Information Sciences 000 (2016) 1–15

Contents lists available at ScienceDirect

Information Sciences

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

Secure independent-update concise-expression access control for video on demand in cloud

Kun He[a], Jing Chen[a,*], Yu Zhang[a], Ruiying Du[a], Yang Xiang[b], Mohammad Mehedi Hassan[c], Abdulhameed Alelaiwi[c]

[a] State Key Laboratory of Software Engineering, Computer School, Wuhan University, Wuhan, 430072, China
[b] School of Information Technology, Deakin University, Burwood, VIC 3125, Australia
[c] College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia

ARTICLE INFO

Article history:
Received 27 December 2015
Revised 25 July 2016
Accepted 8 August 2016
Available online xxx

Keywords:
Video-on-demand
Attribute-based encryption
Cloud computing
Independent-update
Concise-expression

ABSTRACT

Video on demand (VoD) is a popular application on the Internet. In the past few years, more and more VoD services are shifted to cloud. Although this transformation introduces many benefits, it arouses new challenges of data security due to the outsourcing storage on untrusted cloud servers. For satisfying the requirements of fine-grained access control in cloud, Attribute-Based Encryption (ABE) algorithms are applied to this field. However, due to the large number of videos and users in cloud, there exist frequent subscribing/unsubscribing behaviors and numerous categories, which induce the challenges for higher flexibility and efficiency. Most of existing schemes do not discuss these challenges sufficiently. In this paper, we propose an ABE-based Secure Independent-update Concise- expression Access Control (SICAC) scheme in Cloud, to provide flexible and efficient authentication and authorization for VoD services. In the aspect of access policy update, to guarantee that users cannot affect each other, we design an independent-update key policy ABE (KP-ABE) algorithm which allows users to update their keys separately, while most of existing schemes require that all members of a group should be updated simultaneously. In the aspect of attribute description, to reduce the storage cost, we propose a concise-expression access structure which can describe various logic relationships flexibly and efficiently. The security is proved in standard model and the experiment is implemented with Pairing-Based Cryptography(PBC) library. Both the theoretical analysis and the experimental results show that our scheme is efficient and effective for VoD services in cloud.

1. Introduction

Video-on-demand (VoD) [21] is popular. The amount of multimedia traffic accessing via the Internet has already broken through the order of exabytes(10^{18}) per month [4]. Traditionally, the providers of VoD service have to invest in commodity servers as business grows. Nowadays, they can focus on their main industry by relying on the cloud services [12,28,29,33,42,44]. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be

* Corresponding author.
E-mail address: chenjing@whu.edu.cn (J. Chen).

http://dx.doi.org/10.1016/j.ins.2016.08.018
0020-0255/

rapidly provisioned and released with minimal management effort or service provider interaction [27]. In recent years, cloud computing has become one of the most influential paradigms in the IT industry.

The benefits of cloud computing include reduced costs and capital expenditures, increased operational efficiency, scalability, flexibility and immediate time to market [1,45]. Therefore, many VoD service providers begin to use cloud services. For instance, Netflix has moved all of its streaming servers, encoding software, search engines, and video data to Amazon Web Services (AWS) in 2010 [29].

Although cloud computing introduces many benefits to VoD providers, this new model also induces some security concerns [7,8,11,18,24,36,39,41]. Due to the work mode of cloud computing, VoD providers have to outsource their data to a cloud service provider, which is usually a commercial enterprise and cannot be trusted fully [46]. Therefore, it is necessary to enforce access control to restrict the behaviors of curious cloud service providers and unauthorized users. However, traditional access control schemes rely on the trustability of servers, which could not be guaranteed in cloud. Access control could also be achieved by encrypting data and distributing associated keys to authorized users. Owing to one-to-one work mode, however, VoD providers have to prepare a separate copy for each user if traditional cryptography adopted, which is impractical.

Attribute-based encryption (ABE) [19,35] is an advanced technique of public key encryption, which allows users to encrypt and decrypt messages based on attributes. The work mode of ABE is also extended to one-to-many. Therefore, ABE is suitable to guarantee data security under cloud [16,38,43]. In practice, ABE is usually used as a key distribution scheme for some secure symmetric encryption algorithms [17,20], e.g. AES. Considering the relationship between access rules and private keys, ABE can be classified into two types, *key-policy ABE* (KP-ABE) and *ciphertext-policy ABE* (CP-ABE) [34]. In KP-ABE [22], attributes are used to describe access contents, access policies are issued to a user with its private key, which reflect the user's permissions. In CP-ABE [2,14,26], attributes are used to describe the user, access policies are attached to ciphertext, which reflect the requirements for decryptors. It is easy for VoD providers to tag videos by attributes and distribute private keys to users by their subscriptions. On the contrary, it is hard for VoD providers to tag users since they may know nothing about users except their subscriptions. Therefore, KP-ABE is more suitable to enforce access control for VoD services [15]. In KP-ABE system [10], a protected video can be tagged with a set of attributes, such as "area: America", "category: movie", "topic: action", "classification: PG",[1] "year:2012", etc. The master authority of system can distribute private decryption keys with different access policies to various users [13], such as sending Bob a decryption key which can decrypt any ciphertext whose attributes satisfy "area: Korea" OR ("area: America" AND "category: TV drama" AND "year:2013").

VoD is a real-time service, which imposes higher requirements of flexibility and efficiency on access control schemes. On one hand, in a VoD system, membership may change frequently in various situations, which brings challenges to key update process. For example, users may join or quit the system at any time. In addition, a user who previously subscribed for "action movie" may change to the subscription "science fiction movie". However, most of the existing ABE schemes do not research this problem sufficiently. The limitation of those schemes is that if any membership changes, such as revoking or updating, all users must update their private keys. Obviously, this approach is inefficiency. The scheme used in [20] designed a mechanism, which reduces the number of users involved in update or revocation process. Nonetheless, the operation of regenerating key cannot be avoided. Fan et al. [9] proposed a scheme, which has a small influence range when membership changes, but it introduces some security vulnerabilities. In that scheme, since a ciphertext element is proportional to the hash values of attributes, users could convert the ciphertext beyond their permissions into the form that they could decrypt. Hence, secure *independent-update* access control, which means that the membership update process of a user does not affect other irrelevant users of the system, is still a challenging problem for VoD systems in cloud. In other words, forward and backward security can be guaranteed while one can update its key without others' cooperations.

On the other hand, due to the limited resources of users' equipments, especially for mobile devices, the efficiency of access policy representation is very important. For instance, a user may subscribe all action movies except those tagged with "classification: NC-17", all comedy films except in this year. To authorize appropriate privileges to this user, the access policy should be "category: movie" AND (("topic: action" AND NOT "classification: NC-17") OR ("topic: comedy" AND NOT "year:2015")). This form is called as *concise expression*. Otherwise, the same policy should be "category: movie" AND (("topic: action" AND ("classification: G" OR "classification: PG" OR "classification: PG-13" OR "classification: R")) OR ("topic: comedy" AND ("year:2014" OR "year:2013" OR "year:2012"...))). Obviously, this method is more complex. Therefore, concise-expression is essential to VoD systems.

1.1. Related work

ABE is a suitable scheme to enforce access control for VoD services in cloud. Generally, ABE can be classified into ciphertext-policy ABE and key-policy ABE. Researchers have proposed many CP-ABE schemes [9,25,26,31,34]. Sahai [34] provided the first construction of CP-ABE, using access tree to denote access rule, which can support complicated access policy. However, the efficiency of access tree is low [13]. Ning et al. [26] proposed a practical CP-ABE, which supports large universe and white-box traceability. Ning et al. [25] proposed a CP-ABE which solves the problem of key abuse. Peng et al.

[1] According to The Motion Picture Association of America, movies can be classified into 5 stages, G(GENERAL AUDIENCES), PG(PARENTAL GUIDANCE SUGGESTED), PG-13(PARENTS STRONGLY CAUTIONED), R(RESTRICTED Under 17) and NC-17(NO ONE 17 AND UNDER ADMITTED).

Please cite this article as: K. He et al., Secure independent-update concise-expression access control for video on demand in cloud, Information Sciences (2016), http://dx.doi.org/10.1016/j.ins.2016.08.018