Computers and Electrical Engineering 57 (2017) 241–256

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing☆

Rohit Ahuja[a,*], Sraban Kumar Mohanty[a], Kouichi Sakurai[b]

[a] Department of Computer Science and Engineering, PDPM Indian Institute of Information Technology, Design and Manufacturing Jabalpur, India
[b] Department of Informatics, Kyushu University, Japan

ARTICLE INFO

Article history:
Received 30 January 2016
Revised 24 November 2016
Accepted 24 November 2016
Available online 1 December 2016

Keywords:
Privacy-preserving
security
Full-fledged delegation
Cloud computing
Shared access privileges
Cloud storage security

ABSTRACT

The benefits of cloud computing motivate enterprises to migrate their IT infrastructure on cloud servers. Enterprise needs to entrust untrusted cloud service provider, which gives rise to various security and privacy concerns. To address these concerns, numerous schemes in cloud computing employed attribute-based encryption schemes. However, existing schemes are neither flexible enough to provide users complete liberty on delegation of their access privileges nor grant shared access privileges among users of a group to jointly address a responsibility. This paper introduces hierarchical attribute-set-based access control scheme by employing ciphertext-policy attribute-set-based encryption with a hierarchical structure of users to achieve scalability. The proposed scheme simultaneously achieves the notion of fine-grained cum flexible access control, privacy preserving, efficient data utilization and imperatively provides users full-fledged liberty on delegation of their access privileges. Furthermore, we formally prove that proposed scheme is secure under decisional bilinear Diffie–Hellman assumption.

1. Introduction

Cloud computing is a revolutionary paradigm to provide unlimited storage and computation services to its users on "pay per use" basis. The most prominent and discussed issue due to which various enterprises are reluctant from migrating to cloud servers are data privacy and confidentiality [1]. The most common mechanism to achieve privacy and data confidentiality is encryption. However, classical encryption techniques, degrade efficient data utilization. Data owner shares information corresponding to all the users, while an individual user is interested in retrieving files related to him only. For instance, suppose a manager uploads data files corresponding to all the employees on cloud servers but an employee is interested to retrieve data related to him only. The straightforward solution is to download all the files and decrypt them to find the desired data. This solution is infeasible due to certain shortcomings. Firstly, this solution requires huge amount of bandwidth cost in downloading all the data. Next, this solution overburdens user due to storage and computation cost

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. M. S. Kumar.

* Corresponding author.
E-mail address: rohitsureshahuja@gmail.com (R. Ahuja).

http://dx.doi.org/10.1016/j.compeleceng.2016.11.028
0045-7906/

involve in storing and decrypting downloaded files. For efficient utilization of data, user should be permitted to query Cloud Service Provider (CSP) for desired data. CSP processes the query and provides desired data as a response to the user. In addition, privacy concerns need to be addressed, while sharing data using cloud servers, e.g., CSP or any illegitimate user should not be able to derive any meaningful information about data, data-owner and data-consumer from "Query and Response" as well as the outsourced data [2,3].

Furthermore, the imperatively required feature with every enterprise is to grant employees access to the outsourced data corresponding to their assigned roles and responsibilities within the organization, i.e., fine-grained access control. In addition, access control should be flexible, i.e., employees in the organization may address different roles for different span of time. Hence, the access control should be flexible enough to support access to the outsourced data corresponding to all the roles played by an individual simultaneously for the specified period of time [4,5]. In enterprises, certain roles are mutually addressed by group of users. It is preferable to subdivide the access privileges among group of users, rather than trivially generating the copies of access privileges for every individual in the group, i.e., to provide them shared access privileges. It enhances trust among users and frees key issuing authority from unnecessary computation [6].

Nowadays, in enterprises delegation of roles among associates emerges as a tool to efficiently address any responsibility. It enhances the productivity and innovation by distributing the workload among associates and developing trust among them. Along with assigned roles, employees need to be provided access privileges corresponding to a delegated role. Indeed, in enterprises delegation of role is expressed beyond two individuals to conveniently address responsibilities. In group delegation, roles are delegated among group members to efficiently address different responsibilities. In many to one delegation, group of employees delegates their roles to an individual employee, while in many to many delegation group of employees delegates their roles to other group of employees. In addition, roles in the enterprises are always delegated with a determined period of time, which is called control delegation [7–10].

Attribute-Based Encryption (ABE) schemes emerge as a useful cryptographic primitive to communicate messages among multiple recipients [4,5,11]. Since introduction of ABE schemes, many variants of ABE have been proposed namely Key-Policy Attribute-Based Encryption (KP-ABE) [11], Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [4] and Ciphertext-Policy Attribute-Set-Based Encryption (CP-ASBE) [5].

Traditional cryptographic schemes fail to support search on encrypted content. Searchable encryption schemes like Public key Encryption with Keyword Search (PEKS) is a cryptographic technique, which enables searching on encrypted content [12]. This scheme lacks expressiveness; to improve the same, Hidden Vector Encryption (HVE) was proposed [13]. However, these techniques were proposed to share data with single recipient only, which limits its application in cloud environments where single message has multiple recipients [3].

A solution proposed in [14] employed KP-ABE to enable data-owner to securely share data using cloud servers. A CP-ABE based secure and efficient data retrieval scheme was proposed to achieve efficient data utilization, privacy-preserving and fine-grained access control [3]. To achieve scalability, flexibility and fine-grained access control a Hierarchical Attribute-Set-Based Encryption (HASBE) scheme was proposed by employing CP-ASBE [15]. Another major challenge associated with sharing of data using cloud servers is integrity and privacy of user's data. A secure and efficient public auditing scheme was proposed, which employs third party to audit user's data stored in cloud on behalf of a user [16]. A remote data possession checking scheme was also proposed to check the integrity of users' data on cloud storage [17]. However, existing access control schemes in cloud computing are far away from providing users full-fledged liberty on delegation of their access privileges and shared access privileges to system users. Hence, it is desired to propose a holistic access control scheme, which simultaneously realizes the notion of one-to-many encryption, efficient data utilization, scalability, fine-grained cum flexible access control and privacy-preserving. In addition, the access control should support full-fledged delegation and shared access privileges.

In this paper, we propose a Hierarchical Attribute-Set-based Access Control (HASAC) Scheme to provide data access privileges among users corresponding to their defined roles and responsibilities, i.e., users individually or jointly address the role by employing CP-ASBE scheme [5]. HASAC incorporates CP-ASBE with hierarchical structure to achieve scalability by decentralizing the key-issuing authority at different levels of hierarchy. Moreover, the scheme employs hierarchical identity-based encryption [18] to hierarchically generate anonymous keys and pseudonyms for users to conceal their identities, while sharing and retrieving data from cloud servers. The proposed scheme supports hierarchical user grant and revocation, file creation and deletion. In addition, the scheme provides users full-fledged liberty on delegation of their access privileges to efficiently address their responsibilities. We formally prove that HASAC is secure under decisional bilinear Diffie–Hellman assumption [19]. Shared access privileges and hierarchical structure may give rise to cheating and collusion attacks respectively. We also prove that HASAC is resistant against such attacks. We analyze the performance of HASAC for computation and storage overhead and compare it with existing schemes. Further, we implement HASAC to evaluate its performance and our experimental results illustrate that HASAC has satisfying performance.

The rest of the paper is organized as follows. Section 2 describes the related works of ABE, searchable encryption schemes and existing access control solutions in cloud computing. System model and assumptions are described in Section 3. Our proposed scheme is discussed in Section 4. Section 5 analyzes the security of our proposed scheme. The features, computational, storage overhead of our scheme and empirical analysis are discussed in Section 6. Lastly, the paper is concluded in Section 7.