To design a dynamic searchable encryption scheme over Encrypted Cloud Data

[1]S. BHANU PRASAD RAO [2]NANCHARLA VINAY

[1]Assistant Professor, Computer Science and Engineering, Tirumala Engineering College, Keesara, Medchal District, Telangana State, India

[2]Assistant Professor, Computer Science and Engineering, Tirumala Engineering College, Keesara, Medchal District, Telangana State, India

ABSTRACT:

Because of the expanding prominence of distributed computing, more information proprietors are inspired to outsource their information to cloud servers for extraordinary accommodation and diminished expense in information administration. Then again, delicate information ought to be scrambled before outsourcing for security prerequisites, which obsoletes information use like catchphrase based report recovery. In this paper, we show a safe multi-essential word positioned inquiry plan over encoded cloud information, which at the same time bolsters element overhaul operations like cancellation and insertion of archives. Specifically, the vector space model and the broadly utilized TF×IDF model are joined as a part of the record development and question era. We build a unique tree-based file structure and propose an "Avaricious Depth-first Search" calculation to give efficient multi-magic word positioned inquiry. The protected kNN calculation issued to scramble the file and question vectors, and in the interim guarantee exact pertinence score count between encoded list and inquiry vectors. With a specific end goal to oppose factual assaults, apparition terms are added to the list vector for blinding indexed lists. Because of the utilization of our exceptional tree-based file structure, the proposed plan can accomplish sub-direct inquiry time and manage the erasure and insertion of archives flexibly. Broad analyses are led to exhibit the efficiency of the proposed scheme.

1. Introduction

Cloud computing has been considered as another model of enterprise IT infrastructure, which can compose gigantic resource of computing, storage and applications, and empower users to appreciate pervasive, helpful and on-demand network access to a mutual pool of configurable computing resources with incredible efficiency and insignificant economic overhead. Pulled in by these engaging features, both individuals and enterprises are roused to outsource their data to the cloud, rather than buying software and hardware to deal with the data themselves. In spite of the different points of interest of cloud services, outsourcing delicate information, (for example, e-mail, individual health records, organization account information, government archives, and so forth.) To remote servers brings privacy concerns. The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization. A general way to deal with secure the data privacy is to encrypt the data before outsourcing. On the other hand, this will bring about a gigantic expense in terms of data ease of use. For example, the current techniques on keyword-based information retrieval, which are broadly utilized on the plaintext data, can't be straightforwardly connected on the encrypted data. Downloading all the data from the cloud and decrypt locally is clearly unrealistic. With a particular final objective to address the above issue, analysts have illustrated some all around helpful arrangements with totally homomorphism encryption or missing RAMs. In any case, these schedules are not down to earth in light of their high computational overhead for both the cloud server and user. In spite of what may be normal, more useful unique reason arrangements, for instance, searchable encryption(SE) plan have made specific responsibilities to the extent productivity, value and security. Searchable encryption scheme engage the user to store the encrypted data to the cloud and execute unequivocal word look for over cipher text domain. As being what is indicated, abundant works have been proposed under assorted risk models to finish distinctive interest value, for instance, single keyword search, closeness look, multi-keyword Boolean search, ranked search, multi-keyword

ranked search, etc. Among them, multi keyword positioned quest finishes more thought for its pragmatic propriety. Starting late, some component arrangements have beenproposed to reinforce embedding and erasing operations on archive gathering. These are colossal goes about asset is exceptionally possible that the data owner need to overhaul their data on the cloud server. Yet, few of the dynamic plan support successful multikeyword situated look. Inverse document recurrence (IDF)" model are the list development and inquiry era to give multi keyword positioned seek. Keeping in mind the end goal to get high search Effectiveness, we develop a tree based list structure and based on this tree list we propose a "Greedy Depth–first Search" calculation. Because of the uncommon structure of our tree-based list, the proposed search scheme can flexibly accomplish sub-straight search time and manage the deletion and insertion of reports. The protected kNN algorithm is used to encrypt the index and query vectors, and in the interim guarantee relevance score calculation between encrypted index and query vectors. To oppose distinctive attacks in different threat models, we build two secure search schemes: the basic dynamic multi-keyword ranked search.

2. Related work

2.1 Single Keyword Searchable Encryption Searchable encryption schemes

Usually build an encrypted searchable index based on the keywords within document set, by which its content is hidden to the cloud server. Given appropriate search trapdoors generated by authorized user(s) (who has the secret key given by the data owner),the server can search the index and return corresponding search result.. After this work, some schemes are proposed to improve the security definition and search efficiency. Solve s the fuzzy keyword search which utilizes edit distance to extend keyword set. Schemes in solve the result ranking search utilizing order-preserving techniques. With frequency related information, they can rank search result and return more accurate result. Propose the first searchable encryption scheme based on public key cryptography. However, public key methods are always computationally expensive. Kamara, et al. , propose a dynamic searchable encrypted

scheme which supports both keyword search and document update. However, all the schemes expressed above only provide single keyword search.

2.2 Multi-keyword Searchable Encryption

As an attempt to improve system usability, a lot of works have been do ne in the public key setting to enrich search functionalities, including conjunctive keyword search, range queries and subset search. But these schemes usually result in large computational burden caused by some significant operation (for example, bilinear map). We are focused on predicate encryption which supports both conjunctive and disjunctive search. Although these schemes can provide more general search, they does not support result ranking. a privacy-preserving multi-keyword ranked search scheme which adopting “coordinates matching” to realize ranked search. This scheme ranks search result by the number of matched keywords, without considering more accurate ranked result. Since the scheme uses the inverted index as the index structure, it leads to traverse all indexes of document set executed by the cloud server for each search query. Propose a secure multi-keyword ranked search scheme based on vector space model (VSM). The VSM can measure the similarity between document index vector and query vector and hence support more accurate ranked search result. Schemes in use an MDB-tree as its index structure and propose a search algorithm based on the tree structure, which improve the search complexity in that the cloud server only need to search the part of the tree.

3. Frame work

The first symmetrical searchable encryption (SSE) scheme and the search of the scheme is linear in the size of the data collection. Proposed formal security definitions for SSE and developed a system based on Bloom filter. It is proposed that two systems (SSE-1 and 2) that the optimal search time is reached. Your SSE 1 scheme is secure against attacks Chosen-Keyword (CKA1) and SSE-2 is secure against adaptive chosen-keyword attacks (CKA2). These early works are single keyword Booleansearch schemes that are very simple in terms of functionality. After plenty of plants have been proposed under different threat models to search various search functions, such as single keyword search,

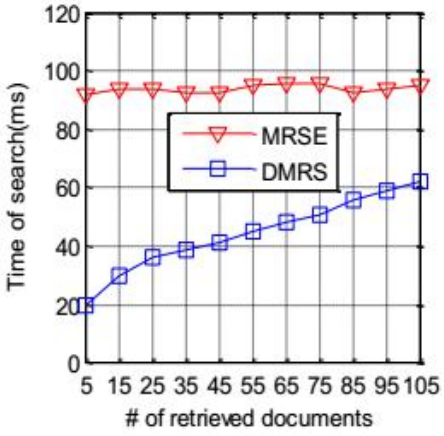
similarity search more keyword Boolean search space and multi keyword search on place, etc. Multi-keyword Boolean search allows achieve the user to enter multiple query keywords to request appropriate documents. Among these works, combining keyword search systems give only the documents that contain all of the query keywords. Disjunctive Keyword Schemes return all documents that contain keywords proposed. Predicate search schemes a subset of the query, both connecting divisive to support search. All these schemes More Keyword retrieve search results based on the presence of keywords, which can provide not acceptable result ranking functionality. Proposed guide can achieve sub linear search time flexible and deal with the deleting and inserting documents. The safe kNN algorithm used to encrypt the index and query vectors, in the meantime accurate relevancy score calculation between encrypted index and query vectors. Ensure to withstand various attacks indifferent threat models, build two secure search systems: the dynamic top k multi-keyword search scheme selected in the known cipher text model, and improved dynamic top k multi-keyword space search procedure in the known background model, proposed scheme can achieve higher search efficiency by executing our "Greedy Depth-first Search" algorithm. Moreover, parallel search can be flexibly performed tofurther reduce the time cost of search process Access Group Key Generation Process Module Access Key and Authentication is the process, in fact, to be determined. In private and public computer networks (the Internet), the authentication is often done through the use of logon passwords. Knowing the password is assumed to guarantee that the user is authentic. Each user initially registered (or registered by someone else), an assigned or self-declared with password. On each subsequent use, the user must know and use the previously specified password. The weakness in this system for transactions that is significant (such as the exchange of money) is that passwords are often stolen, accidentally revealed, or forgotten. The process of authorizing an individual , usually based on a username and password in the security system which is the process of giving individuals access to system objects based on their identity authentication merely identifies that the

individual is who he or she allowed to be , but says nothing about the access rights of the individual .Public Cloud Server Implementation The cloud server is considered honest in our work as "a model is used extensively by that the cloud server characterized honestly follow designed protocol hosted data and analyze the received requests to get additional information. When users their private data to outsource cloud, the cloud service providers capable of the data and the communication between the users and the cloud will, lawful or unlawful to control and monitor. Instances like the secret NSA program work, the recorded on the data to divide and should also create and splitted data signatures are saved for all.

4. Experimental results

During the search process, if the similarity scores at node u is larger than the minimum similarity score of the current selected top-k

Documents, the cloud server examines u's children, else it returns. Thus, lots of nodes are not accessed during a real search. We denote the number of leaf nodes that contain one or more keywords in query as r, which is generally larger than k but far less than n. Since the maximum height of the red-black tree is maintained to belong, the search time without pruning.



However, different search paths may share same nodes during the search, and based on our "Greedy Depth-first Traverse Strategy", the search process terminates after the top-k documents have been selected.

5. Conclusion

In this paper, a safe, effective and dynamic search scheme is proposed, which underpins the exact multi-keyword ranked search as well as the dynamic deletion and insertion of documents. We assemble a specialkeyword balanced binary tree as the index, and "Greedy Depth-first Search" algorithm to acquire preferable effectiveness over linear search. Likewise, the parallel search procedure can be

completed to further lessen the time cost. The plan's security is ensured against two risk models by utilizing the safe kNN algorithm. Trial results display the efficiency of our proposed scheme. In the proposed scheme, the information proprietor is in charge of producing overhauling data and sending them to the cloud server.

References:

[1] K. Ren, C. Wang, Q. Wang *et al.*, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*. Springer, 2010, pp. 136– 149.

[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," *Journal of the ACM (JACM)*, vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in CryptologyEurocrypt 2004*. Springer, 2004, pp. 506–522.

[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in *Advances in Cryptology-CRYPTO 2007*. Springer, 2007, pp. 50–67.

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*. IEEE, 2000, pp. 44–55.

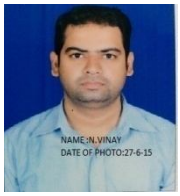
Author Profiles:

Author 1:

S. Bhanu Prasad Rao, Assistant Professor, Computer Science and Engg., Tirumala Engineering College, Affiliated to JNTUH and Approved by AICTE, Bogaram, Near Keesara, Medchal District, Telangana State, India, PIN: 501301.

Email: prasadshapally86@gmail.com

Author 2:



Nancharla Vinay, Assistant Professor, Computer Science and Engg., Tirumala Engineering College, Affiliated to JNTUH and Approved by AICTE, Bogaram, Near Keesara, Medchal District, Telangana State, India, PIN: 501301.

Email: nvinay624@gmail.com