SECURITY ANALYSIS ON CLOUD DATA SEARCH USING ORDER PRESERVING ENCRYPTION

Shibi S[1],Dhanya D[2].

[1,] Dept of CSE, Mar Ephraem College of Engineering and Technology, Marthandam, Tamil Nadu,India.
Email:shibijegan@gmail.com

[2.] Dept of CSE,Asst.Prof, Mar Ephraem College of Engineering and Technology, MarthandamTamil Nadu, India.

Abstract- As cloud computing become more flexible and effective in terms of economy, data owners are motivated to outsource their complex data systems from local sites to commercial public cloud. Considering the large number of data users and documents in cloud, it is necessary for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. In this project, we proposed a probabilistic OPE, for applications of searchable encryption, which can flatten the distribution of the plaintexts to solve the problem of Secured Multi-keyword search (SMS) over encrypted cloud data (ECD). When using deterministic OPE, the cipher texts will reveal the distribution of relevance scores. Further it show effectively our scheme provides security and how effectively improves system performance and reduces communication overhead and also eliminates unnecessary traffic.

Keywords: cloud computing, order preserving encryption, Binary search, Multi keyword search.

I. INTRODUCTION

As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud, such as e-mails, personal health records, company finance data, and government documents, etc. It uses various computing resources that are delivered as a service over a network. These services typically provide access to advanced software applications and high-end networks of server computers. Cloud Computing focuses on maximizing the effectiveness of the shared resources. These resources are not only shared by multiple users they are also dynamically reallocated per demand. Cloud computing, also known as on-demand computing, is a kind of internet-based computing, where shared resources and information are provided to computers and other devices on- demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third- party data centers. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computingis the broader concept ofconverged infrastructure and shared services.

2 RELATED WORK

Cengiz Orenciket.al [7] proposed a novel order- preserving encryption (OPE) based ranked search scheme over encrypted cloud data, which uses the encrypted keyword frequency to rank the results and provide accurate results via two-step ranking strategy. The first step ranks the documents with the measure of coordinate matching, which is it classifies the documents according to the number of query terms included in each document.

Ruihui Zhao et.al [8] focus on addressing personalized search over encrypted cloud data [10] and proposed a Privacy-preserving Personalized Search over Encrypted Cloud Data Supporting Multi-keyword Ranking (PPSE) scheme that supports Top-k retrieval in stringent privacy requirements. For the first time, they formulated the privacy issue and design goals for personalized search in SE. Open Directory Project was proposed to construct a formal model for integrating preferential ranking with keyword search reasonably and automatically, which can help eliminate the ambiguity of any two search requests. In PPSE, vector space model and the secure kNN scheme were employed that guarantees sufficient search

Ming Li et.al [4] proposed and addressed the problem of authorized private keyword searches (APKS) on encrypted PHR in cloud computing environments. In this paper a framework was presented for searching on encrypted PHR, where users obtain query capabilities from localized trusted authorities according to their attributes, which is highly scalable. Two novel solutions for APKS was proposed based on a recent cryptographic primitive, hierarchical predicate encryption (HPE), one with enhanced efficiency and the other with enhanced query privacy. In addition to document privacy and query privacy, other salient features of these schemes include: efficiently support multi-dimensional, multiple keyword searches with simple range query, allow delegation and revocation of search capabilities.

Curtmola R.et.al [14] proposed a method searchable symmetric encryption (SSE) that allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem focused on active research and several security definitions and constructions have been proposed. In this paper existing notions of security is reviewed and proposed new and stronger security definitions. Two construction methods are proposed for security. In addition to satisfying stronger security guarantees, constructions are more efficient than all previous constructions. Further, prior work on SSE considered only the setting where the owner of the data is capable of submitting search queries. SSE is defined in this multi-user setting that present an efficient construction.

R. Agrawal et.al [15] proposed in protecting sensitive data. However, once encrypted, data can no longer be easily queried aside from exact matches. An order-preserving encryption scheme is proposed for numeric data that allows any comparison operation to be directly applied on encrypted data. Query results produced are sound i.e, no false hits and complete. The scheme handles updates gracefully and new values can be added without requiring changes in the encryption of other values. It allows standard database indexes to be built over encrypted tables and can easily be integrated with existing database systems. The proposed scheme has been designed to be deployed in application environments in which the intruder can get access to the encrypted database.

3 PROPOSED SYSTEM

To meet the effective data retrieval, the result must be returned based on some ranking criteria based on one-to many order preserving encryption(OPE). The multi ranked keyword search result improves system usability and resource, also eliminates un-necessary traffic by returning relevant and accurate result. It also improves system performance. The system architecture involves five special Models:

- **The Cloud Holder:** A person or the company, they are the Owner of the cloud.
- **The Cloud superintendent:** The responsible person, he has the right to controls over all the operations of the cloud server.
- **The cloud server:** It provides huge storage space and remote access to all its users
- **The data Holder:** Owner of the data, it may be a person or company they may have collection of data.
- **The data user:** A user or the customer, they can search, view the data.
- **Hackers:** Here Hackers are the unauthorized persons their main job is to hack the data

The advantages of this proposed system metods are, To provide a data privacy and data security, Decrease the computational overhead, Provide accurate ranked search result, Increase the communication capacity, Increase the performance by decreasing network traffic to improve the system usability.

4 PROBLEM DESCRIPTION

The fact that data owners and cloud server are no longer in the same trusted domain may put the outsourced unencrypted data at risk, the cloud server may leak data information to unauthorized entities or even be hacked. It follows network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm.

In short, lacking of effective mechanisms to ensure the file retrieval accuracy is a significant drawback of existing searchable encryption schemes in the context of Cloud Computing. Nonetheless,the state of the art in information retrieval (IR) community has already been utilizing various scoring mechanisms to quantify and rank order the relevance of files in response to any given search query .It directly outsourcing relevance scores will leak lots of sensitive frequency information against the keyword privacy, we then integrate a recent crypto primitive order-preserving symmetric encryption (OPSE) and properly modify

it to develop a one-to-many order preserving mapping technique for our purpose to protect those sensitive weight information, while providing efficient ranked search functionalities. Our contribution can be summarized as follows

1. For the first time, we define the problem of secure ranked keyword search over encrypted cloud data, and provide such an effective protocol, which fulfills the secure ranked search functionality with little relevance score information leakage against keyword privacy.
2. Thorough security analysis shows that our ranked searchable symmetric encryption scheme indeed enjoys "as-strong-as-possible" security guarantee compared to previous searchable symmetric encryption (SSE) schemes.
3. We investigate the practical considerations and enhancements of our ranked search mechanism, including the efficient support of relevance score dynamics, the authentication of ranked search results, and the reversibility of our proposed one-to-many order-preserving mapping technique.
4. Extensive experimental results demonstrate the effectiveness and efficiency of the proposed solution.

4.1 Block Diagram

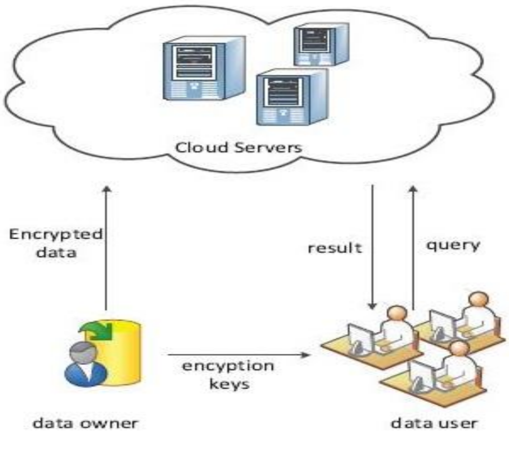
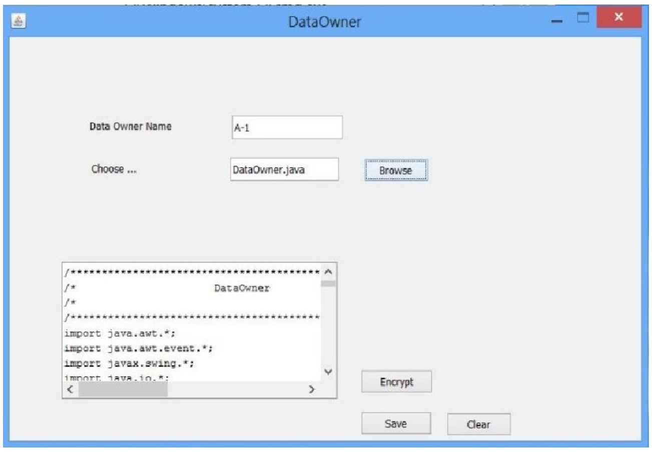


Figure 4.1: Block diagram of retrieval over encrypted cloud data

Directly outsourcing relevance scores leaks lots of sensitive frequency information against the keyword privacy, order-preserving symmetric encryption (OPSE) is integrated to a recent crypto primitive order-preserving symmetric encryption (OPSE) and is modified to develop a one-to-many order preserving mapping technique to protect sensitive information, while providing efficient ranked search functionalities. It defines the problem of secure ranked keyword search over encrypted cloud data, and provides an effective protocol,tha fulfills the secure ranked search functionality with little relevance score information leakage against keyword privacy. The analysis shows that our ranked searchable symmetric encryption scheme retrieves the keywords faster than previous searchable symmetric encryption (SSE) schemes. The proposed method meets the effective data retrieval, the result must be returned based on some ranking criteria based on one-to many order preserving encryption (OPE). The multi ranked keyword search result improves system usability and resource, also eliminates un-necessary traffic by returning relevant and accurate result. It also improves system performance. The advantages of the proposed system methods are, to provide a data privacy and efficient data retrieval , decreases the computational overhead, provides accurate rankedsearch result, increases the communication capacity, increases the performance to improve the system usability.

5 RESULT ANALYSIS

In this paper we designed the experiment using simulator tool cloudsim, the analysis result solves the problem of supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in Cloud computing. our ranked search mechanism were also investigated, including the efficient support of relevance scorethe authentication of ranked search results, and the reversibility of our proposed one-to-many order-preserving mapping technique. Through thorough security analysis, it is found that our proposed solution is secure and privacy preserving, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of our solution.The file upload module process, when a data owner desires to outsource and share a file with some group of users, the data owner encrypts the file first and then it is to be uploaded under a specified attribute set. The module helps to access the file, when a user wants to access an outsourced file; the user downloads cipher text from cloud database and decrypts it with the help of key.This module helps the new user to access various file, with the help of multiple keywords. Based on the system model provided we attempt to define an One –to-many OPE model to map the search key words and give priority for decrypt files through our access control system.



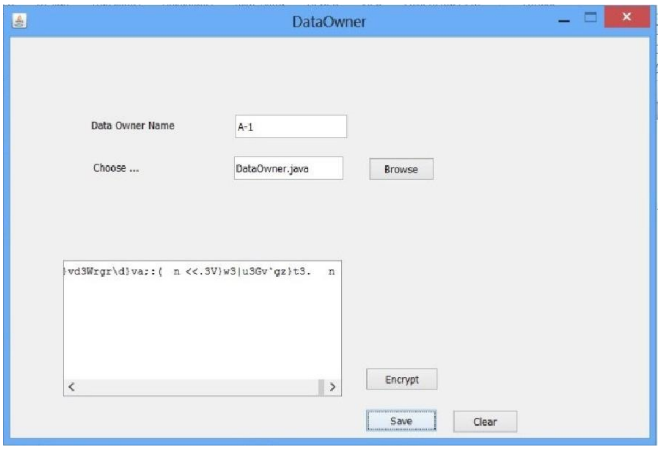
Data Owner Name: A-1

Choose ...: DataOwner.java

```
/***************************************
/*                         DataOwner
/*
/***************************************
import java.awt.*;
import java.awt.event.*;
import javax.swing.*;
import java.io.*;
```

Figure 5.1: File upload

The file upload module process, when a data owner desires to outsource and share a file with some group of users, the data owner encrypts the file first and then it is to be uploaded under a specified attribute set

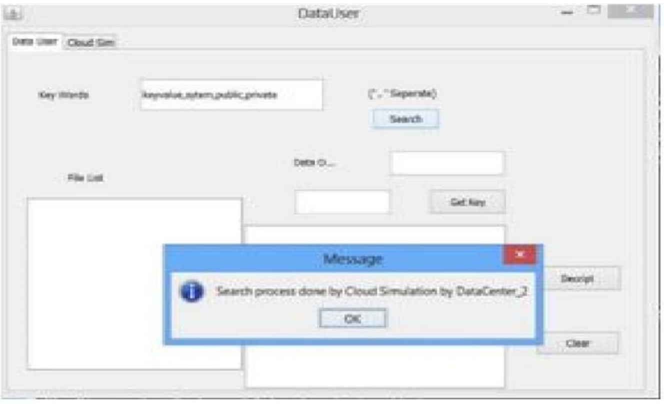


Data Owner Name: A-1

Choose ...: DataOwner.java

```
}vd3Wrgr\d}va;:(  n <<.3V)w3|u3Gv`gz}t3.   n
```

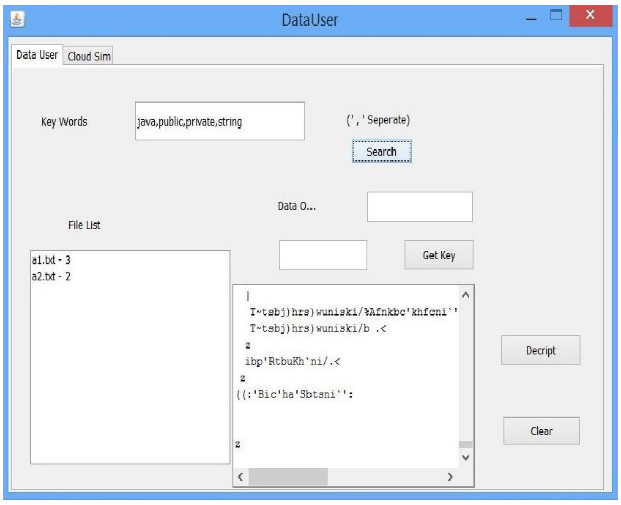
Figure 5.2: Upload data encryption



Key Words: keyvalue,sytem,public,private (',' Seperate)

Search process done by Cloud Simulation by DataCenter_2

Figure 5.3: Multi keyword search



Key Words: java,public,private,string (',' Seperate)

File List:
a1.txt - 3
a2.txt - 2

```
 |
  T~tsbj)hrs)wuniski/%Afnkbc'khfcni`'
  T~tsbj)hrs)wuniski/b .<
 z
 ibp'RtbuKh`ni/.<
z
((:'Bic'ha'Sbtsni`':


z
```

Figure 5.4: Decrypt data

This module helps to access the file, when a user wants to access an outsourced file; the user downloads cipher text from cloud database and decrypts it with the help of key.

6 CONCLUSION

In this paper we investigate efficient data retrieval from the cloud database. The demand for cloud computing increases day by day, consumers can store their data and can retrieve it since it is valuable and soothing process. As the demand increases it is necessary for the search service to allow multi keyword query and provide results based on similarity ranking to meet effective data retrieval. Here we proposed one to many order preserving encryption (OPE), for applications of searchable encryption, which flattens the distribution of the plain text to solve the problem of secured multi keyword search over encrypted cloud data (ECD). The result shows that data can be retrieved faster by efficient multi keyword search from remotely stored encrypted data. Future work, elaborates these ideas to design secure methods of probabilistic OPE and schemes for search in encrypted data.

REFERENCES

i. Jin Li, Qian Wang, Cong Wang, Ning Cao, KuiRen, and Wenjing Lou, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing," This paper was presented as part of the MiniConference at IEEE INFOCOM 2010.

ii. Dongyoung Koo, JunbeomHur and Hyunsoo Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage·"^{IEEE}28TH International conference on data engineering, 2012.

iii. Mehmet Kuzu, Mohammad Saiful Islam and Murat Kantarcioglu, "Efficient Similarity Search over Encrypted Data," IEEE 28th International Conference on Data Engineering, 2012. iv.Ming Li, Shucheng Yu, NingCaoandWenjing Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," 31st International Conference on Distributed Computing Systems, 2011.

v. Jun Xu, Weiming Zhang, Ce Yang, JiajiaXu and Nenghai Yu, "wo-Step-Ranking Secure Multi-Keyword SearchOver Encrypted Cloud Data," International Conference on Cloud Computing and Service Computing, 2012.

vi. Sandeep K. Sood, "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications 35 (2012) 1831–1838.

vii. CengizOrencik, Murat KantarciogluandErkaySavas, "A Practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data,"Sixth International Conference on Cloud Computing , IEEE 2013.

viii. Ruihui Zhao and HongweiLi,"Privacy-preserving Personalized Search overEncrypted Cloud Data Supporting Multikeyword Ranking," Sixth International Conference on Wireless Communications and Signal Processing (WCSP), 2014. ix.P. Mell and T. Grance, "The NIST definition of cloud computing," NIST special publication, 800(145): 7, 2011.

x. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, 34(1): 1-11, 2011.

xi. B. Krebs, "Payment processor breach may be largest ever," http://voices. washingtonpost. com/securityfix/2009/01/payment processor breach may b. html, 2009

xii. M. Abdalla, M. Bellare and D. Catalano, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," Advances in Cryptology–CRYPTO, 2005. Springer Berlin Heidelberg, pp. 205-222, 2005.

xiii. D. Song, D. Wagner and A. Perrig, "Practical techniques for searches on encrypted data," Security and Privacy, 2000. Proceedings. 2000 IEEE Symposium on. IEEE, pp. 44-55, 2000.

xiv. R. Curtmola, J. Garay and S. Kamara, "Searchable symmetric encryption: improved definitions and efficient constructions," Proceedings of the 13th ACM conference on Computer and communications security. ACM, pp. 79-88, 2006. xv.R. Agrawal, J. Kiernan and R. Srikant, "Order preserving encryption for numeric data," Proceedings of the 2004 ACM SIGMOD International conference on Management of data.
ACM, pp. 563-574, 2004.

XV. A.Leninfred,D.Dhanya,S.L Helen mary,s.shibi"Security Analysis on Multi keyword Data Search in Cloud using Encryption Techniques"international journal on engineering research Volume No.5, Issue No.2,pp : 137-140 1stFebruary2016.