Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Parallel search over encrypted data under attribute based encryption on the Cloud Computing☆

*Thouraya Bouabana-Tebibel**, *Abdellah Kaci*

*Laboratoire de Communication dans les Systèmes Informatiques, Ecole nationale Supérieure d'Informatique, Alger, Algeria*

ARTICLE INFO

*Article history:*
Received 26 December 2014
Received in revised form
20 March 2015
Accepted 18 April 2015
Available online 28 April 2015

*Keywords:*
Attribute based encryption
Cloud computing
Cryptographic access control
Searchable encryption

ABSTRACT

Data confidentiality in the Cloud Computing is a very challenging task. Encryption is one of the most secure methods ensuring this task, and searchable encryption techniques are used to search on encrypted data without the need for decryption. But, despite this secure measure some leaks may appear when searching over data. In this article, we propose to improve confidentiality of outsourced data. We are particularly interested in reinforcing the access control on the search result, when the search is performed over encrypted data. The property behind this aspect of security is known as ACAS (Access Control Aware Search) principle. We present a hybridization of Searchable Encryption and Attribute Based Encryption techniques in order to satisfy the ACAS property. The proposed model supports a personalized and secure multi-user access to outsourced data, presenting high search performance. It deals with multi-keywords searches and is designed to speed up the search time by taking advantage of High Performance Computing, which is widely used in Cloud Computing. Two Attribute Based Encryption techniques are considered on the side of the Cloud and some conducted experiments show the efficiency of the proposed method.



## 1. Introduction

The Cloud Computing services offered by large-scale data centers of companies like Amazon, Google, or Microsoft attract every day many new clients. For small and medium enterprises, migration to the Cloud Computing evolves significant economic savings. In fact, the Cloud Computing migration is based on a 'pay per use' pricing model, where users pay according to their resources consumption (Buyya et al., 2010). However, despite the benefits provided by the Cloud migration, new problems and challenges arise like inter-provider data portability, energy conservation, and security (Rong et al., 2013).

With respect to security, the main challenge to deal with is keeping confidentiality of sensitive data. The most powerful mechanism to ensure data confidentiality is encryption. However, the classical cryptographic primitives make data unusable; even authorized users cannot retrieve information from encrypted data. To overcome this problem, Song et al. (2000) proposed a pioneering work dealing with search on encrypted data. Many articles have afterwards been published

☆ This is a revised and extended version of a paper that appeared initially in the proceedings of the 15th IEEE International Conference on Information Reuse and Integration (IEEE IRI 2014) held in San Francisco, CA, USA on Aug 13-15, 2014

* *Corresponding author.*
E-mail addresses: t_tebibel@esi.dz (T. Bouabana-Tebibel), ab_kaci@esi.dz (A. Kaci).

http://dx.doi.org/10.1016/j.cose.2015.04.007
0167-4048/

on this subject (Goh, 2003; Boneh et al., 2004; Curtmola et al., 2006; Tang, 2013).

However, approaches for searching on encrypted data, also known as *Searchable Encryption* methods, present a security breach. They return to the user the identifiers of all requested documents, including those to which he has a denied access. To address this vulnerability, an access control on the searched resources is required. Indeed, in addition to encryption, confidentiality often requires access control mechanisms (Ruj et al., 2012).

In a Cloud Computing environment, the classical access control techniques, such as access control lists (ACLs), show their limits due to the huge number of resources and users. A new encryption approach, based on descriptive attributes, called ABE (Attribute Based Encryption) was introduced. It supports grouped access control facilities rather than only individual. The first publication of ABE appeared in Sahai and Waters (2005), where authors provide a cryptographic access control mechanism based on descriptive attributes. These attributes are used to describe the encrypted data and user's key. Next, the technique is revised in Goyal et al. (2006) and later in Bethencourt et al. (2007) to provide two more elaborate ABE schemes, namely KP-ABE (Key-Policy Attribute Based Encryption) and CP-ABE (Cipher text-Policy Attribute Based Encryption), with enhanced cryptographic access control system. In KP-ABE, descriptive attributes are used to encrypt data, while a user's key contains an access policy defining data to which the user is allowed to access; whereas in CP-ABE, data is encrypted with an access policy based on the users' attributes and the latter serve to construct the user's key. Later, Many other publications on Attribute Based Encryption followed including Ibraimi et al. (2009), Lounis et al. (2013), Yin and Zhang (2011), Yu et al. (2008).

More recently, Han et al. (2014) proposed a new encryption scheme, ABEKS (Attribute Based Encryption with Keyword Search), which ensures confidentiality and multi-user access control based on KP-ABE. They encrypt data documents with KP-ABE using the document keywords as attributes and provide KP-ABE with Searchable Encryption semantics. Search is realizable thanks to a sequential decryption of all documents, based on the user's private key which is made of the searched keywords. The pertinence of the idea behind this work appears in the use of the keywords as document attributes and access policy within the user's decryption key. This strategy allows for gathering, in a judicious way, encrypted search and access control under a unique ABE scheme. CP-ABE may also be, at first, applied to encrypt the original documents in clear, before they undergo the KP-ABE encryption. This added protection reinforces access control that they directly attach to the users' attributes. However, even if ABEKS ensures access control on encrypted search, it leaks the number of documents containing the searched keywords. This leakage refers to the Access Control Aware Search (ACAS) property stated by Singh et al. (2009).

ACAS requires that no additional information should be inferred from the result returned by the search mechanism. Authors of Singh et al. (2009) illustrated their idea by invoking a situation where the violation of the ACAS property leads to the divulgation of the total number of files including a given keyword. For example, an attacker could monitor the enterprise's file system to see the number of files containing the word "bankruptcy". A sudden increase in the number of such files could alert him/her to sell off the company stock, practically amounting to insider trading (Singh et al., 2009). This violates the ACAS property, as this information should not be determined by the attacker through the search result.

The purpose of this work is to improve the SE-ACAS technique proposed in Kaci and Bouabana-Tebibel (2014), Kaci et al. (2014) with a view to integrate access control with search on encrypted data, such that users receive only the results they are authorized to access. Contrarily to ABEKS which resorts to the use of a transformative KP-ABE mechanism to assure search on encrypted data, we dedicate KP-ABE to access control and perform search on encrypted data using the SSE-1 technique (Curtmola et al., 2006) which is index-based search. Access control is based on the Key-Policy Attribute Based Encryption technique (KP-ABE) in Kaci and Bouabana-Tebibel (2014) and the Ciphertext-Policy Attribute Based Encryption technique (CP-ABE) in Kaci et al. (2014). Besides ensuring control access, SE-ACAS was also designed to satisfy the ACAS property. However, the proposed scheme for that purpose showed some limits. It necessitated the use of an additional Filter Authority on the side of the user, requiring, itself, trust mechanisms and maintenance. Furthermore, the experimental results provided high search times due to the cryptographic access control functions performed by the Authority. Thus, we propose herein, a new approach, xSE-ACAS, that improves the SE-ACAS scheme by (1) revising the Searchable Encryption technique in a way it takes advantage of High Performance Computing (HPC), which is widely used in the Cloud, to considerably reduce the search time. The revision is concerned with Searchable Encryption parallelization; (2) performing the access control ABE on the side of the Cloud, thus supporting the ACAS property on one hand and reducing the ABE decryption time thanks to the HPC calculation power, on the other hand; (3) supporting multi-keywords search queries in a form of logical expressions; (4) showing the benefits behind the use of the two main access control techniques based on their performance.

The remainder of the article is organized as follows. In section 2, we present works related to ours. Sections 3 and 4 describe, respectively, the search on encrypted data SSE-1 and the access control ABE, which are the mechanisms on which is based the proposed model. This one is developed in sections 5 and 6. Section 5 describes the parallelization process introduced in the search mechanism; whereas section 6 presents the integration of access control into search. Section 7 provides the solution analysis and section 8 shows the experimental results. We conclude the study in section 9.

## 2. Related works

The pioneers of Searchable Encryption are Song et al. (2000). They proposed the Searchable Symmetric Key Encryption (SSKE) scheme, which enables a user to retrieve the ciphertext bloc containing a word based on a trapdoor including the searched keyword. Goh proposed in Goh (2003) a more efficient scheme that provides O (1) search time per document. Later, an adaptive solution for Symmetric Searchable