ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Improve Security and Search overEncrypted Cloud Data Using Blind Storage and Gateway Encryption

[1]T.C.VIDHYA,[2] POORNIMA.R,[3]K.PANIMALAR

[1] Assistant Professor,[2,3] UG Scholars, Department of Information Technology
Kings Engineering College,Chennai,India
tcvidhya88@gmail.com[1],poorni5595@gmail.com[2],malar12694@gmail.com[3]

Abstract:-

In Cloud Computing,We would like to store the outsourced data in the cloud server for the scalable storage. The outsourced data should be encrypted format. For, improving security we use gateway encryption and blind storage. Themain aim of this project is to preserve the outsourced data in cloud through gateway encryption and blind storage, and to implement multi keyword ranked search over the encrypted data in a secure way by NLP process without downloading and decrypting the entire group member file contents.Multi-keyword search directly over encrypted data is a desirable technique for effective utilization of encrypted data outsourced to the cloud.

Introduction

Research in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure). Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced.

In order to search in cloud, some requirements is needed, search over encrypted data should support the following three functions. First, the searchable encryption schemes should support multi-keyword search, and provide the same user experience as searching in Google search with different keywords; single-keyword search is far from satisfactory by only returning very limited and inaccurate search results. Second, to quickly identify most relevant results, the search user would typically prefer cloud servers to sort the returned search results in a relevance-based order ranked by the relevance of the search request to the documents.

In contrast to the theoretical benefits, most of the existingproposals, however, fail to offer sufficient insights towards the construction of full functioned searchable encryption as described above. As an effort towards the issue, in this paper, we propose an efficient multi-keyword ranked search (EMRS) scheme over encrypted mobile cloud data through blind storage. Our main contributions can be summarized as follows:

- We introduce searchable encryptionto achieve multi-keyword ranked search over the encrypted cloud data. In addition to that, we construct an efficient index to improve the search efficiency.
- By modifying the blind storage system, we solve the trapdoor unlinkability problem.
- The gateway encryption is used to provide more security in the data storage.

Related Works

Enabling keyword search directly over encrypted data is a desirable technique for effective utilization of encrypted data outsourced to the cloud.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

Existing solutions provide multi-keyword exact search that does not tolerate keyword spelling error, or single keyword fuzzy search that tolerates typos to certain extent. The current fuzzy search schemes rely on building an expanded index that covers possible keyword misspelling, which lead to significantly larger index file size and higher search complexity. In this paper, we propose a novel multi-keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. Our proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionary and effectively supports multiple keyword fuzzy search without increasing the index or search complexity. Extensive analysis and experiments on real-world data show that our proposed scheme is secure, efficient and accurate. To the best of our knowledge, this is the first work that achieves multi-keyword fuzzy search over encrypted cloud data.

Dynamic Searchable Symmetric Encryption allows a client to store a dynamic collection of encrypted documents with a server, and later quickly carry out keyword searches on these encrypted documents, while revealing minimal information to the server. In this paper we present a new dynamic SSE scheme that is simpler and more efficient than existing schemes while revealing less information to the server than prior schemes, achieving fully adaptive security against honest-but-curious servers. We implemented a prototype of our scheme and demonstrated its efficiency on datasets from prior work Christo Ananth et al. [3] proposed a system in which the complex parallelism technique is used to involve the processing of Substitution Byte, Shift Row, Mix Column and Add Round Key. Using S- Box complex parallelism, the original text is converted into cipher text. From that, we have achieved a 96% energy efficiency in Complex Parallelism Encryption technique and recovering the delay 232 ns. The complex parallelism that merge with parallel mix column and the one task one processor techniques are used. In future, Complex Parallelism single loop technique is used for recovering the original message. This is a primitive with several applications other than SSE, and is of independent interest.

Cloud computing as an emerging technology trend is expected to reshape the advances in information technology. In this paper, we address two fundamental issues in a cloud environment: privacy and efficiency. We first review a private keyword-based file retrieval scheme proposed by Ostrovsky et. al. Then, based on an aggregation and distribution layer (ADL), we present a scheme, termed efficient information retrieval for ranked query (EIRQ), to further reduce querying costs incurred in the cloud. Queries are classified into multiple ranks, where a higher ranked query can retrieve a higher percentage of matched files. Extensive evaluations have been conducted on an analytical model to examine the effectiveness of our scheme.

Existing System

In existing system encryption of the documents are done in cloud server. All the files uploaded by the user are encrypted in cloud and stored in static memory locations. Hence Multi keyword search is not possible on the encrypted cloud data. In order to make a search, the existing system downloads all the encrypted files and then decrypt for content based searching which is the traditional way to search. In searchable symmetric encryption (SSE) schemes, large number of documents, search results should be retrieved in an order of the relevancy with the searched keywords using TF-IDF method.

Drawbacks

- Outsourced encrypted Data are directly stored in cloud, which may lead to severe confidentiality and privacy issues.
- Searchable encryption schemes fail to offer sufficient insights towards the construction of full functioned search over encrypted cloud data.
- Server side encryption which is in secure.
- Bulk content retrieval for file searching, which is inefficient.
- Group sharing with access control on encrypted data is not well studied yet.

Proposed System

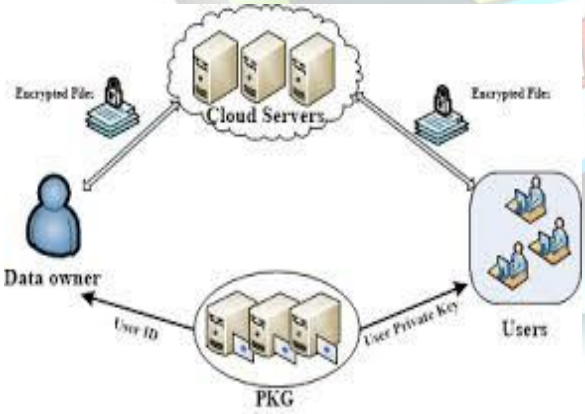
In Proposed system, we introduced an efficient and reliable methodology for search over encrypted data which is splited in to multiple blocks and then stored in blind storage. Here the encrypted multi keyword search pre computes the resulting search documents for the input query from users through Natural language processing Technique which is implemented on gateway (client side) on user file upload. Hence the matching

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

documents which is pre compute the before searching the encrypted cloud contents are retrieved from cloud. Here we does not pull all the encrypted data's from cloud for searching, which is time consuming and ineffective. The matching documents memory locations on blind storage are retrieved from the serializable objects which is stored in the gateway. User can download the resulting documents after getting the keys from the group owner. Asymmetric kind of encryption for key re-encryption and is more secured.

Multiple groups can be created. Each group is having owner and users. User can upload the files in public and private mode. If user uploads files in public mode, the file is to encoded using Base64 algorithm. If user uploads in private mode the file content is encrypted using RSA algorithm and then can give access control for each group user. User search in cloud using keywords, cloud can send the related files to respective user. If data user wants to read the contents of files, data user should request to cloud and then cloud will request to data owner. Data owner checks the user attributes and access control, then the owner forward the private key and data's in secure manner.

Architecture



The data owner register the environment. Data user send request to the data owner. Data owner upload the file in private and public mode. In private mode the base64 algorithm is used to encoded but in private mode RSA algorithm is used to encoded the uploaded file. The file also create the index file using the NLP processes and WordNet tool. The NLP techniques is to identify the related meaning of the keyword in the uploaded file. WordNet is used to serializable the data. Data user search the file using multi-keyword ranked search. The data owner send the his private in encrypted format to data user if the user is a authorized person. Using this private key he decrypt the file content.

Group creation

Data owner should be register in this environment and create a group. Data users also register and give request to group owner to add a group user. Data owner accept the request from the user. Multiple groups can be created. Each group is having owner and users. Data user only can access the respective data owner documents. Data user cannot access the webpage until the data owner accepts the request.

Text mining process

In this module the data owner can upload the document. Data owner can upload the files, the content of file is to be extracted using NLP technique and that words can get synonyms using Word Net tool. In first step of text mining process POS tagger is implemented to extract the keywords in files.NLP process is used to extract the literal meaning of keywords previously extracted. The Words are analyzed in Word Net API so that the related terms can be found for use in the index file. This index file will be generated for each upload from group owner and saved as a serializable object in cloud. All the communication to cloud server will be done through web service.

Blind Storage

The uploaded data's are encrypted in gateway after Natural language Processing is done and stored as index file. The owner can give access control and privileges to user while uploading the data. Access control refers to whether the user has permission to access the file or not. The privilege refers to how much extend that the user has rights over the data (read and write). The file will be splited into blocks and its encrypted using RSA encrypting algorithm and the encrypted blocks will be uploaded to the cloud service and stored in blind storage. Blind storage all documents are divided into fixed size blocks. These blocks are indexed by sequence of random integers. Files content are stored in block randomly so the cloud can view

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

encrypted content only. Encryption key only knows to data owner.

Query search

Data user will try to search a query in cloud server. The cloud servers map the keywords and search the related files. The cloud server gives the related filename to user. To view the content the user should click the filename; at that time user request to cloud server and server send the user details and filename to the data owner. Then data owner knows all public key of user so he encrypt the private key using data user public key and the encrypted key send to server and server send that key details to user, then user decrypt the key using our private key. After that the data user can get private key of data owner and then access the data through blind storage.

Implementation

In this paper we implement the gateway encryption and blind storage. The above two concept is used to reduce the unauthorized access in the data storage. The gateway encryption is used to check the access pattern of the each data access. The blind storage is used to verify the access control of the each authorized user. Here, we also implement multi-keyword ranked search.Which is used to conduct search based on the keywords of the query.

Conclusion

Hence we developed an efficient search in multi keyword through blind storage which enable accurate, efficient and secure search over encrypted data. Privacy is preserved for data in cloud while storing in blind Storage, and also achieved access control for each user.

References

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with PrivacyGrid," in Proc. 17th Int. Conf. World Wide Web, 2008, pp.

[2] M.Armbrust,A.Fox,R.Griffith,A.Joseph,R.Katz,A.Konwinski,G.Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A Berkeley View of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, Tech. Rep. UCB/EECS-2009-28, 2009.

[3] Christo Ananth, H.Anusuya Baby, "Encryption and Decryption in Complex Parallelism", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795

[4] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Cooperative private searching in clouds," http ://www.cis.temple.edu/ cctan/TR1.pdf, Tech. Rep., 2011.9.

[5] Hassan Abid, LuongThi Thu Phuong, Jin Wang,Sungyoung Lee, SaadQaisar Kyung Hee University, Computer Engineering Department, Korea. October 29,2011.

[6] C. E. L. Thomas, H. Cormen, R. L. Rivest, and C. Stein, Introduction to Algorithms, 3rd ed. Cambridge, MA: MIT Press, 2009.

[7] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," NIST special publication, pp. 800–144, 2011.

[8] W. Wong, D. Cheung, B. Kao, and N. Mamoulis, "Secure knn computa- tion on encrypted databases," in Proc. of ACM SIGMOD, 2009.

[9] Hussain, J. Son, H. Eun, S. Kimand H. "Rethinking Vehicular Communications: MergingVANET with Cloud Computing", Oh Department of Computer Science and Engineering, Hanyang University ERICA Campus, South Korea.2012 IEEE 4th International Conference on Cloud Computing Technology and Science.

[10] E. Cuervo, A. Balasubramanian, D.-K. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl, "MAUI: Making smartphones last longer with code offload," in Proc. ACM MobiSys, 2010, pp. 49–62.

[11] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in CRYPTO, 2013.

[12] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," Advances in Cryptology-EUROCRYPT, 2009.

[13] B. Aslam, P. Wang, and C. Zou, "An economical, deployable and secure vehicular ad hoc network," in Proc. Military Communication Conf., San Diego, CA, Nov. 2008, pp. 1–7.

[14] K. Mershad, H. Artail, and M. Gerla, "We can deliver messages to far vehicles," IEEE Trans Intell. Transp. Syst., vol. 13, no. 3, pp. 1099–1115,Sept. 2012.R.

[15] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proc. 1st Workshop Virtualization Mobile Comput., 2008, pp. 31–35. [14] .

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

[16] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Cooperative private searching in clouds," http : //www.cis.temple.edu/cctan/TR1.pdf, Tech. Rep., 2011.9.

[17] MdWhaiduzzaman, Mehdi Sookhak, Abdullah Gani, RajkumarBuyya, Journal of Network and Computer Applications "A survey on vehicular cloud computing". Received 27 February 2013 Received in revised form 6 June 2013 Accepted 20 August 2013.

[18] X. H. Li, H. Zhang, and Y. F. Zhang, "Deploying mobile computation in cloud service," in Proc. 1st Int. Conf. CloudCom, 2009, pp. 301–311.

[19] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in Financial Cryptography and Data Security, FC (2013), 2013.

[20] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable sym- metric encryption: improved definitions and efficientconstructions," in Proc. of ACM CCS, 2006.