International Journal of Cloud Applications and Computing
Volume 8 • Issue 3 • July-September 2018

A Novel Authorization Scheme for Multimedia Social Networks Under Cloud Storage Method by Using MA-CP-ABE

Cheng Li, School of Information Engineering, Henan University of Science and Technology, Luoyang China
Zhiyong Zhang, School of Information Engineering, Henan University of Science and Technology, Luoyang, China
Lanfang Zhang, School of Information Engineering, Henan University of Science and Technology, Luoyang, China

ABSTRACT

This article finds that with the development of network technology and the change of a users' social habits, the existing multimedia social network, whether it is one-to-one authorization or one-to-many authorization, are having difficulty meeting the needs of users and cloud storage service. In order to solve this problem, this article proposes a new authorization scheme of multimedia community, based on attribute encryption. Use MA-CP-ABE solution to enhance system service efficiency. This program contributes to two aspects: (1) combining user trust with attribute-based authorizations, and (2) enhancing the flexibility and security of the solution. The scheme has been applied in the prototype system and achieved good results. Results prove that the program has good application value for cloud storage technology, IoT and many other fields.

KEYWORDS

Authorization Security, Cloud storage, MA-CP-ABE, Multimedia Social Networks, Policy Update, Relationship Depth

INTRODUCTION

Along with the development of network technology and Cloud storage, Multimedia Social Networks (MSNs) is linking social networks users with cloud storage (Stergiou et al., 2016). The user transmits his own private data to the Multimedia Social Networks Service Provider (MSNSP) through multimedia social networks, then the MSNSP stores its data in the network; at the same time, users can share their private data with other users through a multimedia social network, such as, YouTube, Baidu Netdisk, Amazon Drive and so on. However, multimedia social networks have received widespread attention, but users have to take privacy leaks, information fraud and other security issues. Therefore, how to make multimedia social networks more effectively protect user privacy and data security has become the focus of many scholars.

In the traditional multimedia social network, users upload personal data to the MSNSP provided by cyberspace, while users also need to develop a series of access control policy submitted to MSNSP. When other users visit to upload private data, MSNSP will determine whether it allows access according to the previous data owner specified access control policy (Hu et al., 2015; Morovat & Panda, 2016; Tootoonchian et al., 2009; Li et al., 2015). However, MSNSP is usually considered not entirely credible, although it will not actively disclose user privacy data, it can receive attacks on illegal users, for example, causing users' data leakage (Chaudhary et al., 2016; Chaudhary &

DOI: 10.4018/IJCAC.2018070103

Gupta, 2017); at the same time, use of access control lists to store access control policies in the face of large-scale access to system applications is slightly stretched. (Alsmirat et al., 2017). In order to solve the above problem, when uploading user data, it is encrypted and uploaded, although this can ensure that the user's data is not stolen by the bad service provider, and address the data leakage caused by storage security issues; however, the distribution and management of keys has become a new problem. According to (Zhang et al., 2015), the document adopts the method of writing a user's Content Encryption Key (CEK) into a XML authorization certificate, which effectively solves the problem of distribution and storage of encryption key; but its ability to update the policy is weak. (Feng et al., 2016), Proxy Re-Encryption is adopted to solve the problem of user encrypted data authorization. This method effectively solves the problem of user authorization delivery. However, the above-mentioned scale of authorization is for one-to-one, the efficiency of authorization is not high. (Sun et al., 2010), a one-to-many authorization model is adopted, which effectively solves the problem of authorization scale; but because of the use of broadcast encryption, it is difficult to achieve in the multimedia social networks before the authorization need to know in advance the size of its authorization.

Through the research of the (Zhang et al., 2016), multimedia social networks application attribute-based access control can not only determine the relationship between the user's access control policy, but also take access control for the user's basic attributes and resource environment attributes. According to the research in the (Feng et al., 2016) and (Zhang & Wang, 2013), the relationship (user authorization depth) between users in the multimedia social networks is not static, but as communication between users increases or decreases. In the case of an authorization that only considers giving an attribute, it often results in unauthorized access to the user who is trusted or not trusted, such as unlimited sharing of netdisk data and other issues, so the use of ABE should take into account the impact of the depth of the user relationship on the authorization results. Therefore, in order to solve the above problems, attribute-based encryption (ABE) scheme is applied to multimedia social networks, and proposed Ciphertext-Policy Attributed Based Encryption of multimedia social networks authorization Scheme. In this scheme, the Ciphertext-Policy Attributed Based Encryption (CP-ABE) scheme of the multi-authority is used, that the attributes will be divided into the corresponding attribute authorization agencies, and increase the depth of the relationship between users concept at the same time, which is more secure and efficient multimedia social network license. The goal is to make attribute-based encryption work better for multimedia social networks and cloud storage. But the application of the program is not limited to multimedia social networks. Through the association between the user attributes and the trust between users, the scheme is converged in the attribute-based encryption and authorization scope, which increases the security. The programs described in this paper are generally applicable to multimedia social networks (e.g., YouTube), Cloud Drive (Amazon Drive), city networking, etc., and users who use the services will get a more secure and efficient service.

The remaining of the paper is organized as follows. The first section introduces the research results of the scholars in this paper, including the development process of ABE and the application of ABE. The second section will briefly introduce some definition of system. The third section will introduce the system model and the corresponding specific algorithm. The fourth section will carry out safety and performance analysis. The fifth section will introduce the actual system application. The sixth section will summarize the work of this paper.

RELATED WORK

ABE Related Work

In 2005, Sahai et al. (Sahai & Waters, 2005) used the user's series of identity information (user attributes) to encrypt and decrypt the data, and proposed encryption based on fuzzy identity. In the (Goyal et al., 2006), two ABE constructors are proposed for the first time: (1) Key-Policy Attributes