ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

CONCRETE KEY AGGREGATE SEARCHABLE ENCRYPTION WITH FEDERATED CLOUD

Santhiya. C[1], Vanishree K.A.[2], Gayathri. V[3], Dr.M.K.Chandrasekaran PhD[4]

M.E, Department of CSE, Angel College of Engineering and Technology, Tirupur, Tamilnadu, India[1]
M.E, Department of CSE, Angel College of Engineering and Technology, Tirupur, Tamilnadu, India[2]
B.E, Department of CSE, Angel College of Engineering and Technology, Tirupur, Tamilnadu, India[3]
HOD, Department of CSE, Angel College of Engineering and Technology, Tirupur, Tamilnadu, India[4]

ABSTRACT— The capability of sharing selected confidential information or a group of selected documents with selected group of users is done in public cloud storage. But these documents may also be leaked in public cloud storage. But storage is a main advantage of using a cloud. Hence, to avoid the data leakage encryption and decryption are used which increases the level of security and is achieved both by using single key and multiple keys. When using multiple keys, difficulty in storage and cost occurs. Hence, single key is used to share documents in group via cloud. But when using single key, insiders' attack may occur inside a group. To avoid insider's attack and to share the documents securely and efficiently, a concrete group data sharing scheme is used. This concrete group data sharing is a multi-owner setup. Even though there are multiple owners, there should be only one key between a group and the number of trapdoor should be reduced. Federated cloud is also achieved in this scheme. Federated cloud is a multi owner model. It is defined as the combination of two or more clouds which is used for sharing the resources. When a cloud is used as a federated cloud, it provides a way of sharing the data securely and efficiently.

Keywords—Searchable encryption, fine grained access control, federated cloud**.**

I. INTRODUCTION

Cloud storage is provided as a best solution for sharing large amount of data either to a single user or to a group of users. The main advantages of cloud computing is that data shared in a cloud can be accessed from anywhere in the world only with the help of internet. One of the disadvantages of cloud computing is data leakage. Users want to send their confidential information securely and efficiently. There are several ways to hack this information by hackers. To avoid this situation, users have to encrypt their information and send the encrypted data to certain group of users. If the owner of a document wants to send only particular files in a document, it is possible with the help of Searchable Encryption (SE) technique.

The group can be a static group or a dynamic group. Static group is the group where the number of users is fixed. None of the user is allowed to join in the group in between a process. If the group is dynamic, any number of users can join in the group in between and can use the information. To avoid this, the group should be made dynamic in such a way that any new user who joins in a dynamic group should not know anything about the previous transaction of documents. Similarly, keys are either static or dynamic. If the key is static, a single static key can be used several number of times in a process. But, if a key is dynamic, a new key will be generated each time a user wants to use an application. But it costs more. Hence, in a concrete group data sharing method, keys should be made static and group should be made dynamic. But dynamic user should not know anything about the previous process that is going on in a group.

Searchable encryption scheme (SSE) and Key Aggregate Searchable Encryption (KASE) are the previous work. Both SSE and KASE provide an efficient scheme for sending the documents safely. One of the disadvantages in KASE scheme is that the scheme may lead to insiders' attack inside a group. To avoid this, concrete group data sharing system is used with the help of fine grained access control method.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

II. SEARCHABLE ENCRYPTION

Searchable encryption is used for the easy retrieval of encrypted data. Searchable encryption is an encryption method in which the owner of a document need not send all the documents which the receiver requests for. Instead, the users have to search the exact documents which are exactly required for the receiver based on the request of the receiver and then encrypt those particular documents alone. This will lead to send the exact documents.

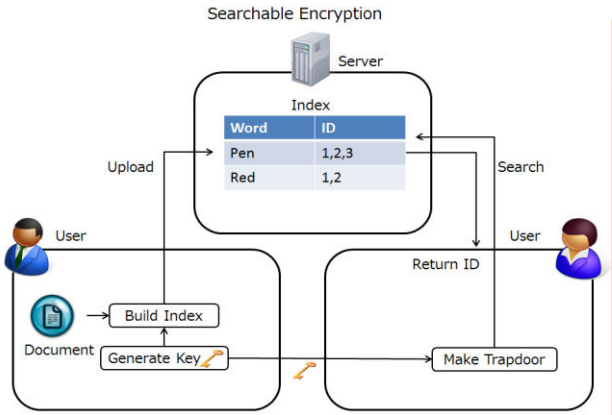


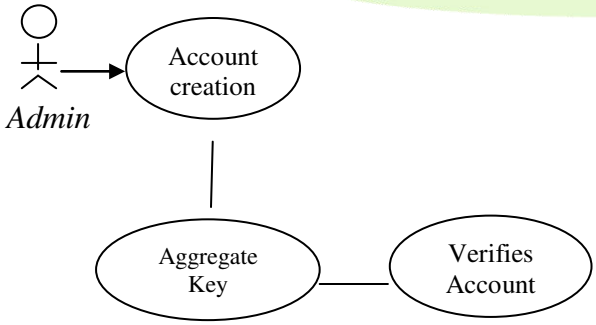
Fig. 1 Searchable Encryption

As the definition suggests, a user will upload a document or a word only to selected users based on their request. For example, let us consider three users, user 1, 2 and 3. A word named *pen* is encrypted and uploads this data to only the users 1, 2 and 3 and not to the other users because the data called pen is required for all the users 1, 2 and 3. Similarly, the user encrypts a word named *red* and uploads this data to only the users 1 and 2 and not to 3, since the data named red is required only for the users 1 and 2 and not to the user 3.

In addition to the data, owner of the data also send index (ID) to the receiver. Here the index of user 1, 2 and 3 is ID 1, 2 and 3. User 1, 2 and 3 will use their ID and trapdoor to search for the data which was send by owner of the data.

III. KEY AGGLOMERATIVE SEARCHABLE ENCRYPTION (KASE) FRAMEWORK

Key Aggregate Searchable Encryption (KASE) is the existing system. In KASE scheme, when a user wants to send information or some documents to other set of users, they have to encrypt their data. After encrypting the data, documents are sent to users along with this key. Once if the users are verified with their master key which is provided for them when creating an account for particular process, the authorized users are added to the database of a particular process.



ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

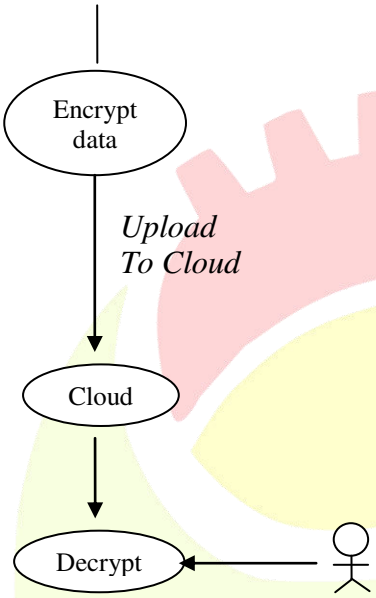


Fig. 2 KASE Scheme

The main advantage of KASE scheme is the delegation of users, which means a third person who is also an authorized user can be given rights to access all the information. Most importantly, KASE scheme is applicable only to the cloud storage that supports the well known *searchable group data sharing* functionality. KASE scheme contains the following modules which are used to make the data process more efficient.

A. Setup Phase

Administrator of a process will run this phase. This phase is also known as the account creation phase, where a user creates an account and all details of the user are collected such as username, phone number, address, mail-id, etc. After collecting all these details, administrator will add user to the corresponding database.

B. Aggregate Key Generation

Each authorized user will receive an aggregate key to their registered mail id. By using this aggregate key, the users have to verify their account.

C. Encryption and Decryption

In the process of sending and receiving a document, owner of a document should encrypt the document before sending and receiver of a document should decrypt the document for avoiding leakage. The plain text in a message is encrypted as cipher text with the sender's private key and is send to the receiver with the sender's public key. The cipher text in a message is received by the receiver's public key and is encrypted by receiver's private key.

D. Extract

Owner of the document runs this extract phase. Extract phase is used to delegation (giving rights to users other than sender and receiver of a document) is done.

E. Trapdoor

Trapdoor is used to in order to search a document quickly and efficiently. This is also known as *Indexing*. This can be done in both the encryption and decryption side.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

F. Adjust

Adjust is one the phases which is run again by the administrator. In this phase, any changes which are required by for the user is one.

G. Test

Test phase is done when the users are verified their account. It shows "yes", if the users are verified with their account and shows "no", if the users are not yet verified with their account.

IV. CONCRETE GROUP DATA SHARING SYSTEM

In concrete group data sharing, all the seven phases considered in KASE scheme is considered. In addition to the KASE scheme, the following table definitions are added.

Table Definition

1) *Table **group**<groupID, groupName, parameters> is to store the system parameters.*
2) *Table **member**<memberID, memberName, password, publicKey> is to store members' information including their public key.*
3) *Table **docs** <docID, docName, OwnerID, EncKey, SEKey, filePath> are to store the uploaded document of an owner with identity OwnerID.*
4) *Table **sharedDocs**<SID, memberID, OwnerID, docIDSet> is to stock up the documents of a member with identity memberID shared by the owner with identity OwnerID.*

Along with these four tables, the following phases are also considered in a concrete group data sharing system.

1. Setup Phase

When user submits a request, the cloud will create a record containing above four tables, assign a groupID for this user and insert a record into table. Then, the group data sharing system will work under the control of owner of the group. To generate the system parameters, manager runs the algorithm KASE **Setup** and updates the field parameters in concrete table.

2. User registration

When adding a new member, the owner of a group assigns memberID, memberName, password and a key pair for them and then stores the necessary information. User 1, 2 and 3's private key should be distributed through a secure channel such that the private key of one user should not be known to other users.

3. User login

A concrete group data sharing system depends on password verification for authenticating users. For further improvement in security, digital signatures may be used when available.

4. Data uploading

To upload a document, the owner runs **KASE Encrypt phase** to encrypt the data and then uploads them to the cloud. The cloud stores the encrypted. In addition, the owner can encrypt the keys using their private key and store them into the table.

5. Data sharing

To share a group of documents with a particular targeted member, the owner runs KASE **Extract** to generate the aggregate keys, and distributes them. If the shared documents for this member are transformed, the owner must re-extract the keys and update the fields.

6. Keyword Search.

To retrieve a document containing an expected keyword, a member should run **KASE Trapdoor** to generate the keyword for documents shared by each owner and then submits each trapdoor and the

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

related owner's identity to the cloud. After receiving the request, the cloud will run **KASE Adjust** and then run **KASE Test** to perform keyword search. Then, the cloud will provide the encrypted documents which contains the expected keyword to the member.

User uses a trapdoor algorithm in order to search which users send data or uploads file to other authenticated users with the help of search option. Trapdoor generation is available in both file upload and file download form. For both searching in encryption side and decryption side, indexing is used. In encryption side, encryption indexing is used. By using this, with the help of searching aggregate key, it is possible to find the details easily. Similar process will be done in decryption indexing.

7. Data retrieving

After receiving the encrypted document, the member will run **KASE Decrypt** to decrypt the document and the user can store this data in their own path and use it later.

V.FEDERATED CLOUD

Federated cloud is defined as the deployment and supervision of multiple external and internal cloud services to match business needs and is also referred to as service aggregation. It is also defined as the union of several smaller parts of a single organization.

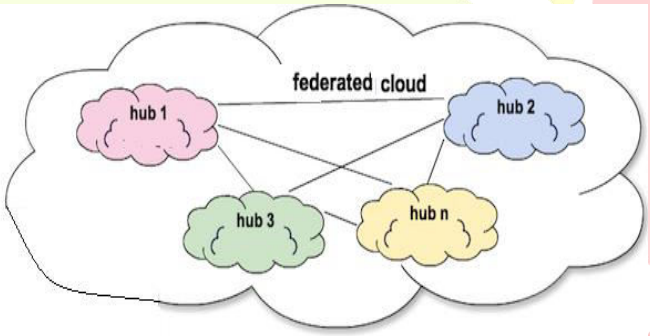


Fig. 3Federated Clouds

As the diagram suggests, a federation cloud is a combination of two or more hubs. There may be n number of hubs in a federated cloud. With the help of this federated cloud all the hubs can communicate easily.

The federation of cloud resources is done through network gateways that may connect public or external clouds, private or internal clouds (retained by a single entity) or community clouds (owned by several cooperating entities). As a result it creates a hybrid cloud computing environment. But federated cloud computing services rely on the existence of physical data centers.

Advantages of Cloud Federation:

1. Federation through different cloud resource pools permits applications to run in the most suitable infrastructure environments.
2. Federation cloud results in the reduction of costs due to partial outsourcing of data from a hub to the federation cloud.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

The disadvantage in cloud federation is the difficulty in brokering connectivity between a user and a given external cloud provider. To resolve this problem, cloud providers must give clients the permission to specify an lecturing structure for each server the cloud provider has extended to the internet.

Federated cloud is achieved through the concept of Triggering. In triggering concept,

SYNTAX:

```
mysql> CREATE TABLE table_name (attributes, amount DECIMAL (10,2));
Query OK, 0 rows affected (0.03 sec)

mysql> CREATE TRIGGER ins_sum BEFORE INSERT ON account
   -> FOR EACH ROW SET @sum = @sum + NEW.amount;
Query OK, 0 rows affected (0.06 sec)
```

Triggering concept is tough to implement and hence it takes more time.

A. Fine Grained Access Control

Fine grained access control is a mechanism which means that the users are finely refined. But the key should be single. Hence, the key between groups should be made single and a group may contain n number of dynamic users. But the dynamic users should not know any transactions that were done inside a group before the user joins in a group. Users are also given priority/rank and trees are used to assign users to the tree like structure.

A user level encryption enables high level privacy in cloud for user's data. Processing of data before sending to cloud involves encryption and decryption. In addition to that Cluster Formation is also done.

Cluster Formation:

Clustering is the process of grouping similar objects in a group. Here, users are to be clustered based on the priority of users. Each cluster will have a separate key.

Example:

Let us consider the Principal of a college wants to send some information to the students who belong to computer science department alone. Groups are available for principal with all Head of the Department. Hence this group is a cluster. Likewise, each of the HOD's will have a group with their department students. Hence, this group is a cluster. As the data is to be shared only with the computer science students, the Principal first needs to send the information to the Head of Department of computer science. Then the head of department will send that information to the students of computer science department. Here priorities/ranks are assigned to the users, such that rank 1 is assigned to the principal, rank 2 is assigned to the Head of the department and all the students in computer science department are assigned to rank 3.

When fine-grained controls are used and user wants to request for viewing a data, there are three possible authorization outputs.

Grant: The requesting user can access all available data.

Deny: The requesting user can't access any of the data.

Grant-with-conditions: The requesting user can access only the records that meets filtering conditions.

With the help of fine grained access control, insiders' attack is overcome by identifying the path in the tree

B. Multi-tenancy Model:

A multi-tenancy model is an architecture where users share the resources. In a multi-tenancy environment, numerous customers share the same application, which is running on the identical

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

operating system, on the same hardware, with the same data-stock up mechanism. This is similar to a number of tenants occupying sharing a same room. Here, each user is considered as a tenant.

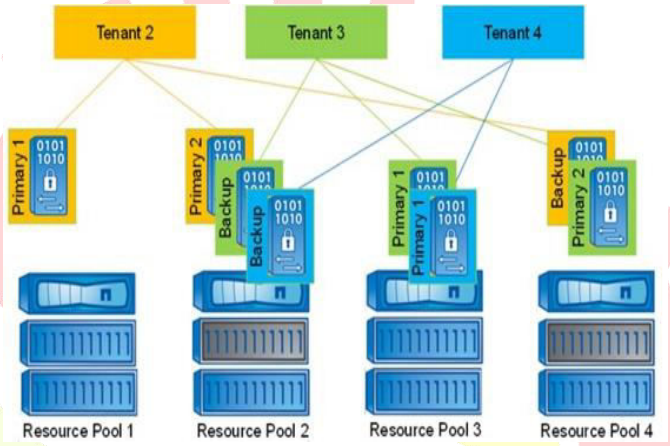


Fig. 4 Multi-tenant Model

Here, Tenant 2, 3 and 4 share the data. A multi-tenancy model is used in order to manage the resource utilization efficiently. The advantages and disadvantages of multi-tenancy model are as follows.

Advantages:

1. Economical
2. Streamline Release Management
3. Simplify Data Mining

Disadvantages:

1. As single application and database instance is shared with multiple customers, same set of tables and same database are used to store the records of multiple customers.
2. A fault in the software occurs while querying the data and lead adversary to access the record.

C.Multi-user searchable encryption:

A multi-user searchable encryption scheme suggests that multiple users in group can search a file using searchable encryption and can access the file by using a trapdoor. Trapdoor is also known as indexing, which means that trapdoor is used to search and find a file easily by using users aggregate key. This is just like searching a particular topic in a book with the help of index page.

Trapdoor is available in both file uploading and file downloading form. If the user wants to search for a file, they have to enter their aggregate key which is provided to the user for that particular file.

CONCLUSION

With the concrete group data sharing system, an efficient multi owner model is designed and developed to send selected documents to selected users. It is also possible to overcome insiders' attack with the help of identifying path in a tree like structure. Federated cloud is also achieved and by using which it is easier for the users to share their documents with other users safely and efficiently.

When using fine grained access control mechanisms, even there is a chance of allowing attackers to be added as an authorized user by creating an account in the group and they can use the confidential

information. This is also a leakage issue. Hence resolving this is a future work. Also, a triggering concept is tough to implement and it takes much time to implement. So achieving a federated cloud by avoiding triggering concept and using other methods for saving time is a future work.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Com-puting", Proc. IEEE INFOCOM, pp. **534-542, 2010.**

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[3] Z. Liu, Z. Wang, X. Cheng, et al. "Multi-user Searchable Encryption with Coarser-Grained Access Control in Hybrid Cloud", Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), IEEE, pp. 249-255, 2013.

[4] L. B. Oliveira, D. F. Aranha, E. Morais, et al. "Tinytate: Computing the tate pairing in resource-constrained sensor nodes", IEEE Sixth IEEE International Symposium on Network Computing and Applications, pp. 318-323, 2007.

[5] M. Li, W. Lou, K. Ren. "Data security and privacy in wireless body area networks", Wireless Communications, IEEE, 17(1): 51- 58, 2010.

[6] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012

[7] R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption". Cryptology ePrint Archive, Report 2013/508, 2013.

[8] J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou. "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014.

[9] D. H. Phan, D. Pointcheval, S. F. Shahandashti, et al. "Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts", International journal of information security, 12(4): 251-265, 2013.

[10] J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681-1689, Elsevier, 2010.

[11] J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490-502, 2012.

[12] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.