WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Efficient Method For Highly Secured Retrieval of Cloud Data Using a Key Aggregation Crypto System Based Ring Signature in Cloud Computing

Dr.S.Thavamani M.Sc., M.Phil., Ph.D.,

Associate Professor in Computer Applications,
Sri Ramakrishna College of Arts and Science (Autonomous)
[Re-Accredicted with 'A+' Grade by NAAC]
Coimbatore - 641006, TamilNadu, India.

A B S T R A C T

Cloud computing nowadays is being comprehended as the potential solution to the problem of ever rising demand for resources, storage, and computing power. Owing to the growth of cloud computing the Outsourced Electronic Health Records to the cloud for the high quality of retrieval, resources and storage service has experienced large security violation. However it may lead to leakage of sensitive information of the patients. In order to protect the data leakage, highly efficient secure data sharing models has been proposed. Here it analyses 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 searching keywords which enables the data users to search on the encrypted information without decrypting it and proxy re- encryption can be introduced to conjunctive searching keyword 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. To handle the implication on this study, this system proposes " An Efficient Method For Highly Secured Retrieval of Cloud Data Using A Key Aggregation Crypto System Based Ring Signature In Cloud Computing" is proposed. It reduces the complications of existing schemes over decrypting the Electronic Health Records on saving time, and achieves high level of security.

Keywords: Cloud Computing, Electronic Health Records, Security, Data Retrieval, Encryption, Ring Signature, Key Generation

1. OVERVIEW

Electronic Health Record (EHR) Systems has emerged a paradigm for health information shared in the cloud. It have made to 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 handled by using secure data sharing paradigms. This ring signature scheme is more efficient to compute than the 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 [2], 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 the data users to operate several searching keywords which is considered as conjunctive keywords on their records within the specified time and providing resistance against guessing attacks. In order to achieve the very unique solution motivation behind this work is design and development in a proposed scheme key aggregation crypto system based ring signature generation in cloud computing.

1.1 ACCESS CONTROL MECHANISM IN THE CLOUD

The cloud-based architecture facilitates secure access to EHR resources by enforcing cryptographic access control with context and location awareness. Many models has been available ensure flexible and scalable access control to PHR data in cloud computing environments with multiple tenancies as depicted in the figure 1.

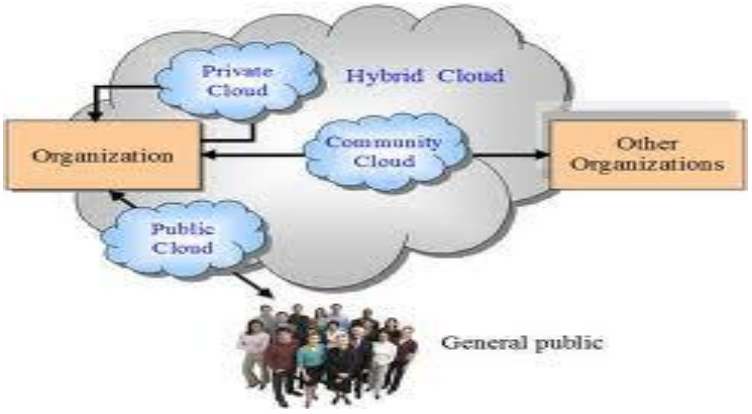

Figure 1: Architecture Diagram of multi tenancy cloud infrastructure

The above diagram illustrates the architecture of cloud infrastructure. There are four cloud deployment models. They are private cloud, public cloud, community cloud, hybrid cloud.

- **Private cloud:** A private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
- **Public cloud:** The general public provisions the cloud infrastructure for open use. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Community cloud:** The community cloud is a type of cloud hosting in which the setup is mutually shared is mutually shared between many organizations that belong to a particular community that is banks and trading firms.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more distinct cloud deployment models (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application probability (e.g., cloud bursting for load balancing between clouds).

II. RELATED RESEACHS

There exist many techniques to secure the health records are designed and implemented efficiently. Each of these techniques follows some sort of security principles, among few performs nearly equivalent to the proposed framework is described as follows.

Pengliang Liu et al.[5] , Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE 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. VABKS is examined depth as it permits 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 (Verifiable attribute-based keyword search).

Changjiang Hou et al.[6] 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, this scheme is protected in contrast to keyword guessing attack is only protected below the random oracle model [8], which does not reflect its security in the actual world. Moreover, secure network free schemes has been created for security against chosen keyword attack, chosen cipher text attack, and against keyword guessing attacks. The toughest model of this scheme is secure channel free and secure against chosen keyword attack, chosen cipher text attack, and

keyword guessing attack through time enabled delegation process.

Q. Liu, G, et al. [7], time-based proxy re-encryption (TimePRE) scheme is to allow the 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 [9]. Each data is associated with encrypted index structure and an access time. 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.

X. Liang et al. [3],private health record (PHR) is considered as an emerging patient-centric model of health information interchange, which is often outsourced to be stored at a third party, such as cloud providers. Though, at hand wide privacy concerns as private health information could be showing to those third party servers and to unauthorized parties. To guarantee the patients' control over right to use to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. However, problems such as risks of secrecy exposure, scalability in key management, flexible access, and proficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control.

Smitha Sundareswaran et al [11], it analyzes the Cloud computing as highly scalable services to be easily consumed over the Internet on an as-needed basis. A most important eye of the cloud services is that employers' data are frequently processed remotely in unknown machines that users do not own or operate [12]. While delight in the accessibility brought by this new developing technology, employers' fears of losing control of their own data (particularly data on financial and health records) can become a major barrier to the inclusive adoption of cloud facilities. To talk about this problem, in this system, highly spread out information accountability framework to keep track of the actual usage of the employers' data in the cloud has been intended.

J. Li, Y. Shi [12] has proposed Searchable ciphertext-policy attribute based encryption with revocation it protects the sensitive data outsourced to cloud server, outsourcing data in an encrypted way has become popular nowadays. However, it is not easy to find the corresponding cipher text efficiently, especially the large cipher text stored on cloud server. Besides, some data owners do not want those users who attempt to decrypt to know the sensitive access structure of the cipher text because of some business or private reasons. In adding, the handler data's revocation and key updating are important problems, which affect application of cipher text-policy attribute-based encryption (CP-ABE) in cloud storage systems. To overcome the previous problems in cloud storage, it presents a searchable CP-ABE with attribute revocation, where access structures are partially hidden so that receivers cannot extract sensitive information from the cipher text. The safe keeping of our system can be reduced to the decisional bilinear Diffie–Hellman (DBDH) assumption. Key aggregation based ring signature generation towards data access and revocation Mechanism. Key generation process is carried out using RSA Algorithm which is polynomial time algorithm [4].

Here discussed only limited papers on literature survey there are many more techniques in same area [10]. In order to overcome these drawbacks here the proposed methodology has presented Suspension and Secure Accessing of Cloud Data Using a Key Aggregation Based ring Signature. Privacy of the outsourced electronic health data is modeled as privacy issue in the cloud data service during the data sharing as mostly data is private data's. The Cloud System will be usually vulnerable to potential leakage due to insider attack and eavesdropping attacks. This serious issue has explored to model a secure access control mechanism to EHR data. Here the proposed mechanism is defined as "An Efficient Method For Highly Secured Retrieval Of Cloud Data Using A Key Aggregation Crypto System Based Ring Signature In Cloud Computing".

III.PROPOSED METHODOLOGY

A. Problem Description

Digital Signature is generated towards aggregating the private key of data user to form aggregate key towards data access. In this system decryption key is more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size. And also proposed system allows the user to access the record without decrypting it every time. To best of our knowledge, it is considered as more secure against various threats in the cloud system.

B. Proposed Scheme

Secure Searching is carried out using Ring Signature as it is a new primitive supports both abilities and provides flexible keyword update service. Ring Signature play an important role in aggregate key updating during user joining and user leaving for particular record access. In Particular Specified group of user matching a sharing policy has granted access to the record without decryption of the document. The proposed model greatly reduces the key management complexity for owners and users.

C. ***Encryption Algorithm (RSA Algorithm)***

Messages can be encrypted to ciphertext using RSA Encryption Algorithm. It decides what ciphertext class is associated with the plaintext message to be encrypted. The EHR documents of the patients are encrypted by a symmetric encryption algorithm and the symmetric key is encapsulated with the patient's public key by the key encapsulation mechanism. The algorithms in the following focus on the searchable keywords encryption and the timing controlled delegation function.

i) Extract Algorithm **in the Cloud**

The owner can use the master-secret key to produce an aggregate decryption key for a set of ciphertext without the knowledge of others in the Cloud.

ii) Decryption Algorithm **in the Cloud**

Employer with an aggregate key can decipher any cipher text provided that the ciphertexts class is contained in the aggregate key. The proxy server makes use of the re-encryption key to transform the ciphertext encrypted by delegator's public key into another form, which can be searched by the delegatee using his own private key. The delegatee will be divested of the search authority when the effective time expires. In order to achieve the time controlled access right revocation, the predefined time information is embedded in the re-encrypted ciphertext with a time seal. With the help of the time seal, the delegate is able to generate a valid delegation trapdoor. All above mentioned algorithms using secret key can release a constant-size aggregate key.

iii) Ring Signature For Data Sharing in the Cloud Architecture

Ring signature is a group signature for data sharing in the cloud architecture. Ring Signature is to construct an anonymous and authentic data sharing system for end user. The signatures vary in two different ways initially there is a way to revoke the anonymity of a single signature, and second, any group of users can be used as a group without additional setup.

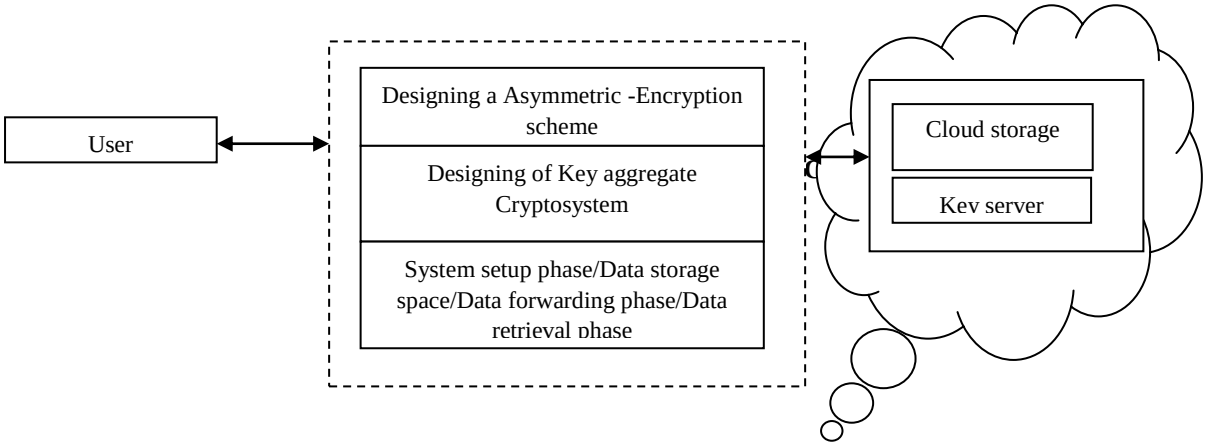

Figure 2: Architecture of Key Aggregate Cryptosystem

The above figure 2 illustrates the architecture of key aggregate cryptosystem. Finally, the verify algorithm, on input taken the ring R, a signature σ, and a message m, outputs 1 if some member of R created the signature σ on m and 0 otherwise.

Algorithm.1 : Ring Signature Generation

- A group consists of n members G1,G2,G3,G4,G5….Gn Users which are outside the group G is U1,U2,U3,U4…….Un
- Each group member have their own (private, public) key pairs
- Any group member can upload encrypted file in cloud which is signed by ring signature
- Ring signature of a member = his/her private key and all group members public key
- Each file encrypts with sym
- metric keys E1, E2, E3…..

Ring signature scheme consists of three algorithms: Key Gen, Sign, and Verify. Each user will run KeyGen

individually, on input the security parameter k is taken and will output a keypair (pk, sk). The Sign algorithm on input, it takes a secret key sk, a ring R (typically just a list of public keys belonging to members of the ring), and a message m, outputs a signature σ on m.

IV.RESULTS AND DISCUSSION

In this section, it analyses the security of the proposed model against the various attacks.

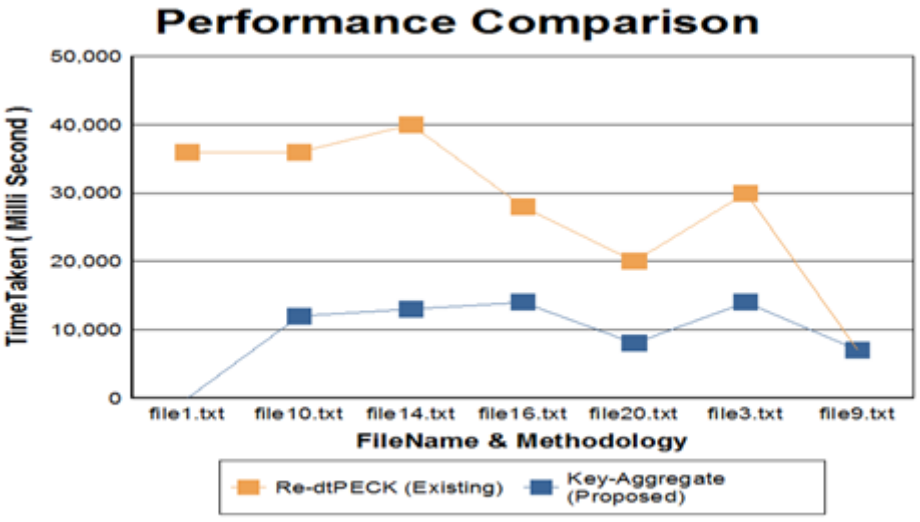

Figure 3: Performance Evaluation of the Secure Models

Table 1: Performance Comparison Table for Re-dtPECK and Key-Aggregate Schemes

FILE NAME	NUMBER OF DECRYPTION	TIME TAKEN IN (MILLISECONDS)	METHODOLOGY
File10.txt	2	24,000	Re-dtPECK
File14.txt	2	27,000	Re-dtPECK
File 3.txt	2	16,000	Re-dtPECK
File10.txt	2	12,000	Key-Aggregate
File14.txt	2	13,000	Key-Aggregate
File3.txt	3	14,000	Key-Aggregate

Here the above table1 represents the comparison of time taken to decrypt the data by the user on same files using existing scheme Re-dtPECK with scheme proposed Key-Aggregation cryptosystem based signature generation. It shows the variation on time taken in (milliseconds) where says this proposed scheme is better.

Initially the encryption and decryption time of multi-authority attribute based encryption and user usage based encryption is analyzed for various data size.

Table 2: Performance Computation of the Secure Model

Technique	Number. of File or File Size	Time Take in milliseconds	Number of Decryption
Time enabled proxy re-encryption function	5	24000	2
Key Aggregation Crypto system based Signature generation	5	12000	2

The above Table 2 represents the performance comparison of the existing scheme Time enabled proxy re-encryption function and proposed scheme Key Aggregation Crypto system based Signature generation where number of files and time taken to decrypt those files. In order to be used in multi-client setting, the scheme has to be performed in terms of high security and reduced decryption of the record by using proxy re encryption scheme as displayed in the Table 1.

V.CONCLUSION AND FUTURE WORK

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. The Experimental analysis proves that proposed model holds much better efficiency in terms of time, Scalability and Security compared with state of art approaches. In future the proposed work can be enhanced using three layer security on key generation.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm'10, Sept.2010, pp. 89–106.

[2]. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[3]. X.Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation,"Technical Report, University of Waterloo, 2010.

[4] R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07). ACM, 2007, pp. 185–194.

[5]. Peng liang Liu, Jianfneg Wang, Hua Ma, HaixinNie, "Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE " in Ninth International Conference on Broadband and Wireless Computing, Communication and Applications,2014, pp: 584 – 589.

[6]. ChangjiangHou, Fei Liu,HongtaoBai, LanfangRen, " Public Key Encryption with Keyword Search from Latice ", Eight International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (IEEE Conference Publications), 2013, pp. 336-339.

[7]. 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.

[8] S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient Unidirectional Proxy Re-Encryption," in Progress in Cryptology - AFRICACRYPT 2010, ser. LNCS, vol. 6055. Springer, 2010, pp. 316–332.

[9] C. Hu, P. Liu, "An enhanced searchable public key encryption scheme with a designated tester and its extensions," Journal of Computers, vol. 7, no. 3, pp. 716-723, 2012.

[10] V.Ramya, S.Thavamani, "A Study On Security Mechanism Employed On The Electronic Health Records In The Cloud", in International Journal of Contemporary Research in Computer Science and Technology (IJCRCST), Sep- 2017,pp. 208-210.

[11] Smitha Sundareswaran, Anna Squicciarini, DanLin "Ensuring Distributed Accountability for Data Sharing in the Cloud" IEEE Transactions on Dependable and Secure Computing, Volume: 9, Issue: 4, July-Aug. 2012.

[12] J. Li, Y. Shi, Y. Zhang, "Searchable ciphertext-policy attributebased encryption with revocation in cloud storage," International Journal of Communication Systems, published online, DOI: 10.1002/ dac.2942, 2015.

[13] Mr.M.Rajakumar and Dr.S.Thavamani "Privacy Preserving Healthcare Data using Cloud Computing", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, ISSN: 2278-3075, Volume-8, Issue-10S, Pages 118-124, August 2019.

AUTHORS PROFILE

Dr. S. Thavamani is an Associate Professor in Department of Computer Applications, Sri Ramakrishna College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu, India. She has a teaching experience of 22 years in the field of Computer science. She has received various awards like the "***Best Faculty Award"*** *from ARUNAI International Research Foundation (AIRF Awards – 2017),* **" *Incessant Service Award"*** for recognizes "***Being A Truly Inspirational Teacher****",* and *"****Best Team Award - MOOC – "Spoken Tutorial",*** from Sri Ramakrishna College of Arts and Science (Autonomous), ***" The Best Paper Award ", from*** Tiruppur Kumaran College for Women, Tiruppur, Appreciation Award for the " **Using ICT based Teaching and Learning methodology"** for students of Tamil Nadu from **Spoken Tutorial IIT Bombay.** Her area of Specialization is Distributed Computing and Network Security. She has presented more than 30 Papers in various International and National Conferences and she has published 27 international Journals. She is currently a supervisor for M.Phil. and Ph.D research works of various Universities. She acted as a coordinator of various Workshops and Seminars.