International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 30h Nov 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-12

Title: EFFICIENT DATA OWNER AUTHORIZED SEARCH OVER ENCRYPTED CLOUD DATA

Volume 07, Issue 12, Pages: 693–698.

Paper Authors

ANUGULA SREENIVASULU, B.SIVAKUMAR
SIR C.V. RAMAN Institute of Technology & Science, AP, India

.
.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

EFFICIENT DATA OWNER AUTHORIZED SEARCH OVER ENCRYPTED CLOUD DATA

ANUGULA SREENIVASULU[1], B.SIVAKUMAR[2]
[1]PG Scholar, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, India
[2] Assistant Professor, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, India

ABSTRACT: In this paper, we ponder the issue of catchphrase look with access authority over encoded information in distributed computing. We initially propose an adaptable system where client can utilize his quality qualities and an inquiry question to locally determine a pursuit ability, and a document can be recovered just when its catchphrases coordinate the question and the client's characteristic qualities can pass the approach check. Utilizing this structure, we propose a novel plan called KSAC, which empowers Keyword Search with Access Control over encoded information. KSAC uses an ongoing cryptographic crude called HPE to uphold fine-grained get to control and perform multi-field inquiry look. In the mean time, it likewise underpins the hunt ability deviation, and accomplishes effective access arrangement refresh and additionally watchword refresh without trading off information protection. To improve the security, KSAC additionally plants clamors in the question to shroud clients' entrance benefits. Concentrated assessments on true dataset are directed to approve the materialness of the proposed plan and exhibit its assurance for client's entrance benefit.

I. INTRODUCTION

The cloud has become an important platform for data storage and processing. It centralizes essentially unlimited resources (e.g., storage capacity) and delivers elastic services to end users. However, a number of challenges, including concerns about data security and users' privacy, still exist [2]–[5]. For example, a user's electronic health records are sensitive data and, if uploaded into the cloud, should not be disclosed to the cloud administrators and any other unauthorized users without data owners' permission. Thus data confidentiality protection (to hide the plaintext against unauthorized parties) and data access control (to grant user's access privilege) are usually required when storing data onto the cloud. 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 [6], [7].Aiming at enabling secure and efficient search over encrypted data, Searchable Encryption (SE) (e.g., [6]–[15]) receives increasing attentions

in recent years, in which a query is encrypted as a search capability and a cloud server will return files matching the query embedded in the capability, without having to know the keywords both in the capability and in file's encrypted index. The first symmetric-key-based searchable encryption scheme is proposed by Song et al. [10]. After that, Goh et al. [13] presented secure indexed over encrypted data by employing Bloom Filter. To securely process the retrieved files and make them more conform to users request, Wang et al. [11] introduced secure ranked keyword search based on "order-preserving encryption [16]. In the public key setting, Boneh et al. [6] first introduced the searchable encryption scheme by using bilinear mapping [46]. Water et al. [12] fulfilled searchable audit log using symmetric encryption and IBE [17] respectively. Li et al. [18] studied the fuzzy keyword search over encrypted cloud data by utilizing edit distance. To support multiple keywords search, Golle et al. [6] considered conjunctive keyword search over encrypted data. Shi et al. [9] realized multi-dimensional range query over encrypted data. Shen et al. [19] investigated the encrypted search with preference by utilizing Lagrange polynomial and secure inner-product computation. Li et al. [20] considered authorized private keyword search. It only achieved LTA-level authorization which was far coarser than user level access control, and missed the protection of the users access privacy. Based on the uni-gram, Fu et al. [21] proposed an efficient multi-keyword fuzzy ranked search scheme with improved accuracy. To efficiently support dynamic updates, Xia et al. [22] constructed a special tree-based index structure by using vector space and TF_IDF model. Fu et al. [23] found that previous keyword-based search schemes ignored the semantic information. They then developed an semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets. Fu et al. [24] designed a searchable encryption scheme that used vector space model for multi-keyword ranked search and constructed a tree-based index to enable parallel search.

2. EXISTING SYSTEM:

Golle et al. considered conjunctive keyword search over encrypted data.Shi et al. realized multi-dimensional range query over encrypted data. Shen et al. investigated the encrypted search with preference by utilizing Lagrange polynomial and secure inner-product computation. Li et al. considered authorized private keyword search. It only achieved LTA-level authorization which was far coarser than user level access control, and missed the protection of the users access privacy. Based on the uni-gram, Fu et al. proposed an efficient multi-keyword fuzzy ranked search scheme with improved accuracy. Fu et al. found that previous keyword-based search schemes ignored the semantic information. They then developed an semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets.Most of existing SE schemes assume that every user can access all the shared files. Such assumption does not hold in the cloud environment

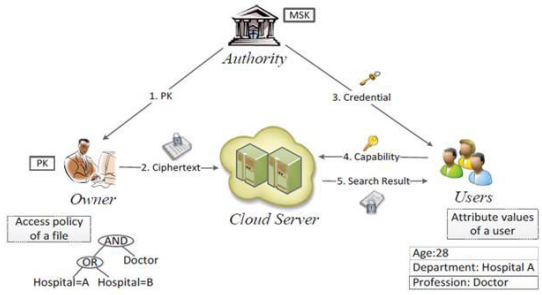
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

where users are actually granted different access permissions according to the access-control policy determined by data owners. Many of proposed SE schemes require a role, such as data owner, to handle the search capability derivation for user's interested keywords every time before search. This requirement places heavy burden on data owners and significantly compromises the system scalability. The weakness should be mitigated by allowing user to locally derive the search capability.

3. PROPOSED SYSTEM:

First, we propose a scalable framework that integrates multi-field keyword search with fine-grained access control. In the framework, every user authenticated by an authority obtains a set of keys called credential to represent his attribute values. Each file stored in the cloud is attached with an encrypted index to label the keywords and specify the access policy. Every user can use his credential and a search query to locally generate a search capability, and submit it to the cloud server who then performs search and access control. Finally, a user receives the data files that match his search query and allow his access. Second, to enable such a framework, we make a novel use of Hierarchical Predicate Encryption (HPE), to realize the derivation of search capability. Based on HPE, we propose our scheme named KSAC. This design addresses the first challenge by fully leveraging the computation power of cloud server. It also solves the second challenge by dispersing the computation burden of capability generation to the users in the system.It enables the service of both the keyword search and access control over multiple fields, and supports efficient update of access policy and keywords. KSAC also introduces some random values to enhance the protection of user's access privacy. To the best of our knowledge, KSAC is the first solution to simultaneously achieve the above goals. Finally, we fully implement KSAC and conduct extensive evaluations to demonstrate its applicability.

4. SYSTEM ARCHITECTURE:



5. IMPLEMENTATION

Users:

User's stores a great quantity of data files in the cloud can be an individual or a organization.Cloud users (data owners), who outsource their Encrypted data in clouds.Users can be relieved of the burden of storageand computation while enjoying the storage andmaintenance service by outsourcing their data into theCSP.

Cloud Service Provider:

A cloud service provider is a third-party company offering a cloud-based platform, infrastructure, and application or storage services. Much like a homeowner would pay for a utility such as electricity or gas; companies typically have to pay only for the amount of cloud services they use, as business demands require.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Besides the pay-per-use model, cloud service providers also give companies a wide range of benefits. Businesses can take advantage of scalability and flexibility by not being limited to physical constraints of on-premises servers, the reliability of multiple data centers with multiple redundancies, customization by configuring servers to your preferences and responsive load balancing which can easily respond to changing demands. Though businesses should also evaluate security considerations of storing information in the cloud to ensure industry-recommended access and compliance management configurations and practices are enacted and met. Cloud Service ProviderManages and coordinates a number of cloud servers to offer scalable and on-demand outs ourcing data services for users.

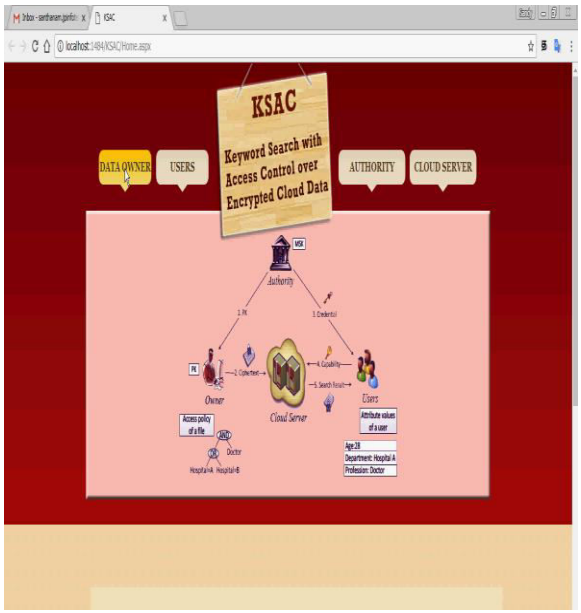
Third Party Auditor (TPA):

TPA can verify the reliability of the cloud storage services (CSS) credibly and dependably o n behalf of the users upon request.TPA is involved to check the integrity of the users data stored in the cloud.However, in the whole verification process, the TPA is notexpected to be able to learn the actual content of the user's data for privacy protection.We assume the TPA is credible but curious. In otherwords, the TPA can perform the audit reliably, but may be curious about the users data.

Dynamic Hash Table (DHT):

A hash table is a dynamic set data structure. It has three basic functions: to store data (SET/INSERT); to retrieve data (SEARCH/RETRIEVE), and to remove data that has previously been stored in the set (DELETE). In this way it is not different from other dynamic set data structure such as linked lists or trees. The interesting about hash tables is their performance characteristics with respect to the store/retrieve/remove operations. In this regard, hash tables offer average constant time to perform any combination of the basic operations. This makes them extremely useful in many scenarios where quickly searching for an element is required, especially if multiple queries must be performed.

6. SCREEN SHOTS:



7.CONCLUSION

In this paper, we propose a scalable framework that allowsusers to locally derive the search capability by utilizing boththeir credentials and a search query. We then utilize HPE torealize this framework and present KSAC. KSAC realizes thefine-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 KSACjust needs 1.08 sec for per-capability generation, and takes0.12 sec for per-index match judgement.

REFERENCES

[1] Zhirong Shen, Jiwu Shu, and Wei Xue. Keyword search with accesscontrol over encrypted data in cloud computing. In Proc. of IEEE/ACMIWQoS, 2014.

[2] Jiwu Shu, Zhirong Shen, and Wei Xue. Shield: A stackable securestorage system for file sharing in public storage. Journal of Paralleland Distributed Computing, 74(9):2872–2883, 2014.

[3] MA Tinghuai, ZHOU Jinjuan, TANG Meili, TIAN Yuan, ALDHELAANAbdullah, AL-RODHAAN Mznah, and LEE Sungyoung.Social network and tag sources based augmenting collaborative recommendersystem. IEICE transactions on Information and Systems,98(4):902–910, 2015.

[4] Yongjun Ren, Jian Shen, Jin Wang, Jin Han, and Sungyoung Lee. Mutualverifiable provable data auditing in public cloud storage. Journal ofInternet Technology, 16(2):318, 2015.

[5] Jiwu Shu, Zhirong Shen, Wei Xue, and Yingxun Fu. Secure storagesystem and key technologies. In Design Automation Conference (ASPDAC),2013 18th Asia and South Pacific, pages 376–383, 2013.

[6] Philippe Golle, Jessica Staddon, and Brent Waters. Secure conjunctivekeyword search over encrypted data. In Proc. of ACNS. Springer, 2004.

[7] Yan-Cheng Chang and Michael Mitzenmacher. Privacy preservingkeyword searches on remote encrypted data. In Applied Cryptographyand Network Security, 2005.

[8] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and GiuseppePersiano. Public key encryption with keyword search. In Proc. OfEurocrypt, pages 506–522, 2004.

[9] Elaine Shi, John Bethencourt, T-HH Chan, Dawn Song, and AdrianPerrig. Multi-dimensional range query over encrypted data. In Proc. OfIEEE Symposium on Security and Privacy., 2007.

[10] Dawn Xiaoding Song, David Wagner, and Adrian Perrig. Practicaltechniques for searches on encrypted data. In Proc. of IEEE Symposiumon Security and Privacy., 2000.

[11] Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou. Secureranked keyword search over encrypted cloud data. In Proc. of IEEEICDCS, 2010.

[12] Brent R Waters, Dirk Balfanz, Glenn Durfee, and Diana K Smetters.Building an encrypted and searchable audit log. In Proc. of NDSS,2004.

[13] Eu-Jin Goh et al. Secure indexes. IACR Cryptology ePrint Archive,2003:216, 2003.

[14] Dan Boneh and Brent Waters. Conjunctive, subset, and range querieson encrypted data. In In Proc. of TCC. Springer, 2007.

[15] Changyu Dong, Giovanni Russello, and Naranker Dulay. Shared andsearchable encrypted data for untrusted servers. Journal of ComputerSecurity, 19(3):367–397, 2011.

[16] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and YirongXu. Order

preserving encryption for numeric data. In Proc. of ACMSIGMOD, 2004.

[17] Dan Boneh and Matt Franklin. Identity-based encryption from the weilpairing. In Advances in CryptologyłCRYPTO 2001, 2001.

[18] Jin Li, Qian Wang, Cong Wang, Ning Cao, Kui Ren, and Wenjing Lou.Fuzzy keyword search over encrypted data in cloud computing. In Proc.of IEEE INFOCOM, 2010.

[19] Zhirong Shen, Jiwu Shu, and Wei Xue. Preferred keyword search overencrypted data in cloud computing. In Proc. of IEEE/ACM IWQoS,2013.

[20] Ming Li, Shucheng Yu, Ning Cao, and Wenjing Lou. Authorized privatekeyword search over encrypted data in cloud computing. In Proc. OfIEEE ICDCS, 2011.

[21] Zhangjie Fu, Xinle Wu, Chaowen Guan, Xingming Sun, and Kui Ren.Toward efficient multi-keyword fuzzy search over encrypted outsourceddata with accuracy improvement. IEEE Transactions on InformationForensics and Security, 11(12):2706–2716, 2016.