Secure Ranked Multi-Keyword Search in Encrypted Cloud Data

[1] J.Rajender,[2] S.Sandhya, [3]P.Srinivas Rao
[1]M.Tech ,SE, Jayamukhi Institute Of Technological Sciences,Warangal,India
[2]Assistant professor,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India
[3]Associate professor,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India

Abstract:
There are many Fine-grained multikeyword search schemes over encrypted cloud data. Our innovative contributions are three-fold. First, we start the appliance scores and partiality motives upon keyword that facilitate the sure keyword search and changed shopper familiarity. We tend to auxiliarly take the non-public subdictionaries method to accomplish higher effectiveness on index structure, trapdoor producing and question. Lastly, we tend to summary the sanctuary of the projected schemes in stipulations of discretion of credentials, privacy fortification of manifestation and trapdoor, and unlink capability of trapdoor. Through common experiments utilising the actual-world dataset, we tend to ensure the live performance of the projected schemes. Both the safekeeping analysis and tentative outcomes categorical that the projected schemes will accomplish the equal safety level scrutiny to the presented ones and higher events in phrases of performance, question complication and competence.

Keywords: Searchable encryption, Multikeyword, Fine-grained, Cloud computing.

I. INTRODUCTION

Transmitting the info to the cloud servers. the info secret writing, although, would considerably decrease the usability of {data|of knowledge} rattling to the quality of penetrating over the encrypted data primarily encrypting the records ought to still groundwork completely different sanctuary problems. as an example, Google Search makes use of SSL (secure Sockets Layer) to encipher the organization among search client and Google server once steer, paying homage to credentials and emails, show up within the search outcome. However, if the explore user clicks into a distinct web site as of the search penalties page, that electronic computer is additionally skilful to reason the explore terms that the user has impaired. Firstly, the statistics man of affairs needs to provide varied key terms in step with the outsourced information. These key terms area unit then encrypted and hold on at the cloud server. once a explore person needs to admission the outsourced information, it will decide upon some appropriate keywords and send the nothing text of the popular keyword phrases to the cloud server. The cloud server then makes use of the cipher text to healthy the outsourced encrypted key terms, and at last returns the matching outcome to the search user. to achieve the similar search potency and preciseness over encrypted information as that of plaintext keyword search, associate massive body of study has been developed in literature. recommend a multi-keyword text content search theme that considers the connectedness many keywords and makes use of a flat tree method to attain effective search question. Yu et al. recommend a multi-keyword top-okay retrieval theme that uses totally similarity secret writing to encipher the index/trapdoor and ensures excessive security. Cao et al. Advocate a multi-keyword hierarchal search (MRSE), that applies coordinate portable computer because the key phrase matching rule, i.e., come back information with the foremost matching keywords. Though several search functionalities had been developed in previous literature nearer to specific and economical searchable secret writing, it's still difficult for searchable secret writing to get the identical user expertise as that of the plaintext search, like Google search. The connectedness many keyword phrases will enable further precise back results, and therefore the choice reasons of keywords represent the importance of keywords within the search key phrase set specific with the help of search users and correspondingly permits personal search to cater to such as person preferences. It thus further improves the hunt functionalities and person experience.

II. LITERATURE SURVEY:

B. Wang, S. Yu, W. Lou, and Y. T. Hou, Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud.

Enabling keyword search directly over encrypted data is a desirable technique for effective utilization of encrypted data outsourced to the cloud. Existing solutions provide multi-keyword exact search that does not tolerate keyword spelling error, or single keyword fuzzy search that tolerates typos to certain extent. The current fuzzy search schemes rely on building an expanded index that covers possible keyword misspelling, which lead to significantly larger index file size and higher search complexity. In this paper, we propose a novel multi-keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. Our proposed scheme achieves fuzzy matchingthrough algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionary and effectively supports multiple keyword fuzzy search without increasing the index or search complexity.

C. Wang, N. Cao, K. Ren, and W. Lou, Enabling secure and efficient ranked keyword search over outsourced cloud data

Cloud computing economically enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data have to be encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords, they support only Boolean search and are not yet sufficient to meet the effective data utilization need that is inherently demanded by large number of users and huge amount of data files in cloud. In this paper, we define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Specifically, we explore the statistical measure approach, i.e., relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. The resulting design is able to facilitate efficient server-side ranking without losing keyword privacy.

C. Orencik, M. Kantarcioglu, and E. Savas, A practical and secure multi-keyword search method over encrypted cloud data

Cloud computing technologies become more and more popular every year, as many organizations tend to outsource their data utilizing robust and fast services of clouds while lowering the cost of hardware ownership. Although its benefits are welcomed, privacy is still a remaining concern that needs to be addressed. We propose an efficient privacy-preserving search method over encrypted cloud data that utilizes minhash functions. Most of the work in literature can only support a single feature search in queries which reduces the effectiveness. One of the main advantages of our proposed method is the capability of multi-keyword search in a single query. The proposed method is proved to satisfy adaptive semantic security definition. We also combine an effective ranking capability that is based on term frequency-inverse document frequency (tf-idf) values of keyword document pairs.

W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, Secure ranked multi-keyword search for multiple data owners in cloud computing

With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches over encrypted cloud data has motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with privacy preserving ranked multi-keyword search in a multi-owner model (PRMSM). To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, 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. 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. Furthermore, PRMSM supports efficient data user revocation.

III. SYSTEM ARCHITECTURE

Cloud Setup Firstly, we have to setup data owner and cloud server. So the data owner will then push the data into the cloud servers . When users outsource their confidential data onto the cloud, the cloud service providers are capable to control and check the data and the communication between users and the cloud will be secured. Cryptography cloud Storage Secondly, while the data is uploaded into the Estorage and retrieve services. Since data may have confidential information, the cloud servers cannot be fully hand over in protecting data. For this cause, outsourced files must be encrypted. Any kind of information leakage that would change data privacy are regarded as Unacceptable Vector Model We used a series of searchable symmetric encryption systems that have been allowing search on cipher text. In the earlier, files are ranked only by the number of get back keywords, which damage search correctness

As seemed in Fig. 1, we remember a framework contains of three elements.

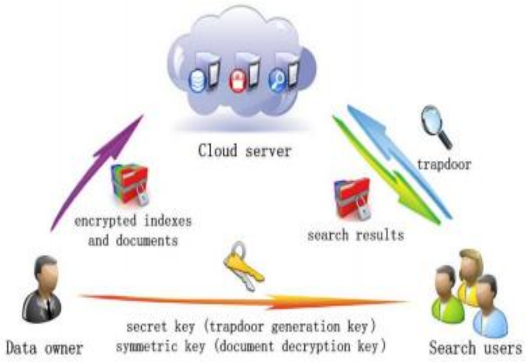

Fig. 1. System model

•**Data owner:** The data owner outsources her data to the cloud for priceless and stable data entry to the pertaining to search clients. To make certain the data privacy, the understanding proprietor encodes the first know-how through symmetric encryption. To increase the pursuit efficiency, the data owner produces a few keywords for each and every outsourced archive. The relating report is then made by way of keywords and a secret key. After that, the data owner sends the encoded records and the referring to files to the cloud, and sends the symmetric key and secret key to inquiry clients.

•**Cloud server**: The cloud server is a core of the road element which outlets the scrambled documents and relating records that are gotten from the data owner, and offers data access and search services to inquiry customers. At the point when a search client sends a keyword trapdoor to the cloud server, it would provide again an accumulation of coordinating files in view of specific operations.

•**Search user**: An inquiry client inquiries the outsourced records from the cloud server with taking after three levels. To with, the search purchaser gets each the secret key and symmetric key from the data owner. Secondly, as indicated by means of the keywords, the search client makes use of the secret key to supply trapdoor and sends it to the cloud server. Final, she will get the coordinating archive gathering from the cloud server and unscrambles them with the symmetric key.

A. Security requirements

In the EMRS, we remember the cloud server to be curious but honest which means that it executes the task assigned via the info proprietor and the hunt person adequately. Nonetheless, it's curious in regards to the knowledge in its storage and the received trapdoors to obtain further understanding. Furthermore, we recall the knowing background mannequin in the EMRS, which permits the cloud server to understand more background expertise of the records comparable to statistical understanding of the key phrases.

Above all, the EMRS ambitions to furnish the next four security standards:

• **Confidentiality of files and Index**: Records and index will have to be encrypted before being outsourced to a cloud server. The cloud server must be prevented from snooping into the outsourced files and cannot deduce any associations between the files and keywords using the index.

• **Trapdoor privacy**: On the grounds that the quest person would favor to maintain her searches from being exposed to the cloud server, the cloud server will have to be prevented from knowing the precise key words contained in the trapdoor of the search person.

• **Trapdoor Unlinkability**: The trapdoors must no longer be linkable, because of this the trapdoors will have to be absolutely exclusive despite the fact that they incorporate the identical keywords. In other words, the trapdoors will have to be randomized instead than decided. The cloud server are not able to deduce any associations between two trapdoors.

• **Concealing access pattern of the Search user:** Access pattern is the sequence of the searched outcome. Within the EMRS, the access sample should be wholly concealed from the cloud server. Notably, the cloud server can't learn the complete number of the documents stored on it nor the dimensions of the searched document even when the hunt user retrieves this report from the cloud server.

IV. CONCLUSION:

Our planned schema defines that a unique secure and effective theme for k-NN question on codeed cloud data wherever the necessary factor knowledge of information man of affairs to encrypt and decipher outsourced knowledge won't be totally disclose data to any question user. So, our theme will expeditiously aid the relaxed okay-NN question on encrypted cloud knowledge even once question customers square measure sometimes not unhazardous enough. now not handiest that the schema can defend any applied math data on the easy text (data) against assault

References

[1] Zhihua Xia,Xinhui Wang, Xingming Sun, Qian Wang, A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data IEEE Transactions on Parallel and Distributed Systems,2015

[2] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 451–459.

[3] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S&P2000. Proceedings. 2000 IEEE Symposium on*. IEEE, 2000, pp. 44–55.

[4] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in *IEEE INFOCOM*, 2014.

[5] 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.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *IEEE INFOCOM*, April 2011, pp. 829–837.

[7] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM, 2013, pp. 71–82.

[8] https://support.google.com/websearch/answer/173733?hl=en.

[9] C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multi-keyword search method over encrypted cloud data," in *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*. IEEE, 2013, pp. 390–397.

[10] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in *Dependable Systems and Networks (DSN), 2014 44th AnnualIEEE/IFIP International Conference on*. IEEE, 2014, pp. 276–286.