International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue IV, April- 2016

MULTIKEYWORD RANKED SEARCH SCHEME WITH DECENTRALIZED ACCESS CONTROL OVER ENCRYPTED MOBILE CLOUD DATA THROUGH BLIND STORAGE

JITHIKA.M[1], RIJIN I.K[2]
Malabar institute of technology
Anjarakkandy
jithikarejin@gmail.com[1]

Abstract

Cloud computing is known as on-demand computing.Shared data,resources and other services are provided to other computers or devices on-demand.This recent technology that uses internet &central remote servers to maintain data and applications.A fundamental application is to outsource the data into external cloud storage for efficient ,stable,inexpensive storage. The outsourced data contain sensitive information such as personal photos,emails etc.So for getting privacy and confidentiality data has to encrypted before outsourcing them into cloud storage.This will create a problem on the searching some keywords over the encrypted cloud data.In this proposed scheme utilize relevance scoring technique for a multikeyword ranked search. Also an indexing mechanism is used to improve the searching efficiency.Confidentiality of documents and index,trapdoor privacy,trapdoor unlinkability,hiding the access pattern of search user is achieved using blind storage.In this proposed scheme for achieving authentication and access control a decentralized key management mechanism is used which provides user revocation and prevents replay attack.

Keywords—Cloudcomputing,multikeywordranked search,access control,blind storage,access pattern

• Introduction

A fundamental application of mobile cloud computing is to outsource the data into external cloud storage for efficient ,stable, inexpensive data storage. The outsourced data contain sensitive information such as personal photos, emails etc. So for getting privacy and confidentiality data has to encrypted before outsourcing them into cloud storage. Data encryption is the encoding of information, only authorized entity can read it. Encrypting the data will create a problem on the searching some keywords over the cloud data. For easy access or search over the encoded data over the cloud there is a need of searchable encryption scheme. A symmetric searchable encryption scheme proposed by Cash et al.[1].By adopting kNN technique Cao et al.[2] propose a multi keyword result ranking search. By blind storage Naveed et al.[3] proposed a dynamic searchable encryption scheme. With minimum delay most relevant result should be returned by the search scheme from extraordinary large cloud storage. Most of the existing scheme failed to achieve this. Also access control and authentication not handled in the existing scheme. Proposed scheme mainly contributes :

- Relevance scoring mechanism for multi keyword ranked search also an indexing mechanism for efficient search.
- For solving the trapdoor unlink ability and privacy and for hiding the access pattern of search user a modified blind storage system is used.
- To provide authentication and access control used a decentralized key management scheme.
- Also this scheme address user revocation and resistant to replay attacks.

1.1.System Model

System consists of five modules: Data owner, Cloud admin, search user, third party authenticator(TPA),Key distribution centre which is decentralized .

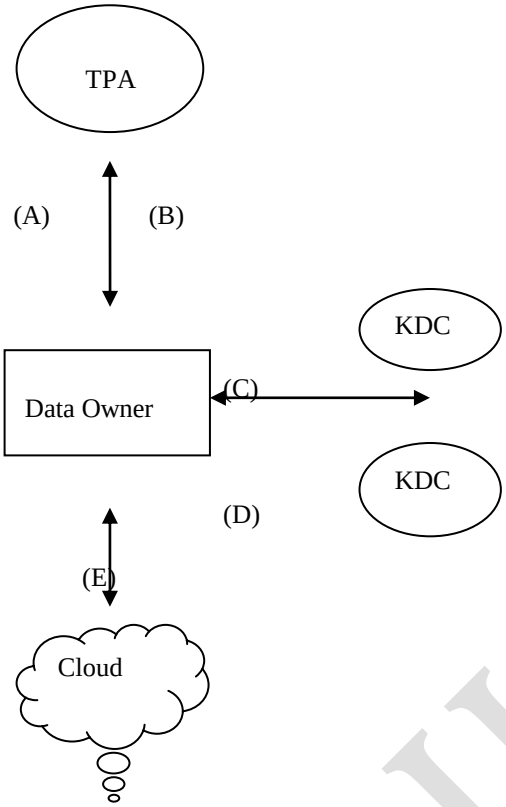

Fig 1: Decentralized key management

(A)-Registering user details

(B)-verify & provides token

(C)-Produce token & request permission

(D)-Sends key for encryption/decryption

(E)-Uploads encrypted documents

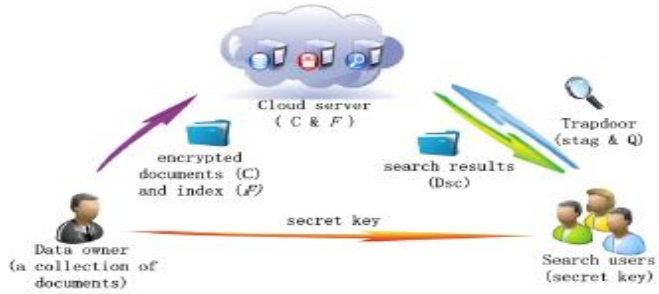

Fig: Overall architecture

1.2.Design Goals

- *Accurate multikeyword ranked search*:Provides searching of multikeyword from encrypted data ranking the results in a relevanc-based scheme.
- *Preserving the privacy and confidentiality*:All the documents and index should be encrypted that helps the cloud server from learning .
- *Hiding the access pattern*:Use blind storage mechanism to hide.
- *Authentication & accesscontrol*:Key distribution is decentralized in nature.Also address user revocation and resist to replay attacks.

2. Proposed System

The data owner stores a large number of documents *Doc* to a cloud server in an encrypted form *C*.The Data owner keeps a keyword dictionary *S* which contains *s* keywords.Owner use cipher text-policy based attribute encryption algorithm(CP-ABE) with AES to maintaining the encrypted database.This keyword dictionary act as the index to the encrypted documents.This is also in an encrypted from .In CP-ABE, cipher texts are generated by using an access structure that defines the access policy .A search user can perform the decryption only if attribute keys present in the search user satisfy the access policy in the cipher text.

1. Generation of secret keys and attribute keys

For the encryption of documents and index ,CP-ABE with AES algorithm is used. The secret key *Sk* that is used for the Enc() and attribute keys associated with access policy are generated by using a Third party authenticator(TPA) & Key distribution centers(KDC).Over all flow of the generation of secret keys and attribute keys:

- Request to the TPA:Data owner sends a registration request to the TPA
- Access policy creation by the TPA:After registration is over TPA provides the tokens along with the rules and regulation followed by the user.
- Data owner request for secret keys and attribute keys from the KDC by sending tokens.
- KDC generates different keys for different users that they are decentralized in nature.
- Whenever there is a misbehavior detected up on a owner then his key is revoked and that particular user cannot use that key or reenter in to the cloud environment.
- Cloud admin has maintain the list of KDC and TPA.It can monitor the abnormal behavior and key generation policies.Overall control is done by the cloud admin

2.2.Uploading the documents to the cloud

- KDC provides 192bit secret key ,it is different for different search users. By using this secret key the documents that are uploading is encrypted using AES.These encrypted documents are uploading to the cloud server through blind storage system.
- For searching keywords related to documents owner maintains an encrypted keyword index using an attribute based encryption.For that attribute keys are generated by the KDC based on the type of user.
- Encrypted documents and encrypted keyword index are stored in the cloud.So the cloud cannot understand the background details or the actual datas that are stored.
- Depending on the type of user the Secret keys and attribute keys that passed to the search user from the data owner through a secure channel.

2.3.Retrieve Documents from the cloud

- For retrieving the documents from the cloud search user needs to compute a trapdoor which includes a keyword related token called *stag* and an encrypted query vector.
- These query vector can be calculated by using the secret key received from data owner.The encrypted query vector *Q*,*stag*,and the number *k* is passed to the cloud server by the search user to get the most relevant k results.
- After getting the keyword related token the cloud server parses it to get the set of integers then the cloud server access the index F and retrieve the blocks indexed by the integers to obtain the tuples contains encrypted form of *id*,*symmetric key&random number* and the encrypted query vector.
- Compute the score for associated document using the encrypted relevance vector and the encrypted query vector.After sorting the socre descriptors of the top k documents can be sends back to the search user.

2.4.Decryption of retrieved documents

- After getting the descriptors if the search user's attribute satisfy the access policy of the document can decrypt the descriptor to get the id of the document and associated symmetric key.

- Compute seed and parse it as the sequence of integers and choose first k integers to retrieve the blocks indexed by these integers.
- By using the symmetric key decrypt the document to get the first block in the document. Combine all those getting blocks with header of document to recover the complete document.

3. Security Analysis

Security analysis of these scheme give the idea about confidentiality and privacy the original documents and the index ,Privacy and unlink ability of the trapdoor used by the search user to retrieve the encrypted document, concealing the access pattern of search user, access control and authentication achieved by using the decentralized key management.

3.1.Preserving privacy and confidentiality

Traditional symmetric cryptography AES is used to encrypt the Documents uploaded by the owner. Only the search user that gets the symmetric key can decrypt the documents. The descriptors in the index is encrypted by using cipher text policy–attribute based encryption algorithms. Only the search user with correct attributes can decrypt the descriptors to get the id of the document and the symmetric key used to encrypt the document.

3.2. Privacy and unlink ability of Trapdoor

Trapdoor consists of keyword related token and encrypted query vector which is totally concealed from the cloud server.unlinkability means cloud server cannot deduce any associations between two trapdoors.

3.3.Authentication and access control

De centralized access control with anonymous authentication is provided here. Also provides user revocation and prevents replay attacks.

4. Related work

A symmetric searchable encryption scheme proposed by Cash et al.[1].By adopting kNN technique Cao et al.[2] propose a multi keyword result ranking search. By blind storage Naveed et al.[3] proposed a dynamic searchable encryption scheme.

Boneh et al.[4] proposed the concept of SPE.But it support only single keyword search with searchable publickey encryption scheme.Liu et al. proposed a ranked search scheme that adopts a mask matrix. Sushmitha et al.[5] proposed a decentralized access control with anonymous authentication of data in cloud.

5.Conclusion

We have presented here a decentralized access control with authentication which supports user revocation ,prevents replay attacks,multikeyword ranked search over the encrypted cloud data via Blind storage mechanism.

6.References

[1] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ro³u, and M. Steiner,
``Highly-scalable searchable symmetric encryption with support for Boolean queries," in *Proc. CRYPTO*, 2013, pp. 353_373.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ``Privacy-preserving multikeyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222_233, Jan. 2014.

[3] M. Naveed, M. Prabhakaran, and C. A. Gunter, ``Dynamic searchable encryption via blind storage," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 639_654.

[4] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ``Public key encryption with keyword search," in *Proc. EUROCRYPT*, 2004, pp. 506_522.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, ``Ef_cient information retrieval for ranked queries in cost-effective cloud environments," in *Proc.IEEE INFOCOM*, Mar. 2012, pp. 2581_2585.

[6] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,"*IEEE Transactions on Parallel and Distributed Systems*, pp. 1045- 9219, 2013.