World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:11, 2016

A Security Cloud Storage Scheme Based Accountable Key-Policy Attribute-Based Encryption without Key Escrow

Ming Lun Wang, Yan Wang, Ning Ruo Sun

***Abstract*—**With the development of cloud computing, more and more users start to utilize the cloud storage service. However, there exist some issues: 1) cloud server steals the shared data, 2) sharers collude with the cloud server to steal the shared data, 3) cloud server tampers the shared data, 4) sharers and key generation center (KGC) conspire to steal the shared data. In this paper, we use advanced encryption standard (AES), hash algorithms, and accountable key-policy attribute-based encryption without key escrow (WOKE-AKP-ABE) to build a security cloud storage scheme. Moreover, the data are encrypted to protect the privacy. We use hash algorithms to prevent the cloud server from tampering the data uploaded to the cloud. Analysis results show that this scheme can resist conspired attacks.

***Keywords*—**Cloud storage security, sharing storage, attributes, Hash algorithm.

I. Introduction

WITH the rapid development of cloud computing, more people start using the organization cloud resources. The cloud storage service mode is divided into two categories: the first category is the storage dedicated to the stored data files in the cloud and only holder of the data files can use, and the other one is the shared storage where the data stored in the cloud can be shared with many users.

Wang et al. [1] designed a middleware based on a cloud storage sharing program, which is divided into two main layers: cloud management and storage management. There is a middle layer between the cloud management and storage management. In this scheme, the data files are stored in Plain text format. There is a problem related to the passive attack in the scheme.

On the 2010 IEEE Conference of cloud computing, Zhao et al. [2] designed a cloud storage sharing program based on elliptic curve (Elliptic Curve Discrete Logarithm Problem). This program prevents the cloud servers and the illegal users from accessing the data stored in the cloud, but it does not take the tampering of data into account.

Sowmya et al. [3] built a scheme with the signature threshold mechanism. They achieved the purpose of sharing data. However, there is a possibility of a collusion attack in this scheme.

In order to solve the cloud server passive attacks, active attacks, and collusion attacks, we design a safe and efficient cloud storage sharing scheme. In this paper, we use proxy re-encryption and distributed storage [4] model to introduce the cloud storage sharing model. In order to solve the problems associated with the cloud storage server's passive attacks, we will use AES encryption to encrypt the data stored in the cloud. In order to ensure the integrity verifiability and integrity of the data, we use Hash function. WOKE-AKP-ABE [5] will be used in the technology of cloud storage solutions to achieve the function that permits many to use the cipher text. In this scheme, we also increase the utilization efficiency of the throughout network. The result shows that our scheme is safe and efficient.

Ming Lun Wang is with the Department of Computer Science, Lianyungang Port Group CO., CLD.Railway Transportation Branch Company, Jiangsu, 222000, China (E-mail: 471014543@qq.com).

Yan Wang is with the Huai'an College of Information Technology, Jiangsu, 223003, China.

Ning Ruo Sun is with the Jiangsu Heng Rui Medicine CO., LTD, Jiangsu, 222000, China.

II. Related Information

Definition 1. Definition of access structures $\{p_1, p_2,\ldots, p_n\}$ is a set of features, the set $A \in 2^{\{p1p2,\ldots,pn\}}$ is monotonic, and if $b \in A$ and $b \subseteq c$, so $c \in A$, $A \subseteq 2^{\{p1p2,\ldots,pn\}} \setminus \{\phi\}$ is a nonempty subset of $\{p_1,p_2,\ldots,p_n\}$ that is an monotonic access structure.

Definition 2. Decisional Diffie-Hellman problem (DDHP) : Suppose (G) is a group of order q, g is a generator of (G). DDHP is: given triples (g^a, g^b, g^c), wherein the random elements a, b, $c \in Zq$ *, judge $g^c = g^{ab}$ established or not.

Definition 3. Bilinear mapping pairing: Bilinear function, e: $G_1 \times G_1 \rightarrow G_2$, complies with the following properties:

A: Bilinear: If P, $Q \in G_1$ and, a, $b \in Z_p$*, then e (aP, bQ) = e (P, Q) ^{ab}.

B: Non-degenerate: satisfy e (P, P) = 1.

C: It can be calculated: If P, $Q \in G_1$, then let e (P, Q) $\in G_2$ be computed in polynomial time.

Definition 4. Q-augmented decisional bilinear Diffie-Hellman exponent assumption (q-ADBDHE): Suppose q-ADBDBHE. Given tuple (h, $h^{\alpha^{q+2}}$ q+2, g, g^{α}, g^{α^2},…., g^{α^q}, $g^{\alpha^{q+2}}$, $e(g,h)^{\alpha^{q+1}}$) and (h, $h^{\alpha^{q+2}}$, g, g^{α}, g^{α^2},…., g^{α^q}, $g^{\alpha^{q+2}}$, $e(g,h)^{\alpha^{q+1}}$), there is no opponent which can distinguish above two Yuan groups with non-negligible probability in polynomial time, where $h \in G_0$, $\alpha \in Z_p$ is random.

III. Secure Cloud Storage Model

CPC model includes six algorithms: AES, KGC-Setup (λ), AA-Setup (PKKGC), KeyGen (T, PKKGC, MKAA, PK, ID) Encrypt (M, PK), Decrypt (E, SK).

A. Alice is the data owner, who uses AES to encrypt the data, AES key (m) = c
B. Alice upload the data encrypted to the storage server
C. KGC-Setup (λ). Input system security parameter λ to initialization algorithm, then, output PKKGC of the system of public parameters of KGC and the master key MKKGC of KGC.
D. AA-Setup (PKKGC). Input the public parameters PKKGC of KGC, output the system public parameters PKAA and the master key MKAA. Thereby, obtain a complete public system parameter (PK=PK∪PKAA4) KeyGen (T, PKKGC, MKAA, PK, ID).
E. KeyGen (T, PKKGC, MKAA, PK, ID). The key generation algorithm is composed of two protocols: ① KGC and user make user identity $d_{ID,T}$ by protocol; ② KGC and AA make user key D relevant part of the structure of T by protocol. d_{ID} and D make up SK the user's key.
F. Encrypt (M, PK). input message M, a set of attributes γ, public system parameter PK, to Encryption algorithm, output cipher text E.
G. Decrypt (E, SK). input cipher text E and key SK to Decryption algorithms. If T (γ) = 1, the user can decrypt E, otherwise fails to decrypt.
H. Bob uses symmetric encryption to decrypt the dat, Dec (c) = m.

This model contains seven stages, such as:

Stage 1. KGC computes and announces public parameters PKKGC;
Stage 2. AA calculates and announces the publicity system parameters PKAA;
Stage 3. KGC confirms Bob;
Stage 4. AA confirms Bob;
Stage 5. Alice encrypts the data and uploads to the cloud storage;
Stage 6. Alice encrypts and announces the cipher text of the key;
Stage 7. Bob downloads the cipher text of c from the cloud storage and decrypts it.

IV. Based WOKE-AKP-BAE Cloud Storage Scheme

G_0 is of a bilinear group of p prime order, g is a generator of G_0. Bilinear map e: $G_0 \times G_0 \rightarrow G_1$ the security parameter λ determines the group size. Lagrange multiplier, Δ_i, $S(x)=\prod_{j\in S, j\neq i} \frac{x-j}{i-j}$, where S is a set of integers, i∈S.

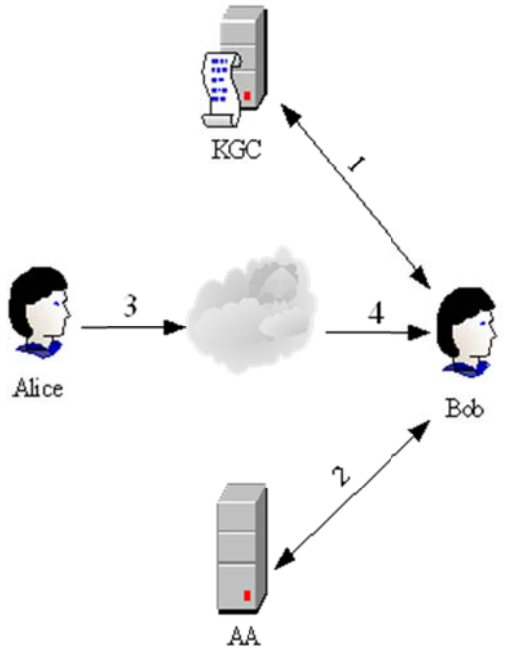

Fig. 1 Secure Cloud Storage Model Based Attribute-Based Encryption

A. KGC-Setup (λ)

KGC chooses a bilinear group (G_0, G_1, e, p) of $P>2^{\lambda}$ prime order, g is a generator of G_0. Select random numbers y_1, y_2, $\alpha \in Z_p$, randomly select an element g_2 from G_0. Thereafter, select $t_1, t_2, \ldots, t_{n+1}$ from G_0, and N = {1, 2, ..., n+1}.

Defined functions T, $T(x)= g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta i, N(X)}$, T can be regarded as $g_2^{X^n}$, $g^{h(x)}$, where h (X) is a polynomial of order n. The public parameters $PK_{KGC} = h=g^{y1}$, $m=g^{\alpha}$, $o=g^{y2}$, $g_2, t_1, t_2, \ldots, t_{n+1}$, the master key is $MK_{KGC}=y_1, y_2, \alpha$.

B. AA-Setup (PK_{KGC})

A is a random number $t \in Z_p$, public parameter $PK_{AA} l=g^{y2t}$, MKAA=t is master key, thus, the system public parameters of $PK=\{h=g^{y1}, m=g^{\alpha}, o=g^{y2}, g_2, t_1, t_2, \ldots, t_{n+1}, l=g^{y2t}\}$

C. KeyGen (T, PKKGC, MKAA, PK, ID)

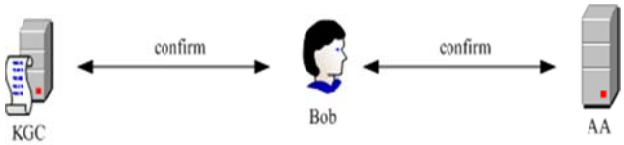

Fig. 2 Confirmation Stage

A. KGC and AA authenticate the user's identity referred to as Bob ID ∈ Zp.
B. Bob randomly selects s_0. θ∈Zp, passed R=g-so(gαg-ID)θ to the KGC, then runs a zero-knowledge protocol to prove that they have (so, θ) to KGC.
C. If the zero knowledge proof protocol failed, KGC outputs ⊥; otherwise, KGC randomly selects $S_1 \in Zp$, sends the $d_{\cdot ID,T}=(d_{\cdot 1}, d_{\cdot 2})=((g_2 y_1 Rg\text{-}s_1))1/(\alpha\text{-ID}), s_1)$ to Bob.

D. Bob calculates $D_{id,T}=(d1,d2)=(d_1 \cdot /g_\theta, d_2'+so)=((g_2 y_1 g-(s_o+s_1))1/(\alpha-ID), s_0+s_1)$

E. The set that is constituted with the leaf node of T referred to AA, KGC; use the Key Generation algorithms of paper [6], the only difference is qr(0)=y2, to calculate D'={D'x =g2qx(o)T(i)rx, where i=att(x),Rx'=grx} x∈AS, then send D' to AA.

F. AA calculated D={Dx=(Dx')l=$g_2$tqx(o)T(i)trx}, i=att(x), Rx=(Rx')t=gtrx}x∈AS, and send D to Bob.

G. The full key of Bob is SK = SK=(d_1, d_2, D)

H. Firstly, Alice selects key∈G_1. Then, calculates the AES key(m)=c, uploads c to the cloud storage.

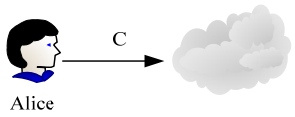

Fig. 3 Alice Uploading Data Phase

D. Encrypt (key, γ, PK)

In order to encrypt key∈G_1 in the tribute set of γ, Alice chooses a random number s ∈ Z_p, announces the cipher text E=(γ, E_1, E_2, E_3, E_4, E_5)

= (γ, keye (hl, g_2)^s), {T(i)^s}$_{i\in\gamma}$,g^s, m^s, e(g, g)^s)

= (γ, keye (g^{y1}, g^{y2t}, g^2)^s, {T(i)^s}$_{i\in\gamma}$, g^s, $g^{\alpha s}$, e(g,g)^s)

E. Decrypt (E, SK)

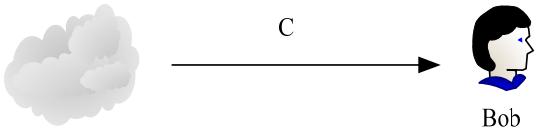

Fig. 4 Bob Downloading Data Phase

If T (x) = 1, Bob can decrypt E.

First, Bob uses calls for the Decryption algorithm of [6], calculates e(g, g_2)^{sy2t}. Then, Bob decrypts E as

$$E=\frac{E_1}{e(E_4 E_3^{-ID}, d_1) E_5^{d2} e(g, g_2)^{sy_2 t}}$$

$$=\frac{keye(g,g_2)^{sy_1} e(g,g_2)^{sy_2 t}}{e(g^s, g_2^{y1} g^{-(s_0+s_1)}) e(g,g)^{s(s_0+s_1)} e(g,g2)^{sy_2 t})}$$

$$\frac{keye(g^{y_1} g^{y_2 t}, g_2)^s}{=e(g^{s(\alpha-ID)}, (g_2^{y1} g-(s_0+s_1)^{\frac{1}{(\alpha-ID)}}) e(g,g)^{s(s_0+s_1)} e(g,g2)^{sy_2 t})}$$

=key

F. TraceD (PK, SK)

We will give a method to judge whether a descrambler D from the user Bob's key SK. D is dongle about the access structure T. In addition, SK corresponding access structures referred to as T '.

A. Choose a random number s, s'∈Z_p, calculated E_3=g^s, E_4=$g^{\alpha s}$, E_5=e(g,g)$^{s'}$

B. Randomly select γ set of attributes, T (γ) = 1, and T '(γ) = 1, calculate E_2={T(i)^s}$_{i\in\gamma}$.

C. Randomly select key∈G_1, calculate E_1=key·e($E_4 E_3^{-ID}$, d_1)E_5^{d2}e(g^{y2t},g_2)^s.

If D output key'∈G_1, and key '= key, then D is from Bob; otherwise, D has nothing to do with Bob.

E. Bob can AES_{key} (c) = m

V. Security Proof

The following programs will prove the correctness, data confidentiality, and verifiability of this program.

Conclusion 1. New scheme satisfies correctness.

Proof: If the parties are to abide by the agreement, then Bob can get the original plaintext m:

$$AES_{key}^{-1}(c) = AES_{key}^{-1}(AES_{key}(m)) = m$$

Conclusion 2. This scheme meets the confidentiality of data.

Proof: Our scheme of data files to be stored uses AES to encrypt.

There are two most effective ways to attack the traditional block cipher. The first one is the linear analysis, and the second is the differential analysis; it has been clearly stated in the literature, the two most important designs from Rijndael [7] algorithm index have a strong anti-linear analysis and differential. So, data encrypted and stored in the cloud program are confidential QED.

Conclusion 3. This scheme meets the resistance of malicious KGC.

It is assumed that KGC wants to decrypt any ciphertext E= (γ, E_1, E_2, E_3, E_4, E_5)= (γ, Me($g^{y1}g^{y2y}$,g_2)^s, {T(i)^s}$_{i\in\gamma}$, g^s, $g^{\alpha s}$, e(g,g)^s), but the KGC did not know t, apparently KGC unable to decrypt the ciphertext. Therefore, the proposed scheme can resist the malicious KGC. QED.

Conclusion 4. The scheme can resist the collusion attack.

AA only knows part of the master key information; therefore, the proposed scheme can resist the adversary 3. Rival 6 is defined as a conspiracy of KGC and malicious users. Since KGC cannot be known, KGC can only be restored e(g, g_2)^{sy2t} by key of the malicious user. If the attribute set of cipher text structure does not satisfy the user's access, the rival cannot get e(g, g_2)^{sy2t}. Therefore, the proposed scheme can resist the adversary.

VI. Summary

This article describes a secure cloud storage solutions based on the technology of accountable key-policy attribute-based encryption scheme without key escrow and distributed storage model. This article uses the AES encryption algorithm to encrypt data files uploaded to the cloud, and the zero-knowledge protocol is used to prove that Bob has (so, θ) to KGC and AA. We prove that this scheme fulfills the correctness integrity and the confidentiality of data. This scheme meets the resistance of malicious KGC and resists the collusion attack, thus this program is suitable for practical use.

REFERENCES

[1] Wang Cong, Wang Qian, Ren Kui, et al. Privace-Preserving public Auditing for Data Storage Security in Cloud Computing(c)//Proceedings of the 29th IEEE Conference on Computer Communications.2010: pp. 1-9.

[2] Zhao Gan-sen, Rong Chun-ming, Jin Li, el. Trusted Data Sharing Over Untrusted Cloud Storage Provides (c)//Proceedings of the 2nd IEEE Conference on Cloud Computing Technology and Science. 2010: pp. 97-103.

[3] M. Sowmya Varshini, D. Palanikkumar, G. Rathi. An Improved Security Enabled Distribution of Protected Cloud Storage Services by Zero-Knowledge Proof based on RSA Assumption (c)// International Journal of Computer Applications, 2012, Volume 40, No. 5: pp.18-22

[4] Hui jun Xiong, Xin wen Zhang, Wei Zhu, Dan feng Yao.CloudSeal: End-to-End Content Protection in Cloud-based Storage and Delivery Services.7th International ICST Conference, Secure Comm. 2011: pp. 491-500.

[5] Zhang Xing, Wen Zilong, Shen Qingni, Fang Yuejian, Wu Zhenghua. Accountable Attribute-Based Encryption Scheme Without Key Escrow (c)// Journal Of Computer Research and Development : 2015:2293-2303.

[6] Goyal V, Pandey O, Sshai A, et al, Attribute-based encryption for fine-grained access control of encrypted data (c)Proc of CCS 2006, New York: ACM, 2006; 89-98.

[7] Dae. men, V, Rij. men. AES proposal: Rij.ndael (Version 2) (EB). Available: NIST AES websitecsrc.nist.gov/ encryption/ aes.

Minglun Wang was born in 1983. Master. His main research interests include cloud computing & data security and privacy. (471014543@qq.com)

Yan Wang, born in 1990. Junior College Student. His main in research interests include Electronic information technology. (87714861@qq.com)

NingRuo Sun was born in 1984. Bachelor. His main research interests include Enterprise planning. (444067611@qq.com)