrainst using different set of cryptographic keys.

Central Authorities will be employed to manage cryptanalysis and key generation for multiowner settings. Attribute based encryption(ABE) is used as encryption primitive [5]. Access policy is derived based on the attributes on usage of ABE Scheme which enables the data owner to share the PHR records among the user groups by encrypting the file under a set of attributes. The key generation, encryption of the data and decryption of the data are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date [6].

In this paper, we undergo an empirical analysis of securing health records in cloud through incorporation of proxy server and time enabled access policies .The rest of the paper is organized as follows, section 2 describes the review of literature on attribute based encryption and automated revocation of access in section 3 outline of the proposed methodology is addressed and finally section 4 conclude the study of the paper.

II. REVIEW OF LITERATURES

In this section, we describe the existing methods applied to cloud data security by incorporating the access control mechanism through usage of attribute based encryption technique is addressed.

2.1 Access Control Mechanism

In analysis of access control mechanism, it provides solution to preserve a data against unauthorized access. Access control mechanism provides flexible, fine grained and secure data accessing. The following techniques describe its importance in the outsourced cloud data.

2.1.1 Fine Grained Two factor Authentication

In this technique, two factor authentications are carried out for health records stored in the cloud. It is included through incorporation of user secret key and a lightweight security device. Data access will be provided to data user on evaluating the holding information's. Authentication mechanism can enhance the security of the system, especially in those scenarios where many users share the same information of the patient for different usage [6]. In addition to the authentication, attribute-based control is used to enable the cloud server with restriction constrainst on the access to specified users with the same set of attributes while preserving user privacy and data confidentiality, i.e., the cloud server only knows the user who fulfills the required predicate, but has no idea on the exact identity of the user.

2.1.2 Robust and Auditable Access Control With Multiple Attribute Authorities

In this literature, multi-authority access control schemes have been analysed in detail, due to the fact that each of the authorities manages a disjoint attribute set. The Authorities do user legitimacy verification and secret key distribution. It embedded with more efficient access control scheme and auditing mechanism to carry out user legitimacy verification through multiple attribute authorities [7]. Multi-authority access control generates secret keys for legitimacy verified users and manages the whole attribute set individually. Auditing mechanism is to detect which attribute authority has incorrectly or maliciously performed the legitimacy verification procedure.

2.2 User revocation Techniques

The user revocation technique is analysed in term of single user revocation and group user revocation towards accessing of the cloud data. The following technique provides processing step of the revocation models,

2.2.1 Group User Revocation

In this literature, outsourced cloud data has been secured using access control mechanism through incorporation access policies towards access of the specified data by data user. In this process, secure group user revocation based on vector commitment and verifier-local revocation group signature is developed for revocating the set of user from accessing of the records [8]

2.2.2 Efficient Attribute Revocation through user Collusion Avoidance

In this literature, Single-attribute revocation for some user towards data access may affect the other users with the same attribute. The revoke of user towards attribute is carried out efficiently by exploiting the concept of an attribute group through computational diffie Hellmann Assumptions. When an attribute is revoked from a user, the group manager updates other users' secret keys towards access of the data [9].

SI.No	Approaches used	Advantages	Problem
1	Fine Grained Two factor Authentication	It provides data confidentiality and user privacy with less computation time	User privacy leakage and data disclosure attack through insider threats
2	Efficient access control scheme with an auditing mechanism as heterogeneous framework	It produces high efficiency in terms of key generation and user verification	Data access control with long waiting queue to generate the secret key
3	GroupUser Revocation	It provides confidently, efficiency, countability and traceability	Revocation of the group
4	Efficient Attribute Revocation through user Collusion Avoidance	User privacy is high and it is free from collusion attacks	Single-attribute revocation for some user may affect the other users with the same attribute

Fig 1.Analysis on existing security technique in cloud

III. OUTLINE OF PROPOSED MODEL

In this section, we contribute a novel model named as Virtual Integrated Data Sharing on multiowner setting to operate on public key cryptosystem modules such as key generation, data encryption for

ciphertext production and data decryption to generate the plaintext will less computation time using homomorphic encryption. In order to achieve the less computation time, proxy server has to be incorporated in parallel with data server for above mentioned [10]. It is a new primitive supports both abilities and provides flexible for data sharing. In addition automation revocation can be enabled by time enabled access policies and location enabled access policies on the data usage. It greatly reduces the key management complexity and revocation complexity for owners and users.

IV. CONCLUSION

The empirical analysis of the securing personnel health record through generation of access policy by ABE schemes and automatic user revocation schemes was analysed against the single owner and multi owner setting at different times. It provides ideas to tackle the critical issues in terms of insider attack and collusion attack. In addition, it provides revocation principles based on several constrainst and technique such as computational diffie Hellmann assumptions. Finally proposed study offloads the difficulties raised due to attribute selection and key generation mechanism towards access policies operations.

REFERENCES

[1]. L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.

[2]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM, 2010, pp. 534–542.

[3]. S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[4]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM CCS, 2006, pp. 89–98.

[5]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[6]. Joseph K. Liu ; Man Ho Au ; Xinyi Huang, Rongxing Lu, Jin Li " Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services" in IEEE Transactions on Information Forensics and Security, Volume: 11, Issue: 3, March 2016

[7]. Kaiping Xue ; Yingjie Xue ; Jianan Hong ; Wei Li ; Hao Yue ; David S. L. Wei ; Peilin Hong "RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage" IEEE Transactions on Information Forensics and Security , Volume: 12, Issue: 4, April 2017

[8]. Tao Jiang, Xiaofeng Chen, Jianfeng Ma "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation" IEEE Transactions on Computers in Volume: 65, Issue: 8, Aug. 2016

[9]. Jiguo Li ; Wei Yao , Jinguang Han, Yichen Zhang, Jian Shen "User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage"in IEEE Systems Journal ,Volume: 12, Issue: 2, June 2018 .

[10]. Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM press, pp. 276-286, 2009.