IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Verifiable ATTRIBUTE BASED & OWNER ENFORCED SEARCH AUTHORIZATION IN CLOUD

Sayaram N Shingote [1] Manisha S Shingote[2] Bhushan M Borhade [3]Yogesh A Shinde[4]

[1](Computer Engineering, SGOI's COE, Belhe /SPPU, Pune India)

[2](Electrical Engineering, SVIT, Nasik/SPPU, Pune India)

[3](Computer Engineering, SGOI's COE, Belhe / SPPU, Pune India)

Abstract: - *In cloud computing, where encryption-before outsourcing is a fundamental solution to protecting user data privacy in the distrustful cloud server environment, search over encrypted data is an extremely important enabling technique. Most of the secure search schemes have been concentrating on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and supervised by the individual owner, typically based on symmetric cryptography. In this paper, we target and concentrate on a diverse yet more challenging and defying scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users, that is multi- user multi-contributor case. We submit the attribute-based keyword search scheme with efficient user revocation (ABKS- UR) that enables scalable fine-grained (i.e. file-level) search authorization which is encouraged by attribute-based encryption (ABE). Our project related scheme will allow numerous owners to encrypt and outsource their data to the cloud server individually. Users can create their own search facilities without relying and depending on an online trusted authority. Fine- grained search authorization is also achieved by the owner-enforced access policy on the indication of each file. Additionally, by combining proxy re-encryption and lazy re-encryption techniques, we are capable to assign large size system update workload during user annulment to the resourceful semi-trusted cloud server. We define the security definition and prove the proposed ABKS-UR scheme selectively secure than chosen-keyword attack. To create confidence of data user in the suggested secure search system, we also build and design a search result authentication and verification scheme. Lastly, performance assessment shows the efficiency and effectiveness.*

Keywords: - *User Revocation, Cloud Computing, Attribute based Keyword Search, Fine-grained Owner-enforced Search Authorization, Multi-user Search, Verifiable*

I. Introduction

Cloud computing has arised as a recent and advanced enterprise IT architecture. Many unique and superlative advantages such as, on-demand computing resource configuration, universal and flexible access, significant capital expenditure savings, etc are been enjoyed by the companies as they are moving their applications and databases into the cloud. However, privacy concern has remained a prime obstruction prohibiting the adoption of cloud computing by a large number of users and applications. The owners of the data naturally become concerned with the privacy of their data in the cloud and beyond, when highly sensitive and confidential data are outsourced to the cloud. Encryption-before-outsourcing has been regarded as a fundamental means of protecting user data privacy against the cloud server, but utilization of that encrypted data becomes another challenge

The main concentration is on the problem of search over encrypted data, which is an important and valuable technique for the encryption-before-outsourcing privacy protection model in cloud computing, or in any networked information system where servers can't be trusted completely. Earlier, systems concentrated more on solutions based on single-contributor scenario, that is individual entity manages the encrypted dataset to be searched. In this, the search over encrypted data is enabled by two cases either the owner has to stay online and generate the search trapdoors, that is the "encrypted" form of keywords are to be searched, for the users upon request or by owner shared secret key with the authorized user. The same symmetric key will be used to encrypt the dataset and also to create the trapdoors. This system in turn limits the search adaptability for the users and applications.

Consider a following file sharing system that hosts an abundant number of files, contributed from various owners and to be shared among various users. This is a highly challenging multi-owner multi-user scenario. And probably the question of how to enable multiple owners to encrypt and include their data to the system and make it searchable by other multiple users was the challenge. To approach these open issues the existing system of authorized keyword search scheme over encrypted cloud data with efficient user revocation in the multi-user multi-data- contributor scenario was introduced. Particularly, the data owner encrypts the index of each file with an access policy which is made by him, which give information about what type of users can search for this index. The user

generates the trapdoor independently without depending on an always online trusted authority. The cloud server, on behalf of user can search over the encrypted indexes with the trapdoor, and then gives result which is matching if and only if the access policies embedded in the encrypted indexes satisfy the user's features related with the trapdoor.

The system framework of ABKS (Attribute Based Keyword Search) scheme involves three bodies: cloud server, many data owners, and many data users. To search the datasets shared from various data owners, a data user creates a trapdoor of keyword of interest using his private key and provides it to the cloud server. So, initializing the complete search process, we initially enforce and apply the coarse-grained dataset search authorization with the per dataset user list such that search does not need to proceed to a particular dataset if the data user is not on the corresponding authorized user list. Next, the fine-grained file-level search authorization is applied on the authorized dataset in the impression that only users, who are granted to access a particular file, can search this file for the expected keyword. More precisely, the data owner defines an access policy for each uploaded file. The cloud server will search the respective datasets and return the valid search result to the user if and only if the attributes of the user on the trapdoor satisfy the access policies of the secure indexes of the returned files, and the intended keyword is found in these files scale file sharing system.

II. Literature Review

1.1 A Survey on Keyword Search over Encrypted Data:

- **Secrete Key versus Public Key:**

Search over encrypted data have been studied broadly. The first searchable encryption scheme was design by D. Song, D. Wagner and A. Perrig [4] to enable a complete text search over encrypted files. From that search scheme, many more secure search schemes have been presented based on secret key cryptography (SKC) or public key cryptography (PKC) to improve the search over encrypted data. An effective single keyword encrypted data search scheme was proposed by R. Curtmola, J. Garay, S. Kamara and R. Ostrovsky [5] by adopting inverted index structure. An influencing version of [5] was design by S. Kamara, C. Papamanthou and T. Roeder [6], which support facilities such as adding and deleting files efficiently. N. Cao, C. Wang, M. Li, K. Ren and W. Lou [7] presented the first privacy preserving multi keyword ranked search scheme to enhance the search functionalities using "coordinate matching similarity measure" over encrypted data. Later on, more secure multi keyword text search scheme was proposed by W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou and H. Li [8] to search encrypted data over cloud using "cosine similarity measure" which gives more accurate search result and practically efficient search process using a tree based secure index structure. The first PKC based encrypted data search scheme was propose by D. Boneh and others [12], which supports single keyword query. As compared to symmetric search scheme, more flexible and more expressive search queries are generated using PKC based search scheme. Later on, scheme [13] supports conjunctive keyword search query by directly mentioning the number of encrypted keywords in an index. Predicate encryption [14], [15] is another efficient scheme that supports the expressive secure search functionality. The scheme [14] supports conjunctive, subset and range queries on encrypted data whereas scheme [15] supports disjunctions, polynomial equations and inner products.

- **Authorized Keyword Search:**

Search capabilities can be granted to multiple uses by enforcing the user authorization. A server enforced user list which contain all the authorized user's corresponding keys is adopted by the authors in [9], [10] for the complete search in enterprise scenario to achieve search authorization. This SKC based scheme has some limitation. It allows only single data owner in the system. Y. H. Hwang and P. J. Lee [11] proposed multi-user multi-owner scenario, which uses relative keyword search scheme. But this scheme has some limitations, it is not suitable for dynamic-cloud based scenario because the search time and the encrypted index is proportional to the total number of legitimate user and the data-owner has to edit all the corresponding indexes in order to append new user. Later on, file-level authorized private keyword search scheme over encrypted data in cloud computing has been introduced by M. Li, S. Yu, N. Cao and W. Lou [16]. In this scheme, whenever users want to search anything, they have to make use of attribute authority in order to obtain search capabilities. Therefore, this scheme includes higher communication cost. It is more suitable for data structure where only few keywords are stored. This scheme is not suitable for arbitrarily structured data search because the searching complexity is proportional to the total number of keywords in the system.

1.2 A Survey on Verifiable Search Based on Authenticated Index Structure:

C. Wang and others [17] proposed a single keyword search scheme with inverted index being the index structure for the search over encrypted data. They used hash chain in order to build search result verification scheme. Later on, in multi keyword text search scenario, W. Sun and others [18] introduced search result verification scheme by changing the proposed secure index tree into authenticated one. These works were only suitable for single user search scenario.

1.3 A Survey on Attribute-Based Encryption:

Attribute based encryption has always been of great interest due to its fine-grained access control property. The first key policy attribute-based encryption (KP-ABE) scheme was introduced by V. Goyal and others [19]. In this scheme, the attributes, which are used for encryption must match with the access structure on the user private key in order to decipher the cipher text. In reverse scenario i.e. CP-ABE, user private key is associated with set of attributes and cipher text is associated with an access structure. In broadcast environment, CP-ABE is always a preferred choice in designing an access control mechanism. Later on, a selectively secure CP-ABE was introduced by L. Cheung and C. Newport [20] using the simple Boolean function i.e. AND gate.
S. Yu and others proposed a selectively secure CP-ABE scheme, which supports attribute revocation by using techniques such as

proxy re-encryption and lazy re-encryption. This scheme is suitable for data outsourced cloud model.

III. Existing System

Features have been used to generate a public key for encrypting data and have been exploited as an access policy to authorize user's access. Using ABE schemes, we can get the advantages such as: (1) to decrease the communication overhead of the Internet, and (2) to give a fine-grained access control. In this paper, we survey a basic attribute-based encryption scheme, two various access policy attribute-based encryption schemes, and two various access structures, which are analyzed for cloud environments.
Application of encrypted data over cloud is a challenging and quite a difficult task. Considerable attention has been provided and huge effort has been made to provide solution to this issue, from secure search over encrypted data, secure function evaluation, to fully holomorphic encryption systems that provide generic solution to the problem in theory but are still too far from being practical due to the acutely large complications. Symmetric cryptography-based schemes are obviously not suitable for this setting due to the high complications of secret key management. Further more challenges involve how to control the updates of the user lists in the case of user enrollment, revocation, etc., under the dynamic cloud environment. In the existing system, the owner of the data has to provide the access policy for the particular data that is being uploaded to the cloud before uploading of the same. This develops complication in the scenario for numerous users to access the same file.

IV. Proposed System

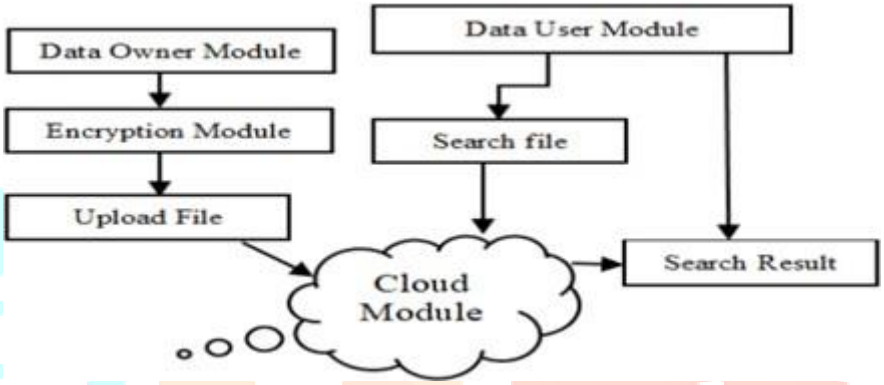

Figure 3.1: Proposed System

- The paradigm projected in our system involves three bodies: cloud server, many data users, many data owners. The authorized owner is implicitly expected to in charge of distributing and generating public, private and encryption keys.
- Data owners creates secure indexes with attribute-based access policies before outsourcing them along with encrypted data into the cloud server for enforcing fine grain keyword search authorization. For this scheme, we are using AES as the algorithm for encrypting data.
- The data user will use the private key which is provided by the data owner of respective file, which gives permission to the user to find the file over the encrypted data. Now the trusted user can search over the data using indexing which has to be done at the time of file uploading.
- It is not essential that all the authorized users would have the authority to access file, so for that we will adopt the fined grained file level search authorization. In fine grained file level search authorization when user will provide the keyword to be search at that time the key shared by that file owner automatically merged with keywords and search over the indexed data.
- If the user is having permit to access file then only, user can access it. At the time of uploading file owner will share key with predetermined user and in the run time owner can modify it.
- In our scheme we will use Advanced Encryption Standard for file encryption which is out of the extent of paper and RSA for Key Generation as their key distribution from owner to user then we are supposed to protect the key so Deffie-Hellman Key Exchange algorithm is been implemented.
- The distinctness between the existing system and our proposed system is that user has to describe the access policy at the time of uploading the file, but in our system, user can describe at the time of uploading file or at paradigm working time.
- Example, in existing system the user uploads file file1 and owner1 define the access list that is user1 and user2 means that user1 and user2 can access the file, but if user3 wants to access file there is no scope to that in such system as settings can't be changed in existing system, but in our system owner1 is uploading file1 and defines some users in access list i.e. user1 and user2, new user that is user3 requested to access file then if owner permits to access file then Access list will updated and now new access list will be user1,user2 and user3.

2. Modules Description

- **Registration Module:**

In this module, the user can register as a data owner or data user. Data owner encrypts and outsource the data on cloud. Data user searches over this encrypted data.

- **Login Module:**

Select the type of user that is Data owner or Data user then login using username and password.

- **Data Storage Module:**

Data owner encrypts the data before outsourcing it on cloud and also sets the access policies. This paradigm makes use of Data Encryption module and Key generation module.

- **Encryption and Decryption Module:**

This module makes use of Advanced Encryption Standard for Encrypting and Decrypting data.

- **Key Generation:**

This module uses the RSA algorithm (Asymmetric Cryptography) for private and public key generation.

- **Data Searching:**

In this paradigm, we are supposed to search over encrypted data, where we use the multi-keyword search and for searching user should have the public key which is provided and distributed by owner.

2.1 RSA Algorithm

The system was discovered by three scholars Ron Rivest, Adi Shamir and Len Adleman and hence, it is termed as RSA cryptosystem. RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys that is Public Key and Private Key. The idea of RSA is based on the fact that it is tough to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. Therefore, encryption strength totally lies on the key size. RSA keys can be typically 1024 or 2048 bits long

4.1.1 RSA Key Generation:

1. Choose two large prime numbers p and q.

2. Compute n = pq and $\phi(n) = (p - 1).(q - 1)$.

3. Choose an integer e, such that gcd $(e, \phi(n)) = 1$ and $1 < e < \phi(n)$. 4.Compute and integer d, such that $ed \equiv 1 \bmod \phi(n)$ and $1 < d <$ $\phi(n)$. 5.Public Key = (e, n).

6.Private Key = (d, n).

Encryption Procedure

To encrypt, the sender encodes the message into a numerical form C. Encryption is carried as follows: $C \equiv M^e \bmod n$

Decryption Procedure

To decrypt, the receiver uses the following formula first and then decodes the obtained number to get the intended Message M,

$M \equiv Cd \bmod n$

2.2 AES Algorithm

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical.

Description of the Algorithm:

1. Key Expansions round keys are derived from the cipher key. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round Add Round Key-each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

i. SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.

ii. ShiftRows - a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

iii. MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column. iv. AddRoundKey

4. Final Round (no MixColumns) i. SubBytes ii. ShiftRows iii. AddRoundKey

V. Conclusion

- Here, we studied various types of cryptographic techniques to understand solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data prior of storing into the Cloud.
- Here, a cloud-based web application was implemented to encrypt data on the cloud servers using AES encryption algorithm. This technique is used to encrypt data and stored on the cloud.
- Confidentiality is attained as the cloud server that operates on it does not know what data it operated upon. Also, if the cloud service provider servers are hacked by malicious attackers, the user's data is secured and cannot be used wrongly as it is encrypted. To search over this uploaded data, we design ABKS (attribute- based keyword search) Scheme.

References

[1] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, Hui Li "Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud 2016."

[2] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner enforced Search Authorization in the Cloud," in IEEE INFOCOM, pp. 226-234, 2014.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. of IEEE INFOCOM, pp. 1-9, 2010.

[4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE S&P, pp. 44-55, 2000.

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS, pp. 79-88, 2006.

[6] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. of ACM CCS, pp. 965-976, 2012.

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," in Proc. of IEEE INFOCOM, pp. 829-837, 2011.

[8] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacypreserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. of ACM ASIACCS, pp. 71-82, 2013.

[9] F. Bao, R. H. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings," in Information Security Practice and Experience, Springer, pp. 71-85, 2008.

[10] Y. Yang, H. Lu, and J. Weng, "Multi-user private keyword search for cloud computing," in Proc. of IEEE CloudCom, pp. 264-271, 2011.

[11] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proc. of Pairing, pp. 2-22, 2007.

[12] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYPT, pp. 506-522, 2004.

[13] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Of ACNS, pp. 31-45, 2004.

[14] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of Cryptography, pp. 535-554, 2007.

[15] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. of EUROCRYPT, pp. 146-162, 2008.

[16] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in Proc. of IEEE ICDCS, pp. 383392, 2011.

[17] C. Wang, N. Cao, K. Ren and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE TPDS, vol. 23, no. 8, pp. 1467-1479, 2012.

[18] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi keyword text search in the cloud supporting similarity-based ranking," IEEE TPDS, vol. 99, no. PrePrints, pp. 1, 2013.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM CCS, pp. 89-98, 2006.

[20] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. of ACM CCS, pp. 456-465, 2007.