International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Encrypted Searching: A Technique To Obtain Information Security In The Retrieval Of Remotely Stored Data

Kamlesh Pawar[1], Kunal Ranawade[2], Vijay Berry[3]
[1 2 3]*(Computer Department, RSCOE/University of Pune, India)*

Abstract:- With the increasing use of cloud for storage and other services provided, security and privacy has become major concern. As the data is outsourced to the cloud, there is chance that it is accessed by the other user or the cloud service provider. To prevent disclosure of database information, the security techniques started emerging for data confidentiality. One of these techniques is cryptography. Encryption is used to change the normal text to encrypted format so that it can be understood by only authenticate user. It can be done using symmetric or asymmetric key. Data is outsourced to cloud to get storage and other services. Data is stored in encrypted format to provide the security and maintain the confidentiality. Encryption assures the security from network threats also. Only storing the data in encrypted format is not the solution, it should also provide the searching and other necessary services. Hence the need of providing efficient search for encrypted data is important. Various techniques are implemented to provide the search over encrypted data storage. Different types of searching techniques are also helpful to retrieve the result fast and efficiently.
Keywords: - security, cryptography, multi-keyword search, symmetric encryption, asymmetric encryption

I. INTRODUCTION

As the use of internet and its services are growing widely, the data over the internet needs to be secure from the unauthorized users and attackers. Most of the companies or individuals have started outsourcing their data to the cloud for economic benefit and to get better services. Despite the tremendous business and technical advantages of the cloud, the security and privacy concern has been one of the major hurdles preventing its widespread adoption [1]. To protect the data stored over the cloud, different schemes are implemented to provide the security. Previously the data is stored in plain format but for the enhancement and the need of security, it is stored in encrypted format. The paper gives the idea about providing security and allowing the search over the encrypted data.

Only outsourcing the encrypted data to cloud is not the solution. The cloud should provide the services which will allow the user to perform the operations like searching, updating the data. The paper explains the various encryption techniques and services to provide the search over the encrypted data. Encryption schemes and their actual usage help the user to make the utilization of better encryption algorithms to maintain the privacy and efficiency simultaneously. Providing the search service over the encrypted data storage is also the important concern. The paper will help to understand the searchable services provided over the encrypted data storage

II. CRYPTOGRAPHY

Cryptography means converting the text from plain text to other format which is not recognizable. It is the technique of achieving security by encoding to make the text non-readable. Cryptography ensures the security of the data because though the unauthorized person gets access to data, he will not be able to manipulate the data. It helps to maintain the properties like data integrity, data confidentiality and non-repudiation. Encryption is the form of cryptography. Encryption converts the text form the normal to cipher text. Cipher text is the form of text which is not readable. Some of the types of cipher are block and byte cipher which is used for cryptography.

2.1 Block cipher

Block cipher is used to convert the plaintext to ciphertext which is encrypted format of text. As the name suggests it takes the fixed size block as input and convert it to the ciphertext. Utilizing all the bits of block simultaneously, it will convert the single input block to the cipher block which is entirely different from input text. Particular algorithm and key is used to convert the text into encrypted form. Also the padding of bits is required as an input data in not the multiple of block size used by an algorithm.

2.2 Stream Cipher

Stream cipher is basically related to the pseudo-random number generator and depends on private key. Random stream of bits is generated and it is used to generate ciphertext by performing XOR operation with the input stream. As the key is private, original text is retained by the person who has the key.

III. ENCRYPTION

As discussed above encryption is the process of converting the text form plaintext to non-readable form. Encryption is done by different by using the key. Similarly the encrypted text is converting to its original format by the process of decryption with the help of key. There are two types of keys. One is public and other is private. Private key is also called as secret key. In cryptography, private key is an encryption and decryption key which is known to the parties that exchanges the data. Public key is provided by some designated authority as an encryption key that, combined with private key that, combined with private key derived from public key, can be used to effectively encrypt messages and digital signatures. Symmetric encryption and asymmetric encryption are the basic types of encryption technique.

3.1 Symmetric Encryption

In this technique both the parties which are involved in communication have the same key for the encryption and decryption of the data. The disadvantage of the symmetric encryption is both the parties have access to the private key. Symmetric encryption is faster than the asymmetric encryption. Once the key is lost, decryption or encryption of the data is difficult. AES, 3DES, IDEA are some of the popular symmetric key algorithms.

3.2 Asymmetric Encryption

In symmetric encryption, there is more threat if key falls into wrong hands over the network. Asymmetric encryption uses both public key and private key. Public key is sent to the one who want to send you the data and private key is kept secret to one who will receive the data. In this way, though one gets the public key over a network, he will not be able to decrypt the data as the private key is with the receiver. It requires more time to process the data for encryption using this type of encryption. Some examples of asymmetric algorithms are Diffie-Hellman key exchange algorithm, Digital Signature Algorithm (DSA).

IV. SEARCHING TECHNIQUES

Searching techniques help to retrieve the required result for the user's search.

4.1 Single keyword search

Single keyword search includes only the single keyword for the search and retrieve the result accordingly. Single keyword search, it may give un-necessary result. To overcome the drawback of the single keyword search, multi-keyword search is used.

4.2 Multi-Keyword Search

More than one keyword is used for this type of searching. Multi-keyword search allows the efficient and faster search over the data. It narrow downs the result which helps to retrieve the exact required result. Now a days, most of the databases allows the multi-keyword search and multi-keyword search is used widely in most of the application.

4.3 Fuzzy keyword search

Sometimes it is not possible the keyword used for the search is exact matches with the available one. In this case the search may not be efficient or search may fail. There may be the distance in two keywords such that we can get the one by replacing, deleting or inserting the text or character in the other word. For the betterment, fuzzy keyword search generates the fuzzy keyword set by some editing distance of the original keyword. This overcomes the disadvantage of the searching techniques which only supports the exact keyword search. Fuzzy keyword search improves the search over the encrypted data.

4.4 Private matching

Private matching, as another related notion, has been studied mostly in the context of secure multiparty computation to let different parties compute some function of their own data collaboratively without revealing their data to the others [3].These functions involve intersection or matching of the two sets. Though this type of techniques is more secure, there is presence of computational overhead which makes it less efficient.

4.5 Multi-dimensional Search

Multidimensional search makes the use of more than one attribute of the entity to be searches over the database. With the help of multi-dimensional search, the search is narrowed down and is faster. Consider the example that we want to find the bank record of person named “Harry” having balance>1000 and from branch “Pune”. Using more than one attribute, the searching technique improves the efficiency.

4.6 Searchable Encryption

Searchable Encryption helps to maintain the privacy of the data.SE also involves a client and a server, where the latter stores an encrypted database ~ D, and the former possesses a private query Q that wants to obtain the query result Q(D) without revealing both Q and plaintext D to the server[1]. Since the data information is not revealed to server, privacy is maintained.

V. RANKING

Ranking of the result helps you to get the result accordingly to the priority. Relevant files to the given search are provided by the searching techniques but their priority is decided by ranking. Ranking of the result involves arranging the files with more relevant files called top-k files. The result is return according to the certain criteria that may include frequency or relevance of that keyword in the document. Ranking helps to sort the result and arrange them in a particular order. Due to ranking, it is possible to ignore the unnecessary document and return the expected refined result only. Such ranked search system enables data users to find the most relevant information quickly, rather than burdensomely sorting through every match in the content collection [2]. Search engines make use of ranking to show the search results and related documents.

VI. SEARCH OVER THE ENCRYPTED CLOUD DATA

To provide the security to the data which is stored over the cloud, encryption techniques are used. Data is stored in the encrypted format over the cloud for the storage purpose. It is necessary that the cloud should provide the searching service; only storing the data is not efficient. To provide the search over the encrypted data, the search keyword should be encrypted using the same techniques as that of the stored data is encrypted. Once the query is submitted in the encrypted format, it is secure while passing through channel. Since the keyword is encrypted using the same technique as that of data, it will provide the search for that keyword over the stored data and the result is retrieved. As described above, multi-keyword search can be used to get the result faster and get the result easily for the given keywords. Ranking is also used to get the top-k files for the retrieved results and removes the overhead of unnecessary files. Different algorithms are used to encrypt the data and outsource to the cloud but the care should be taken that the search keyword should be encrypted using the same algorithm

otherwise the search may fail and give the garbage result. With the usage of encryption and searching techniques, efficiency and privacy can be improved and time can be minimized to get the result.

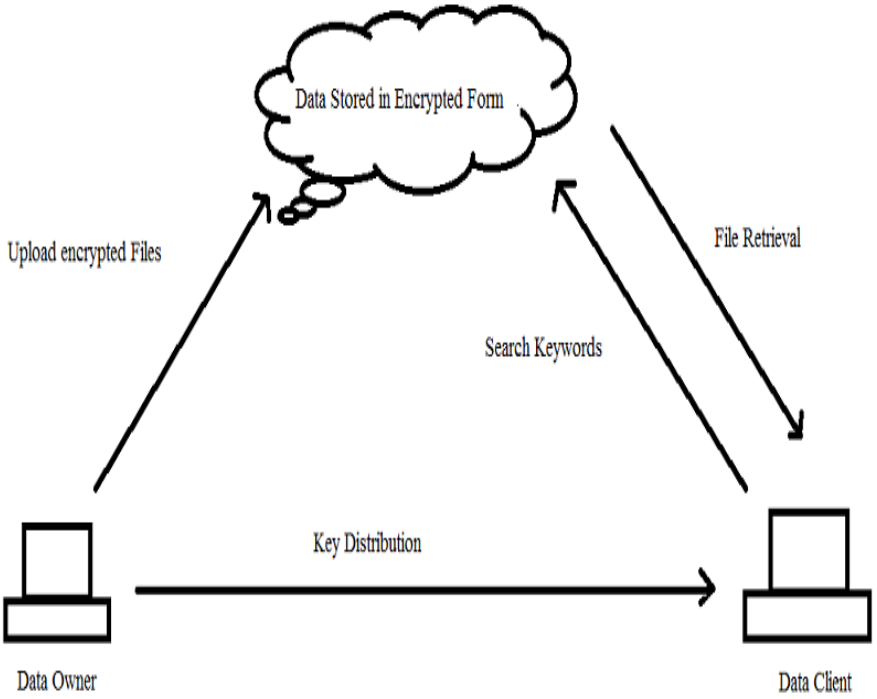

Fig 1

VII. CONCLUSION

To maintain the security, it is necessary to store the data in the encrypted format over the cloud. Privacy can be achieved by using the different techniques. The advantage of storing the data in encrypted format is though data is accessed, it will not be in the readable form and the confidentiality is maintained. The key is needed to be maintained because once the key is lost data cannot be accessed or decrypted to its original state. Highly secure database systems use the encrypted data storage and maintain the privacy also. Further the improvements in the searching techniques can be done and used for the sky computing.

REFERENCES

[1] Ming Li, Shucheng Yu, KuiRen, Wenjing Lou And Y. Thomas Hou,"*Toward Privacy-Assured And Searchable Cloud Data Storage Services*", PROC. IEEE NETWORK, JULY/AUGUST 2013

[2] Ning Cao, Cong Wang, Ming Li, KuiRen And WenjingLou,"*Privacy Preserving Multi-Keyword Ranked Search Over Encrypted Cloud Data*", PROC. IEEE INFOCOM 2011

[3] Jin Li, Qian Wang, Cong Wang, Ning Cao, KuiRen, WenjingLou,"*Fuzzy Keyword Search over Encrypted Data in Cloud Computing*", PROC. IEEE INFOCOM 2010