

Aggregate Searchable Encryption With Result Privacy

Dhruvi 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.

KEYWORDS

Aggregate Search, Chosen Keyword Attack, Conjunctive Search, Search Result Privacy, Searchable Encryption, Semi-Honest Server

INTRODUCTION

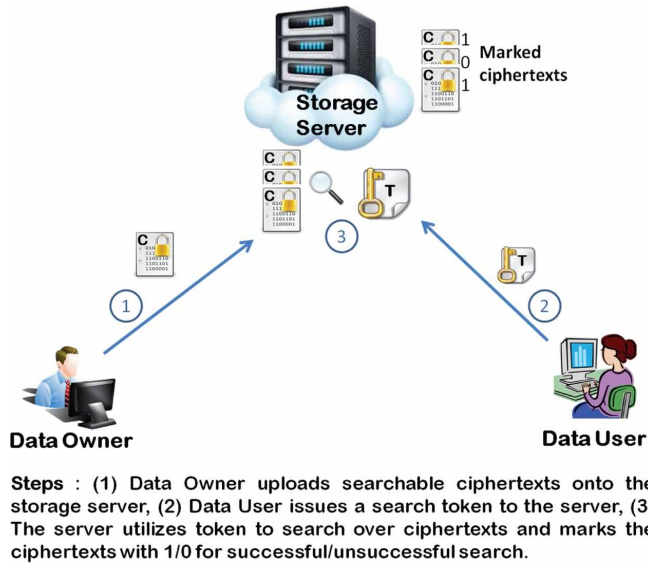
Searchable Encryption (SE) is a cryptographic mechanism to store encrypted data onto a cloud storage server in the way that the data can further be searched at the server side without compromising privacy. In typical SE schemes (Boneh, Di Crescenzo, Ostrovsky, & Persiano, 2004; Goh, 2003; Song, Wagner, & 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).

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

DOI: 10.4018/IJISP.2020040104

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 1. Searchable encryption



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:

1. A number of audio calls made by ‘0919898765610’ in ‘January-2017’:

Query: Count * where (IN=‘0919898765610’) and (MN=‘01’) and (YR=‘2017’) and (TP=‘AC’)

Table 1. Example of keywords with potential values

Keywords	Values
Initiator of call (IN), Receiver of call (RC)	Valid mobile number
Type of conversation (TP)	Audio Call (AC)/ Video Call (VC) / SMS / MMS
Day of call (DY)	Valid date of call
Month of call (MN)	Valid month of call
Year of call (YR)	Valid year of call

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/aggregate-searchable-encryption-with-result-privacy/247427

Related Content

Advanced Cyber Security and Internet of Things for Digital Transformations of the Indian Healthcare Sector

Jonika Lambaand Esha Jain (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 1037-1056).

www.irma-international.org/chapter/advanced-cyber-security-and-internet-of-things-for-digital-transformations-of-the-indian-healthcare-sector/310493

Attacks and Countermeasures

Mukta Sharma (2018). *Handbook of Research on Information Security in Biomedical Signal Processing* (pp. 155-176).

www.irma-international.org/chapter/attacks-and-countermeasures/203385

Information System Integrated Security

Milena Tvrdíková (2012). *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions* (pp. 158-169).

www.irma-international.org/chapter/information-system-integrated-security/63088

Large Key Sizes and the Security of Password-Based Cryptography

Kent D. Boklan (2009). *International Journal of Information Security and Privacy* (pp. 65-72).

www.irma-international.org/article/large-key-sizes-security-password/4002

Factors Influencing College Students' Use of Computer Security

Norman Pendegraft, Mark Roundsand Robert W. Stone (2010). *International Journal of Information Security and Privacy* (pp. 51-60).

www.irma-international.org/article/factors-influencing-college-students-use/50308