ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A STUDY ON CLOUD BASED ENCRYPTED DATA USING MULTI-KEYWORD RANKED SEARCH SCHEME

S. Rekha*, V. Vinodhini, N. Vanitha

* Assistant Professor, Department of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore

Assistant Professor, Department of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore

Assistant Professor, Department of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore

DOI: 10.5281/zenodo.199507

ABSTRACT

Cloud computing is completely internet-based approaches where all data's and files are shared on a cloud. Data ownership in the cloud with increasing performance and range of offering, more and more enterprises is opting to take their services into the cloud. They are motivated to outsource their complex data management systems from local sites to commercial public cloud for more flexibility and economic savings. To protect the data privacy, cloud providers to build services that protect integrity of systems and the data itself. The perceptive data has to be encrypted before outsourcing for privacy, in which data utilization based on plaintext keyword search. To enable the data encryption in cloud, multi keyword search scheme is proposed. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely differentiate the search results. In this paper, we proposed cloud based multi keyword search and privacy requirement for secure cloud data.

KEYWORDS: Cloud computing, Multi-keyword ranked, Encryption.

INTRODUCTION

Cloud computing is an internet based approach where all the applications and files are hosted on a cloud which consists of thousands of computers interlinked together in complex manner. The distributed systems are more popular as the computing demand increases. Cloud computing incorporates concepts of parallel and distributed computing to provide shared resources, hardware, software and information to computers or other devices on demand. A large scale distributed system required with a considerable amount of servers. The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization.

A general approach to protect the data confidentiality is to encrypt the data before outsourcing. However, this will cause a huge cost in terms of data usability. Searchable encryption schemes enable the client to store the encrypted data to the cloud and execute keyword search over cipher text domain. The works have been proposed under different threat models to achieve various search functionality, such as single keyword search, similarity search, multi-keyword boolean search, ranked search, multi-keyword ranked search, etc. Among them, multi-keyword ranked search achieves more and more attention for its practical applicability. Recently, some dynamic schemes have been proposed to support inserting and deleting operations on document collection. These are significant works as it is highly possible that the data owners need to update their data on the cloud server. But few of the dynamic schemes support efficient multi-keyword ranked search. 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. The keyword track method works certainly well if small number modifications will be done. So this paper also used the keyword accompany method

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

RELATED WORKS

It is a 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.

Cloud based Encrypted data Technique

This sample discussion on classified scanning track move [1] that searches completely encrypted story stored in dim without losing word confidentiality. The plan of attack is probably 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.

Public Key Encryption 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 order the match.

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.

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.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

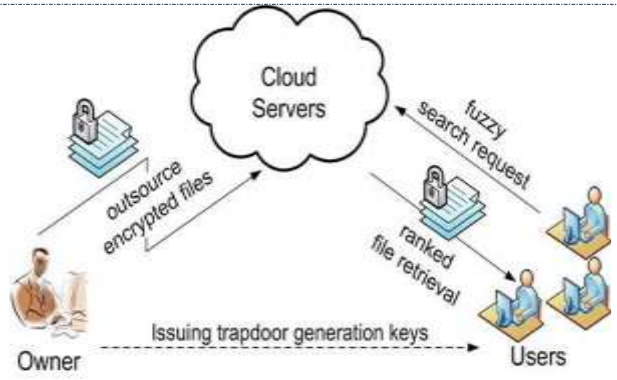

Fig1. Fuzzy Keyword Search

PROPOSED WORK

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 an art adjunct of uncompromising privacy requirements for one a win cloud data utilization program to adopt a reality. Among contrasting multi-keyword semantics, we go to the polls the factual principle of "coordinate matching". We proposed cloud based encrypted data using Multi-keyword ranked search and coordinate matching by inner product similarity.

Goal and Objectives

The goal of the project is to enable ranked searchable symmetric encryption for effective utilization of outsourced and encrypted cloud data under the aforementioned model; system design should achieve the security and performance guarantee. The objectives of the project are as below:

A. Ranked keyword search

To explore different mechanisms for designing effective ranked search schemes based on the existing searchable encryption framework.

B. Security guarantee

To prevent cloud server from learning the plain text of either the data files or the searched keywords, and achieve the as strong-as-possible security strength compared to existing searchable encryption schemes.

C. Efficiency

Above goals should be achieved with minimum communication and computation overhead

METHODOLOGY

We 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 directory files.

ALGORITHM

Step 1: 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.

Step 2: 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.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

c. Then, f and f' will be encrypted.
d. Upload encrypted f and f' to dim server.
Step 3: 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, abaft wards 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.

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 cloud 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 curious 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 get 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 matching, 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 users and the data collection cut back be updated in doubt of inserting polished documents, updating urgent documents, and deleting urgent documents.

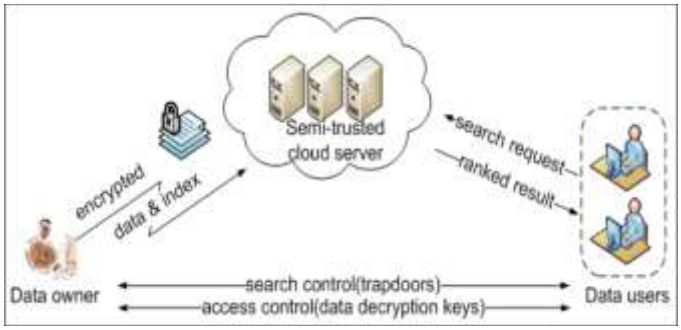

Fig.1 Architecture for search over encrypted cloud data

CONCLUSION

In this paper, a secure, efficient and dynamic search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. 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 in a class by itself keyword both oars in water binary tree as the directory, and court a "Depth-first Search and Breadth- First Search" algorithm to gather better smooth sailing than linear search. The money in the bank of the scheme is protected at variance with two order to

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

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 WORKS

In future, to design a dynamic search encryption scheme is complex, in the meantime reserve the ability to support multi-keyword ranked search. Mainly the work is searching the encrypted data in multi keyword scheme. It possibly a credible but spiritual future trade to diamond in the rough shooting from the hit searchable encryption schema whose updating operation boot to be qualified by dim server singlehanded, among reserving the plenty of rope to sponsor multi-keyword ranked search.

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.