Open access Journal International Journal of Emerging Trends in Science and Technology
Impact Factor: 2.838 DOI: http://dx.doi.org/10.18535/ijetst/v3i04.05

QSCK: Quick Search using Searchable Chipertext Keywords for Cloud Storage

Authors
Vomshi P R, Prof. Mr. Shashidhara H.S.
Department of Information Science and Engineering, MS Ramaih Institute of Technology, MSR College Road, MSR Nagar, Bangalore 560054,Karnataka, India
Email: *vomshi.pandana@gmail.com, 8971485844*

Abstract
At present scenario, data owners are storing their data in semi trusted cloud storage. Since the cloud storage is not fully trusted the data should be encrypted and stored in cloud. If the stored data volume is huge, for retrieval there should be a search engine and index keyword. If hackers are getting the index keyword they have the clue of the important files so that, in this system we are introducing searchable chipertext keywords. That means the keywords are in encrypted form. Consider access control over the cloud data, the technic at present used are Attribute Based Encryption (ABE) or Identity Based Encryption (IBE) these techniques requires lot of computation and slow in retrieval process. In proposed system we are using Bloom Filter based Chipertext index keywords which provide the search result very quickly with less computation and process.

Keywords— *Access Control. Data Security and Integrity. Attribute Based Encryption. Qucik Search. Verifiable Keyword. Ciphertext keyword. identity based Encryption.*

Introduction

Cloud computing allows data owners and data users to use enormous data storage and infinite computation capabilities at an affordable price. The major drawback is that data owners wont have direct control over the data outsourced. To overcome this concerns, data owners should induce encryption of their data before outsourcing to the cloud. The encryption technique causes searching over the outsourced encrypted data to become more tedious and also enforcing an access control policy consumes more time and becomes inefficient. The search operations are outsourced to the cloud, and the outsourced data is kept private. The faithfulness and successful completion of the various tasks associated with the cloud should be verified by the data users. Existing solutions cannot achieve these objectives to our known knowledge.

Our Contributions

We propose a new cryptographic primitive, called Quick Search using Searchable ciphertext keywords (QSCK). This helps the data owner to control and manipulate the search. Also the outsourced encrypted data can be used based on an access control policy. This also allows the legal data users to allow outsourcing of the search operations to the cloud and also to check whether the cloud has executed the search options authentically and successfully. The functionalities associated with this are (i) data can be searched over the owner's encrypted data (ii) search operations can be outsourced to the cloud, and (iii) test whether or not the cloud has executed the search operations uo to the expectaions. Here we define the security properties of QSCK and present a scheme that provably satisfies them. Modular method of construction is used in this scheme. This is implemented by using attribute-based encryption, bloom filter, digital signature, and a attribute-based keyword search (ABKS)

which is an independent value. Based on experimental evaluation it shows that the QSCK solutions are practical.

Associated works

Attribute-Based Encryption (ABE) ABE is a technique that allows entitites to decrypt a ciphertext with proper credentials that has been encrypted with proper access control policy. It is a method for enforcing access control policy through cryptographic mechanisms [1]. Based on the variation in the right of entry for control policy enforcement, there are two types: Key-policy Attribute Based Encryption where the decryption key is associated with entry control policy [2], and cipher text-policy Attribute Based Encryption where the cipher text is associated with access control policy [3]. ABE has got enormous features. Here we use ABE to construct a new technique called attribute-based keyword search (ABKS). Here keywords are encrypted based on an access control policy and data users having proper cryptographic credentials can generate tokens which can be used to search over the data which is outsourced and encrypted. This will prevent a data owner from knowing the keywords that the data user is searching for. Here the to and fro communications between the two entites invloved such as users and owners are not needed. This is in contrast to [8], where to and fro communication is needed between the two entities involved in data sharing inorder to obtain search tokens.

Searching over Encrypted Data using Keyword In this method the data owner generates tokens. These tokens can be used by the data user to search over the data owner's data that has been encrypted. There are two categories of existing solutions for keyword search over the data that is encrypted: searchable encryption with the symmetric-key setting and searchable encryption with the public-key setting. Many techniques have been proposed and researched to support complex search operations over encrypted data. Searchable encryption with the multi-users setting has been investigated [12], [27], and has concluded that distribution of certain secret keys is needed by the data owner to the data user to enforce access control policy. But all these solutions do not gaurantee to solve the problem that is under our study, because (i) some of the above solutions need communications or interaction between the two parties involved in data sharing [8] (ii) all these methods are based on the assumption that the server has faithfully and successfuly executed search operations was needed. Our solution overcomes this by alloing a person who wants to use the data with proper credentials for issuing search tokens using which the cloud can execute search operations based on keyword on behalf of the data user, without requiring any to and fro communication with the data owner. Also the data user can verify whether the cloud has executed the keyword search operations successfully and with honesty. This also holds good even for the l technique called predicate encryption, which is very powerful and which does not offer the verifiability that is desired.

Verifiable Keyword Search In [26]–[28], verifiable keyword search solutions have been proposed. Root of some polynomial is used to represent each keyword. By evaluating and calculating the result of the polynomial equation it is possible to verify and conclude whether a keyword is presen or absent. If the output is zero then it is assumed that keyword is present. These techniques and methods are suitable when keywords are sent through the text which is plain to the cloud, and are not suitable for our study as the cloud should maintian very high confidentaility regarding keywords. Secure verifiable keyword search where the key setting is symmetric cannot ne secure in the key setting which is public as the attacker can infer keywords in question through an off-line keyword guessing attack.

Problem statement

Consider a situation where a corporate has to store huge volume of file data in cloud storage. That file has to be accessed by their employees. If the files are less in number, the employees can able to browse and download. In our situation the number

of file is huge it is not possible to browse and download the file, so the employees need a file search engine. Whenever search engine come into picture, indexing technique also come. The problem here is to safeguard the file content and index keywords, index keywords are usually sensitive and which are linked with the file they are connected when a hacker get this index data he may guess the file content. Our aim is to safeguard the index keyword, file content and to implement access control system.

Access control is a big challenge, in current cloud storage for access control, attribute based encryption (ABE), identity based encryption (IDE) are used. Now in this system we are using Chipertext Index Keyword for access privilege.

The assumption in this system is each department should have one privilege key. While uploading the file into cloud storage, the data owner has to select the departments which are allowed to access the file. Our system will automatically generate the keywords using Term Frequency (TF) concept along with weight and it will undergo hashing process with accessible department keys. For example there are N keywords are generated from the document and the data owner selected M departments which are allowed to access the file. Then in chipertext index keyword it will insert N * M keywords. The idea behind this is each keyword will undergo hashing process with accessible department keys. These keys are unique and which will be created again for the users those who are belongs to accessible department only. Which is show in fig.1.

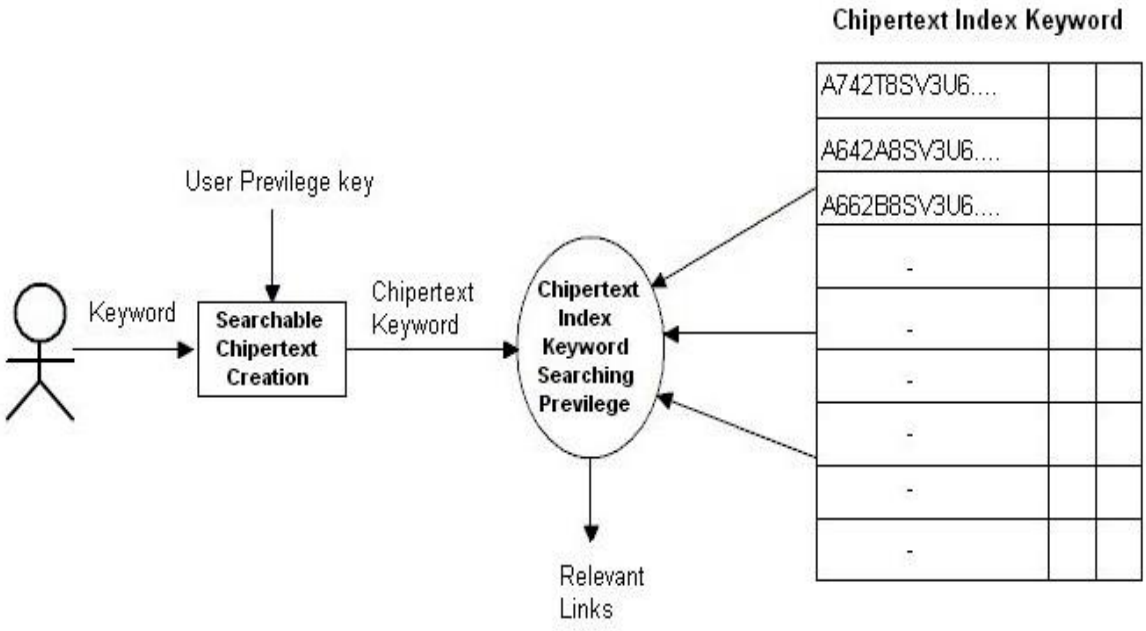

Fig.1. File Retrieval Process

In this paper, we propose the new approach of Quick Search using Searchable cipher text keywords (QSCK) as a better solution, as depicted, in Fig. 2, Here the Data Owner needs to distribute a single key called as aggregate key , instead of $\{k_i\}^m_{i=1}$ for sharing m documents with the User, and User needs to use a single aggregate key called as trapdoor, inplace of $\{Tr_i\}^m_{i=1}$ to the cloud server. The cloud server performs keyword search and returns result to the user using this aggregate trapdoor and some public information. In QSCK, the keyword search right can be

achieved by sharing the single key which is the aggregate of several keys. The major concern is that the delegation of decryption rights can be achieved using the so called key-aggregate encryption approach recently proposed in [4]. The drawback and major disadvantage is that there remains an open problem to delegate the keyword search rights along with the with the decryption rights. This is the major subject topic of this paper. To sumarize, the problem of constructing a QSCK scheme can be stated as:

"To design a Quick Search using Searchable ciphertext keywords scheme under which any subset of the keyword ciphertexts from any set of documents is searchable with a constant-size trapdoor generated by a constant-size department Privilege key."

Implementation

This system is implementing in hybrid cloud architecture there are two actors' data owner and member user. While data owner uploads the file into the cloud storage using Term Frequency (TF) techniques keywords are generated with weigthage. Data owner as to input access privilege hash tags are generated and placed in chipertext index keyword refer fig.1. The uploaded files contents are encrypted and stored in cloud storage refer fig.2. While user wants to download file he as to provide keyword for the searching process. The keyword as to converted into trapdoor based on user privilege key, the trapdoor keyword given as input to chipertext index searching process which in term refer chipertext index keyword and produce relevant links with weightage using Inverse Document Frequency (RFD) Algorithm, the links are ranked and order links are displayed to the user. If the trapdoor keyword is not present in chipertext index, then no links are produced that means the user is not having access over the files. While user clicking on the link corresponding encrypted file as to be downloaded to web server and it will be decrypted then it will produce to client system.

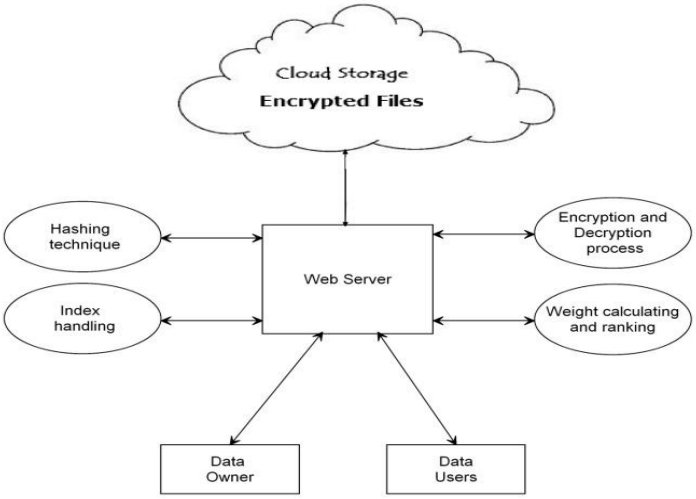

Fig.2. System Architecture

Result and security analysis

To analyze the security of our scheme, and in particular show that the scheme satisfies the security requirements we assume that the public cloud is "honest-but-curious". That is, the cloud server will only provide legitimate services according to pre-defined schemes, although it may try to recover secret information based on its knowledge. We also assume that the data can be accessed by authorized users within or out of the scopes of their privileges. Moreover, communication channels involving the public cloud are assumed to be insecure.

Conclusion

When we consider the practical problem of privacy preserving data sharing system which is based on public cloud storage, this requires that the data owner to distribute very large number of keys to users to allow them to access their documents. We propose the concept of Quick Search using Searchable ciphertext keywords (QSCK) and construct a concrete QSCK scheme in this paper. Exerimental analysis and evaluation results have proved that our work can provide an effective and timely solution in constructing practical data sharing system for public cloud storage. In this scheme, the owner needs to distribute a single key which is an aggregate of several keys instead of multiple keys to the user for sharing any number of files, and the user can

access the documents using the same single key sent by the data owner. He can use this trapdoor over all documents shared by the same ownerfor quering and retreiving data. But, the same technique cannot be applied if a data user wants to query and access over documents shared by different owners, he must generate many trapdoors and send it to the cloud. Minimizing the number of trapdoors when multiple owners are in scenario is a future work. In the recent years , federated clouds have gained a lot of attention, but QSCK cannot be applied directly in this case. QSCK can be further applied in the case of federated clouds.

References

1. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Of EUROCRYPT, pp. 457–473, 2005.
2. 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.
3. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. of IEEE S&P, pp. 321–334, 2007.
4. C. Chu, S. Chow, W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
5. X. Song, D. Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy,IEEE Press, pp. 44C55, 2000.
6. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.
7. P. Van,S. Sedghi, JM. Document. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.
8. J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in Proc. of PKC, pp. 196–214, 2009
9. D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.
10. Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.
11. J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypted data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.
12. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of, pp. 79–88, 2006.
13. C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.
14. F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.
15. J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490-502, 2012.
16. J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681-1689, Elsevier, 2010.

17. X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang."Secure Outsourced Attribute-based Signatures", IEEE Trans. on Parallel and Distributed Systems, DOI.ieeecomputersociety.org/10.1109/TPDS.2013.180, 2013.
18. J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou. "Secure Deduplication with Efficient and Reliable Convergent Key Man-agement", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014.
19. Z. Liu, Z. Wang, X. Cheng, et al. "Multi-user Searchable Encryption with Coarser-Grained Access Control in Hybrid Cloud", Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), IEEE, pp. 249-255, 2013.
20. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", Proc. IEEE INFOCOM, pp. 525-533, 2010.
21. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.
22. D. Boneh, C. Gentry, B. Waters." Collusion resistant broadcast encryption with short ciphertexts and private keys", Advances in Cryptology CCRYPTO 2005, pp. 258-275, 2005.
23. D. H. Phan, D. Pointcheval, S. F. Shahandashti, et al. "Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts", International journal of information security, 12(4): 251-265, 2013.
24. D. Boneh, B. Lynn, H. Shacham. "Short signatures from the Weil pairing", Advances in Cryptology ASIACRYPT 2001, pp. 514-532, 2001.
25. F. Bao, R. H. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings," in Proc. of ISPEC, pp. 71–85, 2008.
26. S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable delegation of computation over large datasets," in Proc. of CRYPTO, pp. 111–131,2011.
27. C. Papamanthou, E. Shi, and R. Tamassia, "Signatures of correct computation." Cryptology ePrint Archive, Report 2011/587, 2011. http: //eprint.iacr.org/.
28. D. Fiore and R. Gennaro, "Publicly verifiable delegation of large polynomials and matrix computations, with applications," in Proc. Of ACM CCS, pp. 501–512, 2012.