letax document

wang xuan

June 7, 2024

Abstract

The attribute-based keyword search (ABKS), which simultaneously achieves searching and fine-grained access control over encrypted data, is frequently applied in cloud computing environments characterized by data storage and sharing. Recently, inspired by attribute-based encryption (ABE) and searchable encryption (SE) primitives, several ABKS schemes have been presented. However, almost all existing ABKS schemes actually only provide an attribute-based keyword equality match function and do not have a structural index to support practical search efficiency and dynamic data updates in real-world applications. To the best of our knowledge, this study is the first to realize an attribute-based keyword search construction supporting numerical comparison expressions with the practical search efficient and dynamic data update capacity (ABKS-NICEST), based on our proposed attributebased keyword secure search scheme supporting numerical comparison expressions (ABKS-NICE) and an exclusive OR-chain-based inverted index structure. To the best of our knowledge, ABKS-NICEST is the first attributed-based keyword search scheme with practical search efficiency and dynamic data update capacity. In addition, numerical values are an important and common attribute, so providing comparison expressions among numerical values can greatly enhance the expressivity of access policy. Therefore, we use the prefix membership verification technique to design a method to support any numeric comparison expression in a flexible and uniform manner. Through theoretical and experimental evaluations, we determine that ABKS-NICEST is the most efficient ABKS scheme.

1 Introduction

Encryption before uploading data to the cloud server is most effective way to guarantee the confidentiality of data [2]. A challenging problem is how to efficiently perform operations over ciphertext exactly like being in the plaintext domain without decrypting them. It is critical for cloud applications, as the cloud computing is characterized by not only massive data storage, but efficient data processing. A number of studies has been conducted to achieve operations directly over ciphertext, among which searchable encryption is a recently vibrant research field, aiming at guaranteeing both confidentiality and searchability over encrypted data. Song et al. [3] presented the first practical searchable encryption construction. Subsequent researches [4], [5] devoted to persistently refining the search complexity and security, even explored the more practical dynamic schemes [6], [7], [8] supporting secure data addition and deletion. As all these constructions were built in the symmetric key system, they are referred to as searchable symmetrical encryption (SSE).

2 related work

2.1 Attribute-Based Encryption and Attribute-Based Keyword Search

Recently, in order to make the encrypted cloud data searchable with the flexible data access control, combining ABE and SE, a number of ABKS schemes are proposed in [10], [11], [12], [13], [14], [15]. However, these ABKS schemes just provide an attribute-based keyword equality test functionality and are short of effective index mechanism for a practical search efficiency in the real application. Though work [14] constructed a raw index by simply associating each encrypted keyword with data files containing the keyword to speed up the search process, without a fullfledged index structure, it still suffers from impractical search efficient in practice due to redundant and expensive search authorizations. To enhance the expressivity of ABE scheme, authors [28] first considered to deal with

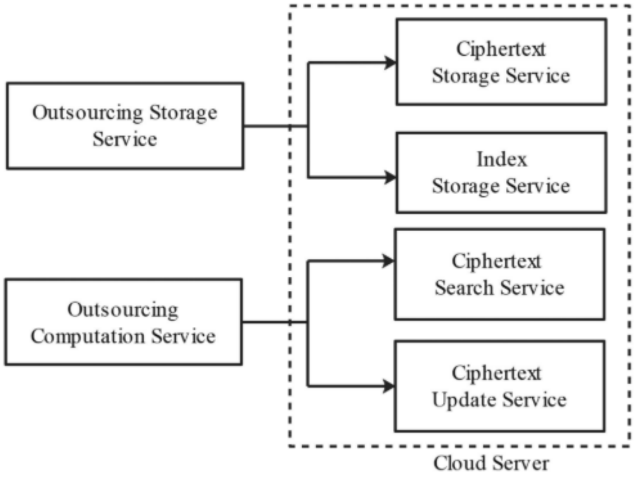
Outsourcing Storage Service
Outsourcing Computation Service
Ciphertext Storage Service
Index Storage Service
Ciphertext Search Service
Ciphertext Update Service
Cloud Server

Figure 1: A service-oriented cloud computing outsourcing environment.

Item	Quantity
Widgets	42
Gadgets	13

Table 1: Functionality and Security Comparison.

numeric comparison expression in the access policy and transformed an integer comparisons into AND and OR gate policies over "bag of bits" divided by a numeric comparison expression. However, this transformation is relatively complex, resulting in the inefficiency. In order to degrade the complexity, Xue et al. [31] used only OR gates to convert access policies of numeric comparison expressions by using 0-encoding and 1-encoding technique. Though this scheme considers two inequality operations

$$x = \frac{b^2}{2n} + \sqrt{n^2} \tag{1}$$

2.2 How to include Figures

Our attribute-based keyword search problem is based on a service-oriented cloud computing outsourcing environment, as shown in Fig. 2, where the cloud server provides powerful data storage and computation services. Roughly speaking, the cloud server provides a service to store outsourced encrypted data and secure index; if the cloud server receives an outsourced computation request, it will provide the corresponding computation services such as data searching or data updating based on ciphertexts. Our service-oriented computation model fully embodies the idea of "Service Computing," including "Storage-as-a-Service," "Software-as-a-Service," and "Security-as-a-Service". We will describe a more detailed system model in Section 4.1.See the code for Figure 1 in this section for an example.

2.3 How to add Tables

Use the table and tabular environments for basic tables — see Table, for example. For more information, please see this help article on tables.

2.4 conclusion

In this paper, we investigate the attribute-based keyword search over encrypted cloud data. First, we construct an ABKS scheme supporting numeric attribute comparison policy, namely ABKS-NICE. Similar to the existing schemes, ABKS-NICE is static and with an impractical search complexity. Based on ABKS-NICE and our proposed encrypted XOR chain, we design the first truly practical and dynamic ABKS scheme, ABKS-NICEST. By the theoretical and experimental performance evaluations, ABKS-NICEST is most efficient ABKS scheme with dynamic data update ability as far as we know. Also, we provide formal security proofs for ABKS-NICE and ABKS-NICEST. As our future work, we will research practical and dynamic multi-keyword ABKS scheme, ABMKS-NICEST.