KEYWORD SEARCH WITH ACCESS CONTROL OVER ENCRYPTED CLOUD DATA

Pushpa Srivani Sureddi, Miss G.Keerthana, Sri.V.Bhaskara Murthy
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT

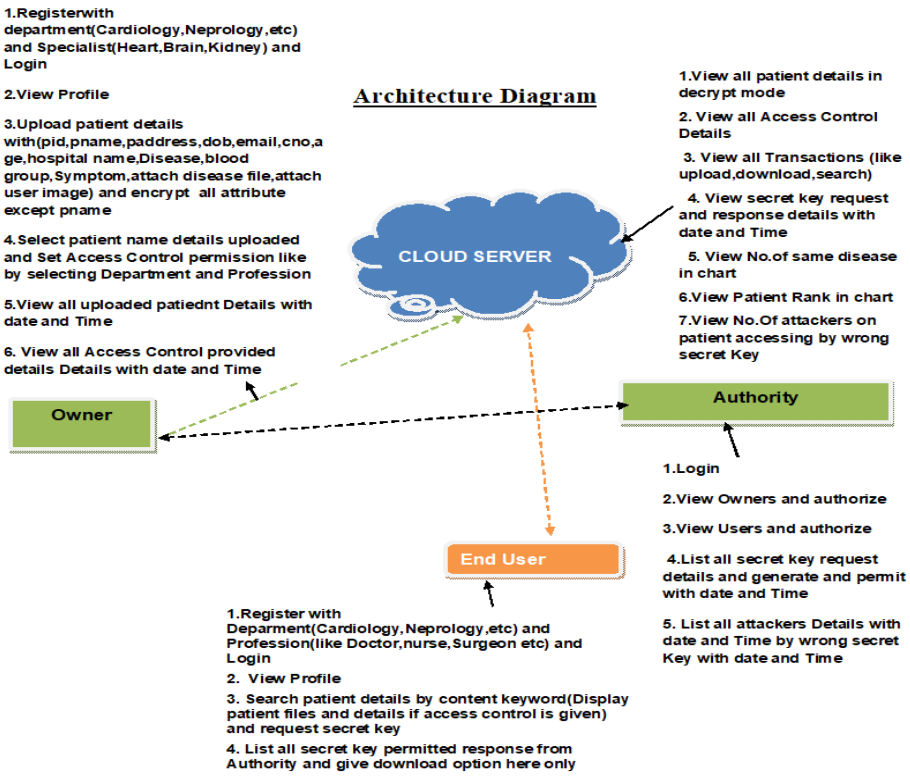
In this we study the problem of keyword search with access control (KSAC) over encrypted data in cloud computing. We first propose a scalable framework where user can use his attribute values and a search query to locally derive a search capability, and a file can be retrieved only when its keywords match the query and the user's attribute values can pass the policy check. Using this framework, we propose a novel scheme called KSAC, which enables keyword search with access control over encrypted data. KSAC utilizes a recent cryptographic primitive called hierarchical predicate encryption 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, KSAC also plants noises in the query to hide users' access privileges. Intensive evaluations on real-world dataset are conducted to validate the applicability of the proposed scheme and demonstrate its protection for user's access privilege.

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 .

II. SYSTEM ARCHITECTURE



III. EXISTING SYSTEM

- 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.

- In the public key setting, Golle et al. [6] first introduced the searchable encryption scheme by using bilinear mapping [46]. Waters 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.

Disadvantages

- There is less security due to lack of Fine-grained Access Control and Multi-Field Keyword.
- There is no Data security due to lack of encryption techniques.

IV. PROPOSED SYSTEM

- In the proposed system, the system proposes a scalable framework as shown in this system 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. 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.
- 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. 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.

Advantages

- More Security on Data due to hierarchical predicate encryption.
- More data security due to Data Confidentiality and Index Privacy.

V. 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 storage and computation while enjoying the storage and maintenance service by outsourcing their data into the CSP.

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.

- 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 Provider

  Manages and coordinates a number o f cloud servers to offer scalable and on-demand outsourcing data services for users.

Third Party Auditor (TPA):

- TPAcan verify the reliability of the c loud storage services (CSS) credibly and dependably on 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 not expected 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 other words, 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.

VI. CONCLUSIONS

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 KSAC. KSAC 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 KSAC just needs 1.08 sec for per-capability generation, and takes0.12 sec for match judgement between a search capability and an encrypted index.

REFERENCES

[1] Z. Shen, J. Shu, and W. Xue, "Keyword search with access control over encrypted data in cloud computing," in Proc. IEEE/ACM IWQoS, May 2014, pp. 87–92.

[2] J. Shu, Z. Shen, and W. Xue, "Shield: A stackable secure storage system for file sharing in public storage," J. Parallel Distrib. Comput., vol. 74, no. 9, pp. 2872–2883, Sep. 2014.

[3] M. Tinghuai et al., "Social network and tag sources based augmenting collaborative recommender system," IEICE Trans. Inf. Syst., vol. 98, no. 4, pp. 902–910, 2015.

[4] Y. Ren, J. Shen, J. Wang, J. Han, and S.-Y. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[5] J. Shu, Z. Shen, W. Xue, and Y. Fu, "Secure storage system and key technologies," in Proc. 18th Asia South Pacific Design Autom. Conf. (ASP-DAC), Jan. 2013, pp. 376–383.

[6] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. ACNS, Jun. 2004, pp. 31–45.

[7] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Berlin, Germany: Springer-Verlag, 2005.

[8] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Eurocrypt, 2004, pp. 506–522.

[9] E. Shi, J. Bethencourt, T.-H. H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 350–364.

[10] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2000, pp. 44–55.

[11] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE ICDCS, Jun. 2010, pp. 253–262.

[12] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Proc. NDSS, 2004, pp. 1–11.

[13] E.-J. Goh et al., "Secure indexes," IACR Cryptol. ePrint Arch., Tech. Rep. 2004/022, 2003, p. 216.

[14] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. TCC, 2007, pp. 535–554.

[15] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," J. Comput. Secur., vol. 19, no. 3, pp. 367–397, 2011.