Volume 1, Issue 8, November 2016 ISSN: 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

An Security Enhancement of One-To-Many Order Preserving Encryption (OPE)

Vrushali D.Ugale[1]
Department of Computer Engg.
Sir Vishweswaraya Institute of Technology
Nashik, India

S.M.Rokade[2]
Department of Computer Engg.
Sir Vishweswaraya Institute of Technology
Nashik, India

Abstract: ***The data on cloud computing is encrypted due to security concern or the factor of third party digging into it. As the consequence to this, the search over encrypted data becomes a complex task. The traditional approaches like searching in plain text cannot be apply over encrypted data. So the searchable encryption techniques are being used. In searchable encryption techniques the order of relevance must be consider as the concern because when it is large amount of data it becomes complex as relevant documents are more in number. The expected result is to be that cloud server cannot penetrate in actual user data and provide the search on encrypted data will be performed and results will appear in order of relevance score. Even though with good security of one-to-many OPE the cloud can get the information of the plain text if differential attack occurred on the cipher text by calculating the differences between the cipher text.***

In this paper, we proposed a differential attack on one-to-many OPE by exploiting the differences of the ordered cipher texts. The experimental results show that the cloud server can get a good estimate of the distribution of relevance scores by a differential attack. Furthermore, when having some background information on the outsourced documents, the cloud server can accurately infer the encrypted keywords using the estimated distributions.

Keywords: Searchable encryption, order preserving encryption, privacy, cloud computing.

I. INTRODUCTION

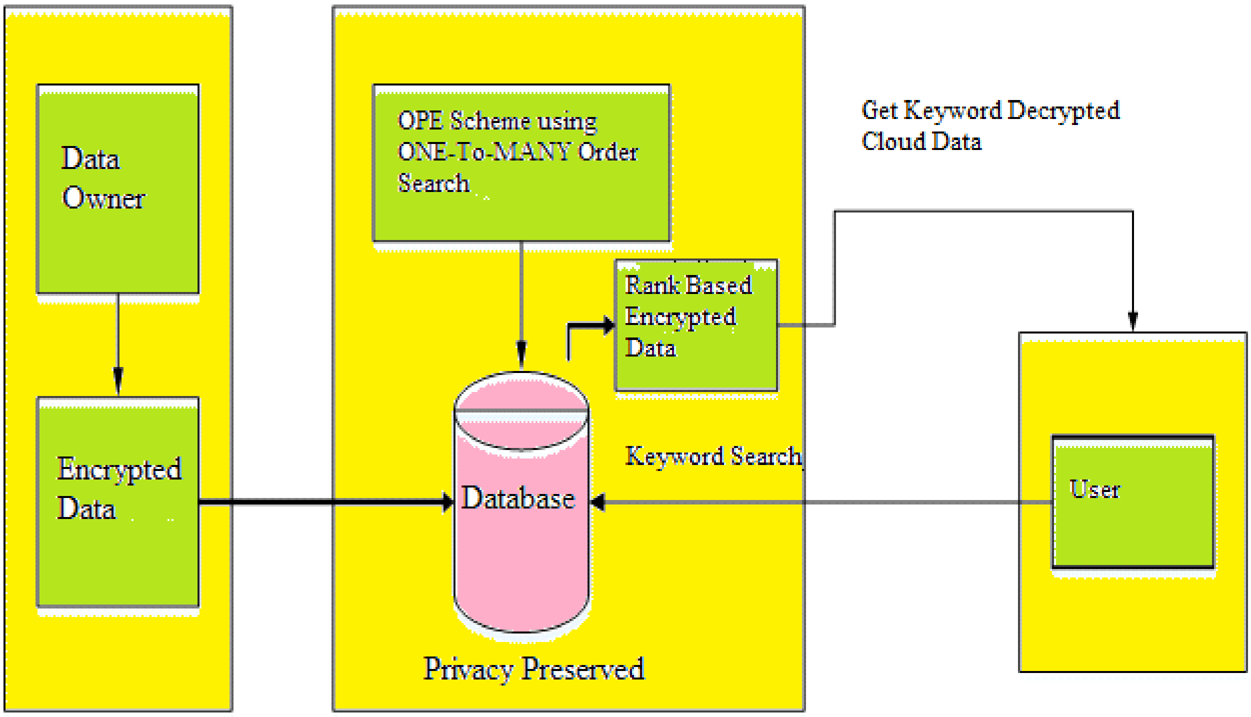
Now day users connected to the Internet may store their data on cloud servers and let the servers manage or process their data. They can enjoy convenient and efficient service without paying too much money and energy, as one of the most attractive feature of cloud computing is its low cost [1]. However, no matter how advantageous cloud computing may sound, large number of people still worry about the safety of this technology. If cloud server get direct access to all these users' data, it may try to analyse the documents to get private information. The initial purpose of this action may be kind. The server wants to provide better service by digging into these data and then displaying customer-oriented advertisement, which could be convenient but also annoying. Besides, when we consider sensitive data such as personal health records and secret chemical ingredients, the situation becomes even more serious [2].

Theoretically, the server is not supposed to have access to sensitive data at all; therefore we should ensure the server has no access to leaking thesedata to an untrusted third party. Thus, sensitive data have to be encrypted before being outsourced to a commercial public cloud [3]. . There are several problems in searchable encryption: fuzzy search, ranked search, multi-keyword search and so on. Song et al. [5] first proposed a search scheme only supporting single Boolean keyword search. After that plenty of searchable encryption methods [6]–[9] arose to improve efficiency and reduce communication overhead.

We discover that the One-to-Many OPE cannot ensure the expected security. In fact, although the cipher texts of One-to-Many OPE conceals the distribution of the plaintexts, an adversary may estimate the distribution from the differences of the cipher texts. So in this paper, we propose a differential attack on the One-to-Many OPE. Our experimental results show that, when applying this attack to the secure keyword search scheme of [16],the cloud server can get an estimation of the distribution of the the relevance scores, and furthermore accurately reveal the encrypted keywords.

II. METHODOLOGY OF PROPOSED SYSTEM

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.


Data Owner
Encrypted Data
OPE Scheme using ONE-To-MANY Order Search
Rank Based Encrypted Data
Database
Keyword Search
Privacy Preserved
Get Keyword Decrypted Cloud Data
User

Block Diagram of Proposed System

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.

III. SYSTEM ARCHITECTURE

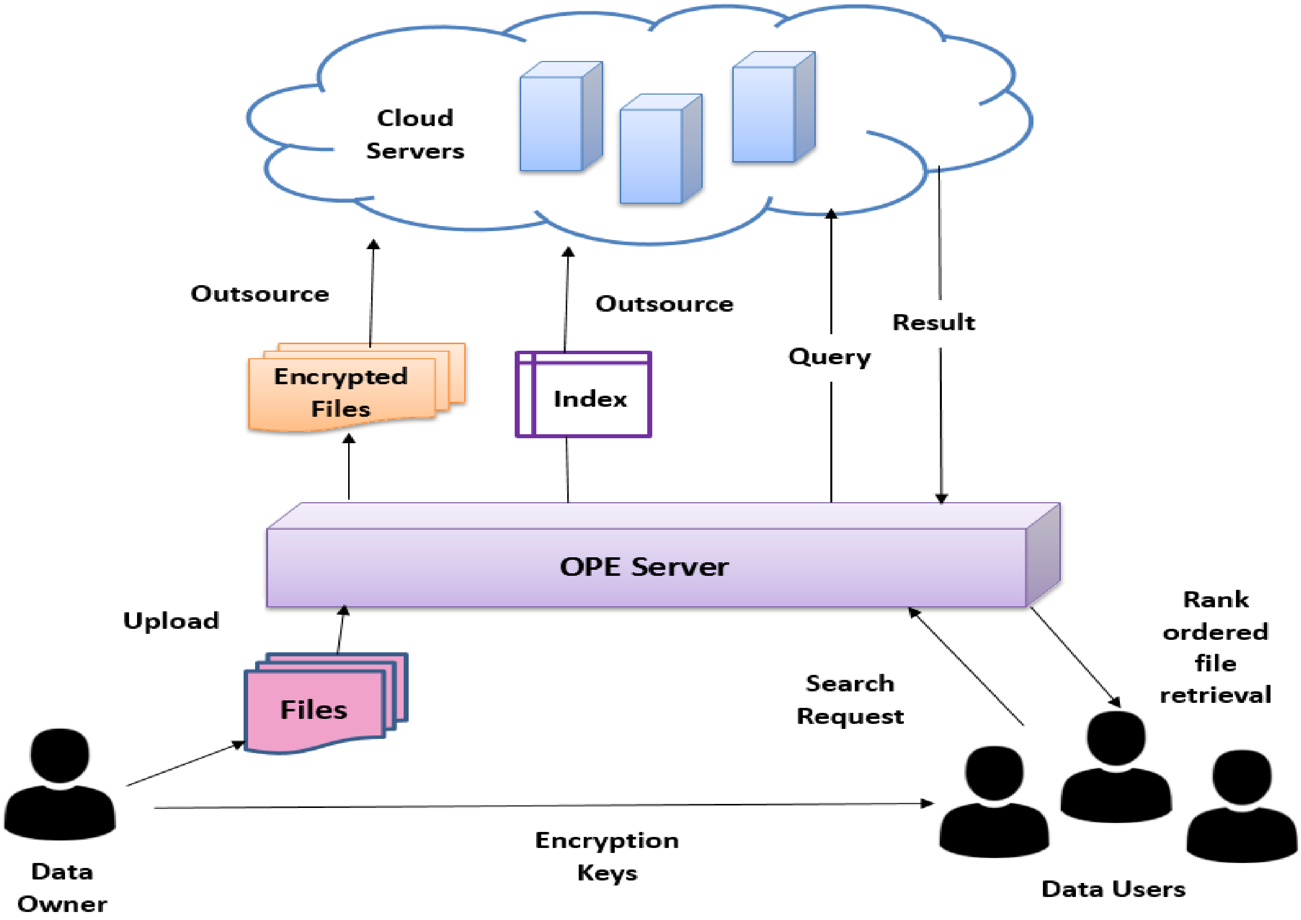


Fig. 2 System Architecture

CONCLUSION

In ranked search of encrypted cloud data, probabilistic OPE is needed to preserve the orderof relevance scores and conceal their distributions at the same time. One-to-Many OPE is a scheme designed for such a purpose. However, in this paper, we demonstrate that the cloud server can estimate the distribution of relevance scores by change point analysis on the differences of cipher texts of One-to-Many OPE. Furthermore, the cloud server may identify what the encrypted keywords are by using the estimated distributions and some background knowledge.

On the other hand, some methods can be used to resist the proposed attack. One is to improve the One-to-Many OPE itself. For instance, we can divide plaintexts having the same value into several sets and divide the corresponding bucket into several sub-buckets. By mapping each plaintext set into one sub-bucket, some new change points will appear in the differential attack, which will cover up the original distribution of plaintexts. Another possible method is to add noise into the inverted index by adding some dummy documents IDs and keywords, and forging corresponding relevance scores. In our future work, we will elaborate these ideas to design secure methods of probabilistic OPE and schemes for search in encrypted data.

ACKNOWLEDGMENT

I take this opportunity to express my sincere thanks and deep sense of gratitude to Prof. S. M. Rokade for valuable guidance. I am also thankful to all faculties of computer department, my colleagues and family who encouraged me to do such a research**.**

REFERENCE

[1]P.Mell and T. Grance. (Jan. 2010).Draft NIST Working Definition of Cloud Computing. http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html

[2] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,”J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[3] B. Krebs. (2009). Payment Processor Breach May Be Largest Ever. [Online]. Available: http://voices.washingtonpost.com/securityfix/ 2009/01/payment_processor_breach_may_b.html

[4] M. Abdalla et al., “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 205–222.

[5] D. X. Song, D. Wagner, and A. Perrig,“Practical techniques for searches on encrypted data,” inProc. IEEE Symp. Secur. Privacy, May 2000, pp. 44–55.

[6] E.-J. Goh. (2003). “Secure indexes,” Cryptology ePrint, Tech. Rep. 2003/216. [Online]. Available: http://eprint.iacr.org/

[7] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 506–522.

[8] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” inApplied Cryptography and Network Security. Berlin, Germany: Springer-Verlag, 2005, pp. 442–455.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 79–88.

[10] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” inProc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

[11] A. Boldyreva, N. Chenette, Y. Lee, and A. O’Neill, “Order-preserving symmetric encryption,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2009, pp. 224–241.

[12] A. Boldyreva, N. Chenette, and A. O’Neill, “Order-preserving encryption revisited: Improved security analysis and alternative solutions,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 578–595.

[13] L. Xiao and I.-L. Yen, “Security analysis for order preserving encryption schemes,” inProc. 46th Annu. Conf. Inf. Sci. Syst., Mar. 2012, pp. 1–6.

[14] A. Swaminathanet al., “Confidentiality-preserving rank-ordered search,” in Proc. ACM Workshop Storage Secur. Survivability, 2007, pp. 7–12.