International Journal of Engineering Research
Volume No.5, Issue No.2, pp : 137- 140
ISSN:2319-6890)(online),2347-5013(print)
1 Feb. 2016

Security Analysis on Multi keyword Data Search in Cloud using Encryption Techniques

A. Lenin Fred[1], D.Dhanya[2], S. L. Helen mary[3], S.Shibi[4]
Department of Computer science and Engineering, Mar Ephraem college of Engineering and Technology
[1] leninfred.a@gmail.com [2]dhanvis@gmail.com

Abstract: With the popularity in cloud computing security and data search from complex data system is considered as one of the major concern. 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 results based on similarity ranking to meet effective data retrieval. In this project we propose 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 (SMS) over encrypted cloud data (ECD). The result shows that data can be retrieved faster by efficient multi keyword search from remotely stored encrypted data

Keywords: Binary search, Cloud computing, Multi keyword search, order preserving encryption

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 computing is the broader concept of converged infrastructure and shared services.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort. Cloud computing has now become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Provisioning of compute resources and have become a major concern. The resource provisioning schemes depends on the cloud architecture and management of cloud infrastructures. The resource provisioning scheme demands also fast discovery of services and data in cloud computing.

II. RELATED WORK

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 accuracy and privacy protection. The weight and the preference weight help to ensure that the search result will faithfully respect the user's interest. As a result, security analysis and Performance evaluation on experiments were performed on the real world dataset.

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 presents 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, but does not have prior domain information such as the distribution of values and cannot encrypt or decrypt arbitrary values of his choice

Cengiz Orencik*et.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. In the next step, a fine ranking process is executed in the documents by adding up the encrypted score. Extensive experiments show that this new method is indeed an advanced solution for secure multi-keyword retrieval.

III. PROPOSED METHOD

The main objective of this paper is to solve the problem of secure ranked keyword search over encrypted cloud data. Existing system is based on the Searchable Encryption (SE). Searchable encryption allows the user to search the data based on keywords, this technique supports various searches such as single keyword , Boolean keyword and pain text search. The issues of these existing methods are, it cannot provide high level system requirement like usability, it is not adequate to provide search result based on ranking, Data sharing is not secured, and it support only single and Boolean keyword searching, it is not flexible and efficient.

Ranked keyword search enhances system usability and enables search result relevance ranking instead of sending undifferentiated results, and in addition ensures file retrieval accuracy. To enable ranked searchable symmetric encryption for effective utilization of outsourced and encrypted cloud data, our system design should achieves following security and high performance. The goals achieved are ranked keyword search that explores different mechanisms for designing effective ranked search schemes based on other searchable encryption framework, that guarantees security that prevents cloud server from learning the plaintext of either the data files or the searched keywords, and achieves security compared to existing searchable encryption scheme, efficiency is also achieved with minimum communication and computation overhead.

Searchable encryption allows the data owner to outsource data in an encrypted manner and maintains the search on appropriate selective encrypted data. The reality is that data owners and cloud server are no longer in the same trusted domain and their data are of high risk. Since it is unencrypted, there is a possibility to leak the data information from the cloud server to unauthorized users or even the trusted data can be hacked. In short, the accuracy of retrieving the file is lacked by existing searchable encryption schemes in one of the major disadvantage in the context of Cloud Computing.

Information retrieval (IR) has already been utilizing various scoring mechanisms to quantify and rank order the relevance of files in response to any given search query. The importance of ranked search has been one of the major concern for users who outsourced huge data in cloud. To enable a searchable encryption system with support of secure ranked search is the problem tackled in this project. Our work is to explore ranked search over encrypted data in cloud computing. Ranked search greatly enhances system usability by returning the matching files based on frequency of a keyword in a ranked order based on certain criteria. To achieve design goals on both system security and usability, we propose to bring together the advance of both crypto and IR community to design the ranked searchable symmetric encryption (RSSE) scheme.

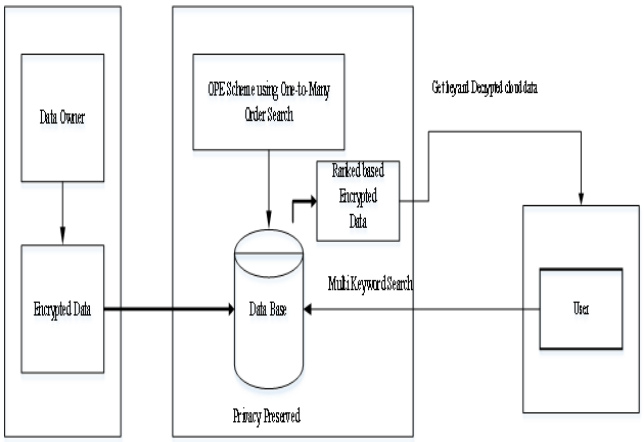

Fig 1. Block diagram of retrieval over encrypted cloud data

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. Extensive experimental results demonstrate the effectiveness and efficiency of the proposed solution.

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 ranked

ISSN:2319-6890)(online),2347-5013(print)
1 Feb. 2016

search result, increases the communication capacity, increases the performance to improve the system usability.

IV.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.

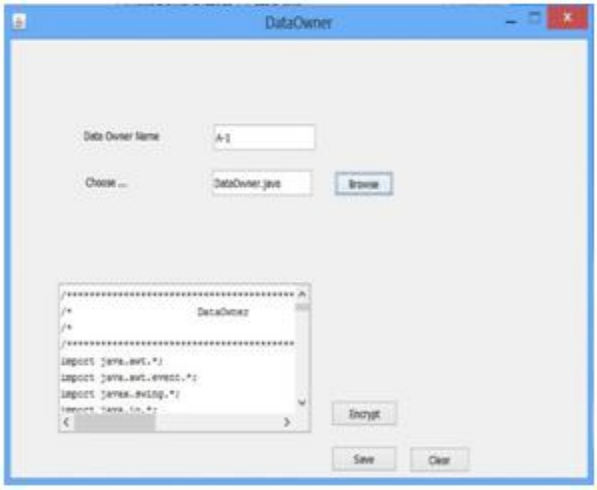

Fig 2: File upload

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. Whenever a data owner wants to create and upload a file the user first defines an attribute set.

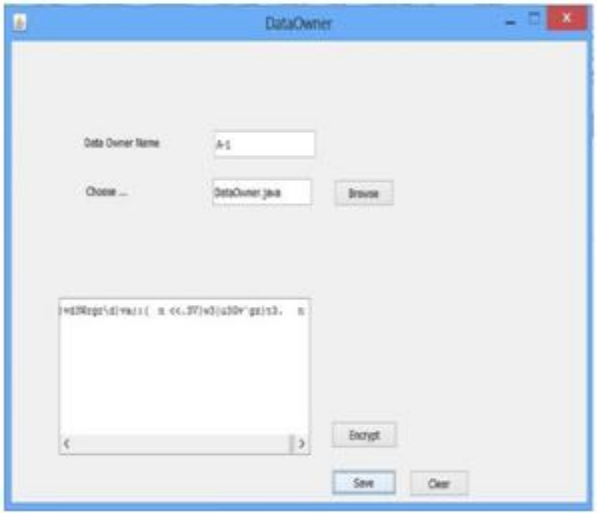

Fig 3: Upload data encryption

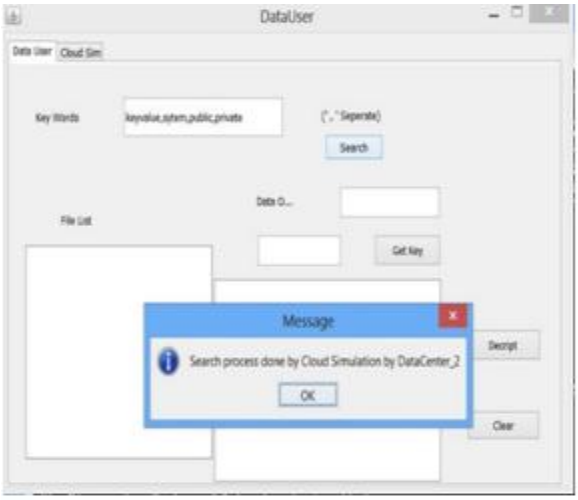

Fig 4: Multi keyword search

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.

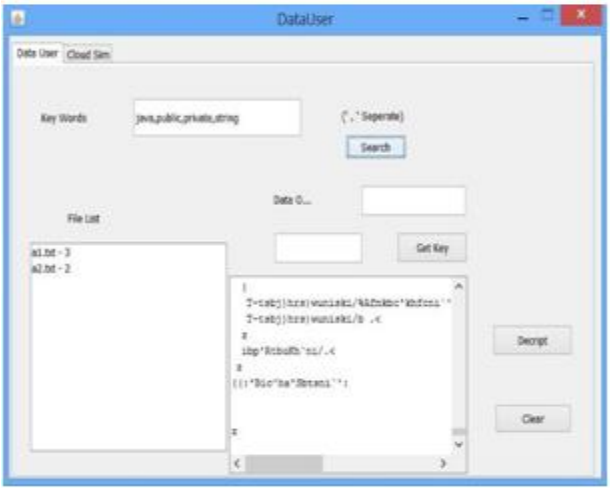

Fig 5: Decrypt data

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.

V.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, Kui Ren, and Wenjing Lou, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing," This paper was presented as part of the Mini-Conference at IEEE INFOCOM 2010.*

ii. *Dongyoung Koo, Junbeom Hur 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, Ning Caoand Wenjing 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, Jiajia Xu 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. *Cengiz Orencik, Murat Kantarciogluand Erkay Savas, "A Practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data,"Sixth International Conference on Cloud Computing , IEEE 2013.*

viii. *Ruihui Zhao and Hongwei Li,"Privacy-preserving Personalized Search overEncrypted Cloud Data Supporting Multi-keyword 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.*