ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey on Privacy-Preserving Multi Keyword Ranked Search Over Encrypted Cloud Data Using Hybrid Encryption

Priyanka D. Deshmukh, Prof. Prashant Jawalkar

M.E Student, Department of Computer Engineering, JSPM's B.S.I.O.T.R, Wagholi, Pune university, India.

Asst. Professor, Department of Computer Engineering, JSPM's B.S.I.O.T.R, Wagholi, Pune university, India.

ABSTRACT: In cloud computing, private data can store in the server and allow for accessing the public users in the cloud server. Outsourced data contain secure message data must be encrypted before uploaded in the cloud. When the encrypted data must be search very difficult manner. We are used to develop the fine grained multi keyword search schemes using encrypted cloud data. This concept is having the three fold. First, introduced in related to one word of one meaning and get the important factors on keywords and enable to search keywords and personalized user experience. Second, develop a very efficient to search the multi keyword. Third, classified sub dictionaries to achieve more efficiency on content table, data can send do not block the other data. We analyze the much more secure proposed schemes in this document to reliability privacy protection of content table and unlinkability of trapdoor. In this base paper used Symmetric and Secret Keys for encryption. Symmetric encryptions are significantly faster than asymmetric encryptions, but require all parties to somehow share a secret key. The asymmetric algorithms allow public key infrastructures and key exchange systems, but at the cost of speed. To tackles the problem, we used hybrid encryption. Hybrid encryption is a mode of encryption that merges two or more encryption systems. It includes a combination of asymmetric and symmetric encryption to take advantage from the strengths of each form of encryption. These strengths are respectively defined as speed and security. In this scheme, it achieves the security level and the better performance in functionality and query complexity.

KEYWORDS: Cloud computing, searchable encryption, multi keyword, fine-grained, hybrid encryption.

I. INTRODUCTION

In Cloud computing, the cloud users can remotely store data into the cloud so as to enjoy the quality applications and services from computing resources. Its having the great flexibility and money savings for both individuals and organizations to outsource their local complex data management system into the cloud. To protect data privacy and deal with unwanted accesses in the cloud and beyond, sensitive data. The outsourced data may have sensitive privacy information. It is necessary to encrypt the private data before transmitting to the cloud servers. The data encryption. Simply encrypting the data may cause other security issues. The solution for this issue is searchable encryption. In searchable encryption owner needs to generate several keywords, and then these keywords are then encrypted and stored at the cloud server.

When a search user want to access the outsourced data, it can select some relevant keywords and send the ciphertext to the cloud server. The cloud server uses the ciphertext to match the encrypted keywords, and returns the matching results to the search user. Later, for achieving the efficient search query Sun et al. propose a multi-keyword text search scheme which uses the relevance scores of keywords and utilizes a multidimensional tree technique. Yu et al. propose a multi-keyword top-k retrieval scheme to encrypt the index and guarantees high security. Li et al. uses the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

relevance score and k-nearest neighbor techniques to develop an efficient multi-keyword search scheme that return the ranked search results based on the precision.

Query with user preferences is popular in the plaintext search, it allows personalized search and represent user's requirements, but not supported in the encrypted data. To improve the user's experience on searching, an important function is the multi-keyword search with the comprehensive logic operations, i.e., the "AND", "OR" and "NO" operations. This is reduce the searching space and quickly identify the desired data. The "OR" operation is for searchable encryption scheme, "AND" operation with the returned documents matching all keywords. most existing proposals can allow search with single logic operation, rather than the mixture of multiple logic operations on keywords,In this work these issues addressed by developing two FMS schemes over encrypted cloud data.

In this paper we introduce relevance scores and the preference factors of keywords for searchable encryption. From this relevance score can give more accurate result and the preference factor represent the importance of keywords in the search keyword. Thus it improves the search functionality as well as user experience. The "AND", "OR" and "NO" operations in the multi-keyword search for searchable encryption. The proposed scheme can achieve more comprehensive functionality and lower query complexity. The use of sub-dictionaries technique to enhance the efficiency. It can achieve better efficiency in terms of index building, trapdoor generating and query.

II. LITERATURE REVIEW

A.).Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data

In cloud computing, data owners outsource their complex data. For protecting data privacy, sensitive data has to be encrypted before outsourcing. Enabling an encrypted cloud data search service is major importance. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely differentiate the search results. In this paper, define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization.

B) Efficient multi-keyword ranked query over encrypted data in cloud computing

To avoid information leakage, sensitive data have to be encrypted before uploading onto the cloud servers. In the current multi-keyword ranked search approach, the keyword dictionary is static and cannot be extended easily when the number of keywords increases. In this paper, author propose a flexible multi-keyword query scheme, called MKQE to address the aforementioned drawbacks. MKQE greatly reduces the maintenance overhead during the keyword dictionary expansion. Therefore, the documents that have higher access frequencies and access history get higher rankings in the matching result set.

C) Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage

In this paper, author gives the searchable encryption for multi-keyword ranked search over the storage data. By considering the large number of outsourced documents (data) in the cloud, the use of relevance score and k-nearest neighbour techniques to develop an efficient multi-keyword search scheme that can return the ranked search results based on the accuracy. Due to this improve the search efficiency.

D) Secure Ranked Keyword Search over Encrypted Cloud Data

In this paper, for the first time author define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly improves system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, author proposes order-preserving symmetric encryption (OPSE).

III.ARCHITECTURAL DESIGN

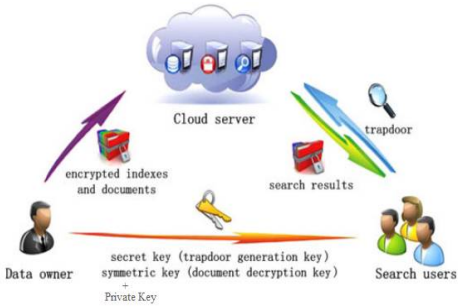

Fig: Architectural diagram

IV.PROPOSED SYSTEM

- In this work, we address by developing Fine-grained Multi-keyword Search (FMS) schemes over encrypted cloud data.
- To tackle the existing problem, we proposed hybrid encryption for security.
- In this system, we introduce the relevance scores and the preference factors of keywords for searchable encryption. The relevance scores of keywords can enable more precise returned results, and the preference factors of keywords represent the importance of keywords in the search keyword set specified by search users and correspondingly enables personalized search to cater to specific user preferences. It thus further improves the search functionalities and user experience.
- In this system, we realize the “AND”, “OR” and “NO” operations in the multi-keyword search for searchable encryption. Compared with schemes, the proposed scheme can achieve more comprehensive functionality and lower query complexity.
- In this system, we employ the classified sub-dictionaries technique to enhance the efficiency.

V.ALGORITHMS

Data Owner:
Step 1) Register
Step 2) Login
Step 3) Symmetric Key, Secret Key, Public and Private Key Generation
Step 4) Enter Document name and contents of Document
Step 5) Enter Some Keywords about Document
Step 6) Encrypt Document based on Symmetric Key (AES Encryption) --> Ciphertext
Encrypt that Ciphertext once again based on Public Key (RSA Encryption) --> Ciphertext1
Step 7) Encrypt Keywords based on Secret Key --> index
Encrypt that index once again based on Data Owner Identity (Identity Based Encryption) --> Encrypted Index
Step 8) Upload Ciphertext1 with Encrypted Index to Cloud Server
Step 9) Send Symmetric, Secret and Private Keys to Authenticated Search Users

Search User:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Step 1) Register
Step 2) Login
Step 3) Choose Data Owner then send Key Request
Step 4) Get Symmetric, Secret and Private Keys from Data Owner
Step 5) Enter Search Keywords
Step 6) Encrypt Search Keywords based on Secret Key --> trapdoor
Encrypt that trapdoor once again based on Data Owner Identity (Identity Based Encryption) --> Encrypted trapdoor
Step 7) Send Encrypted trapdoor with any one Operation (AND, OR, NO) to Cloud Server then Receive the matched encrypted document collections from cloud server.
Step 8) Encrypted Documents (Ciphertext1) --> Decrypt that Ciphertext1 based on Private Key (RSA Decryption) --> Ciphertext Ciphertext --> Decrypt that Ciphertext based on Symmetric Key (AES Decryption) – Document

VI.CONCLUSION

In this thesis, we have investigated on the fine-grained multi-keyword search (FMS) issue over encrypted cloud data, and proposed two FMS schemes. The FMS_I includes both the relevance scores and the preference factors of keywords to enhance more specific search as well as better users' experience. The FMS_II achieves secure and efficient search with practical functionality, i.e., "AND", "OR" and "NO" operations of keywords. We proposed the enhanced schemes supporting classified sub-dictionaries (FMSCS) to improve efficiency. Furthermore our proposed hybrid encryption schemes, the result is the added security of the transmittal process along with overall improved system performance.

REFERENCES

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.
[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. S&P, IEEE, 2000, pp. 44–55.
[3] R. Li, Z. Xu, W. Kang, K. C. Yow, and C.-Z. Xu, "Efficient multikeyword ranked query over encrypted data in cloud computing," Future Generation Comput. Syst., vol. 30, pp. 179–190, 2014.
[4] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, "Enabling efficient multi-keyword ranked search over encrypted cloud data through blind storage," IEEE Trans. Emerging Topics Comput., 2014, DOI:10.1109/TETC.2014.2371239.
[5] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., 2010, pp. 253–262.
[6] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multikeyword top-k retrieval over encrypted cloud data," IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp. 239–250, Jun. 2013.
[7] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in Proc. SIGMOD International Conference on Management of data.. ACM, 2009, pp. 139–152.
[8] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.
[9] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of cryptography, Springer, 2007, pp. 535–554.
[10] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology—Eurocrypt. Springer, 2004, pp. 506–522.

BIOGRAPHY

Priyanka D. Deshmukh is a M.E student in the computer engineering Department, College of JSPM"s B.S.I.O.T.R, Wagholi, Pune University, Maharashtra, India. She received bachelor of Computer science and engineering (B.E) degree in 2013, from D.K.T.E. Ichalkaranji, India. Her research interests in cloud computing.