Chapter 43
Aggregate Searchable Encryption With Result Privacy

Dhruti P. Sharma
S.V. National Institute of Technology, Surat, India

Devesh C. Jinwala
S.V. National Institute of Technology, Surat, India

ABSTRACT

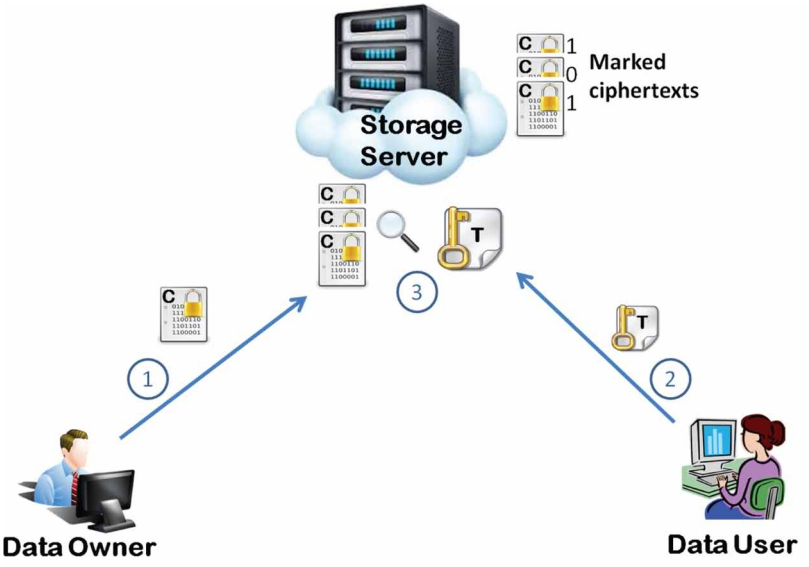
*With searchable encryption (SE), the user is allowed to extract partial data from stored ciphertexts from the storage server, based on a chosen query of keywords. A majority of the existing SE schemes support SQL search query, i.e. 'Select * where (list of keywords).' However, applications for encrypted data analysis often need to count data matched with a query, instead of data extraction. For such applications, the execution of SQL aggregate query, i.e. 'Count * where (list of keywords)' at server is essential. Additionally, in case of semi-honest server, privacy of aggregate result is of primary concern. In this article, the authors propose an aggregate searchable encryption with result privacy (ASE-RP) that includes ASearch() algorithm. The proposed ASearch() performs aggregate operation (i.e. Count *) on the implicitly searched ciphertexts (for the conjunctive query) and outputs an encrypted result. The server, due to encrypted form of aggregate result, would not be able to get actual count unless having a decryption key and hence ASearch() offers result privacy.*

INTRODUCTION

Searchable Encryption (SE) is a cryptographic mechanism to store encrypted data onto a cloud storage server in the way that the data can further be searched at the server side without compromising privacy. In typical SE schemes (Boneh, Di Crescenzo, Ostrovsky, & Persiano, 2004; Goh, 2003; Song, Wagner, & Perrig, 2000), data owner computes searchable ciphertexts and uploads them onto server. To enable search, data user issues a search token to server who then executes the defined search algorithm on ciphertexts without learning any information about original data (Figure 1).

DOI: 10.4018/978-1-7998-7705-9.ch043

Figure 1. Searchable encryption



In SE, a searchable ciphertext comprises of an encrypted payload along with a list of encrypted keywords (to be searched). On the other hand, a search token consists of keyword(s) involved in search query chosen by data user. Practically, any SQL select query, i.e. 'Select * where (list of Values)' could be considered as a search query where 'Value' represents a keyword. With search operation (that implicitly applies token on ciphertext), the server marks '1' to all ciphertexts matching with query and '0' to all unmatched ciphertexts. Subsequently, data user offloads ciphertexts and performs decryption as per the requirements. However, in practice, there exist several applications concerning encrypted data analysis where data user requires fetching only a count of ciphertexts matched with the issued search token, instead of offloading all ciphertexts. One of such applications is given below.

Example

Consider a scenario of Telecommunication Company with millions of customers where Call Detail Record (CDR) for each customer is maintained at storage server in encrypted form. Additionally, the company has given access privileges for the stored CDRs to the authorized users. A CDR is defined with a list of encrypted keywords where each keyword is represented as 'KeywordName=Value'. Few of such keywords with their potential values are listed in Table 1.

In such a scenario, let us take an example of an officer (authorized user) from the intelligence bureau who works on the case of cybercriminal possessing mobile number '0919898765610'. For the primary investigation, suppose officer needs the following statistical data: