International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

A STUDY ON SECURITY MECHANISM EMPLOYED ON THE ELECTRONIC HEALTH RECORDS IN THE CLOUD

V.Ramya,
M.Phil Research Scholar,
Department of Computer science,
S.N.R SONS College,
Coimbatore,TamilNadu, India.

S.Thavamani,
Associate Professor
Department of Computer Applications,
S.N.R SONS College,
Coimbatore,TamilNadu, India.

Abstract: Outsourced Electronic Health Record to the cloud for the high quality retrieval and storage service has experienced large security violation. However it may lead to leakage of sensitive information of the patient. In order to protect the data leakage, efficient secure data sharing models has been proposed in the literature. In this paper, we analyze the several secure data sharing gateways in the cloud utilizing searchable encryption and proxy re encryption. The major primitive is public key encryption scheme with keyword search which enables the data users to search on the encrypted information without decrypting it and proxy re- encryption can be introduced to conjunctive keyword search in terms of the time enabled proxy Re-encryption model. It enables the data owner to delegate the access rights to data user to operate several search keywords which is considered as conjunctive keywords on their records within the specified time and providing resistance against guessing attacks. Time based delegation can also leads to security violation issue. To handle the implication on this study, we propose a novel hybrid constraint based re encryption (HCRE), multiple constraint such as user category, time and Specific intension of the user are taken as a key to re encrypt the data from security violation. The HCRE can improve the performance in terms of security and computation cost.

Keywords: Electronic Health Record, Data Sharing Models, Proxy Re-Encryption, Cloud Computing, Public Key Encryption.

I.INTRODUCTION

Electronic Health Record (EHR) Systems has emerged a paradigm for health information exchange in the cloud. It have made create, storage, retrieval and sharing of the medical information in more flexible and efficient way [1]. Health Care data collected in a data center may contain private information. Hence it is more vulnerable to potential leakage and disclosure to the individual's data to other person or companies. The Cloud Server is exposed to threats. This concern can be handling using secure data sharing paradigms. This signature scheme is more efficient to compute than our cryptographic hashes, but does not simultaneously provide provable privacy and ensure full data integrity. As most of approaches rely on Public key cryptosystem to secure the data, it finds more pitfalls such as creates the burden on data owner for delegate the search rights. Though it can be handled by proxy re encryption methods, access dissemination stands another concern. Time enabled proxy Re-encryption model can withstand the attack by enabling the data owner to delegate the access rights to data user to operate several search keywords which is considered as conjunctive keywords on their records within the specified time and providing resistance against guessing attacks. The rest of the section is organized as follows, section 2 describes the review of literature followed by section 3 to define the proposed methodology as outline and finally section 4 concludes the study of the paper.

II.REVIEW OF THE LITERATURE

The Secure data sharing model on EHR data is carried out using following public key cryptosystem model

A.Secure Data Sharing Models

1) Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE:

In this literature ,The public key encryption with keyword search (PEKS) mechanism is analyzed as it enables users to search on encrypted data, and hence is applicable to the setting of cloud computing. PEKS schemes can allow a user to search encrypted data confidentially, though it failed in verifying the searched result and the system did not specify and allocate the users for encrypted data files stored on the cloud server [6]. Verifiable attribute-based keyword search (VABKS) is analyzed depth as it allows a data user, whose credentials satisfy the data owner's access control policy, to search the encrypted data file and verify the searched result. The scheme which "removes secure channel" and construct a method for verifying the searched result from the cloud server based on key policy attribute-based keyword search (KP-ABKS) of VABKS.

2) Public key encryption with keyword search secure against keyword guessing attacks:

In this literature Public key encryption with keyword search (PEKS) enable a server to search from a collection of encrypted documents given an encrypted keyword which provided by the data user. The keyword guessing attack and secure channel free allows the server to search for a keyword in the encrypted index structure for encrypted data files. Unfortunately, PEKS secure against keyword guessing attack is only secure under the random oracle model, which does not reflect its security in the

real world. Furthermore, secure channel free PEKS schemes has been constructed for security against chosen keyword attack, chosen cipher text attack, and against keyword guessing attacks[7]. The strongest model of PEKS which is secure channel free and secure against chosen keyword attack, chosen cipher text attack, and keyword guessing attack through time enabled delegation process.

3) Time-based proxy re-encryption scheme for secure data sharing in a cloud environment:

In this literature, time-based proxy re-encryption (TimePRE) scheme is to allow user's access right which expires automatically after a predetermined period of time. In this case, the data owner can be offline in the process of user revocations. Each data is associated with encrypted index structure and an access time [8]. The data owner and the CSP are required to share a *root secret* key in advance, with which CSP can automatically update the access time of the data with the time that it receives a data access request.

4) Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage:

As electronic personal data outsourced to cloud server has been growing by data owner for the enjoyment of the high-quality retrieval and storage service without worrying the burden of local data management and maintenance. However, secure share and search for the outsourced data is a formidable task, which may easily incur the leakage of sensitive personal information. Efficient data sharing and searching with security is of critical importance. In this literature, a searchable attribute-based proxy encryption system has been analysed. When compared with the existing models it only supporting either searchable attribute-based functionality or attribute-based proxy encryption, new primitive supports both abilities and provides flexible keyword update service. In particular, the system enables a data owner to efficiently share his data to a specified group of users matching a sharing policy and meanwhile, the data will maintain its searchable property but also the corresponding search keyword(s) can be updated after the data sharing. The new mechanism is applicable to many real-world applications, such as electronic health record systems. It is also proved chosen ciphertext secure in the random oracle model [9].

5) Hybrid Cryptographic Access Control for Cloud-Based EHR:

Cloud-based electronic health record (EHR) systems are next-generation system for storing the data of the big data systems for facilitating efficient and scalable storage and fostering collaborative care, clinical research, and development. Mobility and the use of multiple mobile devices in collaborative healthcare increase the need for robust privacy preservation. Hence large-scale EHR systems require secure access to privacy-sensitive data, data storage, and management [10]. The comprehensive solution with a cryptographic role-based technique to distribute session keys to establish communications and information retrieval using the Kerberos protocol is been analyzed using location- and biometrics-based authentication to authorize users and through a wavelet-based steganographic technique which embed EHR data securely using electrocardiography (ECG) signals as the host in trusted cloud storage. A comprehensive security analysis demonstrates that the model is scalable, secure, and reliable for accessing and managing EHR data.

6) Securing patient-centric personal health records sharing system in cloud computing:

Personal health record (PHR) enables data owner to manage their own electronic medical records (EMR) in a centralized way as it provides flexible way to outsource their information to be stored in a third-party server. In this literature, secure and scalable system for sharing PHRs is been analysed by focusing on the multiple data owner scenario, and divide the users in the system into multiple security domains that greatly reduce the key management complexity for owners and users [11]. A high degree of patient privacy is guaranteed by exploiting hierarchical and multi-authority attribute-sets based encryption (HM-ASBE). The system not only supports compound attributes due to flexible attribute sets combinations, but also achieves fine-grained access control. The scheme supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

7) Analysis of the secure outsourcing of Electronics Health Care Records:

Author	Technique	Advantage	Limitation
Pengliang Liu, Jianfeng Wang, Hua Ma, Haixin Nie	Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE	It increases the data confidentiality.	It is not scalable to high dimensional data
Fang, L., Susilo, W., Ge, C. & Wang,	Public key encryption with keyword search secure against keyword guessing attacks	It authenticates the data user against data access and deny the data against the attacks	It is not reliable to access control mechanism through keyword search mechanism
Q. Liu, G. Wang, J. Wu	Time-based proxy re-encryption scheme for secure data sharing	It provides the key updates and time based access control for automatic user revocation	Data Index Structure is not update for dynamic updates.
Kaitai Liang; Willy Susilo	Searchable Attribute-Based Mechanism with Efficient Data Sharing	Sharing Policies has enabled to data access	It does not support the user revocation.
Uthpala Premarathne et.al	Hybrid Cryptographic Access Control	It provides high Quality Data retrieval	Encryption increase the cost of the system
Chen Danwei, Chen Lining, Fan Xiaowei,	Securing patient-centric personal health records sharing system	It is reliable and provides the multilevel authority system	Data delegation is made manual and its has not updated for dynamic updates

Table 1: literature Review

B.Importance of Securing sharing models

It is to impose the revocation on the delegation rights to user within specified time bound. The time seal is encapsulated in

the cipher text at the very beginning of the encryption algorithm. It implies that all users including data owner are constrained by the time period. Eavesdroppers and off-line keyword guessing attacks could not succeed in guessing keywords.

III.OUTLINE OF THE PROPOSED METHODOLOGY

Hybrid constraint based re encryption (HCRE), multiple constraint such as user category, time and Specific intension of the user are taken as a key to re encrypt the data from security violation in order to impose the delegation rights to the data user. The HCRE can improve the performance in terms of security and computation cost.

IV.CONCLUSION

The Extensive Study on the Secure Data Sharing Scheme for Electronics Health Care Record based time enabled Delegation mechanism is presented and it is analyzed against the guessing attack, keyword attack and cipher text attack. The Secure sharing mechanism supports various automated mechanism such as delegation and revocation of the user against the data access. Searchable encryption scheme with proxy re encryption function provides the high security on preserving the data upon data updating.

V.REFERENCES

[1]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, Interlaken, Switzerland, May 2-6, 2004, vol. 3027, pp. 506–522, Springer.

[2]. W. Yau, R. Phan, S. Heng, B. Goi, "Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester," International Journal of Computer Mathematics, vol. 90, no. 2, pp. 2581-2587, 2013.

[3]. M. Ding, F. Gao, Z. Jin, H. Zhang, "An efficient public key encryption with conjunctive keyword search scheme based on pairings," in Proc. 3rd IEEE International Conference on Network Infrastructure and Digital Content(IC-NIDC), Beijing, China, Sept. 21-23, 2012, pp. 526-530, IEEE.

[4]. D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," in Proceedings of Advances in Cryptology - CRYPTO '01, ser. LNCS. Springer, 2001, pp. 41–62.

[5]. W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188, 2002.

[6]. Pengliang Liu, JianfengWang,Hua Ma, HaixinNie "Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE" on 9th International Conference on Broadband and Wireless Computing, Communication and Applications

[7]. Fang, L., Susilo, W., Ge, C. & Wang, J Public key encryption with keyword search secure against keyword guessing attacks without random oracle. Information Sciences, 2013

[8]. Q. Liu, G. Wang, J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, pp.355-370, 2014.

[9]. Kaitai Liang; Willy Susilo Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage" IEEE Transactions on Information Forensics and Security in Volume: 10, Issue: 9, Sept. 2015

[10]. Uthpala Premarathne ; Alsharif Abuadbba ; Abdulatif Alabdulatif ; Ibrahim Khalil ; Zahir Tari ; Albert Zomaya ; Rajkumar Buyya"Hybrid Cryptographic Access Control for Cloud-Based EHR SystemsIEEE Cloud Computing in Volume: 3, Issue: 4, July-Aug. 2016

[11]. Chen Danwei, Chen Lining, Fan Xiaowei, He Liwen Pan Su, Hu Ruoxiang "Securing patient-centric personal health records sharing system in cloud computing" China Communications Volume: 11, Issue: 13, Supplement 2014

[12].N.Meenakshi, Dr.Vijaykumar "Location based Hierrachical classifier for multidimensional Spatial Data mining "International Journal of Scientific Engineering and Innovative Research, volume 10, issue 1, paper id: I1V102.,