C-MAS: The Cloud Mutual Authentication Scheme

Zhenpeng Liu, Fenglong Wu
College of Mathematics and Computer Science, Hebei University, Baoding 071002, China
E-mail: lzp@hbu.edu.cn, 323wfl@163.com

Kaiyu Shang,Wenlei Chai
Network Center, Hebei University
Baoding 071002, China
E-mail: shang@hbu.edu.cn cwl@hbu.edu.cn

***Abstract*—A cloud mutual authentication scheme (C-MAS) is proposed to solve the problem of authentication between user and cloud computing server. Trusted computing technology and traditional smart card methods are used in cloud computing service platform. The scheme completes the authentication of both sides in cloud computing, generates the session key according consulting, at the same time, verifies the credibility of cloud service platform. Analysis shows that our scheme can resist various kinds of possible attacks, so it is therefore more secure than other schemes. And the computing time meet the requirements of cloud computing environment.**

Keywords-Cloud Computing; Identity authentication; Trusted Computing; Smart Card Introduction

I. INTRODUCTION

As a new concept and technology, cloud computing has attract extensive attention in the world [1]. Cloud security is the most problem in cloud computing [2]. In cloud computing mode, the user's data stored in cloud service provider data center and calculation operation also worked in the environment. Users shared data center and all kinds of resources. In order to ensure the safety of the cloud system, must build a strong mutual authentication mechanism [3]. Due to the special advantages of the trusted computing technology in network, trusted computing technology is applied to cloud computing service platform. A mutual authentication scheme based on the trusted cloud computing platform is proposed to solve the problem of mutual authentication between user and cloud computing server in the cloud computing service environment.

II. TRUSTED CLOUD COMPUTING PLATFROM

The core of the trusted computing technology is trusted platform module (TPM) which is embedded in the terminal platform. TPM provides hardware security for various credible mechanism and function in all types of computing platform [4].

Authentication is the important mechanism and the foundation to realize the security of cloud computing system. It provides the security guarantee for cloud user's real identity [5]. Compared with the traditional security mechanism, utilizing the TPM has more security and privacy. The TPM takes the unique encryption key into hardware which can not encroach. The root storage key which store in TPM key management bottom, for a trusted platform module owner is unique. Using the trusted platform module which is in hardware architecture, the server can create a public and private key instance: (PK, SK). This key is root storage key derivative key, and specific to hardware of server [6]. From the system start to establish execution environment, TPM measures platform hardware and software components. The corresponding hash value integrity measure information saved in a group of PCR register of TPM. At the same time the created events recorded in storage measurement log (SML). PCR value and SML value are together used to verify the platform state for user. The trusted cloud computing platform framework is shown in figure 1:

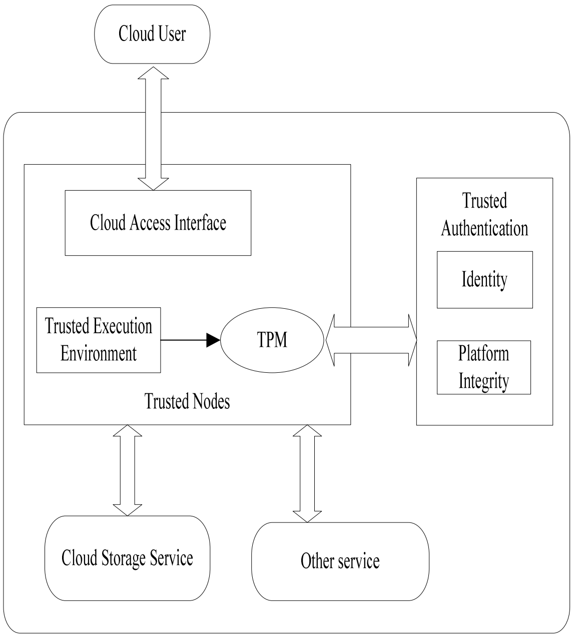

Figure1. Trusted cloud computing platform

III. TRUSTED MUTUAL AUTHENTICATION SCHEME

The scheme scene model is shown in figure 2. User, cloud server (TPM) and CA (Certificate Authority) can access each other in the internet. After finishing registration in cloud server platform, the user gets smart card and accesses to cloud server through client. Cloud server and the user finished the attestation. CA manages the public key which is corresponds to the identity of cloud server (TPM). The user who has smart card can proposes query for CA, tests the consistency about public key and cloud server identity [7].

Published by Atlantis Press, Paris, France.

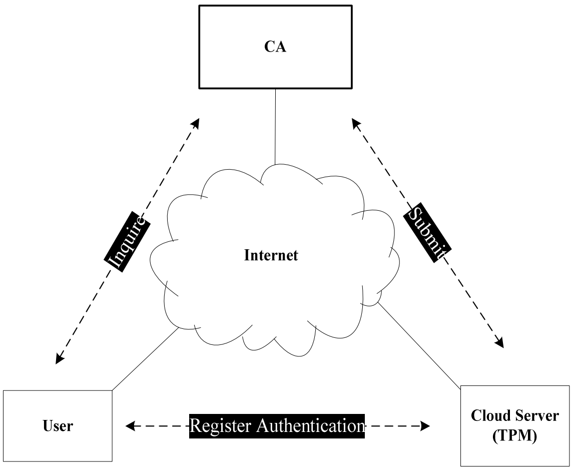

Figure2. Scheme scene model

User sends request to cloud server through the smart card. The scheme include registration, login and password change three phase in the process of implementation. We assume that the user's terminal platform is credible and in registered stage user and cloud server provider are both honest [8]. The symbols in this paper are shown in table Ⅰ:

TABLE Ⅰ. NOTATIONS

Symbol	Definition
S	Cloud Server
U	User
ID	User Identity
PW	User Password
h（•）	Hash Function
PK	Public Key
SK	Private Key
‖	Concat
⊕	XOR
T	System Time Stamp
$Sig\{\}_{SK}$	Signature
Log{}	Security Measure Log
K_{US}	Session Key

A. Registration Phase

The registration phase includes two parts, one is the user sends registration request to cloud server, and the second is cloud server issues registration information to the user. The steps are as follows: ① When user sending register request to cloud server, user should choose a identity (ID), password (PW) and a random number "n", calculate h(PW ⊕ n), send ID and h(PW ⊕ n) to cloud server. ② Cloud server calculates PID=h (ID ‖ x), R=PID ⊕ h(PW ⊕ n) after receive user registration request. "X" is the secret number cloud server select, and for security reason it should be greater than 100 bit. Choose a big prime number "P" and g ∈GF(P); Cloud server uses trusted platform module (TPM) which in hardware architecture to create public key and privacy key (PK, SK); Cloud server takes the message {R、P、g、h(.)、PK} issued to user smart card through security channel. ③ User takes ID and the number "n" input to smart card, and now the information {ID、R、P、g、h(.)、PK、n} stored in smart card. And user doesn't need to remember the number "n".

B. Login Phase

User takes smart card into the terminal card reader, enter ID and PW. Smart card first checks whether the format of ID is valid, if the ID is invalid, the smart card refused user's authentication request. If pass, perform the following operation:

- User generates a temporary random number "r" and a secret number "a", calculates PID=R ⊕ h(PW ⊕ n), $K_U=g^{a}$ mod P, C_1=PID ⊕ h(r ⊕ n), C_2=h(h (r ⊕ n) ⊕ T_1). T_1 is the local time stamp. And then user calculates H_U=h(ID，C_1，C_2，K_U，T_1), sends the message M_1={ID，C_1，C_2，K_U，T_1，H_U} to cloud server.
- After receive the message M_1, Cloud server checks $T_1'-T_1 \leqslant \triangle T$. T_1' is cloud server current time stamp, △T is the legal communication delay. If established, then calculates H_U'= h(ID，C_1，C_2，K_U，T_1). Through judge H_U and H_U is consistent, cloud server verify the integrity of user's message. If the verification passed, calculates PID=h(ID ‖ x), C_1'=PID ⊕ C_1 and C_2'=h(C_1' ⊕ T_1); At last if C_2' is equal to C_2, the cloud server can determine the user is legal.
- Cloud server chooses a secret number "b" and the information K_U, calculates $K_S=g^{b}$ mod P, $K_{US}=(K_U)^{b}=(g^{a})^{b}$ mod P. Through TPM chip cloud server calculates the platform integrity check value PCRS. PCR_S=SHA (PCR_0 ‖ PCR_1 ‖ ⋯ ‖ PCR_N). Signing the message C_3 with private key SK: C_3=Sig{C_1', PCR_S}$_{SK}$; Loading platform security measure log: L=Log(SML); Computing H_S=h(C_3，K_S，L，T_2), T_2 is the time stamp S produce. At last, cloud server sends message M_2= {C_3，K_S，L，T_2，H_S} to the user.
- After receive the news M_2, user first checks the time stamp T_2. Judge T2'−T2⩽△T is right or not. T_2' is the user current time stamp. If right, calculates H_S'=h(C_3，K_S，L，T_2), judges Hs' and Hs is equal or not. If equal, user decryption C_3 gets the value of $C_1'$and PCR_S. If h (r ⊕ n) is equal to C_1', the user can confirm cloud server. At last, user calculates the final session key: K_{US} = (K_S ）^{a} mod P= (g ^{b}) ^{a} mod P.
- User verify the cloud computing service platform integrity to ensure the server system configuration information meet the safety strategy. That means judges the server status is credible or not. Recounting the PCR_S'= SHA(PCR_0 ‖ PCR_1 ‖ ⋯ ‖ PCR_N) make use of the value of L. If PCR_S' and

PCR_S are consistent, we can confirm the integrity of cloud server platform.

Finally, the user and cloud server complete the mutual identity authentication. And at the same time user confirm the integrity of server platform. The cloud server provides services and data which is protected by session key K_{US} to user.

C. Password Change Phase

After finished login and authentication phase, the user can request change password. First enter the new password PW_{new}, the smart card calculates $R_{new} = R \oplus h(PW \oplus n) \oplus h(PW_{new} \oplus n) = h(ID \parallel x) \oplus h(PW_{new} \oplus n)$. Then R_{new} will take the place of R stored in smart card.

IV. Scheme Analyses

A. Security Analysis

This paper provides a mutual authentication scheme for user and cloud service provider in cloud computing environment. With the help of TPM inherent attribute, the scheme realizes the authentication for cloud server identity and platform status. The specific situation analysis is as follows:

- Replay Attack: In login authentication stage, the user sends the message includes time stamp T_1. The time stamp can effectively prevent message replay attack.
- Denial of service attack: User can request access to cloud server by providing the correct ID. The ID has been verified from smart card. User ID and smart card are bound together. If can't receive the smart card and the corresponding ID at the same time, the attacker can't launch denial of service attack to cloud server.
- Password guessing attack: Including online password guessing attack and offline password guessing attack. According to the online password guessing attack the system can restrict user unit time login number to stop the online password guessing attack. The attacker can get the information stored in the smart card when they get the lost smart card. The information are {ID、R、P、g、h (.)、PK、n }, but the attack can't get the information about user's password. In addition, the message h (ID ‖ x) is confidential for others. So attacker can't launch offline password guessing attack through R and n.
- Impersonation attack: Assume that the attacker intercept the message of M_1, obtained the value of C_1 and C_2. But the attacker don't know the secret number "a" of user, the attacker will still can't camouflage user identity contact with cloud server in the subsequent steps. Similarly, if attacker attempt to deceive user, the attack must have a valid message C_3. From the paper we know, the message C_3 is encrypted by the private key SK. And because of the characteristics of asymmetric key, it is not possible for attacker decrypt the message C_3. The attack can't acquire the private key from the TPM platform. The signature can not be falsified. In addition, the attackers don't know the secret number "b" of cloud server. At last, the attack would be failed.
- Cloud platform internal attack: Because user register to cloud server for h ($PW \oplus n$) in stead of PW, the cloud platform internal personnel can't know PW directly. And the number of "n" is not send to cloud server, attacker can't get PW by offline guessing attack from the message h ($PW \oplus n$). So the scheme can resist this attack.
- Forward secrecy attack: Through eavesdropping the login and verification process between user and cloud server the attacker will get the message of {ID，C_1，C_2，C_3，K_U，K_S，L，T_1，T_2}. From C_1, C_2, C_3 and L can't get useful information. $K_U = g^a \bmod P$, $K_S = g^b \bmod P$, $K_{US} = (g^a)^b \bmod P$. The attacker can't obtain the session key K_{US} form K_U and K_S. The above information are noting with password, Even get user's password, the attacker still can't obtain user and server previous sharing key.

B. Performance Analysis

The computing time of this scheme meet the requirements of cloud computing environment. All kinds of computing time symbols defined as shown in table Ⅱ . Analysis shows that the scheme in the paper computing time are $T = 13T_h + 12T_{xor} + 4T_{exp} + 1T_{sig} + 1T_{pk} + 2T_{PCR} + 1T_{log}$. Among them, the registered stage are $2T_h + 2T_{xor}$, the login stage are $9T_h + 7T_{xor} + 4T_{exp} + 1T_{sig} + 1T_{pk} + 2T_{PCR} + 1T_{log}$, the password change stage are $2T_h + 3T_{xor}$. In the stage of validate the credibility of the cloud server platform, the increase time is $2T_{PCR} + 1T_{log}$. The validation just need a couple of times hash operation. User can select a certain number randomly from PCR for validation. So in order to provide more security of the scheme the increase time is necessary.

TABLE Ⅱ. NOTATIONS

Symbol	Definition
T_h	The time of hash operation
T_{xor}	The time of XOR operation
T_{exp}	The time of exponential operation
T_{sig}	The time of signature operation
T_{pk}	The time of decryption operation
T_{PCR}	The time of calculate PCR
T_{log}	The time of load SML

The proposed work has been implemented using Microsoft Visual C++6.0 and SQL Server 2000 as the backed on Windows Platform. The Hardware and Software Configurations used as follows. The hardware configuration used in this implementation work are: The Intel(R) Core(TM) 2 E7500 processor with the operating frequency 2.93GHz, the Main Memory used is 1.98GB RAM, and the 300GB

TABLE Ⅲ. PROCESSING TIME FOR VARIOUS OPERATIONS

	1	2	3	4	5	6	7	8	Average
XOR	1233	1189	955	890	8561	7516	9455	8466	4783.125
Exponentiation	455	852	873	4582	4686	14859	45646	13774	10715.875
Hash	824553	1454260	127645	57842	65542	65466	---	---	432551.333
Encryption	1256731	5614958	874214	3558642	---	---	---	---	2826136.25
Decryption	4245666	9427670	3595233	158579	---	---	---	---	4356787

TABLE Ⅳ. OPERATIONS AND PROCESSING TIME FOR VARIOUS SCHEMES

	JUANG scheme[9]	FAN scheme[10]	SANTHOSH scheme[11]	YANG scheme[7]	The proposed scheme
XOR computations	1	3	12	12	9
Exponentiation	4	1	---	15	7
Hash computations	5	4	6	4	4
Encryption	3	3	2	1	1
Decryption	3	4	2	1	1
Total processing time	23759143.04	27660827.332	17018551.998	9131264.207	9031187.832

Hard Disk Drive. The software configurations used are: 32-Bit Microsoft Windows XP Operating System, the C++ is used as Front End, and the SQL Server 2000 is used as backend. The length of all kinds of operation data is less than 256 bit. The processing time of each operation in login stage is shown in tableⅢ.

TableⅣ shows the operations and the total processing time(in nanoseconds) for different smart card authentication schemes [7,9-11] along with the proposed scheme based on the hardware and software configurations used in the implementation of this authentication scheme.

Analysis shows that the proposed scheme consumes less processing time, when compared with the other mentioned authentication schemes. And the scheme has realized more security goals. Therefore, the proposed authentication scheme performs better than the other compared and discussed smart card authentication schemes.

V. CONCLUSION

This article discussed a new smart card mutual authentication scheme based on the trusted cloud computing platform. The scheme completes the authentication of both sides in cloud computing, generates the session key according consulting, at the same time, verifies the credibility of cloud service platform. This mutual authentication scheme has been implemented. The security analysis shows that the proposed scheme provides more security features and overcomes all the discussed security attack or threats because of the feature of TPM. The performance analysis shows that the proposed scheme takes much less computation time than the other discussed smart card authentication schemes. Due to these features, the proposed scheme is a well-secured scheme for smart card in cloud computing environment.

ACKNOWLEDGMENT

This work was supported by National Science and Technology Support Program (2013BAK07B04).

REFERENCES

[1] Kang Chen, Weiming Zheng. “Cloud Computing: System Instances and Current Research,” Journal of Software, vol. 20, pp. 1337-1348, 2009.

[2] Junzhou Luo, Jiahui Jin, Aibo Song, et al. “Cloud Computing: Architecture and Key Technologies,” Journal on Communications, vol. 32, pp. 3-21, 2011.

[3] Dengguo Feng, Min Zhang, Yang Zhang, et al. “Study on Cloud Computing Security,” Journal of Software, vol.22, pp. 71-83, 2011.

[4] Dengguo Feng, Yu Qin, Dan Wang, et al. “Research on Trusted Computing Technology,” Journal of Computer Research and Development, vol. 48, pp. 1332-1349, 2011.

[5] “Towards Trusted Cloud Computing” http://www.usenix.org/events/hotcloud09/tech/full_papers/santos.pdf. 2009.

[6] Xian Xu, Yu Long, Xian Ping Mao. “Research on TPM based Strong ID Authentication Protocol,” Computer Engineering, vol. 38, pp. 23-27, 2012.

[7] Li Yang, Jianfeng Ma. “Trusted Mutual Authentication Scheme with Smart Cards and Passwords,” Journal of University of Electronic Science and Technology of China, vol. 40, pp. 128-133, 2011.

[8] Tien Ho Chen, Han Cheng Hsiang, Wei Kuan Shih. “Security Enhancement on An Improvement on Two Remote User Authentication Schemes Using Smart Cards,” Future Generation Computer Systems, vol. 27, pp. 377-380, 2011.

[9] Wen Shenq Juang. “Efficient Password Authenticated Key Agreement Using Smart Card,” Computer and Security, vol. 23, pp. 167-173, 2004.

[10] Chun I Fan, Yihui Lin and Ruei Hau Hsu. “Remote Password Authentication Scheme with Smart Cards and Biometrics,” Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM′06). San Francisco, CA, USA: IEEE Press, 2006, pp. 1-5.

[11] S. Santhosh Baboo, K.Gokulraj. “An Enhanced Dynamic Mutual Authentication Scheme for Smart Card Based Networks,” Computer Network and Information Security, vol. 4, pp. 30-38, 2012.