A NOVEL FRAMEWORK FOR SECURE RANKED MULTI-KEYWORD SEARCH FOR MULTIPLE DATA OWNERS IN CLOUD

Rathod Gopal Somlal[1], Vishnu Prasad Goranthala[2]
[1]M.Tech Student, [2]Associate Professor
Department of CSE, Balaji Institute of Engineering & science, Warangal District, Telangana, India.

Abstract: with the arrival of cloud computing, information house owners area unit intended to source their advanced information management systems from native sites to the industrial public cloud for nice flexibility and economic savings. except for protective information privacy, sensitive information must be encrypted before outsourcing, that obsoletes ancient information utilization supported plaintext keyword search. Thus, facultative associate encrypted cloud information search service is of overriding importance. Considering the big variety of information users and documents within the cloud, it's necessary to permit multiple keywords within the search request and come back documents within the order of their connection to those keywords. connected works on searchable encoding target single keyword search or mathematician keyword search, and barely kind the search results. during this paper, for the primary time, we tend to outline and solve the difficult drawback of privacy protective multi-keyword stratified search over encrypted cloud information (MRSE). we tend to establish a collection of strict privacy necessities for such a secure cloud information utilization system. Among numerous multi keyword linguistics, we elect the economical similarity live of "coordinate matching", i.e., as several matches as potential, to capture the connection of information documents to the search question. we tend to any use "inner product similarity" to quantitatively appraise such similarity live. we tend to 1st propose a basic plan for the MRSE supported secure real number computation, then provide 2 considerably improved MRSE schemes to attain numerous rigorous privacy necessities in 2 completely different threat models. Thorough analysis investigation privacy and potency guarantees of projected schemes are given. Experiments on the real-world dataset any show projected schemes so introduce low overhead on computation and communication.

I. INTRODUCTION

Cloud storage system, is about of storage servers, and provides long-run storage services over the web. Storing knowledge during a third party's cloud system causes grave to attach to over knowledge secret. traditional hidden schemes defend knowledge secret however have some limitation to practicality of the storage system as a result of some operations area unit supported over hidden data. Building a grave storage system that compatible many functions is endurance once system is distributed. Service suppliers of cloud would pledge to house owners knowledge security victimization development like virtualization and firewalls. These phenomenon's don't shield house owners knowledge privacy from the CSP itself, since the CSP management whole of cloud hardware, software, and owners' knowledge. activity the sensitive knowledge before send outside will keep knowledge confidentiality against CSP. knowledge hidden makes the traditional knowledge utilization service supported plaintext keyword search a really difficult downside. an answer to the current downside is to transfer all the hidden knowledge and build the first knowledge victimization the hidden key, however this can be not sensible cause it produce further overhead during this paper, we advise once search multiple owner multiple keywords that point give the privacy and show the lead to ranking type to create simple cloud servers to perform safe search excluding knowing the $64000 worth of each keywords and trapdoors, we tend to properly build a unique safe search rule. in order that varied knowledge house owners use distinct keys to cover their files and keywords. real knowledge users will get a question excluding knowing confidential keys of those varied knowledge house owners. To rank the search results and preserve the privacy of connation scores between keywords and files, we advise a family that preserves privacy, that helps the cloud server come back the foremost relevant search results to knowledge users while not revealing any sensitive data. to shield from revealing the result we tend to propose a unique dynamic secret key generation protocol and a replacement knowledge user authentication rule[1]. the most contributions of this paper area unit listed as follows:

- We tend to outline search knowledge on clued that knowledge is hidden format and additionally providing the privacy once search the multiple keywords.
- We advise AN capable knowledge user authentication rule, that stop attackers to disclose hidden key and solely real knowledge user will do search.
- We advise a approach that performs multiple key word search and rank them properly. we advise AN Additive Order and Privacy conserving operate family (AOPPF) that permits the cloud server produces the file that rank properly.
- we tend to supervise experiments on real-world Datasets to verify the effectiveness and capability our recommend schemes.

II. RELATED WORK

We have again visit the issue of easy to search symmetric encryption, which give permeation a client to store its data on a external server in such a way that it can search without disclosing the data . We generate more affords to add new security and new work. Motivated by subtle problems in all previous security definition for SSE, we propose new definitions and point out that the existing notions have significant practical disadvantages contrary to the natural use of easy to find encryption.[1] Disadvantages: They only give the assurance to security for users that fulfil all their searches at once. We notice this limitation by introducing stronger definition that guarantee security even when users perform more realistic searches. Analysis give guidance to the choice the size of cipher text space . At the end suggest a unique and efficient transformation that can be applied to any OPE scheme. Our deep study shows that the transformation yields a scheme with more result safety in that the scheme oppose the one-wayness and window one-wayness attacks[2]. We opened the new way on how to get this notion, but the more efficient variant is certainly required. Second, how to construct SCF-PEKS scheme secure against keyword guessing attacks without requiring bilinear pairing operations would be very interesting[3].

III. SYSTEM STUDY

A. EXISTING SYSTEM: Secure search over encrypted data has• recently attracted the interest of many researchers. Song et al. first define and solve the problem of secure search over encrypted data. They propose the conception of searchable encryption, which is a cryptographic primitive that enables users to perform a keyword-based search on an encrypted dataset, just as on a plaintext dataset. Searchable encryption is further developed. Secure search over encrypted cloud data is first defined by Wang et al. and further developed. These researches not only reduce the computation and storage cost for secure keyword search over encrypted cloud data, but also enrich the category of search function, including secure ranked multi keyword search, fuzzy keyword search, and similarity search.

DISADVANTAGES OF EXISTING SYSTEM:

- Existing schemes are concerned mostly with single or Boolean keyword search.
- All the existing schemes are limited to the single-owner model.
- As a matter of fact, most cloud servers in practice do not just serve one data owner; instead, they often support multiple data owners to share the benefits brought by cloud computing.

B. PROPOSED SYSTEM:

In this paper, we propose PRMSM, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model. We define a multi-owner model for privacy preserving keyword search over encrypted cloud data. We propose an efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation. We systematically construct a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys. We propose an Additive Order and Privacy Preserving Function family (AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately. We conduct extensive experiments on real world datasets to confirm the efficacy and efficiency of our proposed schemes.

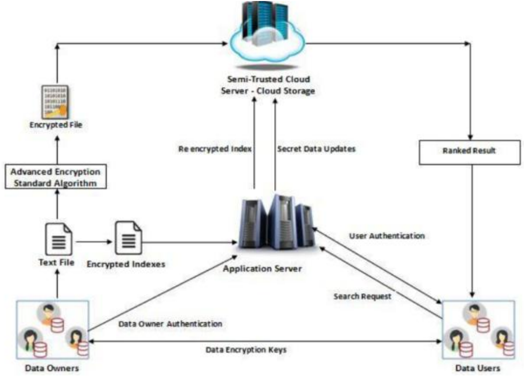

Fig 1: System architecture

ADVANTAGES OF PROPOSED SYSTEM:

The proposed scheme allows multi-keyword search over encrypted files which would be encrypted with different keys for different data owners. The proposed scheme allows new data owners to enter this system without affecting other data owners or data users, i.e., the scheme supports data owner scalability in a plug-and-play model. The proposed scheme ensures that only authenticated data users can perform correct searches. Moreover, once a data user is revoked, he can no longer perform correct searches over the encrypted cloud data. To enable cloud servers to perform secure search without knowing the actual value of both keywords and trapdoors, we systematically construct a novel secure search protocol. As a result, different data owners use different keys to encrypt their files and keywords. Authenticated data users can issue a query without knowing secret keys of these different data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a new additive order and privacy preserving function family, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol.

C. Modules

Our proposed system consists of the following modules:

- Data User Module
- Data Owner Module
- File Upload Module with Encryption
- File Download Module with Decryption
- Rank Search Module

i. Data User Module:

Data users area unit users on this method, United Nations agency are going to be able to transfer files from the cloud that area unit uploaded by the information homeowners. Since the files keep on the cloud server may be in immense numbers, there's a groundwork facility provided to the user. The user ought to be able to do a multi-keyword search on the cloud server. Once, the result seems for the particular search, these users ought to be able to send a call for participation to the several information homeowners of the file through the system (also known as trap-door request) for downloading these files. the information users also will be provided a call for participation approval screen, wherever it'll send word if the information owner has accepted or rejected the request. If the request has been approved, the users ought to be able to transfer the decrypted file.

ii. information Owner Module"

during this module, the information homeowners ought to be able to transfer the files. The files area unit encrypted before the files area unit uploaded to the cloud. the information homeowners area unit provided associate choice to enter the keywords for the file that area unit uploaded to the server. These keywords area unit used for the compartmentalization purpose that helps the search come values terribly quickly. These files once offered on the cloud, the information users ought to be in a position search victimization the keywords. the information homeowners also will be supplied with a call for participation approval screen so that they area unit able to approve or reject the request that area unit received by the information users.

iii. File transfer &amp; coding Module

during this module, the information homeowners ought to be able to transfer the files. The files area unit encrypted before the files area unit uploaded to the cloud. the information homeowners area unit provided associate choice to enter the keywords for the file that area unit uploaded to the server. These keywords area unit used for the compartmentalization purpose that helps the search come values terribly quickly. These files once once offered on the cloud, the information users ought to be able to search victimisation keywords. the information homeowners also will be supplied with a call for participation approval screen so able to approve or reject the request that are received by the information users. The file before transfer can have to be compelled to be encrypted with a key so the information users cannot simply transfer it while not this key. This key are going to be requested by the information users through the trap-door. The coding of those files uses RSA algorithmic rule so unauthorized users won't be able to transfer these files.

iv. File transfer &amp; decipherment Module:

information users area unit users on this method, United Nations agency are going to be able to transfer files from the cloud that area unit uploaded by the information homeowners. Since the files keep on the cloud server may be in immense numbers, there's a groundwork facility provided to the user. The user ought to be able to do a multi-keyword search on the cloud server. Once, the result seems for the particular search, the users ought to be able to send a call for participation to the several information homeowners of the file through the system (also known as trap-door request) for downloading these files. the information users also will be provided a call for participation approval screen, wherever it'll send word if the information owner has accepted or rejected the request. If the request has been approved, the users ought to be able to transfer the decrypted file. The file before transfer can have to be compelled to be decrypted with a key. This key are going to be requested by the information users through the trap-door request. Once the key's provided throughout the transfer, the information users are going to be able to transfer the file and use them.

v. Rank-Search Module:

This module permits the information users to look the files with multi-keyword rank looking. This model uses the oft used rank looking algorithmic rule for gift the output for multi-keywords. "Coordinate Matching" principle are going to be adopted for the multi-keyword looking. This module additionally takes care of making associate index for quicker

IV. CONCLUSION AND FUTURE WORK

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. Moreover, we show that our approach is computationally efficient, even for large data and keyword sets.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS, January 2010, LNCS. Springer, Heidelberg.

[3] A. Singhal, "Modern information retrieval: A brief overview," IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 35–43, 2001.

[4] I. H. Witten, A. Moffat, and T. C. Bell, "Managing gigabytes: Compressing and indexing documents and images," Morgan Kaufmann Publishing, San Francisco, May 1999.

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, Oct. 2006, pp. 79–88.

[6] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, Jun. 2004, pp. 31–45.

[7] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted

cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253–262.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM'11, Shanghai, China, Apr. 2011, pp. 829–837

[9] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFOCOM'10, San Diego, CA, Mar. 2010, pp. 1–5.

[10] 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.

[11] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. S. III, "Public key encryption that allows pir queries," in Proc. of CRYPTO, 2007.

Rathod Gopal Somlal Currently doing M.Tech in Computer Science & Engineering at BALAJI INSTITUTE OF ENGINEERING SCIENCES-NARSAMPET, Warangal, India. Research interests include Networks, Mobile Computing etc.,

Vishnu Prasad Goranthala Completed Master of Technology in Computer Science and Engineering from JNTU Hyderabad. Currently working as an Associate Professor at Balaji Group of Institutions, Narsampet, Warangal, and has 13+ years of experience in Academic. His research areas include Information Security, Mobile and Cloud computing, Cryptography, Network Security etc.,