International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 10
September 2017

An Effective Secure Rating Mechanism for Filtering Process

Y Venkata Ramana Reddy & Dr P Pedda Sadhu Naik
[#] M. Tech CSE, [*] Professor & HOD, Dept. of CSE
Dr. Samuel George Institute of Engineering & Technology, Markapuram, A.P., India

Abstract

The advent of distributed systems uses data owners is motivated to outsource their complex data management systems from local sites to commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data is encrypted before outsourcing which obsoletes traditional data utilization based on plaintext keyword search. We propose the problem of Secured Multi key word Search (SMS) over encrypted cloud data (ECD) and construct a group of privacy policies for such a secure cloud data utilization system. From number of multi-keyword semantics another more imperative component of this framework is data duplication checking with strategy. To store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy problems. Encryption and decryption is overhead for mobile devices because it is very small and have low computation power. Proposed schemes to introduce low overhead on computation and communication and multi-keyword search based on ranking using selection algorithm in clustering method. The Ranked result provides top k retrieval results. Also we propose new system is generate alerts when un-authorized user tries to access the data from cloud the alert will generate in the form of mail and message.

Index Terms: *Encryption, Inner product similarity, Multi key word search, ranking, security, keyword search, hierarchical clustering, big data, security.*

1. Introduction

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources is rapidly provisioned and released with minimal management service provider interaction [1]. This keyword search technique access users to selectively retrieve files of interest and has been widely applied in plaintext search scenarios. Unfortunately, data security, which restricts user's ability to perform keyword search and further demands the security of keyword privacy, makes the traditional plaintext search methods fail for encrypted cloud data [2]. Ranked search greatly improves system usability by normal matching files in a ranked order regarding to certain relevance criteria [3]. The Cloud Service Provider (CSP) would promise is preserve the security of these data by using techniques like firewall, virtualization, and Intrusion Detection System (IDS) [4]. The CSP takes full control of these data these methods is prevented employers of the CSP from revealing sensitive data. Encryption uses alternative way to solve the problem secure conjunctive keyword search secure ranked keyword search, secure fuzzy keyword search, and privacy preserving similarity keyword search [5]. Searchable encryption schemes enable the client to store the secure data to the cloud and execute keyword search over cipher text domain [6].

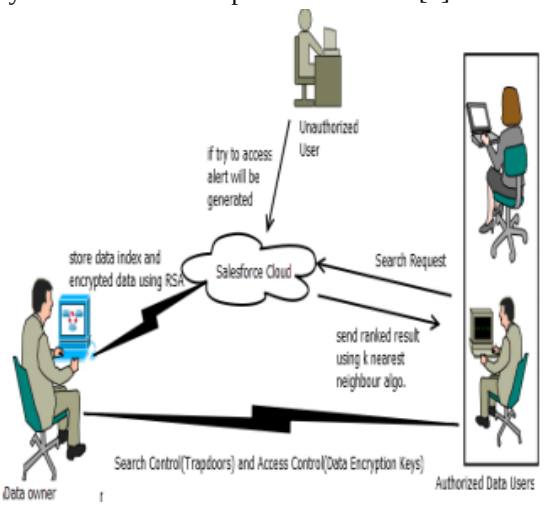

Fig1. Architecture of the search over encrypted data

To achieve many search functionality proposed such as single keyword search, similarity search, multi-keyword Boolean search, ranked search, and multi-keyword ranked search. Many multi-keyword ranked searches achieve more and more attention for its practical applicability [7]. Numerous analysts is created many cipher content search framework by uses the cryptography strategies [8]. These

procedures are demonstrated provable security and requests enormous operations and huge complexity in time. Henceforth already composed systems are valuable for huge data where size of the data is huge likewise it needs online data processing [9].

2. Related Work

To security data privacy sensitive cloud data is encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task [10]. Although present searchable encryption techniques access users to securely search over encrypted data through keywords software, ranked search improves system usability by normal matching files in a ranked order regarding to certain relevance criteria. As directly outsourcing relevance scores will drips a lot of sensitive information against the keyword privacy [11] We proposed asymmetric encryption with ranking result of queried data which will give only expected data [12]. Privacy-Preserving multi-keyword ranked search over encrypted information in cloud computing (MRSE). Then build up a set of strict privacy requirements for such a secure cloud information usage framework [13]. Multi keyword text search (MTS) is similarity-based ranking to address this issue. To support multi-keyword search and search result ranking, the propose to create the search index based on term frequency and also the vector area model with cosine similarity live to attain higher search result efficient [14]. The algorithms is present are simple, fast and introduce almost no space and communication overhead and hence are practical to use today.

2.1 Multi-Keyword Search

Compared with single keyword search, and multi-keyword search would be more practical. A multi-keyword search access data users to input more than one keyword which describes user search request more accurately.

2.2 Ranked Multi-keyword Search

The ranked multi-keyword search access data users to submit a search request with multiple keywords which enables the search the most relevant files corresponding to their search request

2.3 Multi-keyword Search without Ranking

Propose a privacy preserving Cooperative Private Searching (COPS) protocol. They introduce a middleware layer called the Aggregation and Distribution Layer (ADL) to combine queries from data users and divide search results to corresponding data users.

2.4 Fuzzy Keyword Search

To tolerant minor type errors and format inconsistencies fuzzy keyword search is proposed. The fuzzy keyword search not only improves the robustness, but also increases the usability of the search system we review the researches of fuzzy keyword search [15].

2.5 Conjunctive Keyword Search

A conjunctive keyword search is described is data user has several keywords is first generates the trapdoor for each keyword. The search results are the intersection of search results of each keyword [16].

2.6 Similarity Keyword Search

A similarity keyword search asks the cloud server to return all possible files that is similar with data user search requests, which has many applications the security and privacy obstacles, devising a secure similarity keyword search protocol is challenging [17].

2.7 Attribute Based Keyword Search

A practical secure search scheme should support multiple data owners and multiple data users before stating deployed most of backend schemes to support multiple data owners to securely and efficiently share data [18].

3. Proposed System

The propose system consist of entities data owner the data user and the cloud server. The data owner is responsible for collecting documents, building document index and outsourcing data encrypted format to the cloud server [19]. Aside from the data user needs to get the authorization from the data owner before getting to the information. The cloud server gives large storage space and the computation

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 10
September 2017

resources required by cipher text search [20]. To activate ranked search for effective uses of outsourced cloud data our system design should simultaneously achieve security and performance. Secured Multi-keyword Ranked Search: To design search schemes is access multi-keyword query and provide result similarity ranking for valuable data retrieval, instead of returning undifferentiated results [21].

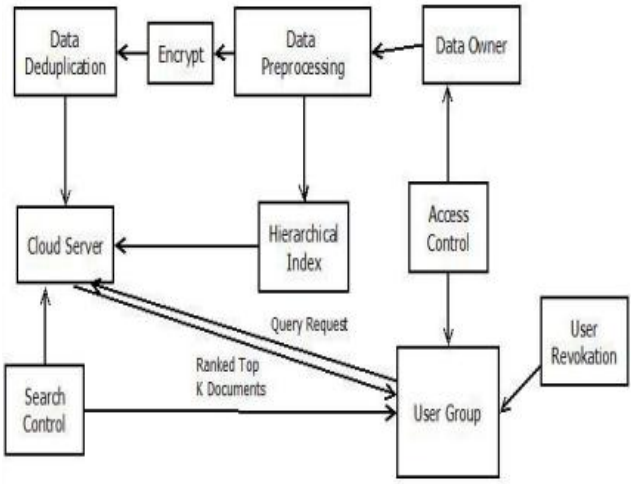

Fig. 2 Proposed System Architecture

3.1 RSA Algorithm

This algorithm is used to encrypt and decrypt file contents. The RSA algorithm updates key generation, encryption and decryption. The public key is known as everyone and is used for encrypting messages [22]. Messages encrypted with the public key are decrypted using the private key. The keys for the RSA algorithm are generated the following way.

1. Choose two distinct prime numbers a & b.
2. Compute n = ab. n is used as the modulus for both the public and private keys
3. Compute φ(n) = (a – 1)(b – 1), where φ is Euler's to tent function.
4. Choose an integer e such that 1 < e < φ(n) and greatest common divisor of (e, φ(n)) = 1; i.e., e and φ(n) are co prime. e is released as the public key exponent. Having a short bit-length.

To prevent cloud server from learning additional information from dataset and index, and to meet privacy requirements

3.2 Algorithm MRSE-HCI

In MRSE-HCI architecture is the data owner builds the encrypted index depending on the dictionary random numbers and secret key the data user submits a query to the cloud server for getting desired documents, and the cloud server returns to the target documents to the data user. This architecture mainly consists of following algorithms [23].

Algorithm: Duplication Checking

1. Input the initial set of k cluster Centers C
2. Set the threshold TH min
3. While k is not stable
4. Generate a new set of cluster centers CΘ by k-means
5. For every cluster centers CΘλ
6. Get the minimum relevance score: min (Si)
7. If the min (Si)

4. Simulation Results

The MRSE which means retrieved documents generated by MRSE-HCI is closer to each other. The relevance in query and retrieved documents [7]. With the size of document set increases from 3200 to 51200, the MRSE to plaintext search ratio fluctuates at 0:75. MRSE-HCI to plaintext search ratio increases from 0:65 to 0:75accompanying with the growth of document set size. When RSA algorithm is applied on the data and gets encrypted data. And that encrypted data is store on the cloud. User is access the data after downloading and decrypting file. For encryption and decryption keys are provided. We observe the relevance of retrieved documents in the MRSE-with clustering is almost twice as many as that in the MRSE-HCI which means retrieved documents is generated by MRSE-with clustering and much closer to each other.

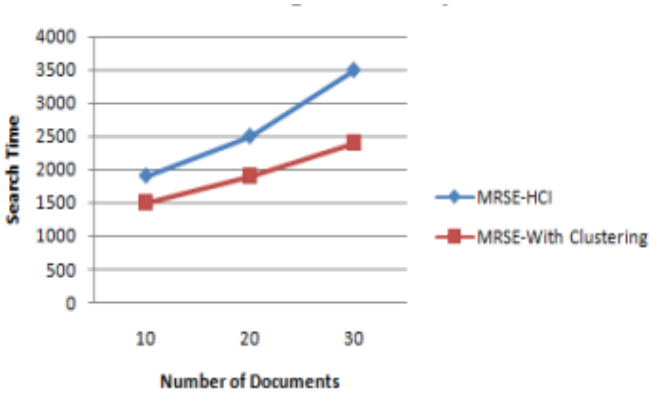

Fig. 3 Search Time Graph

5. Conclusion

We proposed multiple-keyword ranked search over encrypted cloud data is construct a variety of security requirements. We first propose secure inner data computation. Then they achieve effective ranking result using k-nearest neighbor technique to improve the accuracy of the result multi-keyword search should implement. The multi-keyword search improves security of result and reduce the traffic by reducing top-k relevant files. The proposed architecture not only properly solves the multi-keyword ranked search problem, but also brings and improvement and update the system performance by implementing user revocation method where user group relocate Also system reduces the memory overhead and enhances searching speed by implementing data duplication methods.

References

[1] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services," in Proc. IEEE Int. Conf. Consumer Electron., 2011, Berlin, Germany, 2011, pp. 83–87

[2] Ning Caoy, Cong Wangz, Ming Liy, Kui Renz, and Wenjing Louy Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data

[3] Weifeng Su, Jiying Wang, and Frederick H. Lochovsky, Member, IEEE Computer Society Record Matching over Query Results from Multiple Web Databases

[4]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58. Ballard, L., Kamara, S., & Monrose, F. (2005).

[5]. Achieving efficient conjunctive keyword searches over encrypted data. In Information and Communications Security (pp. 414-426). Springer Berlin Heidelberg.

[6] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+ r: Topk retrieval from a confidential index," in Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009, pp. 439–449.

[7] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012

[8] A. Singhal, Modern information retrieval: A brief overview, IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 3543, 2001.

[9] R. Ananthakrishna, S. Chaudhuri, and V. Ganti, Eliminating Fuzzy Duplicates in DataWarehouses, Proc. 28th Intl Conf. Very Large Data Bases, pp. 586-597, 2002.

[10] R. Baeza-Yates and B. Ribeiro-Neto, Modern Information Retrieval. ACM Press, 1999

[11] . Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data Cong Wang, Student Member, IEEE, Ning Cao, Student Member, IEEE, KuiRen, Senior Member

[12] . Privacy Preserving Keyword Searches on Remote Encrypted DataYan-Cheng Chang and Michael Mitzenmacher Division of Engineering and Applied Sciences, Harvard University, and Cambridge, MA 02138, USA 5. D. X. D. Song, D. Wagner, and A. Perrig, "Practical techniques for search.

[13] W. Sun, B.Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preservingmulti-keyword text search in the cloud supporting similarity-based ranking,"inProc. 8th ACM SIGSAC Symp.Inform.,Comput. Commun.Security, Hangzhou,China, 2013, pp. 71-82.

[14] C. Chen, X. J. Zhu, P. S. Shen, and J. K. Hu, "A hierarchical clustering methodFor big data oriented cipher text search," in Proc. IEEE INFOCOM, Workshop onSecurity and Privacy in Big Data, Toronto, Canada, 2014, pp. 559ˆa564.

[15]. Park, H. A., Kim, B. H., Lee, D. H., Chung, Y. D., & Zhan, J. (2007, November). Secure similarity search. In Granular Computing, 2007. GRC 2007. IEEE International Conference on (pp. 598-598). IEEE.

[16]. Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613. Shen, Z., Shu, J., & Xue, W. (2013, June).

[17]. Preferred keyword search over encrypted data in cloud computing. In Quality of Service (IWQoS), 2013 IEEE/ACM 21st International Symposium on (pp. 1-6).

[18]. Practical techniques for searches on encrypted data. In Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on (pp. 44-55). IEEE.

[19] D. Song, D. Wagner, and A. Perrig, ―Practical techniques for searches on encrypted data,‖ in Proc. of IEEE Symposium on Security and Privacy'00, 2000.

[20] E.-J. Goh, ―Secure indexes,‖ Cryptology ePrint Archive, Report 2003/216, 2003,

[21] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ―Public key encryption with keyword search,‖ in Proc. of EUROCRYP'04, volume 3027 of LNCS. Springer, 2004

[22] Ching-Yang Tseng, ChangChun Lu and Cheng-Fu Chou, "Efficient privacypreserving multi-keyword ranked search utilizing document replication and partition," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2015, pp.

[23] C. Wang, N. Cao, K. Ren, and W. J. Lou, "Secure ranked keyword search over encrypted cloud data"The 30th International Conference on Distributed Computing Systems (ICDCS'10), Genoa, Italy, June 21-25, 2010