ACCESS CONTROL FOR THE CLOUD STORAGE

T. Galibus

Belarusian State University, Minsk, Belarus

When the organization or enterprise moves to the cloud infrastructure or rather switches to the distributed system paradigm, the problem of information security becomes especially important. One of the biggest challenges in the field of distributed networking is to provide the ultimate protection for the sensitive data. At the moment the security problem requires the fast-working and effective solution in the presence of mobile and wireless devices which are difficult to control.

One of the best ways to restrict the unauthorized access to the shared data is to use the strong cryptographic algorithm. Once the access policy is set and the secret keys are generated and distributed, the security of the system can be guaranteed.

We propose to control the access by means of attribute-based encryption [1] which allows not only to encrypt the data but also to configure the authorized users. In other words, in such encryption system the secret user keys depend on the additional attributes. In the general case, this encryption method requires a complicated implementation.

In our model the large-scale cloud storage has limited number of access user groups so that each user and each shared file belongs to a specific set of groups. This assumption allows us to propose a simplified key generation for the attribute-based access. Also, we introduce the additional key parameters that allow us to enhance the adaptive properties of the system.

In order to initialize the system of attribute-based encryption based on the simple selective principle we need the following:

1) The set of attributes:

$$t_1, t_2, \dots, t_n \in Z_q \text{where } q \text{ is prime}$$

The set of attributes corresponds to the set of the access group identifications:

$$Group1 \rightarrow t_1$$
$$Group2 \rightarrow t_2$$
$$\dots$$
$$Groupn \rightarrow t_n$$

2) The data M, or the hash-value of the open text.

3) The set of user attributes:

$$\{t_i\}_U$$

The set of attributes of the encrypted text

$$\{t_i\}_M$$

The access rule of the selective scheme is as follows:

If at least one attribute in the set $\{t_i\}_U$ is equal to the attribute in the set $\{t_i\}_M$, the corresponding user U can decrypt the text M.

This access rule is enough for the modeling of a large-scale cloud storage security policy based on the group access. So, the general complex structure of the ABE scheme can be simplified with this access control rules. The encryption system can be implemented as follows:

Initialization:

1) G is the group with the generator g;

2) The secret master-key which is stored on server and is accessible only for the administrator

$$MK = (t_1, \dots, t_n, y);$$

3) Public key which is evaluated according to the master-key and used to access the encrypted data:

$PK = (g^{t_1}, \dots, g^{t_n}, Y = e(g,g)^y)$, where e(g,g) is the bilinear pairing.

Key generation

The secret user key D is generation based on the user U attribute set:

$$\{t_i\}_U \to D = \{D_i = g^{yw/t_i}\}.$$

This key is sent to the user by the administrator. It depends on the master-key parameters and additional parameter $w \in Z_q$. This parameter serves for the D_i modification when the public keys need not to be changed.

Encryption

The encrypted text E consists of the encrypted message along with the attributes and the public key set$\{E_i\}$.

The additional parameter $s \in Z_q$ serves for the text re-encryption so that the secret user key set D_i need not to be changed:

$$E = Me(g,g)^{ysw}, \{E_i = g^{t_i s}\}_{\forall i \in \{t_i\}_M}.$$

Decryption

In order to access the value of M one must evaluate $Y^{sw} = e(g,g)^{ysw}$:

$$M = E/Y^{sw}$$

The user evaluates $e(g,g)^{ysw}$ using the secret key D_i which corresponds to the attribute t_i and the public key E_i:

$$e(g,g)^{ysw} = e(E_i, D_i) = e\left(g^{\frac{yw}{t_i}}, g^{t_i s}\right) = e(g,g)^{ysw}.$$

Our encryption system gives a practical solution to the problem of data security in the distributed networks i.e. providing the effective access control to the sensitive data. The algorithm provides additional adaptive parameters: once the user is deleted from the system, his secret key is not only automatically removed but also loses validity. Other properties include re-encryption, access delegation, key expiry period and collaborative access configuration.

References

J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute-based encryption, in Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334, 2007.