ISSN 2395-1621

A Secure Re- Encryption with key Distribution Scheme for data sharing in Unreliable Cloud Environment

[#1]Vaibhav Mahode, [#2]Shubham Chaudhari, [#3]Rohan Vanga, [#4]Akshay Patil

[1]vaibhavmahode@gmail.com
[2]shubhamchaudhari2017@gmail.com
[3]rohanvanga.rv@gmail.com

[#1234]Department of Computer Engineering,

JSPM's,
Imperial College of Engineering & Research, Wagholi, Pune.

ABSTRACT

The data on cloud computing is encrypted due to security concern or the factor of third party digging into it. As the consequent 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. We have discussed the Re-encryption technique. 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 Re-encryption 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.

ARTICLE INFO

Article History

Received: 30th November 2016

Received in revised form :

30th November 2016

Accepted: 3rd December 2016

Published online :

3rd December 2016

Keywords: **Private Data, Encryption, Data Security, Cloud Computing, Order Preserving Encryption.**

I. INTRODUCTION

In recent era, cloud services are used by many users as well as industries. Cloud provides large amount of space to store data as well as share data so that it can be available any time over network when user requires. Cloud provides such services in low cost. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized [1]. Users can store as well as share pictures, videos or any file over cloud so that it can be accessed on demand. The data stored over cloud has security issues; it is vulnerable to security threats. User can store any sensitive information over cloud. 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 these data to an untrusted third party. Thus, sensitive data have to be encrypted before being outsourced to a commercial public cloud [3].However, encryption on sensitive data presents obstacles to the processing of the data. Information retrieval becomes difficult in the encrypted domain because the amount of outsourced files can be very large and traditional search patterns can not be deployed to

cipher text retrieval directly. Users need to download all the data, decrypt it all, and then search keywords like plaintext retrieval. To overcome this, Searchable Encryption (SE) [4] Applying order preserving encryption (OPE) [5] is one practical way of supporting fast ranked search.

II. LITERATURE SURVEY

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," 2011, in this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

[2] A. Boldyreva, N. Chenette and A. ONeill, "Order-preserving encryp-tion revisited: improved security analysis and alternative solutions," 2011, this paper propose a simple and efficient transformation that can be applied to any OPE scheme. Our analysis shows that the transformation yields a scheme with improved security in that the scheme resists the one-wayness and window one-wayness attacks.

[3] L. Xiao, I.-L Yen, "Security analysis for order preserving encryption schemes,"2012, in this paper we analyze the security of the OP E encryption scheme SEm,n and give the upper bound on the probability for the adversary to recover the plain text encrypted by SEm,n under chosen plain text attacks.

[4] C. Wang, N. Cao and K. Ren, "Enabling secure and efficient ranked keyword search over outsourced cloud data" 2012, in this paper, he define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy.

[5] S. Yu, C. Wang and K. Ren, "Achieving secure, scalable, and fine-grained data access control in cloud computing", 2010, this paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. he achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

III. PROPOSED SYSTEM

Cloud users store their data in encrypted form to maintain data privacy. Two approaches that are used to securely share data in cloud storage. Firstly, encrypt data using a symmetric key and share that key among the authorized users. Secondly, encrypt data using the individual public key of the authorized users. Authorized users can access plaintexts data by decrypting the corresponding ciphertexts using their respective private key.

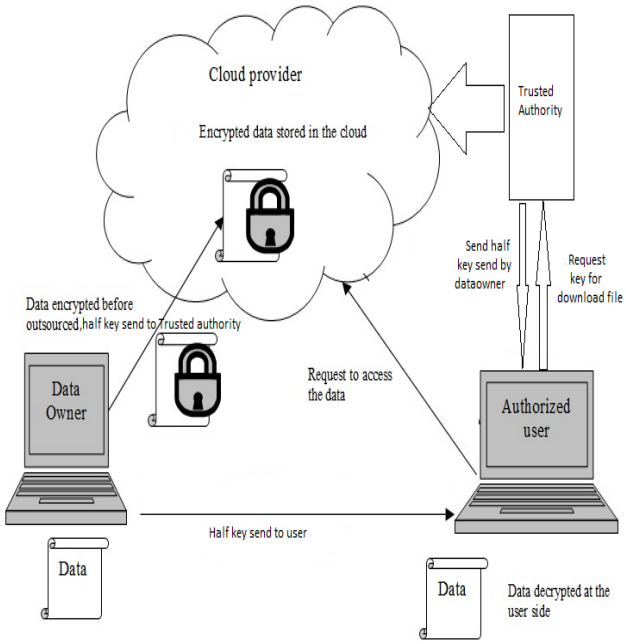

Fig 1. System Architecture

1) Data Owner:

A data owner can be an individual or a corporation, i.e., it is the entity that owns a collection of documents Dc = fD1;D2 : : :DNd g that it wants to share with trusted users. The keyword set is marked as W = fw1;w2 : : :wNw g.

2) Cloud Servers:

It is the place of hardware and software resources where a pool of data files and different applications can store. A cloud server conducts a secure search based on an encrypted index. In the search procedure, a user first generates a search request in a secret form a trapdoor T (w). In this example, the trapdoor is just the hash values of the keyword of interest. Once the cloud server receives the trapdoor T (w), it compares

it with the hash values of all keywords in the index I, then the desired documents which are corresponding to keyword w are found.

3) Data Users:
The user can download all the encrypted documents based on the given IDs and decrypt them. A desirable system is supposed to return the documents in a ranked order by their relevance with the queried keyword, but using traditional encryption schemes will disorder relevance scores.

Algorithm Used:

Data Encryption Standard (DES):

DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. It is scalable algorithm due to varying the key size and Block size. The Data Encryption Standard is one of the most common used encryption mechanisms. Using this algorithm data are encrypted using a 64 bit blocks with an encryption key of 56 bit length. The DES with 64 bit input as steps applied in series gives an output of 64 bits.

IV. MATHEMATICAL MODEL

System Description:
Input:
Upload file ()
U : Upload file.
E : Encryption File.
F : file for security.
S : Store data base.

Output:
Stored Encrypted file to the Database.

Input
Function Encryption (id, request, file, key)
ID : unique id for each file.
Request : User request for particular file.
File : Check file on DB.
Key : Input key for decryption

Output:
File will recover to data user.

Success Conditions: Encryption will done for input file

Failure Conditions: Our system fails when no any security policy apply to the input file.

V. CONCLUSION

One-to-Many OPE is designed for encrypted data over the cloud and to preserve the order of relevance scores. cloud server can estimate the distribution of relevance scores by change point analysis on the differences of cipher texts of One-to-Many OPE. In this system we have described to improve One-to-Many OPE using this method. The system provides query privacy in search process under encrypted cloud data services. Search duration is reduced in the semantic relationship based encrypted keyword search process. Accuracy is improved with relevance score and semantic query model.

REFERENCES

[1] 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.

[2] A. Boldyreva, N. Chenette and A. ONeill, "Order-preserving encryp-tion revisited: improved security analysis and alternative solutions," Advances in CryptologyCCRYPTO, 2011. Springer Berlin Heidelberg, pp. 578-595, 2011.

[3] L. Xiao, I.-L Yen, "Security analysis for order preserving encryption schemes," Proc. of 46th Annual Conference on Information Sciences and System, pp. 1-6, 2012.

[4] C. Wang, N. Cao and K. Ren, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions 23(8), pp. 1467-1479, 2012.

[5] S. Yu, C. Wang and K. Ren, "Achieving secure, scalable, and fine-grained data access control in cloud computing," INFOCOM, 2010 Proceedings IEEE. IEEE, pp. 1-9, 2010.