An Access Control of Ciphertext-Policy Attribute-Based Encryption with Revocation by Version Number in Cloud Computing

Shi-Jinn Horng [(1)], Cheng-Chung Lu [(1)]

[(1)] Dept of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei, 10607, Taiwan, R.O.C.
Phone Number: (02)27376700 and e-mail: horngsj@yahoo.com.tw

1. Introduction – Cloud computing is one of the most popular paradigms in IT industry. The shared data were uploaded to cloud provider by some users and those uploaded data may include valuable information or personal privacy. Since these data are usually essential and out of control by users, users are very concerned about the security of the stored data. On the other hand, the data owners should be able to designate who can access the shared data. Ciphertext-policy attribute-based encryption (CP-ABE) algorithm [1] proposed a party encrypting data determined by a set of attributes to composing a policy for indicating who can decrypt it. Existing CP-ABE schemes cannot be directly applied to multi-authority cloud storage systems, owing to the inefficiency of decryption and revocation. Furthermore, users join or leave are very often and attributes vary frequently; a single authority server may form the bottleneck of the system. In order to make CP-ABE more applicable to the cloud, we proposed a method to include user and attribute revocation mechanisms by the version number of the attribute for CP-ABE. Our method employed multi-authority servers to distribute attributes for making CP-ABE more suitable multi-tenant property in the cloud. In addition, both compromised attack and collusion attack were discussed to the proposed method.

2. Experimental – The system model is shown in Fig. 1. AS generates system public key and master key. ACs register to the AS and generate attribute secret keys and public keys for each attribute. Each AC maintains a local attribute list (LAL). AS collects LAL from ACs and forms the global attributes list (GAL). Users register to AS to get the UID. Then, user can interact with ACs to request attributes to get the private keys. Any user can upload the encrypted data to cloud which can then be downloaded, if attribute set is matched to the attribute policy. The revocation is done by version number.

3. Results and Discussion –Table 1 shows the comparison and the proposed approach is better.

Tabla 1. Comparison of Attribute-Based Encryption schemes

Schemes	Enc time	Dec time	Public key	Ciphertext	Secret key	Privacy	Rev.
CP-ABE [1]	$(1+2n_T)E+P$	$(n_T+n+2)P$	$4\|G_0\|+\|G_T\|$	$(2n_T+1)\|G_0\|+\|G_T\|$	$(2n_{uid}+1)\|G_0\|$	No	No
ABBE [2]	3E+P	2P	$2\|G_0\|+(N(n_{uid}+n_T)n_T+1)\|G_1\|+3\|G_T\|+(N+n_1n_T+n_{uid})\|Z_p\|$	$(n_T+1)\|G_1\|$	$\|G_0\|$	No	Yes
CP-ABE-ET [3]	(2N+11)E	$(8n_T+5)E+12P$	$(N+7)\|G_0\|+6\|G_2\|$	$8\|G_0\|+\|Z_p\|$	$4\|G_0\|+6n_1\|G_1\|$	No	No
ECP-ABE [4]	$3Tz_N$	$3Tz_N$	$(N+4)\ \|Z_p\|$	$3\|G_0\|+\|M\|$	$2\|G_0\|$	No	No
KP-ABE-ET [5]	$(n_1+n_2+3)E$	$(n_1+n_2+2)E+(n_1+n_2)P$	$N\|G_0\|+2\|G_1\|+3\|H\|$	$(2n_2+4)\|G_0\|+2\|Z_p\|$	$2n_1\|G_0\|$	No	No
CP-ABE-CSK [6]	$2(N-n_T+1)E$	$(2n_{uid}-2n_T+1)E+3P$	$N\|G_0\|+(N+1)\|G_1\|+\|G_T\|$	$(n-n_T+2)\|G_0\|+\|G_T\|$	$2\|G_0\|$	No	No
Our scheme	$(1+2n_T)E+P$	$(n_T+n+2)P$	$(2mn_t+5)\|G_0\|+\|G_T\|$	$(2n_T+1)\|G_0\|+\|G_T\|$	$(n_{uid}+1)\|G_0\|$	Yes	Yes

4. Conclusions - In this paper, we have proposed an effective data access control CP-ABE scheme for multiple attributes centers cloud storage systems through version number of attribute with revocation flag. The proposed system not only can keep user privacy but is secure from various attacks.

5. References

[1] J. Bethencourt, etc, "Ciphertext-policy attribute-based encryption," IEEE SP'07, 2007, pp. 321-334.

[2] Canard, S., etc, "Attribute-based broadcast encryption scheme for lightweight devices," IET Information Security, 2018, pp. 52-59.

[3] Wang, Q., etc, "Ciphertext-policy attribute-based encryption with delegated equality test in cloud computing," IEEE Access, 2018, pp. 760-771.

[4] Odelu, V., etc., "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts," IEEE Access, 2017, pp. 3273-3283.

[5] Zhu, H., etc, "Key-policy attribute-based encryption with equality test in cloud computing," IEEE Access, 2017, pp. 20428-20439.

[6] Fuchun Guo, etc, “CP-ABE with constant-size keys for lightweight devices,” IEEE IIFS, 2014, pp. 763-771.