**International Journal of Engineering Inventions**
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 2, Issue 11 [Jul. 2013] PP: 77-80

# Patient Revocation and Secure Multi-Keyword Search Scheme Over Encrypted PHR

K.AMARENDRANATH[1], P.Hasitha reddy[2], N. DEEPIKA[3]
[1,2,3]*Assistant Professor, Computer Science and Engineering, Sree Dattha Institute of Engineering & Science*

**Abstract:** Cloud Computing is an up-and-coming technology now days in this bond in order to store and share enormous volume of data over internet we required Cloud Services. Cloud offering some services like IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS(Software as a Service) etc where it can control storage and share data securely with reduced cost thus sensitive personal Health records should be encrypted before outsource onto cloud for the sake of patient data privacy. As our existing system we noticed some of the privacy challenges over multi-keyword search from the cloud server. i.e patient revocation and lack of encryption scheme over index structure. In this paper we proposed a novel policy for patient revocation for avoiding patient revocation issues for dynamic updating over encrypted Health records by an authority i.e. Trusted Key manager(TKM) which manages keys by Diffie Hellman Algorithms: This algorithm is basically used to generate keys, and Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the PHR owner more direct control on access policies and does not require the PHR to distribute keys. In CP-ABE scheme, there is an authority (TKM) that is responsible for key management. The PHR Owner defines the access policies and encrypts data under the policies using SHA-1. Each patient will be issued a secret key according to its attributes. A Patient can decrypt the cipher text only when its attributes satisfy the access policies under the fine grained approach scheme.

***Keywords****: Trusted Key manager (TKM), Cipher text-Policy Attribute-based Encryption (CP-ABE)*

## I. INTRODUCTION

Cloud computing defined as virtual or remote access over internet. And cloud provides many services to the users based on client requirement the user can access the service. Among all the service storage as a service on of service, using this service any cloud data user can access data from cloud and any data owner can upload the data to the cloud. But due to privacy issues in cloud the data must be protected before sending to the cloud.

Cloud gives a place of work to clients to get to data whenever and from anyplace. It is not required for the client to be in an identical area from the equipment that stores information. At the point when the client has the web association they can get to the administrations of the cloud. It conveys every one of the administrations powerfully through the web as indicated by the client prerequisites. Cloud computing environment consists of two components: the front end and the back end connected through a virtual network or the internet. The front end is visible to the user (client). It consists of interfaces and applications that are required to access the cloud computing platforms. The back end represents a service provider. It consists of interfaces and applications that are required to access the cloud computing platforms.

Cloud services are categorized into these types.

a. Infrastructure as a Service (IaaS): It provides access to computing resources in a virtualized environment. Users use the fundamental computing resources like processing, storage, networking etc. Example: Google Compute Engine, Windows Azure.

b. Platform as a Service (PaaS): Users can hire programming and infrastructure tools provided by the vendors to develop and run the applications.

Examples: Google App Engine, Windows Azure

c. Software as a Service (SaaS): It is a software distribution model in which Users can use the software provided by the vendors.

Examples: Google Apps, Microsoft Office 365.

The deployment model defines the type of access provided to the cloud user. Cloud provides four deployment models:

Security and privacy concerns have been the significant difficulties in cloud computing. The hardware and software security mechanisms like firewalls etc. have been utilized by the cloud vendors. These solutions are not adequate to shield information in cloud from unapproved clients on account of low level of truthfulness [4]. Since the cloud user and the cloud provider are in the distinctive trusted space, the outsourced information

might be presented to the vulnerabilities [5]. In this manner, before putting away the significant information in cloud, the information should be encrypted [2]. Information encryption guarantees the information secrecy and trustworthiness. To save the information security we have to outline a searchable scheming that deals with encrypted information.

## II. LITERATURE SURVEY

*Song et al, "practical symmetric searchable method based on cryptography" [3]*

The encryption on data is an effective way to protect the confidentiality of data in cloud. But when it comes to searching, efficiency gets low. In literature many research works are not efficient in searching specially for complex queries. This inefficiency may lead to leakage of valuable information to unauthorized peoples. Song et al, for the first time proposed the practical symmetric searchable method based on cryptography [3]. In this scheme the file is encrypted word by word. To search for a keyword user sends the keyword with same key to the cloud. The drawback of this scheme is that the word frequency will be revealed.

*Baek et al, "Rhee et al improved hardness of security of Boneh's scheme"*

The first public key encryption with keyword search (PEKS) was proposed by Boneh et al. The scheme suffers from inference attack on trapdoor encryption method. Baek et al, Rhee et al improved hardness of security of Boneh's scheme. Baek's scheme introduces the concept of conjunction of keyword search. The public key encryption methods are computationally time consuming and complex that makes these algorithms inefficient.

*S.Buyrukbilen et al [6], introduce the first method that provides ranked results from multi-keyword searches on public-key encrypted data.* By avoiding a linear scan of the documents and by parallelizing the computations to the possible extent, this method reduces the computational complexity of public key cryptosystem. The scheme encrypts keyword information of each document in a bloom filter [7], and hierarchically aggregate (using homomorphic encryption) the individual indexes into a tree structure. Client will do the query processing, and traverse the tree in best-first manner. The query is hidden from the server or cloud provider by using an efficient private information retrieval (PIR) protocol [20]. In this method the indexes are split into multiple chunks, and use several CPUs in parallel to execute the user queries efficiently.

## III. SYSTEM STUDY

As our system study we understand and noticed some of the issues with Presented system. i.e, Patient revocations, Data Integrity Issues

### 3.1. Problem Statement:

Whenever any PHR owner wants to share any secure records using cloud, the records should be encrypted before outsourcing to the cloud and corresponding key should be shared with corresponding user, In order to download any records from cloud the user must search file from cloud but the records are encrypted in cloud so we can search keyword with plain text so we need to get access from corresponding PHR owner in order to search documents but this leads to burden for PHR owner for every user the PHR owner has to generate keys and he has to distribute the keys and the user. And if user wants to download multiple documents of PHR owner then he has to get multiple keys so this will lead to performance issues.

**Challenging issues:**

There are still many challenge problems in symmetric SE schemes with our presented system. In this scheme, the PHR owner is responsible for generating updating information and sending them to the cloud server. Thus, the PHR owner needs to store the unencrypted index tree and the information that are necessary to recalculate the IDF values. Such a dynamic information owner may not be extremely appropriate for the Cloud computing model. It could be hard to perform dynamic searchable encryption plot whose redesigning operation can be finished by cloud server just, in the interim holding the ability to sustain multi-keyword ranked search.
Really, there are numerous protected difficulties in a multi-user plan. Every one of the clients as a rule keeps the same secure key for trapdoor era in a symmetric SE plan

**Challage-1:**

The revocation of the user is big challenge. If it is needed to revoke a user in this scheme, we need to rebuild the index and distribute the new secure keys to all the authorized users.

**Challenge-2**

Data integrity is another challenging issue for Symmetric SE schemes usually assumes that all the data users are trustworthy. It is not practical and a dishonest data user will lead to many secure problems.

### 3.2 Proposed system

As our proposed system we came up with a novel policy for user revocation i.e. forward secrecy and backward secrecy for avoiding user revocation issues for dynamic updating over encrypted data by an authority i.e. Trusted Key manager(TKM) which manages keys by Diffie Hellman Algorithms: This algorithm is basically

used to generate keys., and Cipher text Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies and does not require the data owner to distribute keys. In CP-ABE scheme, there is an authority (TKM) that is responsible for key management. The data owner defines the access policies and encrypts data under the policies using SHA-1. Each user will be issued a secret key according to its attributes. A user can decrypt the cipher text only when its attributes satisfy the access policies under the fine grained approach scheme.

## IV. SYSTEM IMPLEMENTATION.

### 4.1. Solution: Challenge-1

**User revocation:** User revocation means user account deletion from the authorized list. It means if a user wants to withdraw his account from the cloud server or his login account will be deleted by the service provider then such a user's will no longer access the or share the data to the service providers due to inactive or unauthorized access privileges means may be his account is deleted or inactive, such a user's are called revoked users.

Here, we consider revocation of a data owner i.e his/her attributes/access privileges. There are several possible cases:

**How to solve the user revocation problems:**

Generally where in multi-owner framework, data owners share or access their data from the cloud server using access privileged keys which is assigned by the Trusted Key manager, for the sake of providing users confidentiality and data privacy in this connection data owners need to have privileged keys which is shared by Trusted Key manager (TKM) generated by the Diffie Hellman Algorithms:

**Implement Forward secrecy and backward secrecy**

Message Confidentiality is one of the most imperative components in multi owner framework. Massage guarantees that the sender private information which can be perused just by an approved and intended receiver. Hence, the confidential data is secured in efficient way such that it is not tampered by unauthorized users. Message Confidentiality is achieved mainly by two components namely Forward Secrecy and Backward Secrecy are used for message confidentiality. The two main components provide secrecy as follows.

• **Forward Secrecy:** It is a mechanism to assurance that for each and every time the user leaves the group he/she will not have any rights to the future key access.

• **Backward Secrecy:** It ensures that at whatever time a new user joins the group, he/she will not get any access to the past account details. User must be register with Trusted Key manager (TKM), which will manages both the above the secrecy

### 4.2 Solution: Challenge-2

**Data integrity:** Symmetric SE schemes usually assume that all the data users are trustworthy. It is not practical and a dishonest data user will lead to many secure problems.

For above issue in order to achieve data integrity we proposed Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies and does not require the data owner to distribute keys. In CP-ABE scheme, there is an authority (TKM) that is responsible for key management. The data owner defines the access policies and encrypts data under the policies using SHA-1 (Symmetric ES). Each user will be issued a secret key according to its attributes. A user can decrypt the cipher text only when its attributes satisfy the access policies under the fine grained approach scheme.

### 4.3 Algorithm Implementation

**Diffie Hellman**

In this section each user will generate secret key and send to TKM. The TKM center will retrieve all secret key and compact make the as single secret key and send to each user. The procedure of improved diffiehellman key exchange protocol as follows.

1. Each user select prime number p, g and private key a.
2. Using those values the user will calculate public key using pub=gamod p.
3. After calculating each user will send his public keys to TKM.
4. The TKM will retrieve public key from the each users and generate new private for the each users and calculate another public for individual users after successfully verified by access policies under fine grained approach.
5. After generating each public of users and send to it.
6. Each user will retrieve public key coming from the TKM will generate shared key using shared key=gpub mod p.
7. After generating shared keys of each uses and send to TKM.
8. After generating secret key the TKM will send to all users.

By using above users keys TKM allows user to perform dynamic updates on outsourced data.

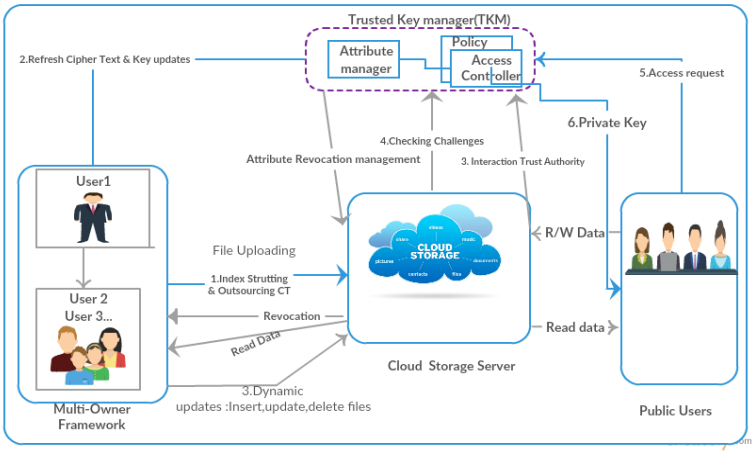


**Fig.1** Proposed System Architecture

## V. SYSTEM FUNCTIONING

**5.1. Trusted Key Manager (TKM):** is the independent party who issue, revoke, and update users' attributes according their authenticity of the particular domain. TKM is responsible for generating public attribute keys and issuing the secret keys to users enrolled in the domain after satisfying access policy under fine-grained approach verified by TKM

.**5.2. Multi-Owner:** PHR owner can outsource their documents for sharing and accessing by the other users. In this connection uploaded data i.e. File data and Index structure both should be encrypted and outsourced

**5.3. Cloud Storage Server:** The cloud server stores owners' data and provides data access service to users. It also helps users decrypt cipher text by generating decryption tokens and helps owners update file records i.e. insert, delete or modify when an attribute revocation happens.

**5.4. Public User:** For the sake of Outsourcing the data, data owners initially encrypts the data with content keys by using Asymmetric encryption techniques i.e. Diffie Hellman Algorithms. Then, the owner defines the access policies for multiple users and encrypts content keys under the policies. They do not trust on the server to do data access control. Instead, they assume that the server may give the data to all the users in the system. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the fine grained access policy with time stamp defined in the cipher text and satisfied by the fine grained policy; then user is able to decrypt the cipher text for the sake of Read or Write or Read-Write Operations

**Symmetric SE schemes for Data Integrity**

In this section for implementing Symmetric SE Schemes, the data owner defines the access policies (CP-ABE) and encrypts data under the policies using SHA-1 (Symmetric ES). Each user will be issued a secret key according to its attributes. A user can decrypt the cipher text only when its attributes satisfy the access policies under the fine grained approach scheme.

## VI. CONCLUSION

In this paper we suggested solutions for user revocations and data integrity issues related to multi-owner framework for multi keyword ranked search Scheme over encrypted data, we have presented solutions for User revocation and achieving data integrity using Trusted Key Manager (TKM) using CP-ABE Scheme.

## REFERENCES

[1] Zhihua Xia, Member et al, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", DOI 10.1109/TPDS.2015.2401003, IEEE Transactions on Parallel and Distributed Systems.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, "Public Key Encryption with Keyword Search", Advances in Cryptology Eurocrypt 2004, Springer, 2004, pp. 506–522.

[3] Dawn Xiaoding Song; Wagner, D.; Perrig, A., "Practical Techniques for Searches on Encrypted Data", Security and Privacy, 2000, S&P 2000, Proceedings 2000 IEEE Symposium, DOI: 10.1109/SECPRI.2000.848445, pp. 44-55, 2000.

[4] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", http://www. cloudsecurityalliance.org, 2009.

[5] R. Brinkman, "Searching in Encrypted Data", University of Twente, Ph.D thesis, 2007.

[6] S. Buyrukbilen and S. Bairas, "Privacy Preserving Ranked Search on Public Key Encrypted Data", Proc. IEEE International Conference on High Performance Computing and Communications (HPCC), November 2013.

[7] B. H. Bloom, "Space/time trade-offs in Hash Coding with Allowable Errors", Communications of the ACM, Vol. 13, No. 7, 1970, pp. 422– 426.

[8] Md. Khalid Imam Rahmani, Neeta Wadhwa and Vaibhav Malhotra, "Alpha-Qwerty Cipher: An Extended Vigenere Cipher", Advanced Computing: An International Journal (ACIJ) 3 (3) 2012, pp. 107-118.