Secure Image Retrieval over Untrusted Cloud Servers

Ayad Ibrahim Abdulsada, Aqeel N. Mohammad Ali, Zaid Ameen Abduljabbar, Haider Sh.Hashim

Abstract-Security issue represents the main barrier facing the wide adoption of cloud computing. Encryption is the best method to mitigate users' concerns. However, this method makes searching the encrypted data a challenging task. Accordingly, several approaches have been proposed to enable searching the encrypted, remotely stored data without decryption. Till now, almost all these approaches are limited to handle text search but not multimedia search.

In this paper, we propose an efficient scheme that provides content based search over encrypted image database. To do so, we utilize a locality sensitive hashing LSH method to build our searchable index. LSH index greatly enhances the system efficiency by returning the matching images in a ranked order with a minimum number of distance evaluations. For security purposes, we turn this index into a secure index to prevent the cloud server from learning any useful information from the contents of that index. Searchable index along with image collection are outsourced to the cloud server in their encrypted format. We provide several empirical experiments to illustrate the efficiency of our proposed scheme.

Key words: cloud computing, searchable encryption, LSH, image retrieval.

I. INTRODUCTION

We are living in a highly connected and data intensive world. The great advances in networking and information technologies have enabled users to collect and generate large amounts of data. However, maintaining and storing such amount of data require additional storage cost and computational power that may be not available to those users, especially in case of lightweight device (e.g. mobile and iPhone devices). Fortunately, cloud computing (utility computing) has been emerged as a new technology that offers to its user's attractive financial and technological advantages [1]. To exploit the benefits of this new paradigm, users have started moving their data and applications to cloud servers.

However moving sensitive data (such as health records, private photos, and secret documents) to the untrusted cloud servers poses a great challenge towards the privacy of user's data. To combat unsolicited access, users usually encrypt their sensitive data before outsourcing it to the cloud servers. However, traditional encryption schemes pose a significant barrier towards searching the encrypted data. Over the years, several *searchable encryption* (SE) approaches have been proposed [2]-[6] to provide the ability for selectively retrieving the encrypted documents. Typically, these systems build a secure index structure and outsource it along with the encrypted documents to the remote server. Authorized users submit their requests as secret trapdoors that are integrated properly with the stored indexing information. The server uses the received trapdoor to search over the stored index, and retrieves the matching encrypted documents.

Traditionally, almost all the previous searchable encryption schemes are limited to handle keyword based search, where a user submits a secure keyword to search an encrypted text documents. In contrast, modern *information retrieval* (IR) [8] systems e.g. Google Goggles[1] introduce new technology that allow their clients to submit a photo as query and search a database of stored images, where images with similar visual content in the database are identified. Such new technology is termed as *content based image retrieval* (CBIR). Thus, it is highly recommended to develop a searchable encryption scheme that handle image based search in an accurate and efficient way.

In this paper, we bring together the developments of both CBIR systems and SE approaches to explore an image-based searchable encryption scheme over remote cloud servers. We build a searchable index from the image collection for speeding the search task. However, unless secured well, such index leaks important statistical information about the underlying stored data to the adversary server. Thus, the main issue here is how we can encrypt this index while preserving its ability to rank the relevant images.

The basic building block of our secure index is *the locality sensitive hashing* (LSH) [9]. LSH index allows answering efficiently near neighbor queries in high dimensional spaces of plain data [10]. In our scheme, we propose to utilize LSH in the context of the encrypted data. In such a context, it is critical to ensure the confidentiality of the sensitive data. We have conducted several empirical analyses on a real dataset to demonstrate the performance of our proposed scheme.

Our notable contributions can be summarized as follows. First, we utilize the appealing features of LSH index in the context of the encrypted data, and design an image-based searchable symmetric encryption scheme on top of this index. Second, our propose scheme indexes huge databases of images, in such a clever way, that reduce both storage requirements and run time, thus making one step closer towards practical deployment of privacy-preserving data hosting services in cloud computing.

The rest of this paper is organized as follows. Related works are reviewed and discussed in section II. Section III introduces the problem definition and the security requirements. Section IV provides the proposed scheme. Performance investigations are provided in section V and conclusions and future works are drawn in section VI

II. RELATED WORKS

Text based searchable encryption. Prior searchable encryption systems have focused on retrieving encrypted text

Manuscript received October, 2013.

Ayad Ibrahim Abdulsada, Computer Science Department, Basrah University/ Education College for Pure Science/ Basrah, Iraq.

Aqeel N. Mohammad Ali, Computer Science Department, Basrah University/ Education College for Pure Science / Basrah, Iraq,

Zaid Ameen Abduljabbar, Computer Science Department, Basrah University/ Education College for Pure Science / Basrah, Iraq,

Haider Sh.Hashim, , Computer Science Department, Basrah University/ Education College for Pure Science / Basrah, Iraq,