ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing

Archana P. Tupkar[1], Manjusha Jagtap[2]

ME Student, Dept. of Computer Engineering, DPCOE, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, DPCOE, Pune, India[2]

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.

KEYWORDS: Cloud computing, ranked keyword search, several owners, privacy preserving, dynamic hidden key

I. INTRODUCTION

Cloud storage system, is set of storage servers, and provides long-term storage services over the Internet. Storing data in a third party's cloud system causes grave to connect to over data secret. Normal hidden schemes defend data secret but have some limitation to functionality of the storage system because a few operations are supported over hidden information.

Building a grave storage system that compatible several functions is endurance when system is distributed. Service providers of cloud would pledge to owners data security using phenomenon like virtualization and firewalls. These phenomenon's do not protect owners data privacy from the CSP itself, since the CSP control whole of cloud hardware, software, and owners' data. Hiding the sensitive data before send outside can stored data confidentiality against CSP. Data hidden makes the conventional data utilization service based on plaintext keyword search a very challenging problem. A solution to this problem is to download all the hidden data and create the original data using the hidden key, but this is not practical cause it create extra overhead In this paper, 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[1].

The main contributions of this paper are listed as follows:

- We define search data on clued that data is hidden format and also providing the privacy when search the multiple keywords.
- We suggest an capable data user authentication rule, which stop attackers to disclose hidden key and only genuine data user can do search.
- We suggest a approach that performs multiple key word search and rank them properly.

- We suggest an Additive Order and Privacy Preserving Function family (AOPPF) which allows the cloud server produces the file that rank properly.
- We supervise experiments on real-world Datasets to verify the effectiveness and capability our suggest schemes.

II. Related work

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.[1]

Disadvantages:

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

We notice this limitation by introducing stronger definition that guarantee security even when users perform more realistic searches. Analysis give guidance to the choice the size of cipher text space . At the end suggest a unique and efficient transformation that can be applied to any OPE scheme. Our deep study shows that the transformation yields a scheme with more result safety in that the scheme oppose the one-wayness and window one-wayness attacks[2].

We opened the new way on how to get this notion, but the more efficient variant is certainly required. Second, how to construct SCF-PEKS scheme secure against keyword guessing attacks without requiring bilinear pairing operations would be very interesting[3].

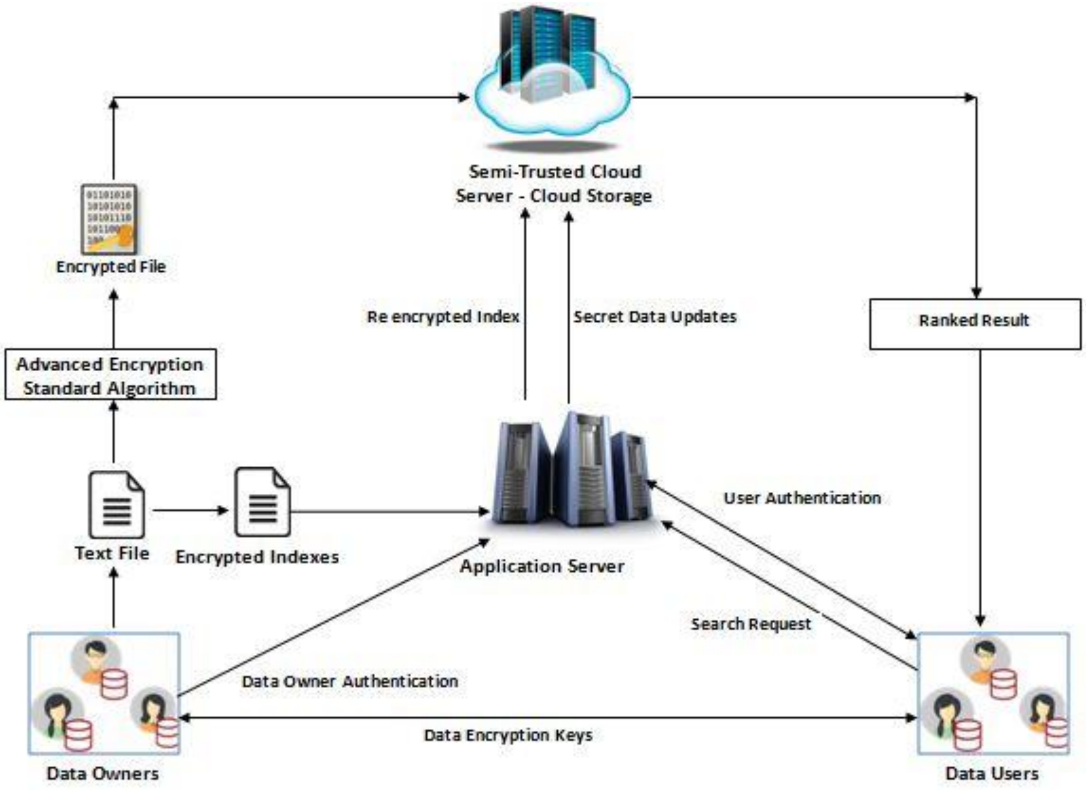

Fig1: System Architecture

System Implementation consist of various parts described as follows:
We are implementing our project by using Java Technology and MySQL database.
Various components of our system are:

1. **Data Owner**
2. **Data user**
3. **Application server**
4. **Cloud server**

1. Data Owner :

Data owner have the set of files ,they create the index file ad send that file to the application server .
Finally Data owner encrypt that file and send encrypted file to the cloud server .as a\well as send the encryption key to the data user .

2. Application server:

Application server re-encrypt the index file of authenticated user and send that re-encrypted file to the cloud server

3. Data user

Data user send keywords to search to words the application server, application server send that request to the cloud server if the data user are the authenticated user by creating the trapdoor

4. Cloud server

Upon receiving the trapdoor, the cloud server searches the encrypted index *of* each data owner and returns the corresponding set of encrypted files.

III. CONCLUSION AND FUTURE WORK

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.

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.