Available online at www.sciencedirect.com

ScienceDirect

December 2017, 24(6): 49–54
www.sciencedirect.com/science/journal/10058885

The Journal of China Universities of Posts and Telecommunications

http://jcupt.bupt.edu.cn

Access control scheme with attribute revocation for SWIM

Wu Zhijun (✉), Cui Zihan, Wang Caiyun, Lei Jin

School of Electronic Information and Automation, Civil Aviation University of China, Tianjin 300300, China

Abstract

Access control scheme is proposed for System Wide Information Management (SWIM) to address the problem of attribute revocation in practical applications. Based on the attribute based encryption (ABE), this scheme introduces the proxy re-encryption mechanism and key encrypting key (KEK) tree to realize fine-grained access control with attribute revocation. This paper defines the attributes according to the status quo of civil aviation. Compared with some other schemes proposed before, this scheme not only shortens the length of ciphertext (CT) and private key but also improves the efficiency of encryption and decryption. The scheme can resist collusion attacks and ensure the security of data in SWIM.

Keywords SWIM, access control, proxy re-encryption, attribute revocation

1 Introduction

The concept of SWIM originated in the late 1990's in parallel in Europe and the United States. International Civil Aviation Organization (ICAO) defined it as the international aviation information release system in 2005. SWIM is a large-scale distributed system. Its ultimate aim is to build a flexible, unified and efficient information interaction platform where the subsystems of business can interact safely [1]. As the cloud platform and other large-scale network, SWIM faces a lot of security threats. Since the data of SWIM involves sensitive information in the national aviation domain, preventing data leakage and privacy protection are the most important issues. The main reason for these problems is the occurrence of illegal access and unauthorized access. Access control is an important means to solve these problems. In order to ensure that authorized users can access the key information legally in SWIM, Federal Aviation Administration stipulates that the implementation of the SWIM concept seeks to provide quality information to the right people at the right time [2].

With continually deepening of security research on SWIM, the ABE has become a hot research topic in the field of access control. ABE can achieve fine-grained access control because of 'one-to-many' nature [3]. Depending on the decryption policy binding location, ABE is classified into two categories: key-policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In CP-ABE, private keys are integrated with attribute sets and CT are integrated with access policies. Only when the attribute set conform to an access policy, users can decrypt the CT, thus realizing access control. Due to the large number of subjects, the complex types of services and the changes of attributes in practical applications, SWIM puts a higher requirement for access control. Users whose attributes are revoked cannot access the previously authorized resource, thereby implementing the permission revocation [4].

Presently, most of the schemes are focused on supporting the decryption strategies which have richer descriptions rather than attribute revocation. Attribute revocation is divided into indirect revocation and direct revocation. Indirect revocation refers to updating private keys by an authorization agency or introducing a trusted third party to implement attribute revocation. This method is flexible, but the cost of revocation is relatively large. Direct revocation is that data owners embed the attribute

Received date: 03-03-2017
Corresponding author: Wu Zhijun, E-mail: zjwu@cauc.edu.cn
DOI: 10.1016/S1005-8885(17)60241-3

revocation list in the CT when implementing encryption, so the cost of revocation will be small. Boldyreva et al. [5] proposed to set a due date for each attribute. But the disadvantage was that attributes cannot be revoked immediately. Hur et al. [6] designed a scheme which revokes attributes immediately, but its efficiency of CT and key updating were low. Xie et al. [7] constructed an anonymous attribute-based encryption scheme, but attributes revocation was not taken into account. Yu et al. [8] used the version number to label the key and the CT, and introduced the proxy server. This method reduced the workload of the authorization agency greatly, but the encryption and the decryption time were associated with the number of the attributes. Consequently, the efficiency is low.

This paper proposes a new access control scheme based on the KEK tree, which integrates the version number and introduces the proxy re-encryption mechanism. According to the safety and the efficiency analysis, this scheme protects the confidentiality of data, and it has advantages in the time efficiency of encryption and decryption.

2 Definitions

2.1 Access structure

$P=\{P_1,P_2,...,P_n\}$ is a collection of participants and the access structure [9], τ is a nonempty subset of the set P. If τ is monotonous, there is $\forall A,B, A\in\tau$ and $A\subseteq B$, then $B\in\tau$. The attribute set belonging to τ is called the authorized set. Otherwise, the set is the non-authorized set.

Access structure tree is a common method used to represent access structures. Any monotonic access policy can be represented by an access structure tree [10]. In access structure tree, each non-leaf node is a threshold gate, which is described by a certain threshold and all the child nodes of the non-leaf node. If x is an arbitrary node, $n_{\text{child},x}$ represents the child of x and k_x is the threshold value of x, then $0<k_x<n_{\text{child},x}$. When $k_x=1$, x represents an 'OR' gate and when $k_x=n_{\text{child},x}$, x is an 'AND' gate. If x is a leaf node, $k_x=1$, and it is described by a specific attribute.

2.2 Bilinear mapping

G_1 and G_T are cyclic groups whose order is a prime p. If the mapping $e:G_1\times G_1\to G_T$ satisfies the following three properties, then e is a bilinear mapping from G_1 to G_T.

1) Bilinear: $\forall a,b\in Z_p, e(g^a,g^b)=e(g,g)^{ab}$.

2) Non-degenerative: if g is the generator of G_1, $e(g,g)$ is the generator of G_T.

3) Computability: $\forall u,v\in G, e(u,v)$ can be effectively calculated.

2.3 KEK tree

KEK tree which is based on the binary tree of users is shown in Fig. 1.

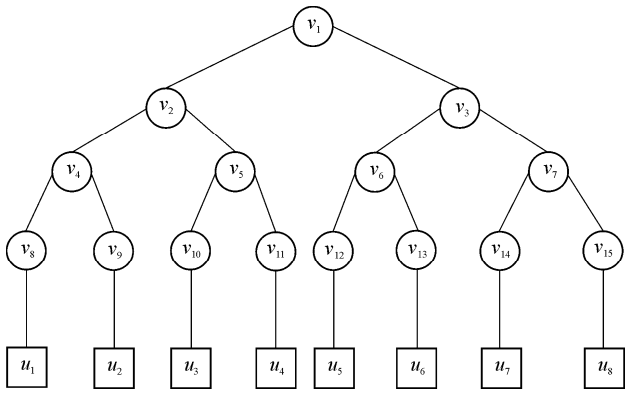

Fig. 1 Example of KEK tree

Users are distributed on leaf nodes which represent a collection of all users in the system. Each node v_j is given a random number K_j. It is obvious that there is a path between a leaf node and the root node, and the set of nodes on this path is defined as the path key $K_{\text{PK}}(t)$. For example, user 6 corresponds to the path key $K_{\text{PK}}(6)=\{K_{13},K_6,K_3,K_1\}$. Minimum coverage element [11] is the minimum node set which can cover all users of the attribute group G_t, $1\leqslant t\leqslant T$, in the KEK tree. For example, the minimum coverage element of $G_t=\{u_1,u_2,u_3,u_6,u_8\}$ is $K(G_t)=\{v_4,v_{10},v_{13},v_{15}\}$.

3 The access control scheme with attribute revocation

3.1 Attribute definition

In order to achieve attribute based access control (ABAC), the attributes of SWIM are defined.

ABAC classifies attributes into three categories: subject,