Enabling Data User Authentication and Revocation by an Efficient Authentication Protocol

K. Himaja¹, I. Siva Lakshmi²

¹PG Scholar, Dept of CSE, Vaagdevi Institute of Technology & Science, Proddatur, Kadapa(Dt), AP, India.
²Assistant Professor, Dept of CSE, Vaagdevi Institute of Technology & Science, Proddatur, Kadapa(Dt), AP, India.

Abstract: To protect information privateness, customers need to encrypt the facts before outsourcing to the cloud, which makes the records utilization, along with facts retrieval, a challenging challenge. It is hence suited to allow the hunt carrier over encrypted cloud facts for helping effective & efficient information retrieval over a huge quantity of information customers & files inside the cloud. Existing approaches on encrypted cloud facts search both recognition on unmarried keyword search or multi keyword come to be inefficient when a big amount of files are present, & for this reason have little assist for the efficient multi-key-word search. In this paper, we are imposing fuzzy search on multi-owner version over encrypted cloud records. By implementing this fuzzy search, cloud users can get the accurate outcomes regarding given query.

Keywords: Multi-Keyword Search, Fuzzy Keyword Search, Cloud Computing.

I. INTRODUCTION

The increasing popularity of cloud store services has lead agencies that take care of critical information to think about the usage of those offerings for his or her store wishes. Medical document databases, strength system, historical statistics & monetary facts are a few examples of vital records that would be moved to the cloud. However, the reliability & protection of information stored in the cloud nonetheless stay most important concerns. DEPSKY, a gadget that improves the supply, integrity & confidentiality of statistics saved inside the cloud thru the encryption, encoding & replication of the facts on diverse clouds that form a cloud-of-clouds. It deployed the system using four business clouds & used Planet lab to run customers accessing the service from one-of-a-kind international locations. The protocols stepped forward the perceived availability and, in maximum instances, the get right of entry to latency when as compared with cloud vendors in my view. Moreover, the economic charges of using DEPSKY in this situation are two times the fee of the use of a single cloud, that's most reliable & appears to be an inexpensive price, given the benefits. Nevertheless, enabling the key-word search over encrypted data isn't always an smooth project. Some strategies permit the user to search over encrypted records securely via single keyword to retrieve files of interest. This is insufficient as many users may additionally generally tend to offer multiple key phrases rather than one as their search interest. Recently, strategies have been proposed for a couple of key-word search in cloud computing. In these techniques, a binary index vector desires to be built for each report & each bit denotes whether the corresponding key-word is included in the file.

The storing & updating index may be of substantial overhead, in particular whilst the range of keywords is huge. Thus, the performance of relaxed more than one keyword search has big room for improvement for enhancing the gadget usability in cloud computing. Traditional searching mechanisms offer Boolean search to look over encrypted information, which is not relevant while the variety of customers & the wide variety of records documents saved in the cloud, is big. They also impose fundamental problems, one being the post-processing that has to be achieved by the users to locate the relevant document in want & the alternative is the network traffic that is unwanted in present situation while all the documents matching with key phrases is retrieved. To date, efficient multi-keyword fuzzy search over encrypted records remains a tough hassle. We need to factor out that the efforts on search over encrypted statistics contain no longer handiest information retrieval techniques together with superior facts systems used to represent the searchable index, & green search algorithms that run over the corresponding facts shape, however additionally the right layout of cryptographic protocols to make sure the safety & privacy of the overall system. Although multi-keyword search & fuzzy search had been implemented one after the other, a mixture of the two does not cause a relaxed & green multi-keyword fuzzy search scheme. In this paper, we propose a contemporary idea for reaching multi-key-word (conjunctive keywords) fuzzy search. Different from present multi-key-word search schemes, our scheme removes the requirement of a predefined keyword dictionary. The fuzziness of the keyword is captured by a modern information shape & algorithmic layout without increasing the keyword index, & therefore famous an excessive efficiency in phrases of computation & storage.
II. RELATED WORK
Since Song et al seminal paintings on searchable encryption, lots effort has been made to design powerful & efficient mechanisms to enable search over encrypted records. Instead of a phrase-with the aid of-word linear test in the complete textual content search, early works built various styles of comfy index & corresponding index-primarily based keyword-matching algorithms to improve seek performance. All those works most effective guide the search of single keyword. Subsequent works extended the search functionality to multiple, conjunctive or disjunctive, keywords search. However, they assist best precise key-word matching. Misspelled keyword phrases within the question will result in wrong or no matching. Zhiyong Xu, Wansheng Kang, Ruixuan Li, KinChoong Yow, & Cheng-Zhong Xu offered a feasible solution for multikeyword ranked query challenges over encrypted information inside the cloud surroundings. They first described the trouble, analyzed the prevailing solutions & designed a novel algorithm referred to as MKQE to deal with the troubles. MKQE used a partitioned matrices technique. When the quantity of encrypted statistics increases & greater key phrases need to be brought, the looking infrastructure may be evidently elevated with the minimal overhead. They additionally designed a new trapdoor technology set of rules, that may solved the out-of-order trouble within the back result set without dropping the information protection & privateness belongings. Furthermore, the weights of the keywords are taken into consideration in the rating set of rules when producing the query result. The DC has high possibility to retrieve the files they actually wanted. The simulation experiments verify that their technique accomplished better overall performance with a first-class security stage.

In public-key encryption with key-word search (PEKS), a proxy server, who responds the keyword queries of a receiver, can realize the content material of key phrases by using implementing KGA. Moreover, it's miles green underneath the realistic circumstance that the scale of the keyword area isn't more than the polynomial degree. In order to resist in opposition to KGA, P. Xu, H. Jin, Q. Wu, & W. Wang novelty described public-key encryption with fuzzy keyword search (PEFKS) & its IK-NCK-KGA protection. & they proposed two widespread differences from IBE to PEFKS below exceptional conditions. Under the circumstance that the keyword space has uniform distribution, they proposed a SS-CKA & IK-NCK-KGA comfy transformation PEFKS-UD, & provided an example based totally on BF01 scheme. Under the situation that the keyword area has non-uniform distribution, they proposed every other SS-CKA & IK-NCK-KGA relaxed transformation PEFKS-ND, & provided two methods to type keywords, which is the key to understand PEFKS-ND. Beyond the perspective of cryptosystem, we mentioned the biased advantage of KGA on PEFKSND, that's prompted most effective by the non-uniform distribution of the keyword area. We remove darkness from that the biased gain has been decreased as a whole lot as feasible. So they made PEFKS-ND comfy in a large sense. L. Ballard, S. Kamara, & F. Monrose presented two protocols for conjunctive look for which it's far provably tough for the server to differentiate among the encrypted key phrases of documents of its very own selecting. Their protocols permit secure conjunctive search with small talents. Their work most effective partially solved the trouble of relaxed Boolean seek on encrypted data. In precise, a entire answer requires the potential to do disjunctive keyword seek securely, both across & within keyword fields.

II. FRAMEWORK
A. Overview of Proposed System
We recommend Privacy keeping Ranked Multi-keyword Search in a Multi-owner model(PRMSM) to save you the attackers from eavesdropping secret keys & pretending to be prison records users submitting searches. As a result, attackers who steal the secret key & perform illegal searches would be easily detected. Furthermore, whilst we need to revoke a statistics consumer, PRMSM ensures efficient information person revocation. The PRMSM retrieve files based totally on actual keyword suit best however Fuzzy keyword search approach extends this selection via supporting commonplace typos & format inconsistencies that happens when the consumer types the key phrases. The statistics privacy this is maintained in the course of genuine key-word seek is ensured while this method is used. Wild card based totally approach is used to create green fuzzy key-word sets which might be used for matching applicable documents. The seek end result this is provided is based on a fuzzy keyword data set this is generated every time the precise suit seek fails. Fuzzy key-word system is formalized to remedy the hassle of supporting efficient but privateness preserving fuzzy searchfor accomplishing powerful usage of remotely stored encrypted records in multicloud Computing as shown in Fig.1.

Fig1. Proposed System Overview.

Fuzzy key-word search, opposing to exact keyword suit, tolerates minor typos & layout inconsistencies in consumer search request, & significantly complements gadget usability & person looking enjoy.

B. Trapdoor Generation
To make the information users generate trapdoors securely, conveniently & efficiently, our proposed scheme has to satisfy two main situations. First, the records user does now not need to ask a large amount of records owners for secret
Enabling Data User Authentication and Revocation by an Efficient Authentication Protocol

keys to generate trapdoors. Second, for the equal key-word, the trapdoor generated whenever should be exclusive. To meet this condition, the trapdoor technology is carried out in two steps: First, the facts consumer generates trapdoors primarily based on his search key-word & a random variety. Second, the management server re-encrypts the trapdoors for the authenticated facts person.

C. User Authentication

To prevent attackers from pretending to be prison records customers performing searches & launching statistical assaults primarily based on the search result, data users should be authenticated earlier than the administration server re-encrypts trapdoors for statistics customers. Traditional authentication techniques often observe three steps: First, data requester & information authenticator percentage a secret key; second, the requester encrypts his individually identifiable records the use of secrete key & sends the encrypted statistics to the authenticator. Third, the authenticator decrypts the acquired records with secrete key & authenticates the decrypted facts.

IV. EXPERIMENTAL RESULTS

In this experiment, we are taking multiple owners & data users. We have one cloud server which is stored the uploaded files.

In this experiment, we implemented user revocation along with user authentication to search & download an encrypted file from the cloud server. The searching will be done by using the fuzzy keyword search. By implementing fuzzy search the cloud users can get the optimal searched results as shown in Fig.2. We can observe the searched keyword size for every data owner in the cloud as shown in Fig.3.

V. CONCLUSION

We conclude that in this paper, we extended the previous Privacy preserving Ranked Multi-keyword Search in a Multi-owner model by adding fuzzy keyword search. This extended searching scheme can greatly enhances system usability along with user searching experience. We also implemented user revocation technique as well user authentication technique to improve the cloud data security.

VI. REFERENCES

Author's Profile:

K. Himaja is currently pursuing her M.Tech (CSE) Computer Science And Engineering Department, Vaagdevi Institute of Technology And Science Engineering College, Kadapa, A.P. She received her B.Tech in Computer Science and Engineering, Department from Vaagdevi Institute of Technology And Science, Proddatur.

I. Siva Lakshmi is currently working as an Asst Professor in Computer Science And Engineering Department, Vaagdevi Institute of Technology and Science, Proddatur, Kadapa. Her research includes cloud computing, networking and data mining.