International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Empowering Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data

[1] Mr. B.SHIVA KUMAR, [2] Mrs.N.SUJATHA

[1] Pursuing M.Tech(CSE)from Jagruti Institute of Engineering and Technology
[2] Associate Professor, Department of Computer Science and Engineering,
Jagruti Institute of Engineering and Technology, Telangana State, India.

Abstract

Fine-grained multi-keyword search schemes over encrypted cloud data. Our innovative donations are three-fold. First, we start the application scores and inclination variables upon catchphrases which encourage the specific watchword look and adjusted client nature. we helper take up the private sub-dictionaries technique to achieve better viability on list structure, trapdoor producing and address. Ultimately, we assess the asylum of the anticipated plans in stipulations of prudence of accreditations, security stronghold of sign and trapdoor, and unlink ability of trapdoor. Through general tests utilizing this present reality dataset, we affirm the show of the anticipated plans. Both the supervision examination and provisional results express that the anticipated plans can finish the same security level contrasting with the exhibited ones and better routine as far as usefulness, query complication and skill.

Keywords: *Searchable encryption, Multi-keyword, Fine-grained, Cloud computing.*

1. INTRODUCTION

Transmitting the information to the cloud servers. The data encryption, though, would considerably lower the usability of data outstanding to the complexity of penetrating over the encrypted data purely encrypting the statistics may still basis other sanctuary concerns. For example, Google Search uses SSL (Secure Sockets Layer) to encrypt the association among search user and Google server when confidential data, such as credentials and emails, appear in the search results. Nevertheless, if the explore user clicks into a different website as of the search consequences page, that website may be talented to categorize the explore terms that the user has worn. Firstly, the statistics owner needs to produce numerous keywords according to the outsourced data. These keywords are then encrypted and stored at the cloud server. When a explore user requirements to admission the outsourced data, it can select some appropriate keywords and send the nothing text of the preferred keywords to the cloud server. The cloud server then uses the cipher text to match the outsourced encrypted keywords, and lastly returns the matching results to the search user.

To achieve the similar search efficiency and precision over encrypted data as that of plaintext keyword search, an extensive body of research has been developed in literature. Propose a multi-keyword text search scheme which considers the relevance scores of keywords and utilizes a multidimensional tree technique to achieve efficient search query. Yu et al. propose a multi-keyword top-k retrieval scheme which uses fully homomorphism encryption to encrypt the index/trapdoor and guarantees high security. Cao et al. propose a multi-keyword ranked search (MRSE), which applies coordinate machine as the keyword matching rule, i.e., return data with the most matching keywords. Although many search functionalities have been developed in previous literature towards precise and efficient searchable encryption, it is still difficult for searchable encryption to achieve the same user experience as that of the plaintext search, like Google search. 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.

2. SYSTEMMODEL, THREAT MODEL AND SECURITY REQUIREMENTS

System Model

We consider a system consists of three entities.

Data owner: The data owner outsources her data to the cloud for convenient and reliable data access to the corresponding search users. To protect the data privacy, the data owner encrypts the original data through symmetric encryption. To improve the search efficiency, the data owner generates some keywords for each outsourced document. The corresponding index is then created according to the keywords and a secret key. After that, the data owner sends the encrypted documents and the corresponding indexes to the cloud, and sends the symmetric key and secret key to search users.

Cloud server: The cloud server is an intermediate entity which stores the encrypted documents and corresponding indexes that are received from the data owner, and provides data access and search services to search users. When a search user sends a keyword trapdoor to the cloud server, it would return a collection of matching documents based on certain operations.

Search user: A search user queries the outsourced documents from the cloud server with following three steps. First, the search user receives both the secret key and symmetric key from the data owner. Second, according to the search keywords, the search user uses the secret key to generate trapdoor and sends it to the cloud server. Last, she receives the matching document collection from the cloud server and decrypts them with the symmetric key.

Threat Model and Security Requirements

In our threat model, the cloud server is assumed to be “honest but- curious”, which is the same as most related works on secure cloud data search. Specifically, the cloud server honestly follows the designated protocol specification. However, the cloud server could be “curious” to infer and analyze data (including index) in its storage and message flows received during the protocol so as to learn additional information.

3. SYSTEM ARCHITECTURE

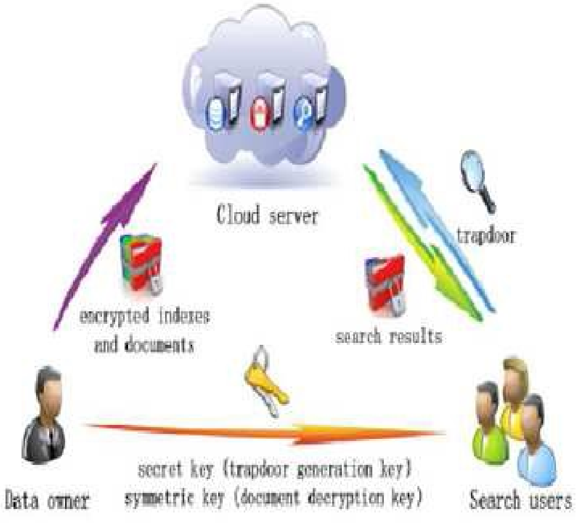
Cloud server
trapdoor
encrypted indexes and documents
search results
Data owner
secret key (trapdoor generation key)
symmetric key (document decryption key)
Search users

Fig: System Model

3.1.SYSTEM ANALYSIS

EXISTING SYSTEM:

Using cloud computing, individuals can store their data on remote servers and allow data access to public users through the cloud servers. As the outsourced data are likely to contain sensitive privacy information, they are typically encrypted before uploaded to the cloud. This,
however, significantly limits the usability of outsourced data due to the difficulty of searching
over the encrypted data performance in terms of functionality, query complexity and efficiency.
However, most existing proposals can only enable search with single logic operation, rather than the mixture of multiple logic operations on keywords, which motivates our work.

PROPOSED SYSTEM:

In this paper, we manage this issue by expanding the fine-grained multi keyword seek plans over scrambled cloud information. Our inventive gifts are three-fold. To start with, we begin the significance scores and inclination components upon catchphrases which encourage the characterized keyword seek and adjusted client recognition. Second, we build a self evident certainty and exceptionally proficient multi-watchword look plan. The anticipated technique can support troublesome rationale explore the blended "AND", "OR" and "NO" operations of keywords.

Third, we extra use the confidential sub dictionaries practice to perform better capability on aide development, trapdoor creating and question. Finally, we research the sanctuary of the longed for plans in stipulations of tact of certifications, security insurance of record and trapdoor, what's more, unlink ability of trapdoor. Both the guard examination and speculative results show that the anticipated plans can understand the same barrier level contrasting with the realistic ones and better presentation in stipulations of usefulness, question multifaceted nature and productivity.

Proposed system algorithms:

The data owner firstly uses symmetric encryption calculation. The security of this encryption calculation has been demonstrated in the known figure content model. Subsequently, the substance of list and trapdoor can't be recognized. In this way, security insurance of record and trapdoor can be accomplished. In spite of the different points of interest of cloud administrations, outsourcing delicate data such as emails, personal health records, company finance data, government documents, etc.

4.RELATED WORK

This is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system. There are mainly two types of searchable encryption in literature, Searchable Public-key Encryption (SPE) and Searchable Symmetric Encryption (SSE).

SPE (Searchable Public-key Encryption)

SPE is first proposed by Boneh et al which supports single keyword search on encrypted data but the computation overhead is heavy. In the framework of SPE, Boneh et al. propose conjunctive, subset, and range queries on encrypted data. Hwang et al. propose a conjunctive keyword scheme which supports multi-keyword search. Zhang et al. propose an efficient public key encryption with conjunctive subset keywords search. However, these conjunctive keywords schemes can only return the results which match all the keywords simultaneously, and cannot rank the returned results. Qin et al. propose a ranked query scheme which uses a mask matrix to achieve cost-effectiveness. Yu et al. propose a multi-keyword top-k retrieval scheme with fully homomorphism encryption, which can return ranked results and achieve high security. In general, although SPE allows more expressive queries than SSE, it is less efficient, and therefore we adopt SPE in the work.

SSE (Searchable Symmetric Encryption)

The concept of SSE is first developed by Song et al. Wang et al. develop the ranked keyword search scheme, which considers the relevance score of a keyword. However, the above schemes cannot efficiently support multi-keyword search which is widely used to provide the better experience to the search user. Later, Sun et al. propose a multi keyword search scheme which considers the relevance scores of keywords, and it can achieve efficient query by utilizing the multidimensional tree technique. A widely adopted multi keyword search approach is multi-keyword ranked search (MRSE). This approach can return the ranked results of searching according to the number of matching keywords. Within this framework, they leverage an efficient index to further improve the search efficiency, and adopt the blind storage system to conceal access pattern of the search user. Li et al. also propose an authorized and ranked multi keyword search scheme (ARMS) over encrypted cloud data by leveraging the cipher text policy attribute-based encryption (CP-ABE) and SSE techniques. Security analysis demonstrates that the proposed ARMS scheme can achieve collusion resistance. In this paper, we propose FMS(CS) schemes which not only support multi-keyword search over encrypted data, but also achieve the fine grained keyword search with the function to investigate the relevance scores and the preference factors of keywords and, more importantly, the logical rule of keywords. In addition, with the classified sub-dictionaries, our proposal is efficient in terms of index building, trapdoor generating and query.

5.CONCLUSION

We have analyzed on the fine-grained multi keyword look (FMS) subject over encoded cloud information, and future two FMS plans. The FMS I incorporate both the criticalness scores and the prejudice elements of catchphrases to increase more precise hunt and upgraded clients' experience, in a specific order. The FMS II acknowledge secure and skillful inquiry with practical usefulness, i.e., "AND", "OR" and "NO" operations of catchphrases. Moreover, we have arranged the better plans behind classified sub-word references (FMSCS) to propel fitness. For the future work, we propose to add extend the application to think about the extensibility of the record set and the multi-client cloud situations. Towards this pattern, we have made some starting results on the extensibility and the multiuser cloud situations. Another striking subject is to expand the extraordinarily adaptable searchable encryption to empower capable investigate on extensive reasonable databases.

REFERENCE

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An smdpbased service model for interdomain resource allocation in mobile cloud networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 5, pp. 2222–2232, 2012.
[2] M. M. Mahmoud and X. Shen, "A cloudbased scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEETransactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1805–1818, 2012.
[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geo distributed clouds for e-health monitoring system with minimum service delay and privacy preservation," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 2, pp. 430–439, 2014.
[4] T. Jung, X. Mao, X. Li, S.-J. Tang, W. Gong, and L. Zhang, "Privacy preserving data aggregation without secure channel: multivariate polynomial evaluation," in *Proceedings of INFOCOM*. IEEE, 2013, pp.2634–2642.
[5] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, "Secure dynamic searchable symmetric encryption with constant document update cost," in *Proceedings of GLOBCOM*. IEEE, 2014, to appear.
[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222– 233, 2014.
[7] https://support.google.com/websearch/answer/173733?hl=en. [8] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of S&P*. IEEE, 2000, pp. 44–55.
[9] R. Li, Z. Xu, W. Kang, K. C. Yow, and C.- Z. Xu, "Efficient multi keyword ranked query over encrypted data in cloud computing," *Future Generation Computer Systems*, vol. 30, pp. 179–190, 2014.
[10]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 Transactions on Emerging Topics in Computing*, 2014, DOI10.1109/TETC.2014.2371239.
[11]C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proceedings of ICDCS*. IEEE, 2010, pp. 253–262. [12]A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," in *Advances in Cryptology- EUROCRYPT*.Springer, 2009, pp. 224–241.
[13]W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacypreserving multi-keyword text search in the cloud supporting similarity-based ranking," *IEEE Transactions on Parallel and Distributed Systems*, vol. DOI: 10.1109/TPDS.2013.282, 2013.
[14] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multikeyword top-k retrieval over encrypted cloud data," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239–250, 2013.
[15]A. Arvanitis and G. Koutrika, "Towards preference-aware relational databases," in *International Conference on Data Engineering (ICDE)*. IEEE, 2012, pp. 426– 437.

ABOUT THE AUTHORS

Mr. B.SHIVA KUMAR is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mrs.N.SUJATHA is presently working as Associate Professor in, Department of computer science and engineering, Telangana State,India.She has published several research papers in both International and National conferences and Journals.