International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

A Security on Multi Keyword Search over Outsourced Cloud Data Using N-Gram

Sunitha Pachala[1], Pagadala Kala Harsha[2], Kodali Meghana[3]

[1]Assistant Professor, Department of Computer Science and Engineering, PhD Scholar, (JNTUK),Dhanekula Institute of Engineering and Technology, A.P., India.
[2]B.Tech (CSE), Dhanekula Institute of Engineering and Technology, A.P., India.
[3]B.Tech (CSE), Dhanekula Institute of Engineering and Technology, A.P., India.

Abstract *— In recent years, Cloud computing is gaining much momentum in the IT industry which can be used to organize various resources of computing, storage and applications. Many IT enterprises and individuals are outsourcing their databases to cloud server. Variety of users can access and share information stored in the cloud independent of locations. The outsourced data may contain very sensitive information such as e-mails, company financial data, government documents, Personal Health Care records, facebook photos and business documents.We define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics with N- gram Features.*

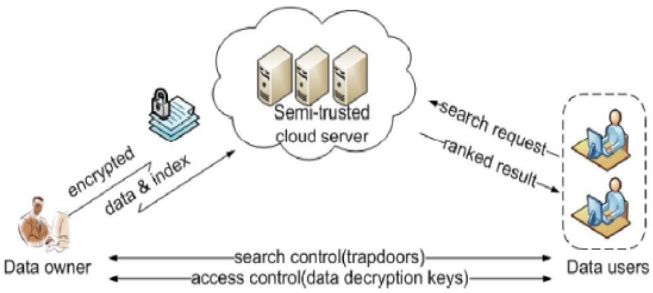
Keywords — *keyword search, ranked search, encryption, Cloud computing.*

1. INTRODUCTION

In cloud computing, data owners share their outsourced data with a number of authorized users. Keyword based retrieval allows users to retrieve files they are interested in. Keyword-based retrieval is widely used in plaintext search schemes, in which user can retrieve relevant files based on the keyword in the search request. However, it is a difficult task in ciphertext scenario due to limited operations on encrypted data. The existing searchable encryption techniques allows performing searches securely and effectively but is not suitable in cloud computing scenario as they support only exact

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

keyword search and does not support minor typos and format inconsistencies are not supported. Sometimes users searching input might not exactly match those pre set keywords due to the possible typos, representation inconsistencies and lack of exact knowledge about the data. Simple spell check mechanisms are used to support fuzzy keyword search. However, this approach will not completely solve the problem and sometimes can be ineffective as it requires additional interaction of user to determine the correct word from the candidates generated by the spell check algorithm, which costs extra computation effort for the users. If a user types some other valid keywords by mistake the spell check algorithm will not work because it cannot differentiate between two actual valid words. Due to these new techniques that has searching flexibility which support both minor typos and format inconsistencies is required. In this paper, we use edit distance to evaluate keywords similarity for the construction of fuzzy keyword sets and a search scheme based on this set.



2. PROPOSED SYSTEM

Existing System

The large number of data users and documents in cloud, it is crucial for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. The searchable encryption focuses on single keyword search or Boolean keyword search, and rarely differentiates the search results.

Limitations of Existing System

- Single-keyword search without ranking
- Boolean- keyword search without ranking
- Single-keyword search with ranking

Proposed System

We 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 system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching".

Advantages of Proposed System

- Multi-keyword ranked search over encrypted cloud data (MRSE)

- "Coordinate matching" by inner product similarity.

3.LITERATURE SURVEY

1] Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud:

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

[2] Secure Ranked Multi-keyword Search for Multiple Data Owners in Cloud Computing: With the advent of cloud computing, it becomes increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve these data. For privacy concerns, secure searches over encrypted cloud data motivated several researches under the single owner model. However, most cloud servers in practice do not just serve one owner, instead, they support multiple owners to share the benefits brought by cloud servers. In this paper, we propose schemes to deal with secure ranked multi-keyword search in a multiowner model. To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family.

ALGORITHM FOR ENCRYPTION AND DECRYPTION

I. Elliptic Curve Cryptography Algorithm: 1. Select the file type then select plain text from the

file 2. After selecting file select the output file 3. After selecting output file check if file compress or not 4. If the file compress then check the plain text is converted to cypertext or not(encrypted file) 5. If text in file are hidden or converted to cypertext then encryption is successful. 6. For retrieving encrypted, hidden, compressed message select the output file for retrieving output file enter key or password. Key generation: (q, FR, a, b, G, n, h). 1. Select a random number d, d ∈ [1, n – 1] 2. parameters Compare Q = dG. 3. public key is Q and private key is d. A public key Q = (xq, yq) associated with the domain parameters (q, FR, a, b, G, n, h) is validated using the following procedure 1. Check that Q ≠ O 2. Check that xq and yq are properly represented elements of Fq 3. Check if Q lies on the elliptic curve defined by a and b. 4. Check that nQ = O II. **N-Gram Algorithm:** We are using N-GRAM Algorithm for fuzzy searching keywords presents in file. It is actually perform on keyword search using scanning of all character in file on gram level. we are separate each character on 1ST level then compare each character with our keyword .this procedure is repeat until we are reaching n-level .

CONCLUSION

In this paper, In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files.

REFERENCES

Good Teachers are worth more than thousand books, we have them in Our Department.

[1] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", SIAM J. Comput., vol. 32, no. 3, pp. 586-615, 2003.

[2] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, et al., "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking", Proc. IEEE 8th ACM SIGSAC Symp. Inf. Comput. Commun. Security, pp. 71-81, May 2013. [3] J. Hur, "Improving security and efficiency in attribute-based data sharing", IEEE

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271-2282, Oct. 2013.

[4] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, "Order preserving encryption for numeric data", Proc. ACM SIGMOD Int. Conf. Manage. Data, pp. 563-574, Jun. 2004.

[5] A. Boldyreva, N. Chenette and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions", Proc. 31st Annu. Conf. Adv. Cryptol., pp. 578-595, Aug. 2011.

[6] Y. Yi, R. Li, F. Chen, A. X. Liu and Y. Lin, "A digital watermarking approach to secure and precise range query processing in sensor networks", Proc. IEEE INFOCOM, pp. 1950-1958, Apr. 2013.

[7] R. A. Popa, F. H. Li and N. Zeldovich, "An ideal-security protocol for order-preserving encoding", Proc. IEEE Symp. Security Privacy, pp. 463-477, 2013.

[8] F. Kerschbaum and A. Schroepfer, "Optimal average-complexity ideal-security order-preserving encryption", Proc. ACM SIGSAC Conf. Comput. Commun. Security, pp. 275-286, 2014.

[9]. R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, ―Searchable Symmetric Encryption: Improved Definitions and Efficient Con-structions,‖ Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.

[10]. D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, ―Public Key Encryption with Keyword Search,‖ Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2004.