Middle-East Journal of Scientific Research 24 (S2): 71-77, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.S2.119

Efficient User Revocation Scheme in Multi User Searchable Encryption over Cryptographic Cloud Storage

D. Eswaran and T. Rathika

Department of Computer Science & Engineering, SRM University,
Ramapuram Campus, Chennai. Tamil Nadu, India

Abstract: Cloud computing has played a major role in improving efficiency of Data Centre resources. One of the key advantages is the user organizations need not invest in infrastructure and resources. But, security considerations remain one of the main issues in adopting cloud technology. Usage of cloud should not lead to increased risks in compromising confidential information and unauthorized access to cloud data. Confidential information should be encrypted before outsourcing which obsoletes keyword based search. The Key challenge in the symmetric encryption is all the cloud users have the same encryption / decryption key which leads to problem in revocation of users. This paper proposes Efficient User Revocation Scheme (EURS) in Multi User Searchable Symmetric Encryption (SSE) over encrypted Cloud. In order to revoke the users, we present Efficient User Revocation Scheme (EURS) by combining the Searchable Encryption Scheme with Broadcast Encryption which prevents the revoked user from accessing the encrypted cloud data by updating the Server State. Thus, using the proposed scheme, a revoked user no longer able to perform searches on the cloud data which increases the security in Cryptographic Cloud Storage.

Key words: Symmetric Encryption · Broadcast Encryption · Cloud Computing · User Revocation

INTRODUCTION

Uring the past few years, cloud computing has become a $_{D}$key IT buzzword. The simplest definition for cloud computing is the ability to retrieve files, data, programs and use other services through the Internet which are hosted by cloud service provider and pay only for the computing resources utilized.

Cloud computing offers the following advantages to the users:

- The cloud service provider (CSP) owns and manages all the computing resources. The cloud users do not need to invest in computing resources and the cost of maintaining and administering the system.
- The cloud users can increase or decrease the level of use of the computing resources and services.
- The cloud users pay much less for the services, because they pay only for the computing resources and services they use.
- The cloud users can access the cloud for services anytime from anywhere.

Despite the various advantages of cloud services, outsourcing sensitive information to Cloud servers brings privacy concerns. The Cloud Server that hosts the data of users may access users' confidential information. Normal approach to guard the data confidentiality is to encrypt the data before hosting in the cloud. But, this will increase the cost while decrypting the data and using it.

In the plaintext data, keyword-based search is possible which cannot be directly applied on the encrypted data. The cloud user needs to download all the data from the cloud server and decrypt the data locally before using them, which is impractical. But encrypting the data and decrypting methodologies lead to high computational cost for both the cloud system and the cloud user.

On the contrary, more practical special purpose solutions, such as Searchable Symmetric Encryption (SSE) schemes have been used which improved the efficiency, functionality and security. Searchable Symmetric Encryption schemes allow the client to store the encrypted data to the cloud and execute keyword based search over cryptographic cloud.

Corresponding Author: D. Eswaran, Department of Computer Science & Engineering, SRM University,
Ramapuram Campus, Chennai. Tamil Nadu. India.

Initial work on searchable encryption only considered the single-user setting. The extension of this setting, namely, the multi-user setting, where Data owner owns the data, a group of Data users can submit queries to search the document collection.

There are many secure challenges in a multi-user setting. All the users usually keep the same secure key for trapdoor generation in a symmetric encryption. In this case, the revocation of the user is a big challenge. If a user is to be revoked, we need to encrypt all the documents with a new key and distribute the new secure keys to all the authorized users.

To overcome the above problem, this paper proposes an efficient user revocation scheme in Multi User Searchable Symmetric Encryption (SSE). In order to revoke the users, we present Efficient User Revocation Scheme (EURS) by combining the Searchable Symmetric Encryption (SSE) with Broadcast Encryption (BE), which provides that a revoked user no longer be able to perform searches on the cloud data.

Related Work: Searchable Encryption allows the data owners to store the encrypted data in the cloud and search based on keyword. Searchable encryption schemes can be created using public key based cryptography [1, 2] or symmetric key based cryptography [3, 4]. Song *et al*. [5] proposed the first symmetric searchable encryption (SSE) scheme and the search time of their scheme is linear to the size of the data collection. Curtmola proposed two schemes (SSE-1 and SSE-2) which achieve the minimum search time. Their SSE-1 scheme is secure against chosen-keyword attacks (CKA1) and SSE-2 is secure with respect to adaptive chosen-keyword attacks (CKA2).

These early works are single keyword boolean search schemes, whose functionalities are simple. Afterward, abundant works have been proposed for various search functionality, such as single keyword search, multi-keyword boolean search [6] ranked search and multi-keyword ranked search etc.

Among Multi-keyword boolean search, conjunctive keyword search schemes [7-9] retrieve the documents that contain all of the query keywords. Disjunctive keyword search schemes [10, 11] retrieve all of the documents that contain a subset of the keywords.

Predicate search schemes [12, 13] are proposed for both conjunctive and disjunctive search. All these multi keyword search schemes retrieve search results based on the search keywords supplied.

Whenever the Data Owner desires to revoke the privilege given to any user, it is a major issue. After revoking the user, entire documents need to be encrypted again and the new symmetric key to be shared to rest of the users.

User Revocation schemes in cloud storage [14] use Proxy and Trusted Server which adds to the overhead and whenever a user is revoked all the documents need to re-encrypt [15].

Symmetric Encryption: Now we describe the Symmetric Encryption Scheme

Symmetric Encryption: A symmetric key encryption scheme is a set of three polynomial-time algorithms SKE = (Gen; Enc; Dec) such that

- Gen takes a parameter k and returns a secret key K;
- Enc takes a key K and a plaintext p and returns a encrypted text e;
- Dec takes a key K and encrypted text e and returns p if K was the key under which p was produced.

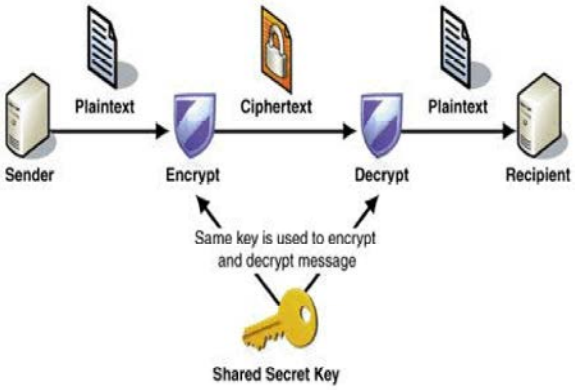

Fig. 1: The architecture of Symmetric Key Encryption

Intuitively, a symmetric key encryption scheme is secure against chosen-plaintext attacks (CPA) if the ciphertext it outputs do not leak any useful information about the plaintext. The Advanced Encryption Standard (AES) private-key encryption scheme can be used.

Searchable Symmetric Encryption: Searchable Symmetric Encryption let the cloud data owner to store the encrypted data to the cloud server and allow keyword based search over encrypted documents. Searchable Encryption methods are very useful in terms of efficiency, functionality and security.

There are two types of approaches while using Searchable encryption. One is to build an index for and lists the documents that contain those keywords. An alternative approach is to perform a sequential scan without using any index. The search will be faster when using an index. The disadvantage is storing and updating the index will be an overhead. So using an index is advisable for read-only data. For applications with large data, general technique used to speed up the searching is to use a pre-computed index.

The pre-computed index contains a list of key words; with each keyword having list of address for the documents where the key word appears. The key words are words of interest that Cloud user may want to search for later. The Data owner can generate the index in clear text documents. The clear text index is then encrypted and stored in the Cloud.

When Cloud User searches for a keyword and finds a match, it returns matching documents from the searchable encrypted index. Cloud User may decrypt the encrypted entries and retrieve the relevant documents.

The searchable index will be secure, if the search operation for a keyword w can only carried out by the Cloud users who possess a trapdoor and if the trapdoor can only be generated with a secret key. The index will not leak any information about its contents without the proper trapdoor.

Problem Formulations

Multi-user Searchable Symmetric Encryption: Previous work on searchable encryption only considered the single-user setting. The extension of this setting, namely, the multi-user setting, where Data owner owns the data and a group of Data users can submit queries to search the document collection. The Data owner can administer the search access by granting and revoking searching privileges to Data users. We define searchable encryption in the multi-user setting by using access control mechanisms.

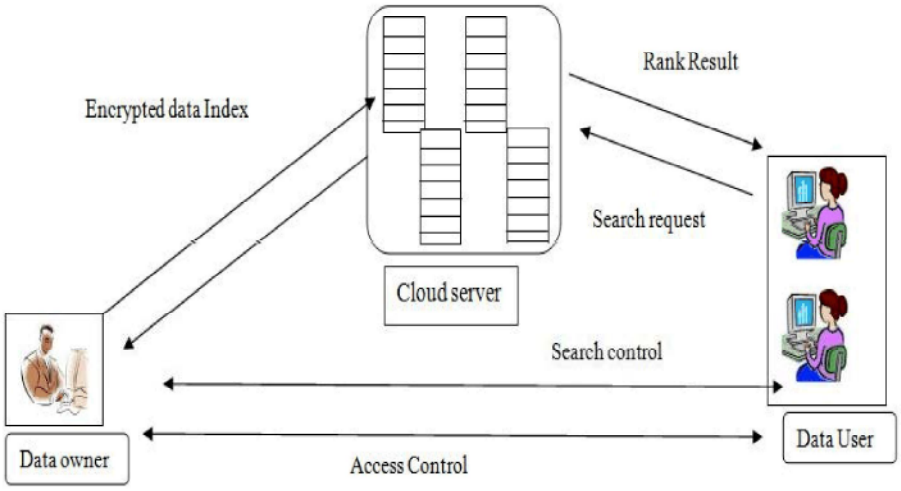

Fig. 2: The architecture of Searchable Symmetric Encryption (SSE)

The Multi User SSE has three different entities: Cloud Data Owner, Cloud Data User and Cloud Server.

Cloud Data Owner: Has a collection of documents that he wants to host in the cloud server. For security purpose, the documents are encrypted with the capability to search them for effective utilization. Cloud Data owner also need to undertake update operation of his documents hosted in the cloud server. The data owner updates the information locally and hosts it in the server.

Cloud Data Users: Can access the documents of cloud data owner. With keywords, the data user will generate a trapdoor which will fetch encrypted documents hosted in the cloud server. Then, the data user can decrypt the documents with the shared secret key.

Cloud Server: Hosts the document collection in encrypted form and encrypted tree index in searchable form for cloud data owner. Upon receiving the trapdoor from the cloud data user, the cloud server executes search in the index tree and returns the document collection.

The requirements are:

- Only authorized Cloud users can search and view the documents.
- In case of any dispute arises with a user, Data Owner should be able to revoke that user's access without affecting other Users.
- In case a user is revoked out of Group of data users, the documents should not be re-encrypted.

The Proposed Scheme: We propose to use Broadcast Encryption to meet the above requirements.

Broadcast Encryption: A Broadcast encryption scheme consists of four polynomial-time algorithms BE = (KeyGen; Encrypt; AddUser; Decrypt) such that;

- *KeyGen* is a probabilistic algorithm that takes as input a security parameter k and outputs a master key M_K.
- *Encrypt* is a probabilistic algorithm that takes as input a master key M_K, a set of users G and a message m and outputs a ciphertext c.
- *AddUser* is a probabilistic algorithm that takes as input a master key M_K and a user identifier U and outputs a user key UK_U.
- *Decrypt* is a deterministic algorithm that takes as input a user key UK_U and a ciphertext c and outputs either a message m or the failure status f.

A Broadcast encryption scheme is said to be secure if the ciphertext does not reveal any useful information about the plain text messages to any user who are not in G.

Multi User Searchable Symmetric Encryption: The Multi User Searchable Symmetric Encryption construction is defined below:

The documents in the collection D are encrypted using symmetric encryption. Then the encrypted documents are stored in the cloud server.

The data structure used in the Multi User Searchable Encryption scheme is given below:

First, each document in D is encrypted using a random generated symmetric encryption key. Then a secure searchable index I is created which consists of the following:

A: An array in which, encryption of all documents D are stored.

T: A look-up table is created for all documents D that facilitates one to locate and decrypt the corresponding element from A which is stored.

For each distinct keyword w in D, linked list L_I is created in which each node will consists of identifier of a document in D. All the nodes in the array A permuted in a random order are stored and encrypted with randomly generated keys. Before encrypting the jth node of list L_I, it is augmented with a pointer to the (j +1)th node of L_I, together with the key used to encrypt it. By this, the location in A and the decryption key for the first node of a list L_I, the server will search and decrypt all the nodes in L_I.

A look-up table T which enables locating and decrypting the first node of all list L_I. Each entry in T will point to a keyword w in D and consists of a pair <address, value>. The field value will consist of the location in A and the decryption key for the first node of L_I. value is itself encrypted using the random function. The other field, address, is used to locate an entry in T. The look-up table T uses indirect addressing as given in Figure 3

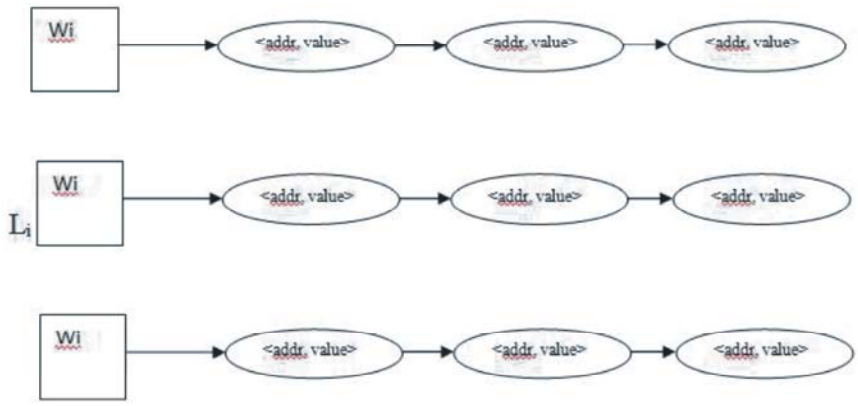

Fig. 3: List containing address and key

The Data Owner creates both the array and the lookup table based on the document collection D and stores them on the server together with the encrypted documents. When the user wants to retrieve the documents that contain keyword W_l, it computes the decryption key and the address for the document in T and provides them to the server. The server decrypts the given entry and gets a pointer to and the decryption key for the document. With the decryption key, the searched encrypted document is decrypted successfully.

Efficient User Revocation Scheme (EURS): We propose Efficient User Revocation Scheme (EURS) by combining the Searchable Encryption Scheme with Broadcast Encryption. The Efficient User Revocation Scheme is defined with six algorithms namely: KeyGen, Encrypt, AddUser, RevokeUser, Trapdoor and Search.

Key Gen: A Key generation algorithm executed by the Data Owner.

KeyGen (k) → (K_O)

It takes as input a parameter k and outputs a Data Owner secret key K_O.

Encrypt: An Encryption algorithm executed by the Data Owner to encrypt the document collection.

Encrypt (K_O,R,D) → (I,C)

It takes as input the owner's secret key K_O, Random record encryption key and a document collection D. It outputs a secure searchable index I with look up Table and a collection of ciphertext C. The look up table will consists of document id and randomly generated key for that document.

AddUser: Algorithm executed by the Data Owner to add a user to the Scheme.

AddUser (K_O,U)→ K_U

It's inputs are Data owner's secret key K_O and the unique user id U and outputs Users's secret key K_U.

Revoke User: It's a user revocation algorithm run by the Data Owner to revoke a user.

RevokeUser (K_O,K_U) → St_S

It takes as input the owner's secret key K_O and unique user id K_U. It outputs an updated server state St_S, where the revoked user will be marked as 'R' Revoked in the Authorised User List.

Trapdoor: A secured algorithm executed by the Data User to generate a trapdoor for a keyword to the authorised user.

Trapdoor (K_U,K_W) → t or f

It takes as input a user's secret key K_U and a keyword K_W and outputs a secret trapdoor t or the failure status f. It checks Authorized User List (AUL) wherein, if the User Status is 'A' Authorised it will output a secret Trapdoor. If the User Status is 'R' Revoked, it will output a Failure Status f.

Search: It is a deterministic algorithm run by the server S to perform a search.

Search (I,t,St_S) → SSE.Search(I,t)→ BE.Decrypt(C)

It takes as input an searchable secure index I, a trapdoor t and Server State St_S and outputs a set of documents X matching the keyword or failure status f. The selected document will be decrypted using the random record encryption key stored in the lookup table corresponding to that document. The main property in this Scheme is user revocation. After revocation, the revoked user will not be able to perform searches on the Data Owner's document collection over cryptographic cloud.

Authorised User List (AUL): Authorised User List is designed to implement the access control of users in searching the Cloud Data. The structure of AUL is shown in the following table

Table 1: User List with User State

User	*User State*
U1	A
U2	A
U3	R
U4	A

Whenever a new user is added by the Data Owner by using the AddUser Function, one entry is added to the Authorised User List with user state as 'A' i.e Authorised. When a user is revoked, the user state is changed to 'R' – Revoked. Whenever, the cloud user

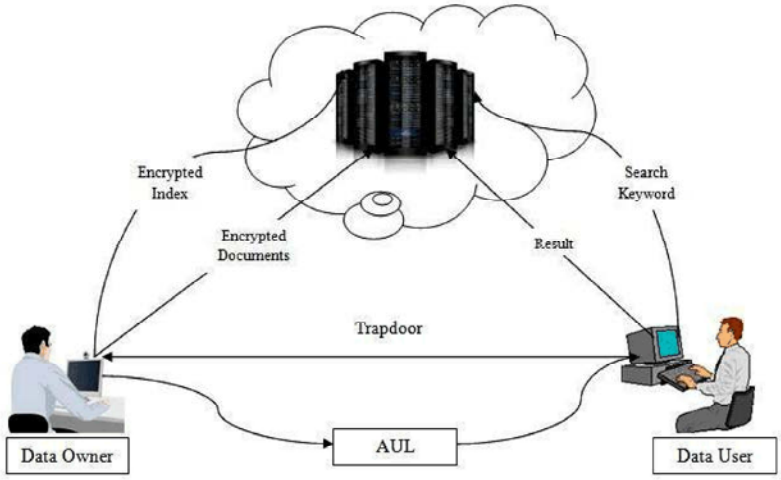

Fig. 4: The architecture of Searchable Symmetric Encryption incorporating Authorized User List (AUL)

sends a request for Trapdoor to the cloud storage by passing the Keyword and user key, system first checks the Authorised User List whether the user is an authorized user or he is a revoked user.

If the status is R-Revoked user, the failure state is returned to the user. If the status is A-Authorised user, then the secret Trapdoor is send to the user.

With the failure status, the user will not be able to proceed further and search the cloud documents.

Concurrent Revocation and Search Request: Data owner has issued a revoke command for a particular user and the same user has issued a search request to the cloud server concurrently. This situation needs to be handled meticulously.

In this scenario, whenever the Data owner issues a revoke command, it will have high priority and it will first update the Server State. Whenever the Server is executing a revoke statement, the server state will be set to 'Updating' and the Search request will again check the AUL after the Server State returned to 'Normal'. If the user status is revoked, then it will output Failure status to the user and the Data User will not be able to Search the contents in the Cloud.

Algorithm 1 Search (I,t,St_S,U_K)

Input: Index, Trapdoor and Server State
Output: Document collection or failure

1. **If** St_S is not equal to "Updating" then
2. C=SSE.Search(I,t)
3. X=BE.Decrypt(C)
4. Return X
5. **Else**
6. Wait till Server State returns to Normal
7. **If** U_K.UserState='R' then
8. Return "Failure"
9. **Else**
10. C=SSE.Search(I,t)
11. X=BE.Decrypt(C)
12. Return X
13. **Endif**
14. **Endif**

Security: The security of Efficient User Revocation Scheme (EURS) is analyzed in this section.

Confidentiality: The index and documents are stored in encrypted form. Every document is encrypted using random record encryption key. The encryption key is not shared with the Cloud Data Users. Also, after revocation of Users, the documents need not be encrypted again as the encryption key is not shared with the Cloud Data Users. Thus confidentiality is achieved.

Unforgeability: After execution of Adduser, there will be a unique key generated for the user. When executing Trapdoor, trapdoor must be called along with the user key and sent to cloud server to make a search. Without key, it is impossible to make a search request to cloud storage server. Thus unforgeability is achieved.

Revocation of User: After execution of RevokeUser, user id will be marked as 'Revoked' in the Authorized User List (AUL) which prevents the parse of trapdoor. In other word, the revoked user's search request is refused and the revoked user will lose the ability to search on the files stored in the cloud server. Revoking a user will not have any influence with other user's secret key.

CONCLUSIONS

In this paper, a secure and efficient User Revocation Scheme has been proposed to overcome the User Revocation issue in Multi User Searchable Symmetric Encryption. User Revocation has been carried out for a User without affecting other Authorised Users by implementing User Secret Key, Authorized User List and Server State. After revocation of Users, the documents need not be encrypted again as the encryption key is not shared with the Cloud Data Users.

REFERENCES

1. Boneh, D., G. Di Crescenzo, R. Ostrovsky and G. Persiano, 2004. Public key encryption with keyword search, in Advances in Cryptology-Eurocrypt 2004. Springer, pp: 506-522.
2. Boneh, D., E. Kushilevitz, R. Ostrovsky and W.E. Skeith III, 2007. Public key encryption that allows pir queries, in Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp: 50-67.
3. Goh, E.J., *et al*., 2003. Secure indexes. IACR Cryptology ePrint Archive, pp: 216.
4. Chang, Y.C. and M. Mitzenmacher, 2005. Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third international conference on Applied Cryptography and Network Security. Springer-Verlag, pp: 442-455.
5. Song, D.X., D. Wagner and A. Perrig, 2000. Practical techniques for searches on encrypted data, in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, pp: 44-55.
6. Kuzu, M., M. S. Islam and M. Kantarcioglu, 2012. Efficient similarity search over encrypted data, in Data Engineering (ICDE), 2012 IEEE 28th International Conference on. IEEE, pp: 1156-1167.
7. Golle, P., J. Staddon and B. Waters, 2004. Secure conjunctive keyword search over encrypted data, in Applied Cryptography and Network Security. Springer, pp: 31-45.
8. Hwang, Y.H. and P.J. Lee, 2007. Public key encryption with conjunctive keyword search and its extension to a multi-user system, in Proceedings of the First international conference on Pairing-Based Cryptography. Springer-Verlag, pp: 2-22.
9. Ballard, L., S. Kamara and F. Monrose, 2005. Achieving efficient conjunctive keyword searches over encrypted data, in Proceedings of the 7th international conference on Information and Communications Security. Springer-Verlag, pp: 414-426.
10. Boneh, D. and B. Waters, 2007. Conjunctive, subset and range queries on encrypted data, in Proceedings of the 4th conference on Theory of cryptography. Springer-Verlag, pp: 535-554.
11. Zhang, B. and F. Zhang, 2011. An efficient public key encryption with conjunctive-subset keywords search, Journal of Network and Computer Applications, 34(1): 262-267.
12. Katz, J., A. Sahai and B. Waters, 2008. Predicate encryption supporting disjunctions, polynomial equations and inner products, in Advances in Cryptology-EUROCRYPT 2008. pp: 146-162.
13. Shen, E., E. Shi and B. Waters, 2009. Predicate privacy in encryption systems, in Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography. Springer-Verlag, pp: 457-473.
14. Swaminathan, Y. Mao, G.M. Su, H. Gou, A.L. Varna, S. He, M. Wu and D.W. Oard, 2007. Confidentiality-preserving rank-ordered search, in Proceedings of the 2007 ACM workshop on Storage security and survivability. ACM, pp: 7-12.
15. Cao, N., C. Wang, M. Li, K. Ren and W. Lou, 2011. Privacy-preserving multi-keyword ranked search over encrypted cloud data, in IEEE INFOCOM, pp: 829-837.