AN EFFICIENT RANKED KEYWORD SEARCH METHOD IN CLOUD ENVIRONMENT FOR PRIVACY-PRESERVING

ARUNIMA RATANKUMAR

A, Computer Department, Vidyalankar Institute of Technology, Maharashtra, India.

ABSTRACT

As data in cloud is outsourced documents require privacy preserving in an encrypted form. The data encrypted has a challenge as it documents are encryption which will require proper accuracy performance degradation. As he data is massive this has become more difficult .This makes it even more challenging to provide an efficient and reliable system to design a cipher text search scheme as online information retrieval on large volume of encrypted data. In this paper to support more search semantics, clustering method is proposed. To enable similarity search which is also efficient, data owner builds a secure index along with the encrypted data items is outsourced to the cloud server. Server performs searching on the index according to the queries of the data users without learning anything about the data other than what data owner allows an adversary to learn.

Keywords: *Cloud computing, cipher text search, ranked search, multi-keyword search, hierarchical clustering, security.*

1. INTRODUCTION

Cloud Computing is computing utility where cloud customers can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from shared pool of configurable computing resources. It is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In simple terms, cloud computing means storing and accessing data and programs over the internet instead of a computer's hard drive.

In today's data intensive environment, cloud computing becomes prevalent due to the fact that it removes the burden of large scale data management in a cost effective manner. Hence, huge amount of data, ranging from personal health records to e-mails, are increasingly outsourced into the cloud. At the same time, transfer of sensitive data to untrusted cloud servers leads to concerns about its privacy. The basic building block of our secure index is the state-of- the-art approximate near neighbor search algorithm in high dimensional spaces called locality sensitive hashing (LSH).LSH is extensively used for fast similarity search on plain data in information retrieval community. There will be provide a real world application of our scheme and verify the theoretical results with empirical analysis. In this, there is utilization it in the context of the encrypted data. In such a context, it is critical to provide rigorous security analysis of the scheme to ensure the confidentiality of the sensitive data. In this, provide a strong security definition and prove the security of the proposed scheme under the provided definition.

The method of decrypting locally each file after downloading it is an insignificant solution, due to the large amount of bandwidth cost in cloud scale systems. This proposed system also provides image tagging in MRSE scheme to Images as they also contain useful and important information. Moreover, aside from eliminating the local storage management, storing data into the cloud doesn't serve any purpose unless they can be easily searched and utilized [8].

1.1 AES

The Advanced Encryption Standard (AES) is a symmetric key encryption standard adopted by the U.S. government. The standard comprises three block ciphers AES-128 AES-192 and AES-256 adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size with key sizes of 128, 192 and 256 bits respectively.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input called the plaintext into the final output called the cipher text. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

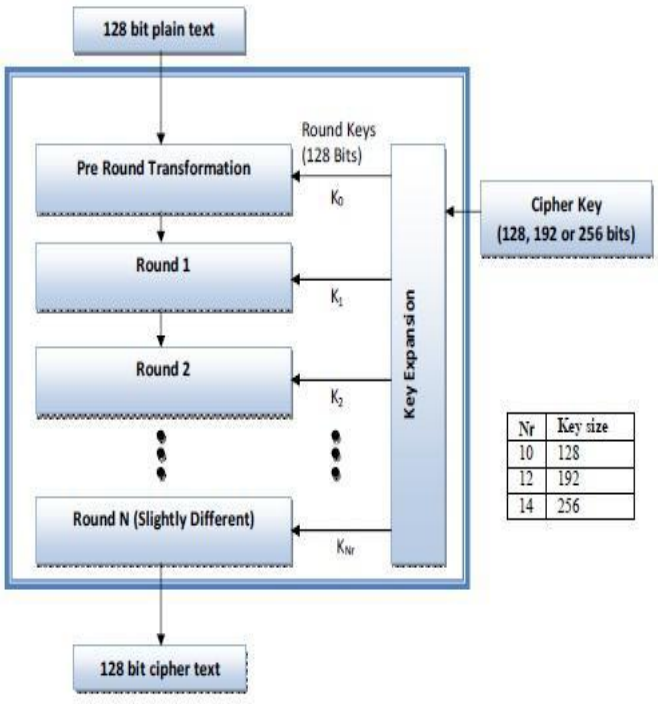

Figure 1 AES

2. PROBLEM DEFINITION

Computing is the long dreamed vision of computing as a utility, where cloud customers can remotely store their data into the cloud so as to enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources. Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud. To protect data privacy and combat unsolicited accesses in the cloud and beyond, sensitive data, for example, e-mails, personal health records, photo albums, tax documents, financial transactions, and so on, may have to be encrypted by data owners before outsourcing to the commercial public cloud.

3. THE PROPOSED MECHANISM

To enable efficient similarity search, data owner builds a secure index and outsources it to the cloud server along with the encrypted data items. Server performs search on the index according to the queries of the data users without learning anything about the data other than what data owner allows an adversary to learn. In Phase-I, we present the index structure. In Phase-II, we describe the search scheme that is built on top of the index. There are different phases on which we are going to work in our dissertation:

Phase –I: The index structure

Our similarity, Searchable Symmetric Encryption (SSE) scheme is based on a secure index structure that is built through locality sensitive hashing (LSH). LSH maps objects into several buckets such that similar objects collide in some buckets while dissimilar ones do not with high probability. Index structure is constructed on top of this property.

Phase -II: Basic secure search scheme

In this part, we describe the basic protocol for our similarity SSE scheme, overview of which is presented in Figure. Initially data owner gets private keys and then he creates the index for the data collection. Alice encrypts the items with key to form the encrypted collection. Suppose a user is interested in retrieving the items, the user generates search query. Once the query is identified, user sends it to the server. Server performs search on the index for each component and send back the corresponding encrypted file. Once the user receives file, user decrypts encrypted file. Once the encrypted items corresponding to the search request are retrieved, user decrypts them with the key to obtain their plain versions.

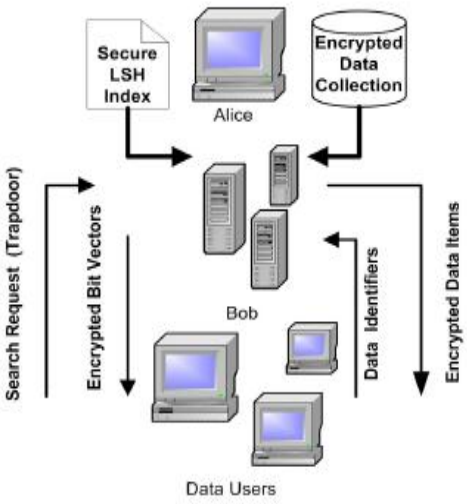

Figure 1: Basic secure search protocol

3. CONCLUSIONS

In this paper, we proposed an efficient similarity searchable symmetric encryption scheme. To do so, we utilized locality sensitive hashing which is widely used for fast similarity search in high dimensional spaces for plain data. We proposed LSH based secure index and a search scheme to enable fast similarity search in the context of encrypted data. In such a context, it is very critical not to sacrifice the confidentiality of the sensitive data while providing functionality. We provided a rigorous security and proved the security of the proposed scheme under the provided definition to ensure the confidentiality.

REFERENCES

[1]. Chi Chen, Member, IEEE, Xiaojie Zhu, Student Member,IEEE, Peisong Shen, Student Member, IEEE,Jiankun Hu, Member, IEEE, Song Guo, Senior Member, IEEE, Zahir Tari, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE, " An Efficient Privacy-Preserving Ranked Keyword Search Method" , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 4, APRIL 2016

[2]. Ning Cao†, Cong Wang‡, Ming Li†, Kui Ren‡, and Wenjing Lou††Department of ECE, Worcester Polytechnic Institute, Email: {ncao, mingli, wjlou}@ece.wpi.edu,‡Department of ECE, Illinois Institute of Technology, "Privacy Preserving Multi Keyword Ranked Search Over Encrypted Cloud Data.

[3]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search[C]," in Proc. Adv. Cryptol.,Berlin, Heidelberg, 2004, pp. 506–522.

[4]. D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean que-ries," in Proc. Adv. Cryptol,. Berlin, Heidelberg, 2013, pp. 353–373.

[5]. S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. Conf. Comput. Commun. Secur., 2012, pp. 965–976.

[6]. S. Grzonkowski, P. M. Corcoran, and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services," in Proc. IEEE Int. Conf. Consumer Electron., 2011, Berlin, Germany, 2011, pp. 83–87.

[7] T. Jothi Neela1* and N. Saravanan2," Privacy Preserving Approaches in Cloud", Vol 6 (5) | May 2013

[8]. Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahmood_, and AtaUllah Ghafoor, " Analysis of Classical Encryption Techniques in Cloud Computing", TSINGHUA SCIENCE AND TECHNOLOGY ISSNll1007-0214ll09/10llpp102-113Volume 21, Number 1, February 2016