Searchable encryption for secure cloud storage

Yashvantkumar Pandya

Gtu pg school, Gujarat, India

ABSTRACT

Due to major increase in use of cloud storage by IT firm companies there is also increase the interest of stealing data from storage. There are so many methods to prevent the data from attacker but it increases the complexities of using the storage. The third party or the vendor may sell the data to some competitor for money so the data is not in safe hand on cloud. Also searchable symmetric encryption (SSE) is method to prevent from colludes but as security it growing tight the search complexity increases. As from survey we can develop a new method which is based on attributes rather key which provides more security and will be less time consuming to other existing methods. Third party storage is not as trusted as own so there must be some secure scheme or policy which protects data on other storage platform. Sahai and Water [1] find a better technique for securing data on vendor by encrypting the users credential and attaching it with the cipher-text so only person which can pass the access pattern can access the data from storage. Also there are other work done on this methods but protecting the credential is the main difficult task as access pattern may leak and if it is done nothing will be private. Identity based encryption [3] for securing the cloud storage and searching the data over it is now a trending scheme in cloud storage.

Keywords: *- searchable encryption, cloud storage, symmetric encryption, identity based encryption*

1. INTRODUCTION

As now in world every second billions of data is generated and the giant companies related to that firm have to store that data for reason. They can't hold that much of data and can develop large storage infrastructure so a new technology comes in market which provides its own storage space to user with some payment of money.

This technology of virtually providing a storage space to user is called as cloud. Cloud storage is mostly provided by third party vendor to whom companies might not trust but also companies can't afford so much big storage house for their own use where trillions of data generated daily. As the cloud storage provider may not provide much security its their own duty of user to protect their from hackers and their competitor. Data stored on cloud in plain form like file stored in pdf format in original form , credential stored in plain text form, encryption methods are used to protect data[2] on untrusted platform. More techniques like attribute based encryption [1][5] and ciphertext policy[1] used to encrypt and then searching that encrypted data which provide the searched data in encrypted form and then using key provided by data provider the data will be decrypted. The title gives idea that data should be searched in encrypted form [6] on cloud storage so only data provider and user can get data with proper credential. The keys are shared using LSSS (linear secret sharing scheme) [1] method or key distribution algorithm [4] between the data provider and search user.

Cloud storage is huge source of different-different information stored by so many data owner and so it is interested storage for hacker and people who are eager to know what data is stored by some data owner. The protection of data is the own duty of the data owner using some methods by implementing the algorithms and cryptography. More and more data is transferred to cloud storage the data on cloud is subject to leak or still by attacker. So there is need of developing a solid scheme which protects the credential and the data on cloud storage. There are so many researchers who have done work on it and find a way to secure the data on cloud storage. The solution to this problem was firstly as encrypt the whole data and then put it on cloud storage but what happen when we want only single file from the data storage? At that time vendor will give you whole bunch of data and now you have to find out which one you want. It is so much time consuming. Later a more advance scheme is given by Reza Curtmola and Juan [6] who proposed method for symmetric key encryption over data and then it is said as searchable symmetric encryption which is more advanced then prior scheme but more sophisticated as the key sharing needs extra time which increases the complexity. Identity based encryption [4] for securing cloud storage is more advanced method in cloud. It mostly attaches the credential of the user or attributes to the ciphertext so only user who satisfies the access pattern given access to the cloud storage.

2. BACKGROUND

Now a day's these is always an account for everything which is protected so only authorized user can access it and modify it. But as the data increases the IT firm is moving to cloud storage which is third party storage so no need to develop a separate infrastructure for businesses. As the data is stored on third party vendor so there is a threat of stilling the data and vendor may sell it to person who may give more money. There are some schemes and methods to protect the data on cloud storage which are used to grant access to only authorized user who has proper credential.

2.1 Symmetric key encryption

In Symmetric key encryption only one key is maintained for encryption and decryption for document so only one key is there for sender and receiver. This scheme is used in cloud storage as the data stored on cloud by client will be encrypted and then using some keyword list and symmetric key the user will be given access grant to the document from cloud storage.

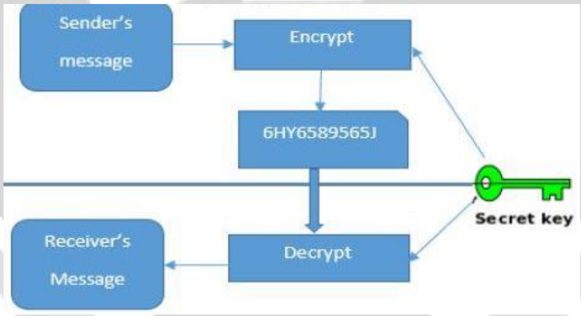

Fig. Symmetric key encryption

2.2 Attribute based encryption

Attribute based encryption is more secure method to encrypt the document where there is no trust on storage provider. In this scheme the set of attributes are encrypted and uploaded on policy server with some access ID so only authorized person. The existing method is not feasible for lightweight devices because of long calculation so attribute based encryption provide some faster method to protect the document.

2.3 **Searchable encryption**

Searchable encryption enables to search over encrypted files. It uses shamir's secret sharing scheme [10] to split the keyword. It allows searching the document without downloading it. Using both for same we can make searching possible without downloading and decrypt the document. In this method access IDs are created for set of words and searching is performed on these set of attribute. So it is called searchable encryption.

3. RELATED WORK

There are so many researches done on this area as this is the fastest growing trend now in world;

- Identity based encryption from the Weil pairing by Dane Boneh and Matt Franklin [3] proposed an identity based encryption scheme based on Weil Pairing in which they proposed a algorithm for securely allow the user access to the document. According to them this scheme is successful but not popular because it is not secure again chosen ciphertext attack. In this scheme the key is distributed at different site using different techniques of cryptography but the key distribution is problem.

- Searchable symmetric encryption by Reza Curtmola and Juan Curtmola [6] proposed a technique of protecting the data on cloud by encrypting it and some keyword will be stored with another document and the searching on storage will be done by keyword matching to document. A single key is maintained by both the sender and receiver which is used to access the document with keyword matching. In this scheme key will be distributed by some cryptographic technique.

- Ciphertext policy attribute based encryption by Amit Sahai, Brent Waters and Bethercourt [8] proposed a more secure and advanced encryption policy which attaches the attribute of the user to the ciphertext and by doing this the owner of the data himself will decide that who will access his document. There is no key sharing between any parties so time complexity will be less. Also only the user who can satisfy the access pattern given access to the document. Also to restrict the access of user who is previously allowed accessing, a time stamp will be attached to access pattern so by that time that user also not allowed to access the documents.

4. PROPOSED WORK

As per some survey mostly all smart phone producing company provides cloud storage to their phone user. If user uploads data in unencrypted form it is risky. To secure this data attribute based encryption is used. This is good way to secure data but to implement it on lightweight devices require to many resource when user wants to download it. This thing motivates to develop method which reduces the computation and calculation so this can be used on mobile devices. When searching facility available over encrypted document there is no need to download whole document from cloud, just search using keyword and you will get encrypted document then decrypt on your side. It will reduce the computation and fasten the searching of document. It is advantageous as due to searchable encryption you can search without downloading the documents.

The existing system is slow as it requires much calculation on user side. So the system will be developed which can enhance the searching capacity. We have to use searchable encryption with attribute based encryption which secure the document and also provide searching capacity over encrypted data.
In the existing system user have to download whole bunch of data and then find document which is unnecessarily consumes time and require decryption of more data.

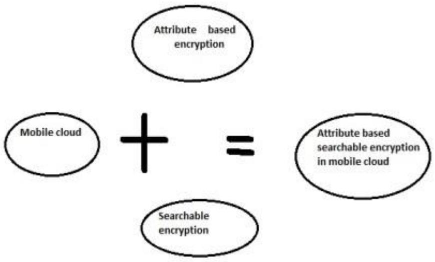
Attribute based encryption
Mobile cloud
+
=
Attribute based searchable encryption in mobile cloud
Searchable encryption

Fig. Attribute based searchable encryption

By using searchable encryption with attribute based data can be downloaded in encrypted form and then it can be decrypted by user.

Here, for encryption Shamir's secret sharing [10] scheme will be used. When policy server receives the ciphertext from user, it stores access tree and ciphertext component. Then remaining portion of ciphertext assigned a access ID and forwarded in storage server. The policy server and storage server are decentralized from each other so no leakage of access pattern through storage provider. The storage server then use these set of encrypted words to generate index. This index makes the fast searching over encrypted document. Here, Notations are C_y, C'_y are ciphertext component, T is access policy, CT_w, CT set of encrypted words, ID(T) is assigned index values to the encrypted words.

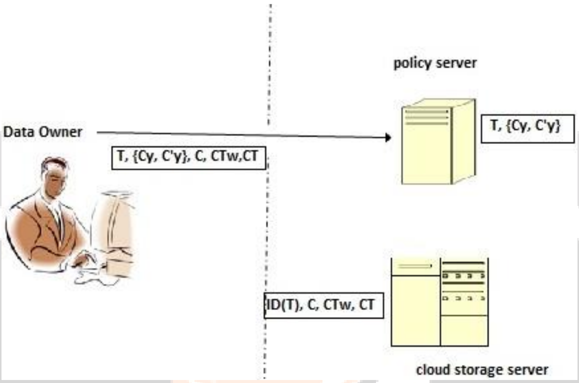

Fig. Policy server and storage provider

5. CONCLUSION AND FUTURE WORK

This paper provides the brief introduction about existing scheme and methods to protect the data on cloud storage. It also provides secure system to protect data on public storage. Using searchable encryption with existing system searching over encrypted word is possible. It also saves much time and provide more secure ways.

6. REFERENCES

[1].Ciphertext-Policy attribute-Based Encryption by Amit Sahai, Brent Waters and John Bethencourt paper for US army (2003).

[2].Identity-Based Encryption from the Weil Pairing by Dan Boneh and Matt Franklin *at J.Kilian CRYPTO 2001*.

[3].Searchable Symmetric encryption: Improved definition and efficient construction by Reza Curtmola, Juan Garay, Seny Kamara, RafailOstrovsky*at CCS'2006 Alexandria, Virginia, USA.*

[4].A Secured and Searchable Encryption Algorithm for Cloud Storage paper by KratiMehto, Rahul Moriwal at *International Journal of Computer Applications (2015)*.

[5].Secure Schemes for Secret Sharing and Key distribution by Amos Beimel*(Thesis paper-Israel Institute of Technology-1996)*.

[6].Provably Secure Ciphertext Policy ABE by Ling Cheung, Calvin Newport *at CCS'2007*.

[7].Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity- Based Cryptography by Liang Yan, Chumming Rong and Gansen Zhao *in Springer-VerlagBerlin (2009)* .

[8].Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization by Brent Waters at *International Association for Cryptologic Research 2011*.

[9].Cloud Computing definition from *https://en.m.wikipedia.org/wiki/Cloud_computing*.

[10].Dawson, E.; Donovan, D. (1994), "The breadth of Shamir's secret-sharing scheme", Computers & Security