s

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

IJARnD

(Volume2, Issue7)

Available online at www.ijarnd.com

Protection saving Positioned Multi-Keyword Scan for Different Information in Distributed Computing

Usha L. G[1], B. N Veerappa[2]

[1]*PG Student, Computer Science and Engineering, UBDTCE Davanagere, Karnataka, India*

[2] *Associate Professor, Computer Science And Engineering, UBDTCE Davanagere, Karnataka, India*

ABSTRACT

Observing the view of cloud computing, it has become augmenting popular for data owners to outside supplier their information to public cloud servers while allowing data users to regain this data. To relate to seclusion, safe searches over encrypted cloud data have provoke more research works under the sole owner model. However, most cloud servers in practice do not just Serve unique owner; instead, they support multiple owners to share the benefits brought by cloud computing .In this paper, we suggest -To keep safe the secrecy and several owner model search several keywords and Ranked. To make possible cloud servers to execute safe to look omission knowing the real information of both keywords and trapdoors, To keep alive the privacy of related scores between keywords and files and rank the search result, we suggest a novel Additive Order and Privacy Preserving Function family and dynamic hidden key creation rule and a new data user to establish as genuine rule.

Keyword: Cloud Computing, Ranked Keyword Several Owners, Privacy Preserving, Dynamic Hidden Keys.

1. INTRODUCTION

Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising crypto graphical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

2. EXISTING SYSTEM

We have again visit the issue of easy to search symmetric encryption, which give permeation a client to store its data on a external server in such a way that it can search without disclosing the data. We generate more affords to add new security and new work. Motivated by subtle problems in all previous security definition for SSE, we propose new definitions and point out that the existing notions have significant practical disadvantages contrary to the natural use of easy to find encryption.

Disadvantages:

- They only give the assurance to security for users that fulfill all their searches at once.

1. Proposed System

we suggest when search multiple owner multiple keywords that time provide the privacy and show the result in ranking form to make easy cloud servers to perform safe search excluding knowing the real value of both keywords and trapdoors, we properly build a novel safe search rule. So that various data owners use distinct keys to hide their files and keywords. Genuine data users can get a query excluding knowing confidential keys of these various data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we suggest a family which preserves privacy, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information. To protect from disclosing the result we propose a novel dynamic secret key generation protocol and a new data user authentication rule.

Advantages:

- We define search data on clued that data is hidden format and also providing the privacy when search the multiple keywords.

2. RELATED WORK

We again visit the issue of search symmetric encryption, which give permeation a client to store its data on external server in such a way that it can search without disclosing data. We generate more affords at add new security and new work. Motivated by subtle problems in all previous security definition for SSE,we propose new definitions and point out that the existing notions have significant practical disadvantages contrary to the natural use of easy to find encryption.[1].

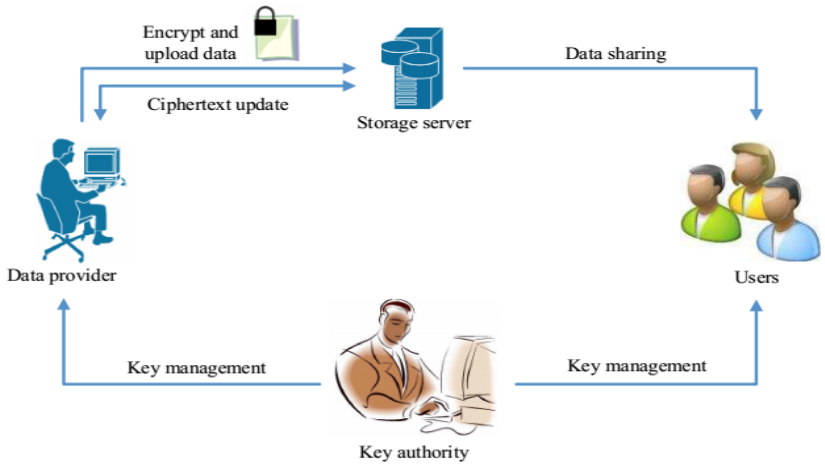

Fig1: System architecture

This architecture follows the bellow method description

Data Provider

Cloud computing is a model which enables the users for storing the data and programs and accessing them easily through an internet instead of using some hardware and software components in the computer. A cloud computing also have many definition based on their different types of models. The cloud models are classified as the deployment and service models. Cloud users will easily access the applications and data content that stored in the cloud from anywhere in the world by the financial model called as pay-as-you-go. Whenever the data is stored in the cloud there may be problem of security issues and once when the data is outsourced to cloud the cloud provider should check for the data content and the information regarding to the privacy and according to that provided information the provider must provide the security. For the purpose of security different attributes based encryption schemes are used for encryption before outsourcing the data to the cloud server.

Key Management

Cryptography is a method which is used for storing and transforming the data in the particular form so that only the intended users can read or process the data easily .Cryptography access control is a commonly used technique for the purpose of securing the data on the entrusted servers. Usually when we use this kind of servers then the sensitive data is encrypted before outsourcing the data and the decryption keys will be given only to the approved users and only by using these keys they can decrypt the data without these keys even the servers are not able to decrypt the data.When data is shared over the distributed cloud environment it can be secured by providing the aggregate key. For the particular data owners the aggregate key consists of some identity to find the perfect identifier along with the attribute based modules. This key is usually used to share the data between each other using some secret keys in between them. Key aggregation authorizes the users/data provider to share data with others in a confident way by using some small cipher text expansion, and this text can be provided to each authorized users by providing a single and small aggregate keys. These aggregate key can be sent to the authorized user through any means of communication mode secretly, the communication mode can be via email, SMS etc. This aggregate key helps the other user to decrypt the data.

Key Authority

Outsourcing is a familiar method where the third party executes some function for the sake of the company, frequently for the IT department which do not have the resources to undertake. It is an important method for the global information sharing. One of the important services in outsourcing is the database outsourcing during this process the data must be secured from the hackers.

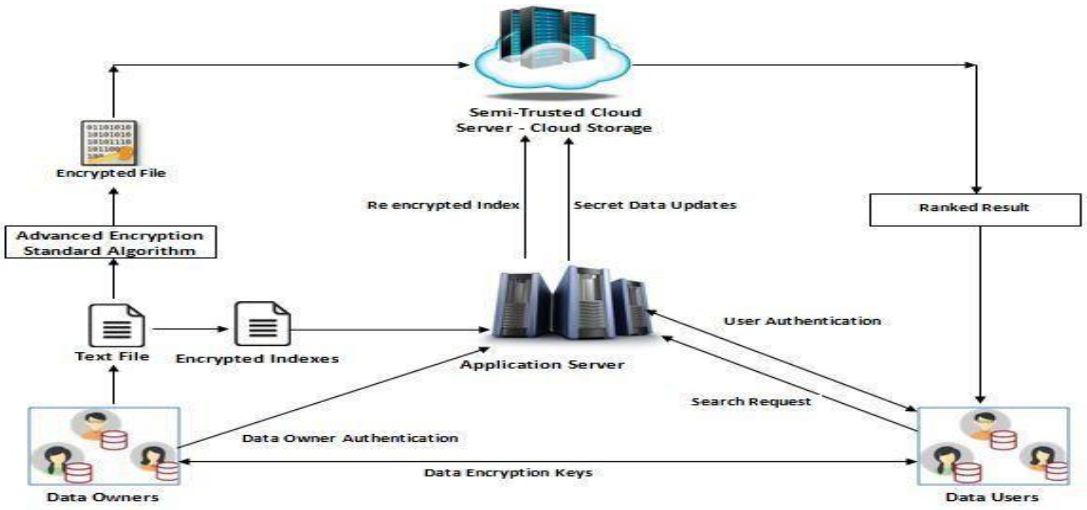

Fig 2: System Design

System Implementation consists of various modules as follows:

a. Data Owners Module
b. Cloud Server Module
c. Administration Serve Module
d. Data Users Module

a. Data Owner:

Data owners have a collection of files F. To enable efficient search operations on these files which will be encrypted, data owners first build a secure searchable index I on the keyword set W extracted from F, and then they submit index to the administration server. Finally, data owners encrypt their files F and outsource the corresponding encrypted files C to the cloud server.

b. Cloud Server:

Upon receiving the trapdoor T, the cloud server searches the encrypted index I of each data owner and returns the corresponding set of encrypted files. To improve the file retrieval accuracy and save communication cost, a data user would tell the cloud server a parameter k and cloud server would return the top-k relevant files to the data user.

c. Administration Server:

Upon receiving index, the administration server re-encrypts index for the authenticated data owners and outsources the re-encrypted index to the cloud server.

d. Data Users:

Once a data user wants to search t keywords over these encrypted files stored on the cloud server, he first computes the corresponding trapdoors and submits them to the administration server. Once the data user is authenticated by the administration server, the administration server will further re-encrypt the trapdoors and submit them to the cloud server.

3. CONCLUSION

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, 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. Moreover, we show that our approach is computationally efficient, even for large data and keyword sets.

4. REFERENCES

[1] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. ACM CCS'06*, VA, USA, pp. 79–88, Oct. 2006.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. ACM SIGMOD'04*, Paris, France, pp. 563–574, Jun. 2004.

[3] D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *EUROCRYPT*, vol. 43, pp. 506–522, 2004.

[4] Amazon.(2014)Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.