IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 10, October 2016

A Survey on Searching Shared and Encrypted Data for Security on Cloud

Swati Virkar[1], Priti Chinchwade[1], Shivani Ajmire[1], Prof. R.A. Badgujar[1]

Department of Computer Engineering, Jaywant Shikshan Prasark Mandal, Bhivrabai Sawant Institute of Technology & Research, Pune, India[1]

Abstract: Cloud computing is a capable, evolving Internet computing of this era. It presents the users with a secure storage for storing the documents online wherein the users can take the benefit of freedom to access it remotely avoiding the usage of the data storage services. When it comes to cloud data security, new technique is required. Protecting data in the cloud can be similar to caring data within a traditional data center or enhanced data center like cloud. Authentication and uniqueness, access control, encryption, protected deletion, is a numerous authentication encryption term. For encryption-based data access control for cloud, in which it shows that the mechanism of security is dealing with revocation could achieve by the different security techniques. It demonstrates that a encryption method in cipher text updating key for authentication for trusted user, so a security susceptibility appears. A revoked user can still decrypt new cipher texts for that user want to request for the new secret keys to access data.

Keywords: Encryption, Trapdoor, Index, Searchable Encryption.

1. INTRODUCTION

Cloud, also known as 'on-demand computing', is a class of Internet-based computing, where shared resources, facts and information are handle to computers and other devices on claim. Data security is the most important issues in cloud. To achieve high flexibility and to strong authentication for multiple data owners are outsourcing their data provides to private cloud. The data encryption reduces the data utilization. Consider large numbers of documents are outsourced on cloud by large number of cloud handler. It is mandatory for the search service to provide results similarity ranking to provide the exact results. Retrieving of all the data files having queried keyword will not be affordable in pay as peruse cloud model. The search techniques are shows that to solve the problem of multiuser data access over encrypted data using trusted third party in cloud. User will encrypt their data nearby. Before encrypting data, the index will be created. Trusted other party will use all these indexes to find data similar to the look for query of user. Using all the finding results, cloud server will send encrypted document to the user.

Data encryption makes effectual data consumption a very difficult task given that there could be a big amount of outsourced data files. In the Cloud, data owners may divide their outsourced data with a big number of authenticated users, who may want to only retrieve certain specific data files they are paying attention in through a given period. This keyword find technique allows users to selectively retrieve files of notice and has been widely useful in original look for scenarios. The data encryption technique, which unauthorized user's ability to perform keyword look for and it demands the protection of data privacy, makes the traditional plaintext examine methods fail for encrypted cloud data.

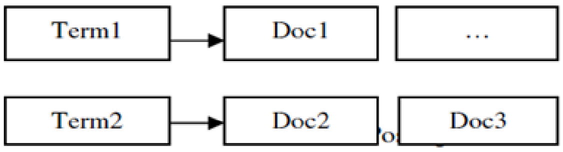
2. LITERATURE SURVEY

1)Selective Document Retrieval Scheme[1] SDR the scheme is secure in security model and can be adapted to support many useful search features, including collecting search results, associate conjunctive keyword search queries, advanced keyword search, search with keyword existence frequency, and search based on central product. These are the parameter are define the SDR parameter: Keygen, Build Index, Trapdoor, Search Index, Retrieve. Keygen(s): Run by a client, this algorithm takes security parameters as input, and outputs a secret key K. It may also produce some other public parameters such as a predicate set F. Build Index (K; d): Run by the client, this algorithm takes the key K and a document d 2 D as input, and outputs an index Id which encodes u(d) (i.e. all keywords from the document d).Trapdoor(K; f): Run by the client, this algorithm takes the key K and a predicate f 2 F as input, and outputs a trapdoor Tf . SearchIndex(Tf ; Id): Run by the server, this algorithm takes a trapdoor Tf and an index Id as input and returns an encrypted result to the client, where Rd implies whether u(d) satisfies the predicate f or not. Retrieve: Run between the client and the server, the client takes the secret key K and the encrypted search results as input and the server takes the encrypted database DB as input. At the establishment of the protocol, the client first decrypts and Decides which documents to retrieve, and at the end of the protocol the Client retrieves the documents user wants. This scheme provide flexible services to the trusted users but it is not efficient to provide Multi-User Authentication Services.[1]

2) Secure Inverted Index Scheme [2] An inverted index is a data structure loading words or numbers in a file along with its location. The determination of an inverted index is to progress the time of full text searches. An inverted

DOI 10.17148/IJARCCE.2016.51028

index holds an index of keywords which stores a different list of terms finding the collection and, for individually term, a posting the updating list of documents that hold the keyword .An inverted index improves search effectiveness which is required for very large text files. An inverted index consists of a distinct terms and a posting list which stores the IDs of the documents that hold that term. In count to an ID, each posting holds list element gives the number of rates occurrences of that term in the document.



Structure of an Inverted Index

It provide good retrieval performance as well as better security for indexes.
The major drawback of this process is that, It Track unnecessary network traffic for retrieval of data. [2]

3) **Password-based Group Key Exchange in a Constant Number of Rounds.[3]**
In the password-based authorization setting, it assumes each player holds a password pw drawn consistently at random from the wordlist Password of size N. This secret of low-entropy (N is often assumed to be small, i.e. typically less than a million) can be used to authenticate the parties to each other unfortunately, one cannot prevent an rival to choose randomly a password in the vocabulary and to try to copy a player. However such online in-depth search (even if N is not so large) can easily be limited by requiring a slight time interval between successive failed attempts or securing an account after a beginning of failures. Security against such active attacks is measured in the number of passwords the rival can "erase" from the candidate list after a failure. Other hand, off-line full search cannot be limited by such practical performances or computational resources considerations. They can be prevented if the protocol is carefully designed and ensures that no data about the password can leak from passively listen in transcripts, but also from active attacks.[3]

4) Public Key Encryption with keyword Search [4]
public-key searchable encryption it gives two constructions for public-key searchable encryption: (1) an well-organized system based on a variant of the Choice Diffie-Hellman assumption (assuming a chance oracle) and (2) a limited system based on general trapdoor variations (without assuming the random oracle), but less well-organized. It enable to send a short secret key TW to the mail server that will enable the server to locate all messages holding the keyword W, but learn nothing else. It produces this trapdoor TW using her private key. The server just sends the relevant emails back to user. This calls such a scheme non-interactive public key encryption with keyword search, or as shorthand.
This Paper suggest the advantage like, It send the mail server a key that will enable the server to identify all messages having some specific keyword, but learn nothing else. But it does not wish to give the gateway the ability to decrypt all messages.[4]

5) Shared and Searchable encrypted data for untrusted severs.[5]
An RSA-Based Proxy Encryption Scheme a proxy encryption scheme, a cipher text encrypted by one key can be transformed by a proxy function into the matching cipher text for another key without revealing any information about the keys and the plaintext. Applications of proxy encryption include: secure email lists , access control systems and attribute based publishing of data .It has feature like, the keys can be easily revoked without any overhead. But, Authorized user in the system has his own keys to encrypt and decrypt data.[5]

3. LITERATURE REVIEW

S.No	Paper Name	Advantages	Disadvantages	Review
1.	Selective Document Retrieval from Encrypted Database	Provide flexible services.	It is not efficient to provide Multi-user authentication Services.	Provide better security with the help of selective document retrieval.
2.	Privacy Preserving Keyword Search over Encrypted Cloud Data	1. Good retrieval performance 2. Provide better security for indexes.	Track unnecessary network traffic for retrieval of data.	Provide security under different attackers model with high performance.
3.	Password-based Group Key Exchange in a Constant Number of Rounds	1.constant-round password-based key exchange protocol for group, derived from the Burmester-Desmedt scheme 2. The use protocol is secure against dictionary attacks under the DDH assumption.	It only requires four rounds of communication and four multi-exponentiations per user.	Security is provide by using the protocol namely password-based constant-round group key exchange. Due to This communication can be happened in minimum rounds.

4.	Public Key Encryption with keyword Search	It send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else.	Does not wish to give the gateway the ability to decrypt all her messages.	It provide the public key which is made by party for encrypt and decrypt data. The key can be checked through gateway.
5.	Shared and searchable encrypted data for untrusted servers.	The keys can be easily revoked without any overhead.	Authorized user in the system has his own keys to encrypt and decrypt data.	It provides security as well as revocation. When unauthorized people can access data then key can be revoke by different techniques.

4. CONCLUSION

In this review, all search schemes that provides both privacy protection capability with less overhead has been proposed. Results on an encrypted data and security analysis using different models show that data privacy can be preserved while retaining very good retrieval performance using enhanced algorithm. Future work will further improve the efficiency and security of search and secure data with the trusted user.

REFERENCES

[1] C. Bösch, Q. Tang, P. Hartel, and W. Jonker, “Selective document retrieval from encrypted database,” in Proc. 15th Inf. Security Conf. (ISC), vol. 7483. 2012, pp. 224–241.

[2] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Proc. 3rd Int. Conf. Appl.Cryptography Netw. Security, vol. 3531. 2005, pp. 442–455.

[3] M. Abdalla, E. Bresson, O. Chevassut, and D. Pointcheval, “Passwordbased group key exchange in a constant number of rounds,” in Public Key Cryptography—PKC (Lecture Notes in Computer Science), vol. 3958, M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds. Berlin, Germany: Springer-Verlag, 2006, pp. 427–442.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 3027,C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer-Verlag,2004, pp. 506–522.

[5] C. Dong, G. Russello, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in Proc. 22nd Annu. IFIP WG 11.3 Work.Conf. Data Appl. Security XXII, vol. 5094. 2008, pp. 127–143 4] F. Bao, R. H. Deng, X. Ding, and Y. Yang, “Private query on encrypted data in multi-user settings,” in Proc. 4th Int. Conf. Inf. Security Pract.Experience, vol. 4991. 2008, pp. 71–85.

[6] Eu-Jin Goh eujin@cs.stanford.edu

[7] R. A. Popa and N. Zeldovich. (2013). Multi-Key Searchable Encryption.[Online]. Available: http://eprint.iacr.org/2013/508

[8] Q. Tang, “Search in encrypted data: Theoretical models and practical applications,” in Theory and Practice of Cryptography Solutions for Secure Information Systems. Hershey, PA, USA: IGI, 2013, pp. 84–108.

[9] E. Bresson, O. Chevassut, and D. Pointcheval, “Dynamic group Diffie-Hellman key exchange under standard assumptions,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science),vol. 2332, L. R. Knudsen, Ed. Berlin, Germany: Springer-Verlag, 2002, pp. 321–336.