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 service storage. 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.

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 Z^{2^{|\{p_1, p_2, \ldots, p_n\}|}} is monotonic, and if \{p_1, p_2, \ldots, p_n\} \subseteq c, so c \subseteq A, A \subseteq 2^{\{p_1, p_2, \ldots, p_n\}} \{ \emptyset \} 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^\alpha, g^\beta, g^\gamma), wherein the random elements a, b, c\inZ_q, judge g^{\alpha \beta} = g^{\gamma \gamma} 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_q^*, 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-ADBDHE. Given tuple \( (h, h^{a \alpha^{q+2}}, g, g^a, g^\gamma, \ldots, g^\alpha q^2, g^{q^{q+2}}, e(h, h^{a \alpha^{q+2}}, g, g^a, g^\gamma, \ldots, g^\alpha q^2, g^{q^{q+2}}, e(h, h^{a \alpha^{q+2}}), there is no exponent which can distinguish above two Yuan groups with non-negligible probability in polynomial time, where h \in G_q, \alpha \in Z_q 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 uploads 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 PKKAA and the master key MKAA of KGC. Thereby, obtain a complete public system parameter (PK=P=PKUPKAA4)
E. KeyGen (T, PKKGC, MKAA, PK, ID).
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 data, 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 PKKAA;
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 × G_0 → G_1, the security parameter λ determines the group size. Lagrange multiplier, Δ, S(x)=

\[ \prod_{j=2, j \neq 1}^{x-j} \frac{x-j}{l-j}, \]  

where S is a set of integers, i∈S.

A. KGC-Setup (λ)

KGC chooses a bilinear group (G_0, G_1, e, p) of P>2^λ prime order, g is a generator of G_0. Select random numbers y_1, y_2, \ldots, t_{n+1}, α \in Z_p, randomly select an element g_2 from G_0. Thereafter, select t_1, t_2, \ldots, t_n, t_0, and N = \{1, 2, ..., n+1\}.

Defined functions T, T(x) = \sum_{i=1}^{n+1} \frac{1}{x_i} \left( \frac{1}{X_i} \right), T can be regarded as \( g_2^{x_i} \cdot g^{h(x)} \), where h (X) is a polynomial of order n. The public parameters PK_KGC = (g_0^{y_1}, \ldots, g_0^{y_n}, g_0^{y_2}, g_0^{t_1}, \ldots, g_0^{t_n}, g_0^{t_0}, g_0^{N}, \ldots, g_0^{N}).

B. AA-Setup (PK_KGC)

A is a random number \( t \in Z_p \), public parameter PK_{AA}=g_0^{t}, MKAA=t is master key, thus, the public system parameters of PK=\{h_0, m_0, g_0, g_2, g_2, \ldots, g_2, t_1, t_2, \ldots, t_{n+1}, l_1 \cdot \ldots l_1 \cdot g_0^{N} \}.

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

![Fig. 1 Secure Cloud Storage Model Based Attribute-Based Encryption](image1)

![Fig. 2 Confirmation Stage](image2)
D. Bob calculates $D_{d, T}=(d_1, d_2)=(d_1, g_{so}d_1^{-1}+s_0)\in\{(g_2^x, g^{-x})(s_0+s_1)\}$
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 $qr(0)=y_2$, to calculate $D'\{D'x$ $=g_2q(x)T(i)x, i=att(x), Rx'=grx\} x\in AS$, then send $D'$ to AA.
F. AA calculated $D'=\{Dx=(Dx')l=g_2tq(x)T(i)x\} x\in AS$, and send $D$ to Bob.
G. The full key of Bob is $SK=(d_1, d_2, D)$
H. Firstly, Alice selects $key\in G_1$. Then, calculates the AES $key(m)=c$, uploads $c$ to the cloud storage.

C. Randomly select $key\in G_1$, calculate $E_1=\text{key}^e(E_4^{-1}, d_1)$
If $D'$ output $key'$, then $key'$ is key, then D is from Bob; otherwise, D has nothing to do with Bob.

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 $m:\n
\text{AESkey}^{-1}(c)=\text{AESkey}^{-1}(\text{AESkey}(m))=m$.

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 $E=(\gamma, E_1, E_2, E_3, E_4, E_5)=(\gamma, Me(g^{y_1}g^{y_2}g^{y_3}), \{T(i)^{y_1}|e, g, g', o, e(g,g)^a\}$.

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 $e(g, g')^{y_2}$ by the key of the malicious user. If the attribute set of cipher text structure does not satisfy the user’s access, the rival cannot get $e(g, g')^{y_2}$. 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 $(so, \theta)$ 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


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)