International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 4 – APRIL 2018.

Reranked Keyword Search Access Control in Secured Cloud

Hemanth G[#1] , Kiran M B[#2], Mohan Kumar H L[#3], Rakesh M [#4] and Seema Kousar R[*5]

[#] *U.G.Students, Department of Computer Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India*

[*] *Assistant Professor, Department of Computer Science Engineering, The National Institute of Engineering, Mysuru, Karnataka, India*

***Abstract*— In this paper, we study the problem of keyword search with access control over encrypted data in cloud computing. We first propose a scalable framework where user can use his attribute values and a search query to locally derive a search capability, and a file can be retrieved only when its keywords match the query and the user's attribute values can pass the policy check. Using this framework, we propose a novel scheme called RKSAC, which enables Reranked Keyword Search Access Control In Secured Cloud. RKSAC utilizes a recent cryptographic primitive called CP-ABE to enforce fine-grained access control and perform multi-field query search. Meanwhile, it also supports the search capability deviation, and achieves efficient access policy update as well as keyword update without compromising data privacy. To enhance the privacy, RKSAC also plants noises in the query to hide users' access privileges.**

***Index Terms*— Reranked Keyword Search, Access Control, Encrypted Data, CP-ABE (Cipher Policy - Attribute Based Encryption).**

I. INTRODUCTION

In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, Storage-as-a-Service offered by cloud service providers (CSPs) emerged as a solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage. Since the data owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. For verifying data integrity over cloud servers, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites. A number of PDP protocols have been presented to efficiently validate the integrity of data. Proof of retrievability was introduced as a stronger technique than PDP in the sense that the entire data file can be reconstructed from portions of the data that are reliably stored on the servers. In another factor Encryption is a commonly used method to preserve data confidentiality. However, traditional plaintext keyword search demands to retrieve all the encrypted data files from the cloud, and perform search after data decryption. This methodology is extremely unpractical for traditional networks, especially for the wireless network (e.g., wireless sensor network and mobile network) seriously constrained by resources like energy, bandwidth, and computation capability.

A. Existing System

Commonly, traditional access control techniques assume the existence of the data owner and the storage servers in the same trust domain. This assumption, however, no longer holds when the data is outsourced to a remote CSP, which takes the full charge of the outsourced data management, and resides outside the trust domain of the data owner. CSP needs to be safeguarded from a dishonest owner, who attempts to get illegal compensations by falsely claiming data corruption over cloud servers. This concern, if not properly handled, can cause the CSP to go out of business.

B. Proposed System

In our proposed system, we propose a scheme that addresses important issues related to outsourcing the storage of data, namely dynamic data, newness, mutual trust, and access control. The remotely stored data can be not only accessed by authorized users, but also updated and scaled by the owner. After updating, authorized users should receive the latest version of the data (newness property), i.e., a technique is required to detect whether the received data is stale. Mutual trust between the data owner and the CSP is another imperative issue, which is addressed in the proposed scheme. A mechanism is introduced to determine the dishonest party, i.e., misbehavior from any side is detected and the responsible party is identified. Last but not least, the access control is considered, which allows the owner to grant or revoke access rights to the outsourced data.

II. ARCHITECTURAL DIAGRAM AND WORKING OF THE PROPOSED SYSTEM

Below information gives a brief knowledge about architectural diagram shown in fig-1 and detailed working of the proposed system.

A. *System Model*

We consider a cloud-data-sharing system consisting of four entities, i.e., data owners, authority, data users and cloud server. Data owners create data files, design the encrypted indices containing both keywords and access policy for each file, and upload the encrypted files along with the indices to the cloud server. Authority is responsible to authenticate user's identity. It issues a set of keys as a credential to represent user's attribute values. Data user generates a search capability according to his credential and a search query, and of attribute fields.

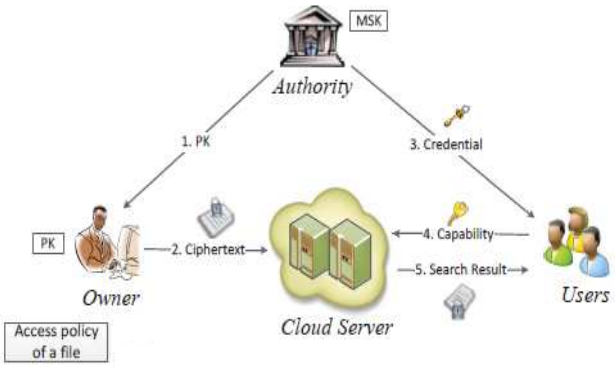

Fig -1: Architectural diagram of proposed system

The framework of RKSAC. P K is the public keys, and M SK is the master secret key that should be securely kept. Credential is the set of keys standing for user's attribute values. Search capability is generated by using user's credential and his interested query.

B. *Threat Model*

Like many previous SE schemes the cloud server is assumed to be "honest but curious". It means that the server will honestly execute the pre-defined protocol, but it is also "curious" to learn the information in terms of index, user's query and attribute values. Besides, the authority is assumed to be honest to generate user's credential according to his possessed attribute values.

C. *Design Goals*

Data Confidentiality and Index Privacy: The data confidentiality should be protected against the cloud server and unauthorized users. Index privacy indicates the cloud server should be unaware of the attribute values in access policy and the keywords embedded in the index. Fine-grained Access Control and Multi-Field Key-word Search: The system should support fine-grained access policy and multi-field keyword search. In this paper, we mainly consider the access policy and the search query in Conjunctive Normal Form (CNF) over multiple fields. Efficiency: The system should promise the efficiency for general operations in practical environment, such as search and search capability derivation. Adaption to Frequent Updates: To cope with the scenario with frequent updates, either to access policy or to keywords, the system should provide an efficient update strategy.

III. CONCLUSION

In this paper, we propose a scalable framework that allows users to locally derive the search capability by utilizing both their credentials and a search query. We then utilize HPE to realize this framework and present RKSAC. RKSAC realizes the fine-grained access control and multi-field keyword search, enables efficient update of both access policy and keywords, and protects user's access privacy. The results show that RKSAC just needs 1.08 sec for per-capability generation, and takes 0.12 sec for per-index match judgment.

IV. ACKNOWLEDGEMENT

We take this opportunity to thank our guide Assistant Professor Ms. Seema Kousar R for giving us all the guidance and support. We would also like to thank our college NIE, Mysuru for their support and encouragement.

REFERENCES

[1] Zhangjie Fu, Xinle Wu, Chaowen Guan, Xingming Sun, and Kui Ren. Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Transactions on Information Forensics and Security, 11(12):2706–2716, 2017.

[2] Zhihua Xia, Xinhui Wang, Xingming Sun, and Qian Wang. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 27(2):340– 352, 2016.

[3] Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, and Fengxiao Huang. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Transactions on Parallel and Distributed Systems, 27(9):2546–2559, 2015.

[4] Fu Zhangjie, Sun Xingming, Liu Qi, ZHOU Lu, and SHU Jiangang. Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Trans-actions on Communications, 98(1):190–200, 2015.

[5] Zhirong Shen, Jiwu Shu, and Wei Xue. Keyword search with access control over encrypted data in cloud computing. In Proc. of IEEE/ACM IWQoS, 2014.