Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (22): 5516-5519, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.5516.5519

Remote Attestation Based on CP-ABE Algorithm

[1]Yong Zhao, [1]Junxi Zhuang and [2]Yanxue Zhang
[1]College of Computer Science, Beijing University of Technology, Beijing, 100124, China
[2]College of Mathematics and Information Science, Hebei Normal University,
Shijiazhuang, 050000, China

Abstract: Remote attestation and CP-ABE (ciphertext policy-attribute based encryption) algorithm are Independent of each other. In this study, by the analysis and comparison of existing remote attestation technology and CP-ABE algorithm, we propose a remote attestation scheme based on the CP-ABE algorithm. Remote attestation scheme based on the CP-ABE algorithm includes both remote attestation with a virtual computing node and remote attestation with a group of virtual computing nodes. By a analysis, we verify the security and efficiency of the program.

Key words: Cloud storage, remote attestation, CP-ABE algorithm, group remote attestation

INTRODUCTION

Cloud storage is an important , basic system in cloud computing and there exist many security problems (Cachin *et al*., 2009) Access control is a important tool to achieve the confidentiality for users' data and privacy protection for users. Cloud storage providers cannot be trusted completely, since it is possible for them to create the data leakage to obtain more. Based on the problem, CP-ABE (ciphertext policy-attribute based encryption) algorithm was proposed (Goyal *et al*., 2006; Bethencourt *et al*., 2007; Flood *et al*., 2010; Sun *et al*., 2011), CP-ABE algorithm defines a user's identity a set of attributes, ciphertext is fully associative with access control structure, decryption relys on user's identity attribute matches access control structures.

In CP-ABE algorithm, the user can access the ciphertext of the key. If and only if the user has the corresponding attribute, the user can decrypt the ciphertext to the plaintext. Essentially, the key ciphertext also has some confidentiality, so it should not be obtained by all platforms. It is necessary to guarantee the trust of the platforms.

In the trusted cloud computing model, if users want to access the storage, they should provide the remote attestation. Remote attestation is one of the core technologies of trusted computing and many achievements have been made in remote attestation. A typical research is the binary remote authentication proof which is supported by TCG and has become the basis of remote attestation (Wang *et al*., 2008; Schelleken *et al*., 2008). The authors (Martin *et al*., 2009; Chen *et al*., 2006; Li *et al*., 2009) proposed property-based remote attestation. The scheme don't need verify the platform configuration, but verify the property certificate of the platform. There is a shortage of the existing remote attestation in cloud computing , that is, the verifier need to verify every remote attestation completely,(both the signature and the trust of the platform), which burden the verifier.

In order to improve the efficiency of cloud storage, the storing virtual computing nodes does not have to verify the trust of all platforms, it only verify the trust of the platform which has certain property. Based on this, in this study, we support the remote attestation based on CP-ABE algorithm.

which combines the CP-ABE algorithm and remote attestation technology and improves the efficiency of cloud storage.

In this study, two types of virtual machines are referred, that is, the user virtual computing node and the storage computing node. The user virtual computing node is operated by users and the storage computing node stores various data.

CP-ABE ALGORITHM

Property: Let $P = \{P_1, ..., P_n\}$ be a set of all properties. Then, the property of the user A is a non-empty subset of P, $A \subseteq \{P_1, ..., P_n\}$. n properties have 2^n subset and can distinguish 2^n-1 users.

Access structure: Access structure is a non-empty subset of $P = \{P_1, ..., P_n\}$, $T \subseteq 2^{\{P1,..., Pn\}} \setminus_{\Phi}$. T stands by a judgment condition of the property. We call the property set as authorization set, If $A \subseteq T$. Otherwise We call the property set A as unauthorized set.

Corresponding Author: Yong Zhao, College of Computer Science, Beijing University of Technology, Beijing, 100124, China

Access tree: The access tree describes the access structure. The leaf node of the tree stands by a property, each inner node stands by a relation, such as and (n of n), OR(1 of n) and n of m (m>n).

CP-ABE algorithm has four steps as follows:

- Setup, generate the master key MK and the public parameter PK
- CT = Encrypt (PK, MT), Using the public parameter PK, the access structure T and the plaintext M to obtain the ciphertext CT
- SK = KcyGen (M, A). Using the master key MK and the property set to generate privacy key Sk
- M =Dncrypt (CT, Sk), Using the privacy key Sk and the ciphertext CT to obtain the plaintext M

DESIGN OF THE SCHEME

G_a are defined as multiplicative group whose order is p and g is the generator of G_a. H: $\{0, 1\}^* \rightarrow G_a$ is a cryptographic security function. So, the public parameter is (G_a, g, P, H).

CP-ABE property generator issues two access structuresT_1, T. The data owner chooses the data secret key key and the challenge number r $\in Z^*_p$. The data owner calculates CT = Enccrypt (PK, key, T), CT_1 = Encrypt (PK, r, T_1). When the user virtual computing node access the data, the user virtual computing node should firstly decrypt CT_2 and obtain r, then the user virtual computing node support the remote attestation for the data owner, finally user virtual computing node decrypt CT_1 and obtain key.

The remote attestation based on CP-ABE algorithm has a advantage that if and only if the user virtual computing node can decrypt CT_2 and obtain r, the user virtual computing node can support the remote attestation.

Remote attestation based on CP-ABE algorithm: Let A be the storage computing node and B be the user virtual computing node:

- A chooses r$\in Z^*_p$. A calculates and stores CT_1 = Encrypt (PK, r, T). A send the PCR number for the remote attestation to B
- B decrypt CT_1 with SKB, r = Dncrypt (CT_1, Sk). If B failed to decrypt CT_1, that is to say the property set B has cannot satisfy the access structure T_1, the access stops. Otherwise B obtain r
- TPMB sends sig {PCR, r, AIK_B} AIKB, PCR to A
- The storage computing node A firstly verify the validity of AIK_B. Then A verify the signature sig {PCR, r, AIK_B}. Finally A determines whether credible platform B by recalculating PCR by SML and comparing the result with the received PCR
- If B is trusted, B B decrypt CT to obtain key. If B failed to v decrypt CT, that is to say the property set B has cannot satisfy the access structure T_2, the access stops. B accesses the data by key as in [2, 3]

Group remote attestation based on CP-ABE algorithm: In 3.1, If the user virtual computing node B can decrypt CT_1 and obtain r, B can support the remote attestation. To support the trust of the scheme, A applies the threshold strategy and chooses a polynomial:

$$f(x) = r + a_1 x ..... + a_t x^{t-1} \bmod p \quad (1)$$

where, t, s, …., $\alpha_t \in Z^*p$.

A issues n numbers $CT_i 1 \le i \le n$ which are mutually independent. Where CT_i = Encrypt (PK, r_i, T_i) , r_i = f (i) and T_i are different access structure.

A issues $g_i = g^{ai}$ $(0 \le i \le n-1)$ and each r_i satisfies:

$$g^{f(i)} = \bigcup_{k=1}^{t} g_i i^k \quad (2)$$

If B wants to obtain r, B need to decrypt CT_i and obtain at least t different r_i. There are two methods:

- B has a property T_B satisfying:

$$T_B = \bigcup_{k=1}^{t} T_k \ (i_k \ne i_j, k \ne j) \quad (3)$$

Then, B can obtain t different r_i and B obtain r from:

$$\sum_{i=1}^{t} L_i r_i = r$$

B decrypt CT_i with the group it lies, the access structures of the group number satisfy:

$$T_l = \bigcup_{k=1}^{l'} T_{i_k} \ (i_k \ne i_j, k \ne j) \ (1 \le l \le m) \quad \sum_{l=1}^{m} l' \ge t \quad (4)$$

Then, B can obtain t different r_i and B obtain r from

$$\sum_{i=1}^{t} L_i r_i = r$$

- **Next steps is the same with 3.1:** Let E be the calculation of verifying the signature in the remote

Table 1: Comparing efficiency with t times remote attestation

	E	D	In all
Efficiency with CP-ABE	t	αt	$t+\alpha t$
Efficiency without CP-ABE	t	t	2t

attestation and D be the calculation of verifying the trust of the platform. We assume the rate that the user virtual computing node cannot obtain r is $\alpha \in [0, 1]$. The efficiency of the scheme is showed as follows.

SECURITY ANALYSIS

Here we give the key exchange process of the protocol. The detailed process is listed as follows:

$$A->B:PCRS,CT_i,g^{N_1} \tag{5}$$

$$B->A:sig\{PCR,r,SAIK_B\},SML,PAIK_B,g^{N_2} \tag{6}$$

$$A->B:CT,\{N\}_{K_{AB}} \tag{7}$$

$$B->A:\{N+1\}_{K_{AB}} \tag{8}$$

Here we use Ban Logic [18] to obtain the Formalized proof of the protocol.

Detailed description of the protocol:

$$B->A:\{PCR,r,B|\Rightarrow AIK_B\}_{SAIK_B},SML,PAIK_B,g^{N_2} \tag{9}$$

$$A->B:CT,\{N,(A\xleftrightarrow{K_{AB}}B)\}_{K_{AB}} \tag{10}$$

$$B->A:\{N,(A\xleftrightarrow{K_{AB}}B)\}_{K_{AB}} \tag{11}$$

Assumption:

$$A|\equiv B|\Rightarrow AIK_B \tag{12}$$

$$B|\equiv CTK \tag{13}$$

where, CTK Guarantee B can obtain r.

Freshness of random numbers:

$$A|\equiv \#(N_1) \tag{14}$$

$$B|\equiv \#(N_2) \tag{15}$$

$$A|\equiv \#(N) \tag{16}$$

Target of the protocol:

$$A|\equiv A\xleftrightarrow{K_{AB}}B \tag{17}$$

$$B|\equiv A\xleftrightarrow{K_{AB}}B \tag{18}$$

$$A|\equiv B|\equiv A\xleftrightarrow{K_{AB}}B \tag{19}$$

$$B|\equiv A|\equiv A\xleftrightarrow{K_{AB}}B \tag{20}$$

Some rules of the Ban Logic applied in this study are listed as follows:

$$\frac{P|\equiv Q\xleftrightarrow{K}P,P\triangleleft\{X\}_K}{P|\equiv Q\sim X} \tag{21}$$

$$\frac{P|\equiv \#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X} \tag{22}$$

$$\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X} \tag{23}$$

$$\frac{P|\equiv X,P|\equiv Y}{P|\equiv (X,Y)} \tag{24}$$

$$\frac{P|\equiv (X,Y)}{P|\equiv X} \tag{25}$$

$$\frac{P|\equiv Q|\equiv (X,Y)}{P|\equiv Q|\equiv X} \tag{26}$$

$$\frac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X} \tag{27}$$

$$\frac{P\triangleleft (X,Y)}{P\triangleleft X} \tag{28}$$

$$\frac{P|\equiv Q\xleftrightarrow{K}P,P\triangleleft\{X\}_K}{P\triangleleft X} \tag{29}$$

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)} \tag{30}$$

Proof: From (9), we have:

$$A\triangleleft\{PCR,r,B|\Rightarrow AIK_B\}_{SAIK_B},SML,PAIK_B,g^{N_2} \tag{47}$$

From (12), (21), we obtain:

$$A|\equiv B\sim\{PCR,r,B|\Rightarrow AIK_B\} \tag{48}$$

It follows from (14), (22) that:

$$A|\equiv B|\equiv\{PCR,r,B|\Rightarrow AIK_B\} \tag{50}$$

By Matsumoto-Takashima-Imai Key exchange protocol:

$$A \mid\equiv A \xleftrightarrow{K_{AB}} B \tag{51}$$

$$B \mid\equiv A \xleftrightarrow{K_{AB}} B \tag{52}$$

$$K_{AB} = g^{N_2 x_A + N_2 x_A} \tag{53}$$

With (10), (21) , we have:

$$A \mid\equiv B \sim \{N, A \xleftrightarrow{K_{AB}} B\} \tag{54}$$

It follows from (60) that:

$$A \mid\equiv B \mid\equiv \{N, A \xleftrightarrow{K_{AB}} B\} \tag{55}$$

Then:

$$A \mid\equiv B \mid\equiv A \xleftrightarrow{K_{AB}} B \tag{56}$$

Then (19) holds true.

From (11), we have:

$$B \lhd \{N, A \xleftrightarrow{K_{AB}} B\} \tag{57}$$

By (12), (21), we obtain:

$$B \mid\equiv A \sim \{N, A \xleftrightarrow{K_{AB}} B\} \tag{58}$$

Then, we have:

$$B \mid\equiv A \mid\equiv A \xleftrightarrow{K_{AB}} B \tag{59}$$

CONCLUSION

Based on the shortage of the existing remote attestation in cloud computing that the verifier need to verify every remote attestation completely,(both the signature and the trust of the platform). we propose aa remote attestation scheme based on the CP-ABE algorithm which combines the CP-ABE algorithm and remote attestation technology. By a analysis, we verify the security and efficiency of the program.

ACKNOWLEDGMENTS

This study was supported by National Science and Technology Major Project under Grant No. 2012ZX03002003.

REFERENCES

Bethencourt, J., A. Sahai and B. Waters, 2007. Ciphertext-policy attribute-based encryption. Proceedings of the IEEE Symposium on Security and Privacy, May 20-23, 2007, Berkeley, CA., pp: 321-334.

Cachin, C., I. Keidar and A. Shraer, 2009. Trusting the cloud. ACM SIGACT News, 40: 81-86.

Chen, L., R. Landfermann, H. Lohr, M. Rohe, A.R. Sadeghi and C. Stuble, 2006. A protocol for property-based attestation. Proceedings of the 1st ACM Workshop on Scalable Trusted Computing, November 3, 2006, Alexandria, VA., USA., pp: 7-16.

Flood, C., M. Zhang and D. Feng, 2010. AB-ACCS: A cloud storage ciphertext access control method. Comput. Res. Dev., 47: 259-265.

Goyal, V., O. Pandey, A. Sahai and B. Waters, 2006. Attribute basedencryptionfor fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security, October 30-November 3, 2006, Virginia, USA., pp: 89-98.

Li, S.J., Y.P. He, D.M. Liu and C.Y. Yuan, 2009. On privacy of property-based remote attestation. J. Commun., 30: 146-152.

Martin, P., T. Ronald, H. Daniel and P. Danner, 2009. A privacy for anonymity and trust. Proceedings of the 2nd International Conference on Trusted Computing, April 6-8, 2009, Oxford, UK., pp: 101-119.

Schelleken, D., B. Wyseur and B. Preneel, 2008. Remote attestation on legacy operating systems with trusted platform modules. Electron. Notes Theor. Comput. Sci., 197: 59-72.

Sun, G.Z., Y. Dong and Y. Li, 2011. CP-ABE based data access control for cloud storage. J. Commun., 32: 146-152.

Wang, J.S., Z. Yu and G. Li, 2008. Study of trusted chain technology of computing trusted. Comput. Eng. Des., 29: 2195-2198.