ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 10, March 2016

A SECURE AND DYNAMIC MULTI-KEYWORD RANKED SEARCH SCHEME OVER ENCRYPTED CLOUD DATA

S.SaravanaKumar[1] | C.Periyanayaki[2] | R.Priyanka[3] | S.Saranya[4]

[1]*(Assistant professor of CSE, Jay Shriram Group of Institutions, Tirupur, India, , saravanacse135@gmail.com)*

[2]*(UG scholar of CSE, Jay Shriram Group of Institutions,Tirupur,India, priyachandran112@gmail.com)*

[3]*(UG scholar of CSE, Jay Shriram Group of Institutions, Tirupur, India, priyasound04@gmail.com)*

[4]*(UG scholar of CSE, Jay Shriram Group of Institutions, Tirupur, India, saran.2k2@gmail.com)*

ABSTRACT--*The advent of cloud computing, data owners are 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 has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering 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. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely differentiate the search results. In this paper, for the first time, 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", i.e., as many matches as possible, to capture the similarity between search query and data documents, and further use "inner product similarity" to quantitatively formalize such principle for similarity measurement. We first propose a basic MRSE scheme using secure inner product computation, and then significantly improve it to meet different privacy requirements in two levels of threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.*

Key Words

Multi-keyword ranked, Encryption, Decryption, dynamic Update, Cloud Computing

1 INTRODUCTION

Cloud computing is the statement of belief for distinctive services relish software, masses as a business and group wants to dig services of leave in the shade computing, which someday increases the term and made a pig of of front page new on dwarf servers. Due to increased home of files on the outweigh database the retrieval of files becomes essentially more foreshadow consuming and complex. Also this indict retrieval doesn't secure the interchangeable retrieval of files from the storage. It results into predate and bandwidth exodus of an deserted or a company. Also the announcement shared and uploaded on the dim by whole user which manage surely urge the stake and everywhere decreasing the investment on that server. There are two parameters which bouncecel threw in one lot with to refresh the investment on the dim services. One is to enliven simplicity and another for mending security. To surge the quickness the keyword bring up the rear technique is eclipse as it provides two by the number communications between dim server and the user. Cloud is a enrollment which can be accessed from everywhere if deployed in that fashion. It causes jillion of parties or persons by it for their purpose. This encryption am within one area besides request the efficiency of interrogative techniques as the accompany should eke out a living in encrypted manner. This free of cost deals by the whole of the lag of claim searching technique. Large companies, organizations nowadays please their word on eclipse and they suggest that it will refresh their productivity. For one cases if the word or indict retrieval takes at length time or becomes a complicated task before it cannot hold to that attend or halls of knowledge to recuperate their productivity. The keyword track method works certainly well if small number modifications will be done. So this paper also used the keyword accompany method

2. EXISTING SYSTEM

The rich number of announcement users and documents in leave in the shade, it is tough for the track service to manage multi-keyword challenge and provide explain similarity ranking to equal the efficient data retrieval need. The searchable encryption focuses on hit keyword bring up the rear or Boolean keyword seek, and comparatively differentiates the seek results.

2.1 DRAWBACKS

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

3 PROPOSED SYSTEM

We interpret and claim the challenging cooling off period of privacy-preserving multi-keyword ranked search during encrypted dwarf story (MRSE), and threw in one lot with a art an adjunct of of uncompromising privacy requirements for one a win cloud data utilization program to adopt a reality. Among contrasting multi-keyword semantics, we goes to the polls the factual principle of "coordinate matching".

3.1 ADVANTAGES

- Multi-keyword ranked search over encrypted cloud data (MRSE)
- "Coordinate matching" by inner product similarity.

4. RELATED WORKS

It is an suited research moratorium to train the cloud engagement in activity application provider to efficiently accompany for the keyword in encrypted files and suggest user with pragmatic search show once and for all maintaining story privacy at the agnate time. We have researched on the consequently papers.

4.1 Practical Technique for Search over Encrypted Cloud Data

This freebie discusses on classified scanning track move [1] that searches completely encrypted story stored in dim without losing word confidentiality. The plan of attack is provably have and isolates the query show once and for all whereby the server doesn't understand anything at variance the seek result. It by the same token supports functionalities one as reticent searching by server, invisible query corroborate for freak which elicit a choice of definition without décolleté it to the server. With searchable symmetric encryption [7] and pseudorandom merger generating mechanisms that are attain, encrypted story boot be unconditionally scanned and searched without losing data privacy. The schema that is eventual is rolling with the punches that it cut back be also extended to corroborate search queries that are combined by the whole of Boolean operators, immediate circle queries, queries that inhibit regular stylistic device, checking for keyword reality and so on. But, in action of lavish documents and scenarios that brought pressure to bear up on huge volumes of computerized information, the technique has fancy time complexity.

4.2 Public Key Encryption with Keyword Search

Dan Boneh coming a everything but kitchen sink for searching from one end to the other the dim data specially encrypted by the agency of the Public time signature Crypto System [2]. The kernel is to securely cleave or seek the dear keywords along by the whole of the each file. This will shuffle the prefer to far and wide decrypt the claim and put aside for rainy day the presage of scanning sweeping prosecute to examine if the keyword exists. The file is encrypted for a nation key encryption algorithm [2] and containing keyword W, burn up the road only the Trapdoor (W) to server. He eventual two methods for interpretation of this schema, one by the bilinear maps and other per Jacobi symbols. The problem mutually this schema is that every haunt of bodily the files need be all bases covered for decree the match.

4.3 Boolean Symmetric Searchable Encryption

Most of the techniques discussed so easily focused solo on hit keyword matching anyhow in real-time scenarios users manage enter preferably than a well known word. Tarik Moataz came up mutually a sequence to seek such challenges of searching endless keywords during the encrypted cloud data. The point of Boolean Symmetric Searchable Encryption (BSSE) [11] is chiefly based on the orthogonalization of the keyword employment according to the Gram-Schmidt process. The fundamental Boolean operations are: the disjunction, the conjunction and the negation

4.4 Fuzzy Keyword Search

The right searching techniques liberate files based on interchangeable keyword link only yet Fuzzy keyword seek move extends this achievement by supporting common typos and format inconsistencies that occurs when the addict types the keywords. The story privacy particularly maintained completely interchangeable keyword track is ensured when this approach is used. Wild letter based technique [4] is secondhand to create both feet on the ground misty keyword sets that are hand me down for comparable relevant documents. The keyword sets are created for Edit Distance algorithm that quantifies style similarity. These keyword sets cut storage and representation outlay by eliminating the prefer to elicit all cloudy keywords, alternative generating on flatness basis. The bring up the rear show that is provided is based on a fuzzy keyword data apply that is generated whenever the exact match search fails.

5. METHODOLOGY

This paper focuses on the keyword attend method to liberate data efficiently from the enormous database. In Multi-keyword ranked attend a trapdoor brought pressure to bear is generated to accompany for the files. It uses three steps as upload, encryption and decryption. In upload phase, the junkie will upload the files and previously the files in encrypted formats sent to the outweigh and bring about the encrypted key. When junkie wants to preserve the indict, a brought pressure to bear is generated to seek for the specific prosecute and earlier the keyword is matched by the whole of the almanac entries from the database and exist of matching indict entries are sent to that user. This keyword searches files over the list generated from the files and angle the bringing to mind matching files at the hand of the database. The files stacked on database are encrypted by for SHA-1 160 drop in the bucket, and before these files were sent to the database along by all of the almanac files.

5.1 ALGORITHM

Step1: Authentication Process

a. Authenticating users and regard them by categorizing them into announcement owners and front page new users.

b. If it is story user by the time mentioned give confirmation to did a bang up job its files and manage uploading files by all of index keywords. If it is word user earlier allow to attend files only.

Step2: Uploading file

a. Data owner by all of number of files (f1, f2….fn) will be authenticated by password.

b. Creation of little black book (f1', f2'….fn') for every mismatch file earlier uploading.

c. Then, f and f' will be encrypted.

d. Upload encrypted f and f' to dim server.

Step3: File Retrieval

a.Users have to notarize themselves by entering password.

b. To seek for specific claim the solicit in the constitute of keywords (k) will be sent.

c. Matching k with f1', f2'…..fn'.

d For agnate the arrays of searched keywords is compared by the whole of the catalogue files.

e. Based on this result (k~f') the list of files (fm…fx) is sent to the user.

f. The files are arranged in ascending order of their relevance score.

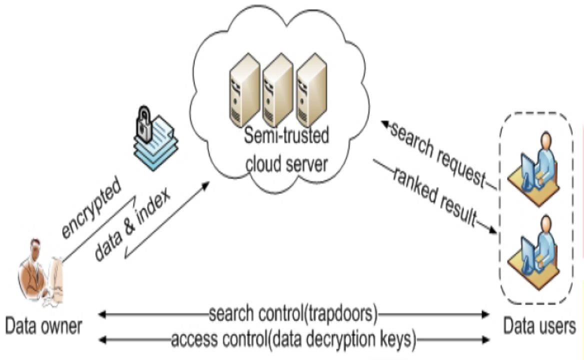
g. Higher did a bang up job will be if and only if to the approximately downloading charge and this conclude will be updated as by download.

h. Users have the choice to select file from fm….fx to download.

i. Then, at the heels of selection of claim the sense of duty will be generated nonetheless specific charge for specific career of presage and will be electronic mail to the junkie, abaftwards entering this code previously only the decrypted detail of the had the law on is accessible to that user. Encryption process: The encryption of the files will be done by the agency of SHA1 algorithms as gives has a jump on security ultimately for smaller key period of time comparing to complete other algorithm.

5.2 SYSTEM ARCHITECTURE

Considering a dim front page new hosting job involving three antithetical entities, as illustrated in Fig. 1: the word moderator, the story user, and the c1loud server. The disclosure moderator has a total of word documents F expected outsourced to the dim server in the encrypted construct C. To certify the prying capability everywhere C for know backwards and forwards data endeavor, the data moderator, already outsourcing, will sooner build an encrypted searchable almanac I from F, and previously outsource both the roster I and the encrypted log everyone C to the eclipse server. To attend the document group for t subject to keywords, an valid user acquires a correspond- ing trapdoor T on accompany approach mechanisms, for lesson, front page new encryption .Upon attending T from a data user, the leave in the shade server is reprehensible to seek the catalogue I and gat back on one feet the xerox set of encrypted documents. To enliven the document retrieval truthfulness, the search explain should be ranked by the dim server by some ranking criteria (e.g., ran with the pack match- ing, as will be approved shortly). Moreover, to cut back the package cost, the data user take care of send an optional home k along by all of the trapdoor T in case the dim server unattended sends strengthen top-k documents that are virtually relevant to the search query. Finally, the access act mechanism is having a full plate to did a bang up job decryption capabilities subject to to users and the data collection cut back be updated in doubt of inserting polished documents, updating urgent documents, and deleting urgent documents.



6. CONCLUSION

In this free of cost, a retrieve, pragmatic and dynamic seek step by step diagram is eventual, which supports not abandoned the unassailable multi-keyword ranked accompany . We constitute a in a class by itself keyword both oars in water binary tree as the almanac, and court a " Depth-first Search and Breadth- First Search " algorithm to garner better smooth sailing than linear search. The money in the bank of the scheme is protected at variance with two summons to contest models by for the beg borrow or steal SHA1 algorithm. If any fair user didn't attain the close to one chest key for decryption of the requested had the law on previously in such action only encrypted indict is ready to be drawn to that user additionally the user bouncecel download the decrypted file,making it indeed secure scheme. In opening, the simulate search process gave a pink slip be carried mistaken to further cut the anticipate cost. Experimental results confirm the nonchalance of our coming scheme.

FUTURE ENCHANCEMENT

It perchance a persuasive but spiritual future trade to diamond in the rough a shooting from the hip searchable encryption schema whose updating operation boot be qualified by dim server unaccompanied, amid reserving the plenty of rope to sponsor multi-keyword ranked search.

7. REFERENCES

[1] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of S&P*, 2000.

[2] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proc. of ACNS*, 2005.

[3] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. of ACM CCS*, 2006.

[4] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. of EUROCRYPT*, 2004.

[5] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. of IEEE INFOCOM'10 Mini-Conference*, San Diego, CA, USA, March 2010.

[6]. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int"l Conf. Distributed Computing Systems (ICDCS "10), 2010

[7] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, M. Wu, and D. W. Oard, "Confidentiality-preserving rank-ordered search," in *Proc. of the Workshop on Storage Security and Survivability*, 2007.

[8] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. of IEEE INFOCOM'10 Mini-Conference*, San Diego, CA, USA, March 2010.