2017 Asia-Pacific Engineering and Technology Conference (APETC 2017)
ISBN: 978-1-60595-443-1

An Improved CPK Identity Authentication Scheme Based on Cloud Environment

Yanyan Song and Jun Qin

ABSTRACT

When cloud computing technology becomes increasingly mature and the application field is expanded gradually, it becomes the focus of attention to perfect the security mechanism under cloud computing environment. Identity authentication technology has some limitations and particularities when applied to cloud environment. In this paper, a bidirectional identity authentication scheme based on CPK technology is proposed, to resist forgery attacks in cloud computing environment. The role based access control plan is integrated with the combined public key authentication scheme, to strengthen the security of access control model and guarantee the security of cloud computing. Simulation experiments are conducted on the cloud computing simulation platform via the improved CPK identity authentication based on cloud environment. According to the experimental results, this scheme can effectively carry out user identity authentication under cloud environment, and the desired effect is obtained in the experiment.

INTRODUCTION

With the rapid development of network technology, cloud computing technology emerges at the right moment [1]. The application of cloud computing becomes increasingly extensive, and the security issue is one of the problems emphasized by users. Terminals of cloud computing are widely distributed. As a result, services provided by cloud computing will be attacked by hackers and other uncertain factors easily. User privacy data protection problem, user data security problem, and haul storage security problem of data in cloud computing are all potential safety hazards. These potential safety hazards have restricted the development of cloud computing. In order to provide corresponding services, cloud service providers must establish a perfect identity authentication mechanism. It is an important issue for experts and scholars in the aspect of network security to change this unordered world lacking trust into an ordered world with trust mechanism via a series of technological means by starting from such absent trust mechanism in network environment [2].

Yanyan Song[1,*], Jun Qin[2]
[1]Communication University of China, Nanguang College, Nanjing, Jiangsu, China
[2]Communication University of China, Nanguang College, Nanjing, Jiangsu, China
Corresponding author: sophiesong1231@163.com

The viewpoint about the existence of identity authentication system was proposed and verified by Shamir in 1984[3, 4]. However, due to various reasons, the first exercisable IBE scheme was put forward and implemented by Dan Boneh in 2001. CPK identity authentication algorithm was proposed by the Chinese scholar NAN Xianghao in 1999[5]. After making a contrastive analysis on different authentication modes, domestic scholars reach a consensus that CPK authentication mode possesses advantages other authentication modes do not have. CPK has attracted high attention from a large number of researchers since then. Compared with common PKI and IBE systems, CPK identity authentication algorithm is superior in the aspects of calculation speed, requirements for band width and occupation of storage space. In this paper, CPK technology is transferred into the cloud computing environment, and identity authentication is combined with multi-level role based access control method. Meanwhile, the ring signature system is introduced into anonymous user operation, providing an idea for researches on the security of identity authentication technology under cloud environment. According to the simulation experiments, effective user identity authentication can be conducted under cloud environment.

CPK PRINCIPLE

The fundamental theory of CPK key combination is key compound theorem of elliptic curve cryptography (ECC). ECC compound theorem can be expressed as follows: multiple pairs of public keys and private keys are selected from the public and private key matrix, and new pairs of public keys and private keys can be gained through point add operation for these public keys and private keys[6]. In another word, the private key $r_i (1 < i < m)$ is selected. If the sum of private keys is $(r_1 + r_2 + ... + r_m) \bmod n = r$, then the sum of corresponding public keys is $R_1 + R_2 + ... + R_m = R$. Hence, r and R will form a new pair of public and private keys.

$$R = R_1 + R_2 + ... + R_m = r_1 G + r_2 G + ... + r_m G = (r_1 + r_2 + ... + r_m)G = rG \quad (1)$$

In this paper, the discrete logarithm problem based on elliptic curve is used to establish a CPK system. The required pairs of public and private keys are obtained by selecting elements from the public and private key matrix with a relatively small scale and conducting point add operation in elliptic curve. In this way, large-scale keys are generated with a few elements, and the requirements of large sale and simplification under cloud computing environment are met.

The generation steps of identity keys are as follows:

(1) Construct the matrix

(2) Build the public key matrix and private key matrix according to the given ECC parameter T(a,b,G,n.p) [7].

(3) The public key matrix is m×h matrix, and m×h elements in the matrix are recorded as $X_{i,j}$. All of them are elements in the subgroup S generated by the base point G, i.e. $X_{i,j} = (x_{ij}, y_{ij}) \in S$. The public key matrix is recorded as PSK, so

$$PSK = \begin{bmatrix} (x_{11}, y_{11}) & (x_{12}, y_{12}) & \cdots & (x_{1h}, y_{1h}) \\ (x_{21}, y_{21}) & (x_{22}, y_{22}) & \cdots & (x_{2h}, y_{2h}) \\ \cdots & \cdots & \cdots & \cdots \\ (x_{m1}, y_{m1}) & (x_{m2}, y_{m2}) & \cdots & (x_{mh}, y_{mh}) \end{bmatrix} \quad (2)$$

(4) The private key matrix is recorded as SSK, so

$$SSK = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1h} \\ r_{21} & r_{22} & \cdots & r_{2h} \\ \cdots & \cdots & \cdots & \cdots \\ r_{m1} & r_{m2} & \cdots & r_{mh} \end{bmatrix}. \quad (3)$$

(5) In the private key matrix SSK, r_{ij} is the multiplying value of X_{ij} for the base point G, i.e. $r_{ij}G = X_{ij} = (x_{ij}, y_{ij})(1 \le r_{ij} \le (n-1))$. Therefore, SSK is the discrete logarithm matrix. Obviously, the element $X_{ij} = (x_{ij}, y_{ij})$ in the position corresponding to any matrix in PSK and SSK and r_{ij} form a pair of public and private keys.

The public key and private key matrix is $m \times h$ matrix; every column of the matrix includes m elements and the matrix has h columns. There are m possibilities when an element is taken out from one column. Therefore, a $m \times h$ matrix can generate m^h pairs of public keys and private keys in principle. One main idea of CPK is to produce a huge number of public and private key pairs through "combination" for small-scale "matrix", to realize the purpose of large-scale key management.

ACCESS CONTROL SCHEME BASED ON CLOUD ENVIRONMENT

The purpose of access control is to prevent unauthorized access and unauthorized operation for information resources and to maintain data integrity and confidentiality. The most mature model studied the most frequently in recent years is role based access control (RBAC). Meanwhile, it is superior to traditional access models like MAC and DAC in many aspects. Moreover, its application in practice is more extensive [8]. When roles are set in the RBAC model, different requirements of different users for the service should be considered, and the user roles should be set according to their tasks in the system. The same user can switch between different roles, and the system can also add, modify and delete role groups[9]. The concept of constraint is introduced into $RBAC_2$ model on the basis of RBAC, as shown in Fig. 1.

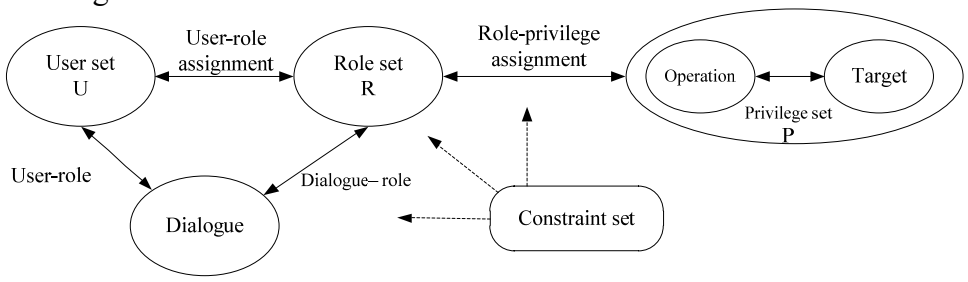

Figure 1. $RBAC_2$ model.

The access control model based on cloud environment is composed of five functional modules which are cloud platform, service catalog, unified access control platform, role based access control module and interactive platform, as shown in Fig. 2.

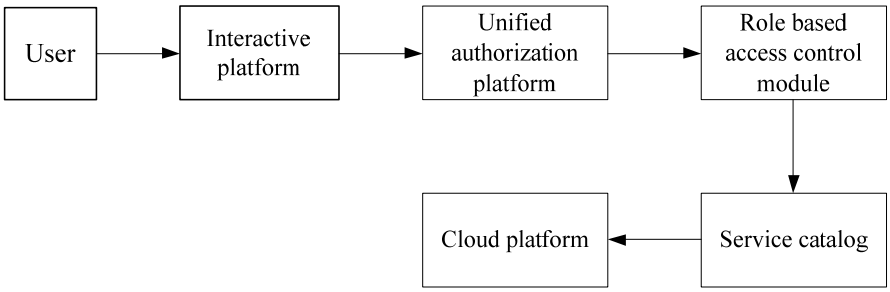

Figure 2. Role based cloud platform access control model.

The access control scheme proposed in this paper has integrated $RBAC_2$ model with CPK authentication method, which has restrained user privilege to access recourses under cloud computing environment more meticulously. The security of users accessing recourses can be better guaranteed via constraint. The integration of $RBAC_2$ model and CPK authentication method can further enhance the access control security under cloud computing environment.

CPK IDENTITY AUTHENTICATION SCHEME BASED ON CLOUD ENVIRONMENT

The advantages of CPK identity authentication scheme are transferred into cloud computing environment. By combining with $RBAC_2$ model, the mode of bidirectional authentication is proposed and ring signature authentication technology is introduced into this scheme.

Selection for the Elliptic Curve Applied by CPK

CPK scheme under cloud environment adopts the combined public key system of discrete logarithm problem based on elliptic curve. At present, common attack modes aimed at elliptic curve mainly include brute-force attack, Baby-Step Giant-Step algorithm, Pohling—Hellman method, Pollard-ρ algorithm, MOV method, etc. A safe elliptic curve able to resist the existing attacks is the guarantee for the security of the whole ECC system. Researches show that some special elliptic curves have potential safety hazards. Therefore, in order to get a safe elliptic curve, the following safety criterion should be followed. The elliptic curve selected is not a hyper-singular elliptic curve; the order of the elliptic curve selected is $n \neq p$; n is a big prime number and has big prime number factors; $n > v(1 + \log_2 u)$, and u and v are the number of rows and number of columns of the key matrix respectively.

In this paper, random choice method is adopted. The big prime number p is given, and the curve parameters $(a, b \in F_p, 4a^3 + 27b^2 \neq 0)$ are selected at random. The order n of the elliptic curve is calculated. A judgment is made for whether n can meet the selection requirements of elliptic curve. It the requirements can be met, the process should be continued. The base point is gained. If the elliptic curve selected cannot meet the security requirement, the above steps should be repeated to select a new curve. NIST has recommended 15 safe elliptic curves, 5 of which are within the large prime field Fp[10]. Moreover, they haven't been successfully attacked till now.

Integration of CPK Authentication and Access Control Model

According to the analysis on the applicability of CPK identity authentication under cloud computing environment, it is feasible to transfer CPK identity authentication scheme into cloud computing environment. In this section, a CPK identity authentication based on cloud environment (Cloud CPK, CCPK) will be given. The role based access control mode is adopted in cloud computing. Keys of corresponding levels will be assigned to users according to the user roles indicated by user identification, making it possible for users to access the cloud computing resources within their privilege. The integration model is shown in Fig. 3. CPK KMC represents the key management center of CPK, and CPK ID means the ID certificate of CPK. When users send a request of cloud computing, a key application will be sent to the key management center (KMC) first, and the key management center (KMC) will issue an ID certificate to users according to the authentication process. In the combination mode of CPK and RBAC$_2$ model, user identification is always an important base to judge the user role.

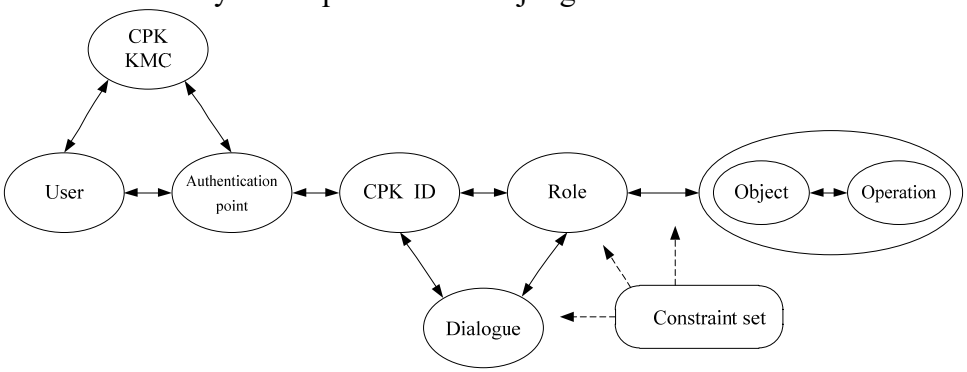

Figure 3. Combination of CPK authentication and RBAC$_2$ model.

Ring Signature Algorithm

Ring signature is a simplified group signature. As for its characteristics, every user in the ring is at the same level and every user can sign on behalf of the whole group. The signer as a representative does not need to obtain consent from other members [11,12]. The verifier is concerned about the group that signs rather than the specific user in the group that signs. Ring signature algorithm is realized mainly through signature generation and signature verification, and the specific implementation steps are as follows:

(1) Signature scheme

Calculation for the HASH value of signing messages: $\text{hash} = \text{HASH}(m)$. Selection for the initial value: The signer selects an initial value $v \in_R \{0,1\}^b$. The signer $x_i (i = 1,2,...,n, i \neq s)$ is determined to select $x_i \in_R \{0,1\}^b$ for other ring members at random, and $y_i = g_i(x_i)$ is worked out. Solving for y_s: y_s is solved from the ring equation $c_{k,v}(y_1, y_2, ..., y_n) = v$. The real signer utilizes his (her) knowledge to solve $x_s = g_s^{-1}(y_s)$ from $y_i = g_i(x_i)$. Generation of ring signature: The ring signature of message m is a 2n+1-dimensional variable and can be identified as $\sigma = (P_1, P_2, ...P_n, v, x_1, x_2, ..., x_n)$.

(2) Signature verification

The verifier calculates $y_i = g_i(x_i)$; the verifier calculates $hash = HASH(m)$; the verifier verifies the ring equation $c_{k,v}(y_1, y_2, ..., y_n) = v$. If these two are equal, the signature will be considered as effective; if they are not equal, the signature will be wrong.

(3) Ring signature based on CCPK

User A needs to prove his/her identity, and user A sends the request Q to B. User B sends a random number Rb to A. User A sends his/her public key PK_A, ring list L_A and ring signature to B. Signature authentication: After user B receives the data in public key PK_A, ring list L_A and ring signature sent by user A, B will examine the ring reputation and check whether entities with insufficient credibility exist in the ring. If such entities exist, B will refuse the verification. If such entities do not exist, B will search the public key of every member in the ring according to L_A, and then verify the ring signature.

EXPERIMENTAL RESULTS AND ANALYSIS

In order to verify the effectiveness of CCPK identity authentication scheme, simulation experiments should be further conducted.

Experimental Environment and Process

Java language is adopted as the programming language of simulation program, and CloudSim cloud simulation open source library is introduced. Hardware configurations of the computer used in the simulation experiment are as follows: Intel Core i5-3850 is adopted as CPU; the internal storage is 8GB; the capacity of hard disk is 500GB; the operating system is Windows 7 ultimate edition 64Bit Service Pack 1; Eclipse is applied as the development software; the experimental simulation can be started by importing the CloudSim pack into the Eclipse item. The simulation steps are shown in Fig. 4.

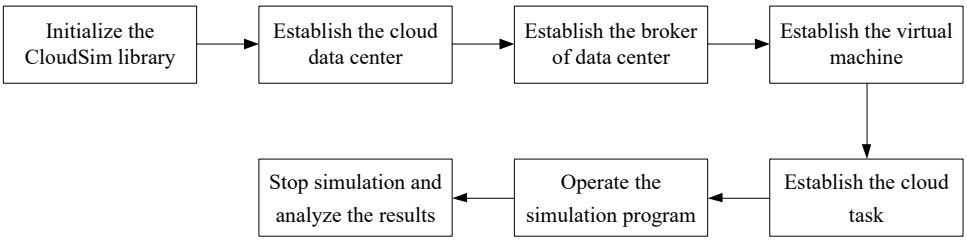

Figure 4. Cloud simulation models.

The design of simulation scheme is as follows:

(1) Selection for an effective elliptic curve

In this paper, P-192 curve among the curves recommended by NIST is selected. Various parameters of P-192 curve are as follows:

P=6277101735386680763835789423207666416083908700390324961279

a=-3

b=0x 64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1

Gx=0x 188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF1012

Gy=0x 07192B95FFC8DA78631011ED6B24CDD573F977A11E794811

n= FFFFFFFFFFFFFFFFFFFFFFFF99DEF836146BC9B1B4D22831

h=1

In the above formula, Gx and Gy are the coordinates of the base point G.

(2) Initiation of authentication

Firstly, user A will initiate an authentication request, connect to user B and send out the authentication parameters needed. After receiving the authentication message sent by user A, user B will begin to verify the message. After passing the verification, user A will receive the authentication parameters sent by user B, and user A will submit the cloud computing task after verifying user B's identity. The authentication process at user A's end is over. If one authentication step is not passed in the authentication process, authentication should be stopped. It will report error and exit. CCPK identity authentication scheme adopts the bidirectional authentication mode, so user A is set as receiving end and user B is treated as sending end in the second authentication.

Experimental Results and Analysis

In the experiment, the CCPK identity authentication scheme is simulated, and user A and user B are used to simulate the authentication between cloud computing users. The program includes two parts which are UserA.java and UserB.java. As for the authentication method, socket in Java is adopted for simulation. At first, user A is set as sending end and user B is treated as receiving end. The mode of bidirectional authentication is adopted, and the identity authentication process under cloud computing is almost completed. Users' CPK ID certificate is saved in users' U-Key. If attackers want to attack the whole system through U-Key, they need to analyze a large number of internal generating programs, but such analysis involves quite a long time and a very huge resource cost. Therefore, the success rate of such attacking mode is very low. Hence, the security problem of identity authentication in cloud computing is solved.

The CCPK identity authentication scheme proposed in this paper is an improved CPK identity authentication scheme based on cloud environment. In order to reflect its superiorities in efficiency, a contrastive analysis is made on the running time of CPK identity authentication scheme and CCPK identity authentication scheme. Five experiments are conducted, as shown in Fig. 5. The experimental data are the running time of authentication process under Eclipse (unit: s), and the calculation time needed by CCPK identity authentication scheme is much less, while its calculation task is heavy. Therefore, CCPK has an obvious advantage in centralized production and distribution of keys. The CCPK identity authentication scheme has not only saved service cost but also improved authentication efficiency.

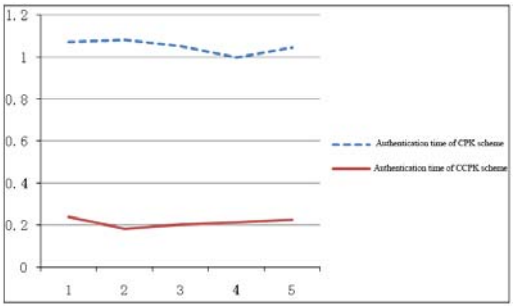

Figure 5. Comparison of authentication time between CPK and CCPK.

CONCLUSIONS

By aiming at the security issue of cloud computing technology in the rapid development process, CPK key combination system is introduced into cloud computing, and the security problem of identity authentication in cloud computing is solved via CPK. Meanwhile, ring signature and role based access control model are introduced to enhance the safety performance of cloud computing. The identity authentication process under cloud computing is completed by simulating the CCPK authentication scheme. The security problem is solved; meanwhile the authentication efficiency is improved and the expected effect is gained.

Supported by the Surface Project of Natural Science Research of Jiangsu Colleges and Universities (15KJD520007) and Science Research Project of CUCN (2016KYPY054).

REFERENCES

[1] Hong Yao, Changmin Bai, Chengyu Hu, Deze Zeng, Qingzhong Liang. Survey on Mobile Data Offloading [J]. *Computer Science*, **41**(11A):182-186(2014).

[2] Wei Wang, Neng Gao, Lina Jiang. Security Demands Analysis of Cloud Computing [J]. *Netinfo Security*, **08**:75-78(2012).

[3] Shamir A. How to Share a Secret. *Communication of ACM.*, **22**(11)612~613(1979).

[4] Shamir A. Identity-based Cryptosystem and Signature Schemes. In Proceedings of Cryptology-Crypto'84, LNCS 196. *Berlin: Springer-Verlag*, 47~53(1984).

[5] Dan Boneh, Matt Franklin. Identity based Encryption from Weil Pairing. In Proceedings of Cryptology-Crypto'01, LNCS 2139. *Berlin: Springer-Verlag*, 213~229(2001).

[6] Feng Zhang, Minghua Wang, Xin Yang. CPK-based Digital Signature System Design and Implementation [J]. *Information & Communications In Chinese*, **5**:104-106(2016).

[7] Jun Luo. Access Control by Encryption Mechanism in Cloud Computing Environment [J]. *Information Security and Communications Privacy In Chinese*, **11**:44-46(2012).

[8] Qiaoyu Liu, Lei Ju, Shigang Li. Research of Identity Authentication Method and Application Based on CPK [J]. *Journal of Beijing Electronic Science and Technology Institute*, **02**:76-80(2013).

[9] Yuding Wang, Jiahai Yang Cong Xu, Xiao Liang, Yang Yang. Survey on Access Control Technologies for Cloud Computing [J]. *Journal of Software*, **26**(5):1129-1149(2015).

[10] Michael Brown, Darrel Hankerson. Software Implementation of the NIST Elliptic Curves Over Prime Fields. *Springer-Verlag Berlin Heidelberg*, 250~265(2001).

[11] L.L. Wang, G.Y. Zhang, and CG Ma. A survey of ring signature [J]. *Frontiers of Electrical and Electronic Engineering in China*, **3**(1): 10-19(2008).

[12] Qiaoyu Liu. Research of Cloud Security Identity Authentication and Access Control Technology Based on CPK [D]. Xidian University(2014).