A Security Protocol for Trusted Access to Cloud Environment

Yanan Chang, Zhiyong Zhang* and Jian Wang

Information Engineering College, Henan University of Science and Technology, Luoyang 471023, China


Z. Zhang

Received: December 24, 2014; Revised: July 30, 2015; Accepted: July 31, 2015

Abstract: When user access to the cloud computing environment, existing security protocols merely authenticate the identity of user and cloud server without considering their credibility of owning platforms. Remote attestation of trusted computing is to provide security evidence of their own platform for the both sides of communication accessed. Introducing the remote attestation mechanism into security protocol can avoid terminal security vulnerability when user accessed. By constructing of trusted access authentication framework using remote attestation mechanism, and a security protocol for trusted access to cloud environment is proposed. The proposed protocol with greater security and efficiency compared to other corrective schemes through attack resisting analysis and computational cost analysis, and proved secure using strand space model. Our scheme realizes two factors identity authentication and platform authentication for Mobile User and Cloud Server, as well as satisfies the privacy protection requirement of the platform configuration in cloud environment or cloud media digital rights management.

Keywords: Cloud computing, digital rights management, remote attestation, formal proof, strand space model, security protocol.

1. INTRODUCTION

In cloud computing environment, the users do not have to buy complex software and hardware, but only pay fees to the suppliers of cloud computing services to acquire the computing and storage resources depending on needs. However, the user data are not stored at the users' own host computers, but on the servers located in Europe, Asia or other countries. To ensure that cloud services can be acceptable to more potential users, Reference [1] presents a user feature-aware trustworthiness measurement approach for potential users. Multi tenant is an important feature of cloud computing, users sharing virtual cloud resources will be faced with data leakage if there is loophole in the software running on the cloud platform [2]. In that case, the sensitive data may be accessed by illegal users. Therefore, the identify authentication should be enhanced for cloud computing [3, 4]. Another problem is that the end users do not have to install any software program in the cloud platform, only the basic hardware facilities are required to access to cloud resources according to needs. The thin terminal weakens the security environment of the users themselves, Users are more likely to be attacked by Trojan horse or virus, there is a higher probability of the untrustworthiness of user identity. Besides, the losing and theft of mobile terminals.

*Address correspondence to this author at Information Engineering College, Henan University of Science and Technology, China; Tel: 0379-65627631; E-mail: xidianzzy@126.com

Identity authentication technique is the basis of information security. To adapt to complex cloud environment, the enhancement of identity authentication technique is highly necessary for cloud computing. Currently, the authentication in cloud computing is either one-directional or bidirectional identity authentication between the users and cloud servers [5-7]. Reference [6, 8] realizes the mutual identity authentication between the users and the servers in cloud environment. However, the trustworthiness of platform identity is not authenticated. The existing protective measures for cloud computing are mainly targeted for the server suppliers and the network. The trustworthiness of the two parties before the access into the network is not authenticated. For the users and servers under the cloud environment, the trustworthiness of platform still cannot be guaranteed even if the identity is authenticated as legal. The principle of remote attestation for trusted computing can be transplanted to the cloud environment as the information of identity and attribute authentication to enhance the authentication of cloud environment. A trusted access protocol under the cloud computing environment is proposed in this article. The proposed protocol not only realizes the identity and platform authentication of the two communicating parties, but also satisfies the requirements for platform privacy and anonymity in the cloud environment.

2. RELEVANT RESEARCHES

2.1. Existing Authentication Methods

Cloud computing mainly adopts the conventional user name/password authentication method. In this method, there

2352-0965/15 $58.00+.00

is no need for memorizing the complex user credentials, which brings convenience for the users. In order to avoid the defect of the simple user name/password method, Reference [5] combines images and words to enhance the security level of cloud computing access and realize the strong authentication of the users. However, the protocol only authenticates user identify, but not the cloud server. In light of this problem, Reference [6] achieved the bidirectional identity authentication between the cloud users and the cloud servers before the access of the cloud environment. The above authentication methods still have security loopholes. Reference [8] proposes a strong user authentication framework. Before the identity authentication of the two parties, the mobile users need to insert the smart card distributed by cloud service suppliers, the user identity is first authenticated locally, If the authentication is passed, the mutual authentication of the two parties is carried out.

However, the above authentication protocols do not measure and authenticate the integrity of the platforms. For the users and servers, even when the identity is authenticated as legal, it does not necessarily mean that the platforms are secure and trustworthy. If the platforms carry the Trojan horses or viruses, the security risk to the users' access of the cloud environment is increased.

2.2. Trusted Access and Remote Attestation

Trusted computing can control the insecurity factors from terminals and solve the security problem fundamentally. Trusted measurement technology is the core of trusted computing [9], achieving the measure of the security for software and hardware environment and protect system against invasion of Trojan horses and viruses. Integrity measure is completed by the local trusted measurement chip TPM, and the trusted measurement values are stored in Platform Configuration Register (PCR) that is provided by the underlying hardware security module. The trusted measurement values can also act as the attribute information of platform identity when the end users access to the cloud servers. Trusted Network Connection (TNC) increases authentication of platform identify on the basis of conventional user identity authentication, and the trusted mechanism extending credibility to the entire network, Enhancing the security of the system Identity authentication and platform authentication is performed before terminal users accessed to network. After the identity authentication is passed, the platform integrity is then measured and authenticated [10].

Trusted platform module can attest the configuration information of local platform to the remote platform. The trustworthiness of the platform is authenticated by integrity authentication. During the process of remote attestation, Challenger requests and gets validated platform information based on remote attestation. Remote attestation can be used to establish trust relationship in cloud. At present, it has become a new favorite in the cloud computing security research field that trusted computing is used to solve the cloud computing security, Reference [11] constructs a trusted cloud platform using the trusted platform module (TPM) to guarantee the security of the cloud platform. Reference [12] also uses remote attestation in trusted computing to solve the cloud computing security problems. To support dynamic remote attestation, Reference [13] designed a TBVMM to extend the existing chain of trust into the software layers to solve the dynamicity of the trusted relationship. There are security vulnerabilities and inadequacies as the cloud platform provides remote attestation, the platform attribute information is exposed to attackers, so that they may trace those information to carry out directional attacks [14]. To protect the details of the configuration information and security attributes of terminal and cloud computing platform Reference [15] proposes a remote attestation model that supports the authentication of the proxy with a commission mode (AP^2RA). Thus, the privacy of platform configuration of end users can be protected.

3. TRUSTED ACCESS TA PROTOCOL IN CLOUD COMPUTING ENVIRONMENT

3.1. Trusted Access Framework in Cloud Environment

The trusted access authentication framework is proposed in this section as shown in (Fig. **1**). The framework realizes the bidirectional identity authentication and platform authentication between MU and CS. The framework consists of MU and CS equipped with TPM chip, APS, Smart Card and API licensing server, Trustworthiness Measurement Log (TML), integrity measurement and security policy database.

MU and CS obtain AIK certificate from Certificate and License Server. Acquired platform integrity metric and the security attributes of MU and CS are stored at Trustworthiness Measurement Log (TML) as the platform authentication information. Firstly, Smart Card is authenticated by the local system. If the authentication is passed, after CS authenticates the identity of MU, a request is send to APS to authenticate the platform identity for MU. The integrity metric and security policy values of the device for MU that is stored in the Integrity Measurement (IMR) and Security Policy Database (SPD) of APS. These values serve as the standard values for the platform identity authentication by APS. Similarly, after the identity of CS is authenticated by MU, a request is sent to APS for the platform identity authentication of CS. The bidirectional authentication of identity and platform is realized by the two communicating parties.

3.2. Definitions of Symbols

The definitions of symbols used in the article are listed in (Table **1**).

3.3. Protocol Description

The trusted access security protocol is proposed in this section, and the proposed protocol is composed of registration phase, login and authentication phase and user password update phase.

Assuming the entities MU, CS and APS has acquired AIK certificates from Certificate and License Server, Cert(MU.AIK), Cert(CS.AIK) and Cert(APS.AIK) respectively. After registration phase is over, CS issues a Smart Card to MU.

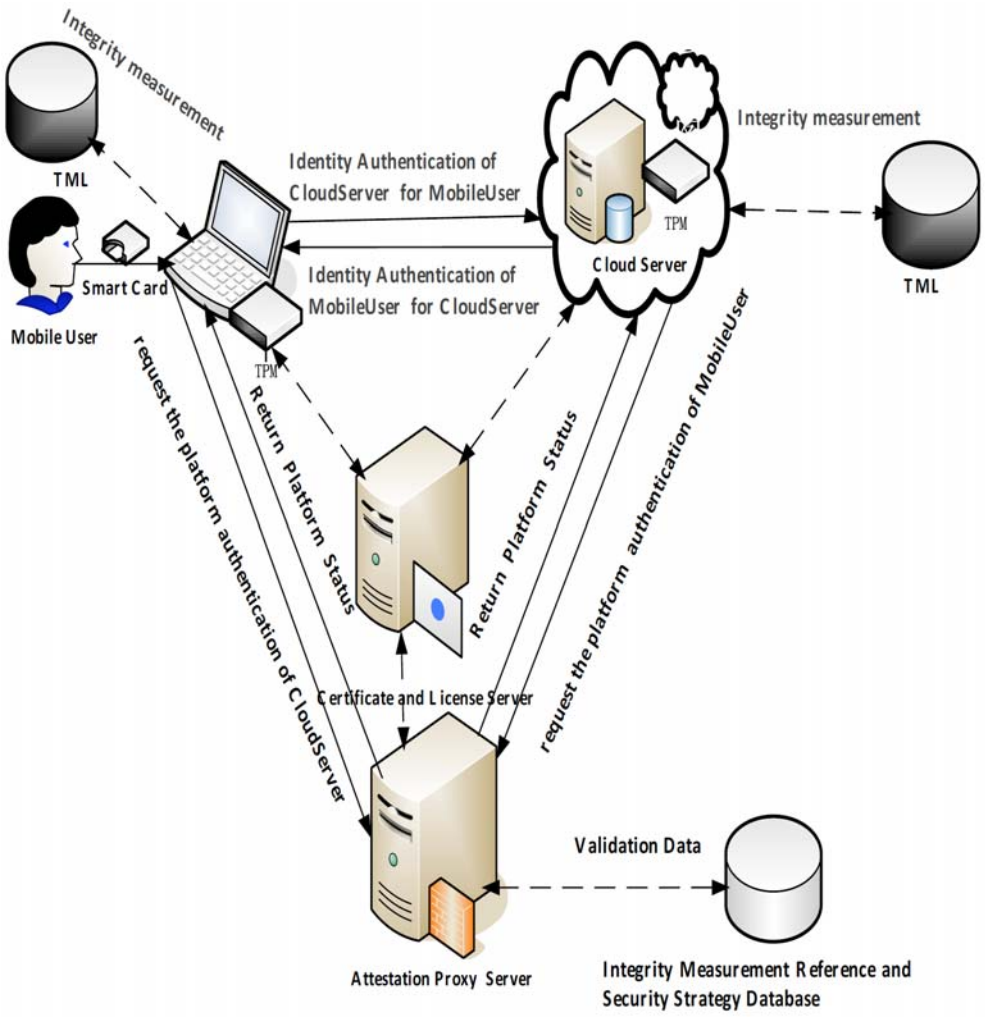

Fig. (1). Framework of trusted access authentication for cloud computing.

First, Smart Card is used for local authentication. Then, in login and authentication phase, integrity measurement values are stored in PCR, in the meantime, the security attributes characteristic values are acquired by of MU and CS, this process is recorded into the TML [16]. After a successful mutual identity authentication for MU and CS, APS authenticates the credibility for their platform and returns the platform status report to the both sides of communication, and realized identity and platform authentication of MU and CS. In the last, description the process of password update.

3.3.1. Registration Phase

Before the MU logs in on the cloud service, he/she has to register at the CS. The procedures of registration are shown as follows:

1. MU generates the random number x, and calculates $h(PW \oplus x)$. The message $\{ID, h(PW \oplus x), h(x), Cert(MU.AIK)\}$ is sent to the CS.

2. CS first inspects Cert(MU.AIK), If the certificate is valid, then the CS accepts MU, considering MU and the platform of MU is legal. Otherwise, the registration request is dismissed. Then inspects whether ID is exists, If it does exist, return to step 1.

3. CS also generates a random number y, and calculates $I = h(ID \oplus h(PW \oplus x))$, $J = h(ID \| y)$ and $V = g^{h(I \| J)+h(I)+h(J)} \bmod p$. CS stores $\{I, J, V, p, g, h(.)\}$ in the Smart Card.

4. MU inputs x into the Smart Card, now the message of the Smart Card is $\{I, J, V, p, g, h(.), x\}$.

3.3.2. Login and Authentication Phase

Before the MU successfully logs in on the CS, the two parties have to perform the bidirectional authentication of identity and platform. Only after the authentication is passed can the MU log in on the CS. The specific procedures are as follows:

1. MU inserts the Smart Card, and inputs ID and PW. The local system calculates $I1 = h(ID \oplus h(PW \oplus x))$ and inspects whether $I1 = I$. Otherwise, the log in by MU is terminated.

2. MU first generates random number Nonce, and calculates $U = h(I \| J), V' = Vg^{-h(x)} \bmod p$ and $R = h(Nonce \| V')$. Then MU measures the integrity of the platform locally, the hash value of measurement is stored in PCRs. $SK^{MU.AIK}$ is used to sign PCRs, Secure Attributes and TML.

Table 1. Definitions of symbols.

Symbols	Definitions
MU	Mobile user
CS	Cloud server
APS	Attestation Proxy Server
$K^{APS\text{-}MU}$	User and APS generate the shared key before platform authentication.
$K^{APS\text{-}CS}$	Cloud server and APS generate the shared key before platform authentication.
Cert(MU.AIK)	The user acquire the AIK certificate from API licensing server.
Cert(CS.AIK)	The cloud server acquire AIK certificate from API licensing server.
Cert(APS.AIK)	APS acquires the AIK certificate from API licensing server.
$SK^{MU.AIK}$	The private key of platform identity certificate AIK for MU
$SK^{CS.AIK}$	The private key of platform identity certificate AIK for CS
$SK^{APS.AIK}$	The private key of platform identity certificate AIK for APS
$PK^{MU.AIK}$	The public key of platform identity certificate AIK for MU
$PK^{CS.AIK}$	The public key of platform identity certificate AIK for CS
$PK^{APS.AIK}$	The public key of platform identity certificate AIK for APS
ID	User identity
PW	User password
x	Private key of cloud server
y	Private key of server
P	A big primer number

$$Sig_{MU} = (PCRs \| SecureAttributes \| TML \| Nonce)_{SK^{MU.AIK}}$$

Then, encrypt Sig_{MU} with $SK^{MU.AIK}$ together with PCRs, TML and Security Attributes.

$$MU_{TPM} = (Sig_{MU}, PCRs, SecureAttributes, TML)_{K^{APS-MU}}.$$

The message M1 is sent to CS.

$$M1 = \{MU_{TPM}, Cert(MU.AIK), U, h(R)\}$$

3. The validity of Cert (MU.AIK) is first authenticated by CS. If invalid, the conversation is terminated. $V'' = Vg^{u+h(y)} \bmod p$ and $R^* = h(Nonce \| V'')$ are calculated. It is determined whether $h(R^*) = h(R)$. If not, the identity authentication of MU fails. MU_{TPM} and Cert(CS.AIK) are sent to APS.

$$M2 = \{MU_{TPM}, Cert(CS.AIK)\}$$

4. The validity of Cert(CS.AIK) is judged by APS. The $K^{APS\text{-}MU}$ is used to decrypt MU_{TPM} to obtain the signed platform information by MU. The signature of MU is authenticated by $PK^{MU.AIK}$, by inquiring the IMR and SPD, the current integrity and platform configuration information of the platform is authenticated. The status value of the platform signed by $SK^{APS.AIK}$ is sent to CS together with *Cert (APS.AIK)* via the security channel.

$$M3 = \{\{(MU\_PlatformStatus \| Nonce)_{SK^{APS.AIK}}, MU\_PlatformStatus\}_{K^{APS-CS}}, Cert(APS.AIK)\}$$

5. The validity of Cert (APS.AIK) is authenticated by CS. According to the status value of the platform sent by APS, the platform identity of MU is judged. CS measures the integrity of platform locally and the hash value of measurement is stored in PCRs. The characteristic value of security attributes SecureAttributes is acquired. The whole process is recorded in TML. $SK^{CS.AIK}$ is used to sign PCRs, SecureAttributes and TML.

$$Sig_{CS} = (PCRs \| SecureAttributes \| TML \| Nonce)_{SK^{CS.AIK}},$$

Sig_{CS} is encrypted by $K^{APS\text{-}CS}$ together with *PCRs*, *SecureAttributes* and *TML*.

$$CS_{TPM} = (Sig_{CS}, PCRs, SecureAttributes, TML)_{K^{APS-CS}}$$

The message *M4* is sent to the MU.

$$M4 = \{CS_{TPM}, Cert(CS.AIK), h(V'')\}$$

6. MU authenticates the validity of *Cert (CS.AIK)*. It is determined whether $h(V') = h(V'')$ hold. If not, the identity authentication of CS fails. CS_{TPM} together with Cert (MU.AIK) are sent to APS.

$$M5 = \{CS_{TPM}, Cert(MU.AIK)\}$$

7. APS determines the validity of Cert(MU.AIK). By inquiring the IMR and SPD, the current integrity and configuration information of the platform is authenticated. The status value of the platform signed by the key is sent to MU together with Cert (APS.AIK) via the security channel.

$$M6 = \{\{(CS\_PlatformStatus \| Nonce)_{SK^{APS.AIK}}, CS\_PlatformStatus\}_{K^{APS-MU}}, Cert(APS.AIK)\}$$

8. MU authenticates the validity of Cert (APS.AIK) and determines whether the platform identity of CS is legal. Thus, the platform identity of CS is authenticated. MU successfully logs in on CS. The flow chart of log in authentication protocol is shown in the following (Fig. **2**).

3.3.3. Password Update

The password is updated by MU inserting the Smart Card on the local system. The specific procedures are as follows:

1. MU inputs ID and PW, and $I1 = h(ID \oplus h(PW \oplus x))$ is calculated.

2. Local system inspects whether $I1 = I$; if not, the request is rejected.

3. MU inputs the new password PW' and generates the new random number x' .

4. Calculates $I' = h(ID \oplus h(PW' \oplus x'))$.

5. The original I and x in the smart card is replaced by I' and x' . The password update is finished.

4. APPLICATION SCENE AND PROTOCOL ANALYSIS

4.1. Application Scene

In order to verify the feasibility and security for the trusted access authentication, the proposed protocol has been applied to cloud media social networking system. Application scenario for Mobile users accessed to Cloud Media Server as shown (Fig. **3**). The system is composed of Mobile User, Cloud Media Server, Server Cent, Friend Server and Music and Video Server. On one hand, the Hardware platform is composed of desktop computer, notebook computer and TPM chip, and the platform of Mobile User and Cloud Media Server with TPM. On the other hand that is Software Settings. Here, the operating system of Mobile User and Cloud Media Server are Windows 8, and we also set the firewall versions are 2.7 and 3.0, respectively. According to the applied protocol, Mobile User registers at the Cloud Media Server based on user name/password. After successful registration, Mobile User log in on the Cloud Server to access to cloud resources. In login and authentication phase, firstly, the software information is verified, such as the version of operating system, firewall version and Virus lib version, and then measured the platform integrity value is sent to Server Cent for Hardware. In the last, Server Cent referencing security policy server to verify integrity measurement values of Mobile User. After identify authentication and platform authentication are successfully verified by Cloud Media Server for Mobile User, he can log in on the multimedia server to access the media content.

4.2. Informal Security Analysis

In this section, we discuss about the security of our proposed trusted access security protocol.

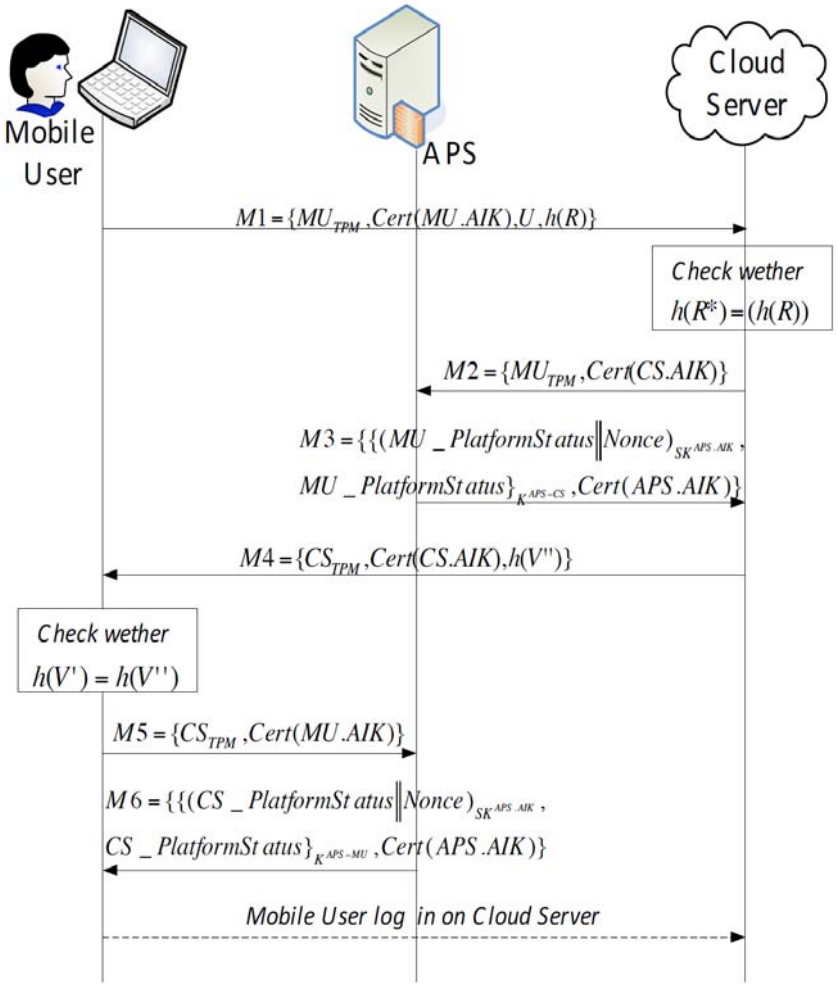

Fig. (2). Time sequence diagram of trusted access authentication in cloud computing.

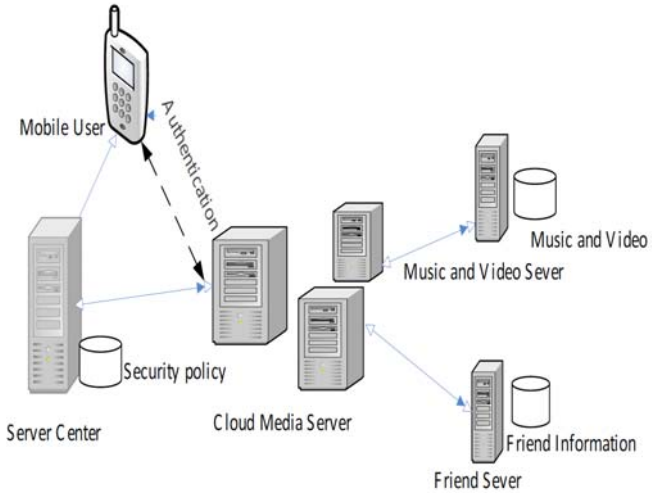

Fig. (3). Application scenario for Mobile users accessed to Cloud Media Server.

The proposed protocol prevents privileged insider attack. In registration phase, $h(PW \oplus x)$ is submitted, instead of submitting password in plain text form. Thus, the privileged insider of the server can not obtain the password.

The proposed protocol prevents parallel session attack. MU and CS sent messages never in plain text during the whole authentication process. Attackers cannot obtain any useful information to legal user or the server.

The proposed protocol prevents playback attack. The entire authentication process is based on challenge-response mechanism for MU and CS. The random number Nonce effectively resists playback attack.

The proposed protocol prevents man-in-the-middle attack. Even the attacker knows the transmitted U and V in message *M1*, but he cannot conjecture V''. Because of V'' is generated by y, he does not known except the CS. Therefore, the man-in-the-middle attack is not established.

The proposed protocol prevents denial-of-service attack. Local system authenticates the legitimacy of the user before communicating with the CS. The password update is competed in the local system as well as. So, denial-of-service attack can be effectively withstood.

The proposed protocol prevents collusion attack. The platform information including uniquely identifies ID and TML are signed by end-user. So, even though the end user has more than one terminal (trusted terminal and untrusted terminal), it also can not pass valid trusted platform metrics report to APS and get platform verification report. The collusion attack is not applicable in the scheme.

The proposed protocol prevents fishing attack. In the login and authentication phase, server needs to provide $h(V'')$ while user authenticates server, only the real server can provide the proper data.

The proposed protocol has realized two factors authentication of identity and platform for MU and CS: In the protocol, after successfully authenticated the identify of MU and CS, the authentication proxy server (APS) completed the attestation to the platform credibility of MU and CS based on remote attestation mechanism, and return the platform status report to MU and CS.

The proposed protocol has no time synchronization problem: The random number is used as the message authentication parameter in the protocol. Thus, the clock synchronization problem induced by the time stamp in the original protocol is avoided.

The proposed protocol satisfies the privacy protection requirement of the platform configuration: To prevent the attack caused by exposed platform configuration information, in our protocol, Authentication Proxy Server (APS) authenticates the credibility of platform for MU and CS and returns the platform status report instead of platform configuration information and security attributes for the both sides of communication.

The proposed protocol's security has been formally proved. As demonstrated in the section 4.2, the protocol was proved to be secure using strand spaces model.

Here, we compare its security properties with the other related protocols [6, 8, 16] in (Table **2**).

4.3. Performance Analysis

This section analyzes the efficiency of the proposed protocol. (Table **3**) provides computational costs of the proposed protocol with the above three protocols in regards to various calculation during the execution of the protocol. Here, considering notation "H" represents hash operation, "C" represents connection operation, "XR" represents Exclusive or operation, "EX" represents modular exponentiation, "EK" represents symmetric encryption operation, "DK" represents symmetric decryption operation, "ES" represents the TPM AIK signature operation, and "DS" represents TPM decryption operation.

Our protocol realizes two factors authentication of identity and platform for mobile user and cloud server. Reference [6, 8] merely achieved a two-way authentication of users and cloud servers without considering their credibility of owning platforms. In terms of the calculation of CPU, our protocol implements 5 hash operations, 4 connection operations, 2 modular exponentiation operations, 1 Exclusive or operation, 2 encryption operations and 2 decryption operations with less computation. It reduces 5 operations, 2 connection operations and 1 Exclusive or operation compared to Reference [6], while the computation complexity of hash operation is much higher than others operations. If adding the trusted authentication function of platform to Reference [6, 8] that they need increasing 2 ES operations and 2 DS operations, and the total amount computation still more complex than our protocol. The Reference [16] merely completes the validation of user platform, the calculation amount is greater than our scheme if achieve the authentication of user and server at the same time.

In our scheme, integrity verification of platform for mobile user and cloud server provides a credible authentication. The CPU and TPM can complete part of operation at the same time, as well as some parameters can be obtained by pre-calculated, which can shorten the operation time and

Table 2. Security properties of the proposed protocol with the other related protocols.

Security Properties	Protocol in Reference [6]	Protocol in Reference [8]	Protocol in Reference [16]	Proposed Protocol
Prevent privileged insider attack	Yes	Yes	No	Yes
Prevent parallel session attack.	Yes	No	No	Yes
Prevent playback attack	Yes	Yes	Yes	Yes
Prevent man-in-the-middle attack	Yes	Yes	No	Yes
Prevent Denial-of-service attack	Yes	No	Yes	Yes
Prevent collusion attack	No	No	Yes	Yes
Prevent fishing attack	Yes	No	No	Yes
Authentication of identity and platform	No	No	No	Yes
No time synchronization problem	No	No	Yes	Yes
Privacy protection for the platform	No	No	Yes	Yes
Formal proof	No	No	No	Yes

reduce the communication delay to some extent. And our protocol with less interactive rounds that is a lightweight security protocol.

Table 3. Performance analysis of the proposed protocol with the other related protocols.

Protocol	Calculation for CPU
Protocol in Reference [6]	11H+6C+2EX+2XR
Protocol in Reference [8]	4H+4C+2XR+4EK+4DK
Protocol in Reference [16]	4C+6ES+6DS+2EK+2DK
Proposed protocol	5H+4C+2EX+1XR+2ES+2DS

As shown in (Table **2** and Table **3**), we can see that the proposed protocol not only provides more security assurances, but also has the reasonable computational costs. What's more, the proposed protocol is proved to be secure. And only our scheme realizes two factors authentication of identity and platform for MU and CS, as well as satisfies the privacy protection requirement of the platform configuration in cloud environment.

5. FORMAL PROOF FOR THE TRUSTED ACCESS (TA) PROTOCOL

Strand spaces theory can correctly describe the sequence and consequence of actions during the protocol process, and provide an effective analysis theory for protocol formal analysis [17]. The proposed protocol contain platform authentication, and is not able to be correctly analyzed by the basic strand spaces model [18], and a extend strand model for trusted access authentication protocols is proposed. Therefore, we will formal analysis the security for the proposed protocol based on the extend strand mode. Reference [19] introduced platform authentication theorem. For the integrity report of platform, if the integrity report shows the platform is credible, and then it is must be originating in regular strand. We analysis of the security in identify and platform authentication using definition and propositions.

Definition 4.3.1 A strand space of the TA is the union of 4 types of strands:

(1) Initiator strands $s \in Init\ [MU, CS, APS, ID, g^x, g^y$ $MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''),$ $Cert(MU.AIK), Cert(CS.\ AIK), Cert(APS.AIK)]$, with trace: $< +m_1, -m_4, +m_5, -m_6 >$. The principal with this strand is MU.

(2) Responder strands $s \in \mathrm{Re}\,sp[MU, CS,\ APS,\ ID, g^x,$ $g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R^*), h(R),$ $h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK), Cert(APS)AIK)]$, with trace: $< -m_1, +m_2, -m_3, +m_4 >$,. The principal with this strand is CS.

(3) Server strands $s \in Serv[MU, CS, APS, ID, g^x,\ g^y, MU_{TPM},$ $CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''), Cert(Mu.AIK),$ $Cert(CS.AIK), Cert(APS.AIK)]$.

(4) Penetrator strand $s \in p$, m_1, m_2, m_3, m_4, m_5 and m_6 are represent the six steps in the login and authentication phase, respectively. Re_{CS} and Re_{CS} are platform status values of MU and CS. K_{ep}, K_{ip} as secret key set for the external attackers and internal attackers, respectively.

Proposition 4.3.1 Suppose: ① Σ is a strand space of the TA, and C is a bundle containing an initiator strant $t \in Init\ [MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM},$

$\mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''), Cert(MU.AIK), Cert$ $Cert(MU.AIK), (APS.AIK)]$; ② $SK^{MU.AIK} \notin K_{ep}$, $SK^{APS.AIK}$ $\notin K_{ep}$; ③ $ID \in N$, g^x, g^y are uniquely originating in Σ, and $g^x \neq g^y$. Then C contains a responder strand $r \in \mathrm{Re}\, sp$ $[MU, CS, APS, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}\ h(R^*), h(R),$ $h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK), Cert(APS.AIK)]$ and a server strand $s \in Serv[MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM},$ $\mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''), Cert\ (MU.AIK),$ $Cert(CS.AIK), Cert\ (APS.AIK)]$.

Proof. (1) if $SK^{MU.AIK} \notin K_{ip}$, according to the assumption ⊖, then $SK^{MU.AIK} \notin K_p$. Known as definition 4.3.1 and assumption⊛, $MU_{TPM} \subset term < s,1 >$ is uniquely originating in a initiator strand t. By assumption⊖ and assumption⊛, g^x and g^y are originating in $< t,1 >$ and $< r,4 >$, respectively. Because the silent and conservative for TA, g^{xy} never originating in C(Theorem 9 in Ref.[18]). so, $h(R^*) \subset term$ (<r, 4>) is uniquely originating in a responder strand $t \in \mathrm{Re}\, sp$ $[MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{CS},$ $h(R^*), h(R), h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK),$ $Cert(APS.AIK)]$. Similarly, $h(R) \subset term(< t,1 >)$ is uniquely originating in initiator strand $t' \in Init$ $[MU, CS, APS, ID, g^x, g^y, MU_{TPM}', CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS},$ $h(R^*), h(R)', h(V'')', h(V'), Cert(MU.AIK)', Cert(CS.AIK),$ $Cert(APS.AIK)]$. According to assumption ⊛, then, $t' = t$, so, $ID' = ID$, $g^{x'} = g^x$, $MU_{TPM}' = MU_{TPM}$, $\mathrm{Re}_{MU}' = \mathrm{Re}_{MU}$, $Cert(MU.AIK)' = Cert(MU.AIK)$.

(2) If $SK^{MU.AIK} \in K_{ip}$, according to definition 4.3.1 and assumption ③, $CS_{TPM} \subset term$(<s, 1>) is uniquely originating in a responder strand r' (theorem 1 in Ref.[18]). And then, g^x and g^y are originating in $< t',1 >$ and $< r,4 >$, respectively. because the silent and conservative for TA g^{xy} is not originating in C (theorem 9 in Ref.[18]), therefore, Re_{MU} $\subset term\ (< t,3 >)$ is uniquely originating in server strand $s \in Serv$ $[MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R),$ $h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK), Cert(APS.AIK)]$.

Proposition 4.3.2. Suppose: ①Σ is a strand space of the TA, and C is a bundle containing a responder strand $r \in$ $\mathrm{Re}\, sp[MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU},$ $\mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''), Cert(MU.AIK), Cert(CS.$ $AIK), Cert(APS.AIK)]$; ② $SK^{CS.AIK} \notin K_{ep}$ and $SK^{APS.AIK}$ $\notin K_p$; ③ $ID \in N$, g^x, g^y are uniquely originating in Σ, and $g^x \neq g^y$, Then C contains both an initiator strand $t \in Init$ $[MU, CS, APS, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS},$ $h(R^*), h(R), h(V'), h(V''), Cert(MU.AIK), Cert(CS.$ $AIK), Cert(APS.AIK)]$ and a server strand $s \in Serv[MU,$ $CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*),$ $h(R), h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK), Cert($ $APS.AIK)]$.

Proof. (1) If $SK^{CS.AIK} \notin K_{ip}$, by the assumption②then, $SK^{CS.AIK} \notin K_p$. And due to the definition 4.1 and assumption ③, $CS_{TPM} \subset term(< s,4 >)$ is uniquely originating in a responder strand $r \in \mathrm{Re}\, sp$ $[MU, CS,$ $APS, ID, g^x, g^y,$ $MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R),$ $, h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK), Cert(APS.AIK),$ $.Cert(APS.AIK)]$.

(2) If $SK^{CS.AIK} \in K_{ip}$, according to the definition 4.1 and assumption③, then, $CS_{TPM} \subset term(< r,4 >)$ is uniquely originating in a initiator strand r (theorem 1 in Ref.[18]). So, g^x and g^y are originating in $< t',1>$ and $< r,4 >$, respectively. As the silent and conservative for TA, g^{xy} is not originating in C (theorem 1 in Ref.[19]). Therefore, $h(R) \subset term$ (<s, 1>) is originating in $t' = t \in Init[MU, CS$ $ID, g^x, g^y,$ $MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''),$ $Cert(MU.AIK), Cert(CS.AIK), Cert(\ APS.AIK)]$. Because C contain a initiator strand, C contains a server strand $r \in Serv$ $[MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU},$ $\mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''), Cert(MU.AIK),$ $Cert(CS.AIK), Cert(APS.\ AIK)]$, too. it is similar to proposition 4.3.1.

Proposition 4.3.3 Suppose: ①Σ is a strand space of the TA, and C is a bundle containing a server strand $s \in Serv$ $[MU, CS, APS, ID, g^x, g^y,$ $MU_{TPM} CS_{TPM},$ $\mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V1), h(V2), Cert(MU.AIK),$ $Cert(CS.AIK), Cert(APS.AIK)]$; ② $SK^{MU.AIK} \notin K_{ep}$, $SK^{CS.AIK}$ $\notin K_{ep}$; ③ $ID \in N$, g^x, g^y are uniquely originating in Σ, and $g^x \neq g^y$, Then C contains both an initiator strand $t \in Init$ $[MU,$ $CS, APS,$ $g^x, g^y,$ $MU_{TPM}, CS_{TPM},$ $\mathrm{Re}_{MU},$ $\mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK)$ $Cert(APS.AIK)]$ and a responder strand $r \in \mathrm{Re}\, sp$

$[MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V'), h(V''), Cert(MU.AIK), Cert(CS.AIK), Cert(APS.AIK), Cert(APS.AIK)]$.

Proof. (1) If $SK^{MU.AIK} \notin K_{ip}$, according to the assumption ②, then $SK^{CS.AIK} \notin K_p$. By definition 4.1 and assumption ③, $h(V') \subset term$ (<s, 4>) is uniquely originating in a responder strand r. and by the assumption③, then, g^x, g^y are originating in $< t', 1 >$, $< r, 4 >$, respectively. Because the silent and conservative for TA, g^{xy} is not originating in C (Theorem 9 in Ref.[18]). As such, $\mathrm{Re}_{MU} \subset term$ (<s, 3>) is uniquely originating in a responder strand $r \in \mathrm{Re}\, sp\, [MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(V''), h(V'), Cert(MU.AIK), Cert(CS.AIK), Cert(APS.AIK)]$. Similarly, $\mathrm{Re}_{CS} \subset term$ (<s, 6>) is uniquely originating in a server strand $s' \in Serv[MU, CS, APS, ID, g^x, g^y, MU_{TPM}, CS_{TPM}. \mathrm{Re}_{MU}', \mathrm{Re}_{CS}', h(R^*), h(R), h(V''), h(V), Cert(MU.APS), Cert(CS.AIK), Cert(APS.AIK)']$. Due to the assumption③, $s' = s$, so, $ID' = ID$, $\mathrm{Re}_{MU}' = \mathrm{Re}_{MU}$, $\mathrm{Re}_{CS}' = \mathrm{Re}_{CS}$, $Cert(APS.AIK)' = Cert(APS.AIK)$.

If $SK^{MU.AIK} \in K_{ip}$, according to definition 4.1 and assumption③, then $CS_{TPM} \subset term$ (<s, 6>) is uniquely originating in a responder strand r' (theorem 1 in Ref.[18]), so, g^x and g^x are originating in $< t', 1 >$ and $< r, 4 >$, respectively. As the silent and conservative for TA, g^{xy} is not originating in C (Theorem 9 in Ref.[18]). By the proof of (1), we can get $r' = r$. As C contains a responder strand, C contains a initiator strand $t \in Init\, [MU, CS, APS, ID, g^x, g^y, MU_{TPM}, , MU_{TPM}, CS_{TPM}, \mathrm{Re}_{MU}, \mathrm{Re}_{CS}, h(R^*), h(R), h(V''), h(V'), Cert(MU.AIK), Cert(APS.AIK)]$, it is similar to proposition 4.3.2.

According to proposition 4.3.1, proposition 4.3.2 and proposition 4.3.3, it is concluded that the proposed protocol realizes bidirectional identity authentication and platform authentication for Mobile User and Cloud Server. The trusted access security protocol can prevent internal and external attacks. Besides, it is proved secure.

CONCLUSION

In light of the access authentication problem in the cloud environment, the existing authentication protocols are analyzed. It is found that these protocols do not consider the security of platform. Trusted computing can radically control the hidden insecurity factors by targeting at the terminal. Introducing the remote attestation mechanism in trusted computing into the protocol, our scheme realizes bidirectional identity and platform authentication for MU and CS with greater security and security compared with the current popular protocol. And we formal analysis of the identity and platform for MU and CS by using strand space model (SSM), to prove the trusted access authentication process is security. Moreover, the privacy protection of the platforms for the two communicating parties is also ensured. Future work is to carry out dynamicity of credible platform verification for the security protocol proposed in this article.

CONFLICT OF INTEREST

The author(s) confirm that this article content has no conflicts of interest.

ACKNOWLEDGEMENTS

The work was sponsored by National Natural Science Foundation of China (Grant No. 61370220), Program for Innovative Research Team (in Science and Technology) in University of Henan Province (Grant No.15IRTSTHN010) Plan for Scientific Innovation Talent of Henan Province (Grant No. 134100510006), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No. 2011HASTIT015), and Key Program for Basic Research of The Education Department of Henan Province (Grant No.13A520240, No.14A520048). We give thanks to the reviewers and editors for their valuable comments, questions, and suggestions.

REFERENCES

[1] H. Ma, Z. G. Hu, L.Yang, "User feature-aware trustworthiness measurement of cloud services vis evidence synthesis for potential users", Journal of Visual Languages and Computing, vol. 25, no. 6, pp.791-799, 2014.

[2] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no. 3, pp.583-592, 2012.

[3] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, P. R. M. Inácio, "Security issues in cloud environments: a survey", International Journal of Information Security, vol. 13, no. 2, pp.113-170, 2014.

[4] Top Threats to Mobile Computing, http://www.cloudsecurityalliance.org/download/mobile-top-treats, 2014.

[5] D. E. Popescu, A. M. Lonea, "An Hrbrid Text-Image Based Authentication for Cloud Services", International Journal of Computers Communications and Control, vol. 8, no. 2, pp.263-274, 2013.

[6] A. J. Choudhurr, P. Kumar, M. Sain, H. Lim, H. J. Lee, "A strong user authentication framework for cloud computing", 2011 IEEE Asia-Pacific Services Computing Conference, Jeju Island, Korea, PP.110-115, 2011.

[7] C. D. Jaidhar , "Enhanced mutual authentication scheme for cloud architecture", Proceedings of the 2013 3rd IEEE International Advance Computing Conference, Ghaziabad, India, pp.70-75, 2013.

[8] S. Lee, T. R. Kim, H. J. Lee, " Mutual authentication scheme for cloud computing", 2013 International Conference on Future Information and Communication Engineering, Shenyang, China, pp.149-157, 2013.

[9] TCG Specification Architecture Overview Revision1.4, https://www.trustedcomputionggroup.org/groups/TCG_1.4_Archiecture_Overview.pdf, 2011.

[10] C. X. Shen, H. G. Zhang, H. M. Wang, J. Wang, *et al*., " Research and development of trusted computing", info.scichina.com, vol. 40, no. 2, pp.139-166, 2010.

[11] E. Ghazizadeh, M. Zamani, J. A. Manan, M. Alizadeh," Trusted Computing Strengthens Cloud Authentication", The Scientific World Journal,Vol. 2014, pp.2-17, 2014.

[12] F. Xie, Y. Y. Du, "Research on Cloud Computing Security Based on the Remote Attestation", International Conference on Mechatronics and Industrial Informatics, Guangtzhou, China, pp.2657-2664, 2013.

[13] S. Z. Mei, Z. Y. Wang, Y. Cheng, "Trust Bytecode Virtual Machine Module:A Novel Method for Dynamic Remote Attestation in Cloud Computing", International Journal of Computational Intelligence System, vol. 5, no. 5, pp.924-932, 2012.

[14] M. Achemlal, S. Gharout, C. Gaber, "Trusted platform module as an enabler for security in cloud computing", 2011 Conference on Network and Information Systems Security, La Rochelle, France, pp.1-6, 2011.

[15] Z. Y. Zhang, Q. Q. Pei, L. Yang, J. F. Ma, "Attestation proxy party-supported remote attestation model and its secure protocol", Journal of Xidian University, vol. 36, no. 1, pp.58-63, 2009.

[16] T. Hang, Z. Y. Zhang, Q. L. Chen, Y. N. Chang, "A Method for Trusted Usage Control over Digital Contents Based on Cloud Computing", International Journal of Digital Content Technology and its Application, vol. 7, no. 4, PP.795-802, 2013.

[17] F. J. T. Fabrega, J. C. Herzog, J. D. Guttman, "Strand space: proving security protocols correct", Journal of Computer Security, vol. 7, no. 2, PP.191-230, 1999.

[18] J. C. Herzog, "The Diffie-Hellman key-agreement scheme in the strand space model", 2003 IEEE 16th IEEE Computer Security Fundamentals of Electronics, Communications and Computer Sciences, PP.665-668, 2012.

[19] Y. L. Xiao, Y. M.Wang, L.J. Pang, "Verification of trusted network access protocols in the strand space model", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 95, no. A(3), PP.665-668,2012.