A User Authentication Scheme Based on Trusted Platform for Cloud Computing

Jiaqing Mo[1(✉)], Zhongwang Hu[1], and Yuhua Lin[2]

[1] School of Computer, Zhaoqing University, Zhaoqing 526061, China
{mojiaqing, huzhongwang}@126.com
[2] Education Technology and Computer Center, Zhaoqing University, Zhaoqing 526061, China
183898054@qq.com

Abstract. Cloud Computing develops rapidly and has been widely used in recent years. Remote user security authentication plays an important role in Cloud Computing security mechanism. Some of remote authentication protocols have high computational cost, and they have much interaction rounds, the credibility of remote user's platform could not be guaranteed. In this paper, we put forward a user identity authentication scheme based on trusted platform for Cloud Computing. In this scheme, the cloud user registers in the trusted certificate authority (CA), and obtains the certificate issued by CA. Afterwards, the certificate is sent to the cloud server, and the cloud server verifies the validity of the remote user identity according to the certificate. At the same time, this scheme provides mutual authentication while it establishes communication key between the remote user and cloud server. The analysis shows that this scheme is secure against insider attack, replay attack, backward/forward attack, and forgery attack. Compared with the related work, the scheme has higher computing efficiency and less interaction rounds.

Keywords: Authentication · Trusted platform · Bilinear map · Key agreement · Cloud computing

1 Introduction

Cloud Computing is a kind of computing resource service model, which fulfills the need of the Internet users with flexible on-demand services. This model enables computing, storage, platforms, and services to be available to users on the Internet in an abstract, virtual, dynamic, extensible and manageable manner [1]. With the rapid development of the Internet and network technology, Cloud Computing has become the main environment for data storage and computing, and the impact is more and more extensive [2, 3].

However, the security problems caused by the openness, dynamic and large scale of the Cloud Computing also attract people's attention, which has become the main factor to hinder its further application. One of them is the authenticity of the user identity and the integrity and the forgery-resistance of the platform. Therefore, on the premise of ensuring the authenticity of the cloud user identity and the integrity of the platform,

G. Wang et al. (Eds.): SpaCCS 2016, LNCS 10066, pp. 122–130, 2016.
DOI: 10.1007/978-3-319-49148-6_11

how can the cloud user access to the cloud server securely and efficiently has become a research hotspot [4–6].

Santos et al. [7] presented a trusted Cloud Computing platform (TCCP) protocol, the purpose is to use trusted computing to solve the problem of the credibility of the Cloud Computing platform. In this protocol, the trusted server first verifies the identity to the TC (Trusted Coordinator) with the EK (Endorsement Key) and the integrity measurement list. TC joined the node which was verified successfully to the list of trusted entities, while TC will participate in the protocol to ensure that the server was in the list of trusted entities. In this protocol, the user needs to trust the TC absolutely, and TC needs to participate in the protocol operation for many times. If TC is paralyzed, TCCP does not work properly; moreover, a large number of trusted cloud servers in the protocol need to interact with TC, which makes TC a performance and security bottleneck for the entire protocol. A robust Cloud Computing user authentication framework is proposed in [8], in which all users must login the cloud server through a strong validation of the legitimacy. This framework provides the functions of identity management, mutual authentication and session key establishment between the user and the server. According to the security analysis of this article, it can resist most of the network attacks. Nimmy et al. [9] proposed an cloud authentication scheme based on mutual authentication using secret sharing and steganography, in this scheme the user authentication process is divided into four phases which included register, login, authentication, and changing password. In order to prevent all attacks the user must pass the server's authentication before interacting with the cloud server. While Vorugunti et al. [10] has pointed out that scheme of [9] cannot resist the off-line password attack and denial of service attacks. At the same time, a new Cloud Computing scheme is proposed based on steganography [11]. This scheme introduced encrypted proxy in user identity authentication in the Cloud Computing, when the users access to the cloud servers, the server would verify their identities with the CUA (Cheat-Based user authentication agent), and then checks whether the user is registered with the MDHA (Modified Diffie-Hellman Agent). The users can access the cloud server via encrypted proxy only if they passed the checking. Chen [12] proposed a computing scheme of identity authentication based on one-way hash function and XOR operation for the cloud computing, the purpose of which is to reduce the computational cost. In addition, several literals [13–16] also put forward the identity based user authentication schemes. Some authentication schemes based on certificate have been proposed, but their computational efficiency and transmission efficiency have much room for improvement. Aiming at low efficiency of authentication scheme based on certificate, Zhang et al. [17] proposed a new user authentication protocol, the protocol used certificateless way to reduce computational time and also used temporary ID instead of its true identity in order to hide the true information. Although these schemes authenticate users in different ways, they do not ensure the credibility of the user's platform and the integrity of the platform.

We can see that in the process of remote user authentication in Cloud Computing, the following issues should be considered: (1) the credibility of their platform should be ensured while users accessing to the cloud computing; (2) at the same time, the users, as the protocol participants, computing capability of their platform is relatively weak, thus computation burden of them should be reduced; (3) in addition, the users as a

remote party, have large communication time delay, the interaction round of the authentication protocol should be decreased.

According to the above considerations, this paper proposes a novel scheme of direct user identity authentication based on trusted platform in the Cloud Computing environment. In this scheme, the user first registers in the trusted third party CA, and obtains a certificate issued by CA, then the user proves the legitimacy of the identity according to the certificate which was sent to the cloud server to ensure user platform security. We show that this scheme reduces the computation burden of the user side in the authentication process and decreases the rounds of message exchanging, and improves the computational efficiency and security.

The reminder of this paper is organized as follows. Section 2 introduces the preliminaries. Section 3 proposes our authentication scheme in detail. Section 4 analyzes the security and efficiency of our proposed scheme. Finally, Sect. 5 concludes the paper.

2 Preliminaries

2.1 Bilinear Map

Let G_2 and G_1 be the additive and multiplicative cyclic groups respectively, and their prime order is q. If the mapping e: $G_1 \times G_1 \rightarrow G_2$ satisfies the following properties, it is called a bilinear map:

(1) Bilinearity: $e(aP, bQ) = e(P,Q)^{ab}$, for all $P,Q \in G_1$, and $a, b \in Z_q^*$;
(2) Non-degeneracy: there exists $P,Q \in G_1$, such that $e(P,Q) \neq 1$;
(3) Computability: for all $P,Q \in G_1$, there exists an efficient algorithm to compute e(P,Q) in polynomial time.

2.2 Computational Problem

Discrete logarithm problem (DL): Let q ($q > 2^k$, k is a safe parameter) be a large prime number, and q is the order of cyclic group G with generator P, finding an integer $a \in Z_q^*$ such that $Q = aP \in G$ is hard.

Computational Diffie-Hellman Problem (CDH): G is a cyclic group with order of q and generator of P, given $a, b \in Z_q^*$ and aP, $bP \in G$, finding abP is hard.

3 Proposed Scheme

Figure 1 shows our proposed authentication scheme for Cloud Computing. This scheme involves the user U and trusted third-party CA, as well as Cloud Server (CS). CA is the certificate Issuer, publishes the relevant parameters and issues direct anonymous attention (DAA) certificate for the user; user U is the signer and his/her host is installed trusted platform module (TPM), obtains DAA certificate; CS is not anly a verifier but also a cloud service provider, and CS verifies the validity of DAA

signature with CA's public key, at the same time CS verifies the authenticity of the platform by the validity of the signature.

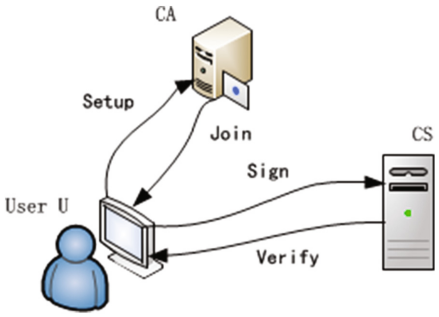

Fig. 1. Our Proposed Scheme

(1) Setup

CA selects the additive group G_1 and multiplicative group G_2 with the same order q which is big prime, the generator of G_1 is P. The bilinear map is defined as e: $G_1 \times G_1 \rightarrow G_2$, and one way strong collision-resistance hash function H(), the asymmetric encryption function E() and decryption function D() are selected, and the random number P_{ri_CA} is selected as the main key, and its public key $P_{ub\_CA} = P_{ri\_CA}P$. Later CA publishes the system parameter set CA_params = $\{G_1, G_2, e, q, P, H(), E(), D()\}$.

Cloud server also chooses random number $P_{ri\_S} \in Z_q^*$ as a master key and the public key $Pub\_S = P_{ri\_S}P$, keeps P_{ri_S} secretly, publishes system parameter set S_params = $\{G_1, G_2, e, q, P, P_{ub\_S}, H(), E(), D()\}$;

(2) Join

TPM of user U chooses random number r_{u_1}, $n \in Z_q^*$, and uses his/her own identity ID_U to generate registration information $R_U = H(ID_U \| n)$ where $\|$ is a concatenation operation, computes $R_M = r_{u\_1}P$, generates message $M_{sg\_u} = E(P_{ub\_CA} \| ID_U \| R_U \| T_{u\_1})$ with local timestamp T_{u_1}, and send M_{sg_u} to CA via the secure channel.

CA verifies the message M_{sg_u} whether TPM is valid, if yes, the validity of user can be assured and CA performs subsequent operation; otherwise, aborts.

CA chooses a random number $r_{CA\_1} \in Z_q^*$, computes $R_{CA} = r_{CA\_1}P + R_M$, $C = H(ID_U \| R_{CA} \| R_U)$, as well as $R_{CA} = r_{CA\_1}P + R_M$, $L_{CA} = P_{ri\_CA}C + r_{CA\_1}$, thus (L_{CA}, R_{CA}) is the registration message generated by CA for user U.

CA chooses random number $r_{CA\_2} \in Z_q^*$, calculates the user's temporary ID information $ID_{U\_T} = H(ID_U \| r_{CA\_2})$, lets the certificate's expiration date be T_E, generates user's ID information $C_{ERT\_CA} = E(P_{ri\_CA} \| ID_{CA} \| ID_{U\_T} \| T_E)$, and sends the certificate to the TPM of user U in security channel. Meanwhile, CA adds user U to the register list.

User U decrypts C_{ERT_CA} from CA with public key P_{ub_CA} as he/she received the certificate, and then checks $R_M + L_{CA}P = P_{ub\_CA}C + R_{CA}$ whether is satisfied or not. If yes, the validity of certificate can be assured. At this time TPM computes $K = L_{CA} + r_{u\_1}$, thus user obtains certificate $C_{CA\_DAA} = (K, R_{CA}, H(ID_U \| R_{CA} \| R_U))$ issued by CA.

(3) Sign

TPM of User U chooses secret random number S_u, $y_u \in Z_q^*$, computes $X_u = S_u R_{CA}$, $Y_u = S_u CP$, $W_u = S_u KP$, $F_u = y_u P$, $M_u = S_u K + y_u H(F_u \| 0)$; Y_u is session negotiation parameters, M_u is the correctness verification information of key agreement parameters, $S_{ig\_u} = (X_u, Y_u, W_u, F_u, M_u, C_{ERT\_CA})$ is the valid information of the user's identity.

TPM reads the current time stamp T_{u_2}, generates message $E(ID_{CA} \| ID_{U\_T} \| S_{ig\_u} \| P_{ub\_u} \| T_{u\_2})$ and sends the message to CS.

(4) Verify

Upon receiving the information from CS, TPM decrypts the message using his/her own private key P_{ri_s}, after that TPM decrypts C_{ERT_CA} with public key of TPM and get the ID information of TPM and CA, that were denoted by ID_{U_T}' and ID_{CA}' respectively, and judges $ID_{U\_T}' = ID_{U\_T}$ and $ID_{CA}' = ID_{CA}$ whether are satisfied or not, if no, subsequent operation will be interrupted. Later, CS consults communication key with TPM. CS chooses secret random number $v \in Z_q^*$, computes $V = vP$, computes the communication key $KEY_{S\text{-}U} = H(vF_u \| 1) = H(vy_u P \| 1)$ between CS and TPM.

CS verifies $M_u P = H(F_u \| 0) \| + W_u$ and $e(Y_u, P_{ub\_CA}) = e(P, W_u - X_u)$ whether are satisfied or not, if yes, thus CS passes the legal authentication of TPM ID of user U, and user U is recognized as a valid user registered on the CA.

CS reads time stamp T_S, generates signature $L_S = Sig(P_{ri\_S} \| T_S \| V)$, sends message $(T_S \| V \| L_S)$ to user U. TPM checks the validity of identity of CS according to LS, and checks time stamp T_S whether is fresh or not, if two check hold, computes the communication key $KEY_{U-S} = H(y_u V \| 1) = H(vy_u P \| 1)$ between CS and TPM. Therefore the communication session key is established between TPM and CS.

4 Security Analysis

4.1 Correctness

In Join phase, because the equation $R_M + L_{CA}P = R_M + (P_{ri\_CA}C + r_{CA\_1})P = R_M + P_{ri\_CA}CP + r_{CA\_1}P = P_{ub\_CA}C + R_{CA}$, the user's TPM confirms that the certificate information generated by CA is legal.

In verify phase, $e(Y_u, P_{ub\_CA}) = e(S_u CP, P_{ri\_CA}P) = e(Su\ (r_{u\_1} + r_{CA\_1} + P_{ri\_CA}C)P - e(S_u\ (r_{u\_1} + r_{CA\_1})P, P) = e(W_u - X_u, P) = e(P, W_u - X_u)$, and $M_u P = H(F_u \| 0) \| + W_u$, CS confirms the validity of the certificate C_{ERT_CA} according to the decryption of the certificate, CS assures that the user U is the legal entity authenticated by CA finally.

4.2 Mutual Authentication and Key Agreement

In Verify phase, CS verifies the correctness with the user U's TPM valid message. The correctness of TPM valid information contains the certificate issued by the CA. In this way, CS will confirm that the user is legitimate one registered on the CA. At the same time, the user U confirmed the identity of the CS according to the CS signature information. The timestamp of the CS signature information also ensures the forgery-resistance of the signature information.

CS generates the secret communication key KEY_{S-U} according to the parameter F_u provided by the user U's TPM in Verify phase, as well as their own choice of secret random number v. Similarly, TPM establishes the same communication key with CS according to the signature information and the parameter v provided by CS, combined with his/her own secret parameter y_u.

Because the TPM sent F_u, which is the critical parameter in negotiating communication key, to CS by way of decryption, and CS sent parameter V to the user U by way of signature, the adversary cannot get the key agreement information. In addition, due to difficulty of DL problem, for the formula $V = vP$, users can't solve v according to the V and P; similarly, for the formula $F_u = y_uP$, CS can't solve the user's secret random number y_u according to F_u and P.

4.3 Anti-attack

(1) Anonymity

In the Join phase, CA generates temporary ID information $ID_{U\_T} = H(ID_U \| r_{CA\_2})$ for user U, and encrypts the temporary identity information in the certificate C_{ERT_CA}, and sends to CS, CS can judge the user's U identity is valid or not. Furthermore, when CA generated temporary identity for user, the selected number r_{CA_2} is different for different users, both CS and the adversary can't determine the true identity information of users U, so that the user anonymity of U is ensured.

(2) Resistance to insider attack

In Join phase, the user generates registered information with $R_U = H(ID_U \| n)$, If another user wants to get the value of the secret number n with the ID of the user U, but the H() is a strong strict one-way hash function, so this is not feasible. At the same time, it is not feasible that the adversary wants to obtain the secret value of r_{CA_2} by temporary identity information ID_{U_T}, also due to strong strict one-way hash function H().

(3) Resistance to replay attack

Assume that the adversary has intercepted messages that user U sends to CS in Sign phase, but he/she could not decrypt the messages, so that he/she is unable to get the user's identity information and temporary identity information, not even get the timestamp, so the adversary cannot initiate replay attack.

(4) Resistance to forward/backward attack

The implementation of forward/backward attack means that the adversary has access to the communication key, but in the process of authentication in this paper, the

adversary cannot construct the communication key between TPM and CS. CS and TPM need to use their own secret random number in the process of generating communication keys, and each time the user login authentication CS used with different secret random number, and these number will not leak out. So the protocol in this paper can resist forward/backward attacks.

(5) Resistance to forgery attack

In Join phase, user U checks $R_M + L_{CA}P = P_{ub\_CA}C + R_{CA}$ whether is satisfied or not, and R_M contains secret random number r_{u_1} of user U, and L_{CA} contains the private key P_{ri_CA} of CA, these can not be faked by the adversary. In addition, CS need to verify $M_uP = H(F_u\|0) + Wu$ and $e(Y_u,P_{ub\_CA}) = e(P,W_u - X_u)$ in verify phase, in order to check whether the identity of the user U is valid or not. If the adversary wants to forge these information, he/she will face DL and CDH problems.

We compare our scheme with exist authentication schemes [15, 18, 19] in terms of functionality. Table 1 shows the result of the comparison.

Table 1. The functionality comparison between our scheme and the existing scheme

Comparison items	This paper	Tsai [18]	Chen [19]	Liao [15]
Single registration	Yes	Yes	No	No
Mutual authentication	Yes	Yes	No	Yes
Communication key agreement	Yes	Yes	No	Yes
User's anomymity	Yes	Yes	Yes	No
Resistance to insider attack	Yes	No	No	Yes
Resistance to replay attack	Yes	No	No	Yes
Resistance to forward/backward attack	Yes	No	No	No
Resistance to forgery attack	Yes	Yes	Yes	Yes

4.4 Computation Efficiency

In order to illustrate the computational efficiency of this protocol, we compare the computational cost of our proposal with other related schemes.

It is well known that time-consuming operation mainly include bilinear pairings computation, asymmetric encryption, signature and verification operations, exponentiation. Table 2 is comparison of computational cost in this scheme and other schemes. The various computing entities in the first four rows of this table are user U, CS, CA, and the last row is the rounds of interaction about U-CA, U-CS, CA-CS.

Table 2. Comparsions with other schemes in computing efficency

Comparison items	This paper	Tsai [18]	Chen [19]	Liao [15]
Bilinear pairings	0/2/0	1/4/0	2/2/1	7/2/5
Asymmetric encryption	1/2/0	N/A	N/A	N/A
Signature and verification	1/1/0	N/A	0/1/1	N/A
Exponentiation	N/A	1/2/0	18/4/16	2/0/1
Rounds of interaction	1/0/1	1/1/2	4/0/1	1/1/3

As can be seen from Table 2, in the process of implementing of this agreement, times of user U's executing the high computational complexity operations is 2, while Tsai [18], Chen [19], Liao [15] were 2, 20, 9 respectively. Since computing capability is limited on user side, this scheme shifts the computational burden to the powerful cloud server and reduces the computational cost required by the user side, improves the computational efficiency; moreover, as it is known to all, the bilinear pairing operation is more time-consuming than other operations, all entities in our scheme operates bilinear pairings 2 times in total, while schemes [15, 18, 19] reach 5, 5, 14 times respectively. In addition, from the table it also can be seen that the rounds of interaction is lower than other protocols, which reduces the communication delay, improves the efficiency of implementation.

Furthermore, the user's certificate C_{ERT_CA} issued by CA contains the expiration date T_E. If user U was authenticated successfully by CS once, he/she can login CS while skipping the Join phase, directly goes into the Sign and Verify phase for many times with certificate C_{CA_DAA}, as long as T_E is valid. This feature makes the calculation more efficient, and CA will not become the bottleneck of the agreement.

While improving the efficiency of execution, this paper utilizes the techniques such as signature and encryption to ensure the security of the remote user the Internet environment.

5 Conclusions

This paper proposes a user identity authentication scheme based on trusted platform for Cloud Computing which includes Setup, Join, Sign, Verify phases. The scheme uses the trusted third party CA for registered users to generate temporary identity ID. User and CA, users and the cloud server achieve mutual authentication. User of the proposed solution has a low computational complexity, high security features. And the entire agreement has fewer interaction rounds, and has lower communication delays too. Security analysis shows that computation efficiency of this scheme is higher than other schemes, and has better security.

References

1. Moghaddam, F.F., Ahmadi, M., Sarvari, S., et al.: Cloud computing challenges and opportunities: a survey. In: Proceedings of the 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), pp. 34–38. IEEE(2015)
2. Lee, B., Awad, A., Awad, M.: Towards secure provenance in the cloud: a survey. In: Proceedings of the IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), pp. 577–582. IEEE (2015)
3. Hussein, N.H., Khalid, A.: A survey of cloud computing security challenges and solutions. Int. J. Comput. Sci. Inf. Sec. **14**(1), 52 (2016)

4. Yassin, A.A., Jin, H., Ibrahim, A., et al.: Cloud authentication based on anonymous one-time password. In: Han, Y.H., Park, D.S., Jia, W.J., Yeo, S.S. (eds.) Ubiquitous Information Technologies and Applications. LNCS, vol. 214, pp. 423–431. Springer, Amsterdam (2013)
5. Gonzalez, N.M., Rojas, M.A.T., da Silva, M.V.M, et al.: A framework for authentication and authorization credentials in cloud computing. In: Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 509–516. IEEE (2013)
6. Jaidhar, C.D.: Enhanced mutual authentication scheme for cloud architecture. In: Proceedings of the 3rd International Conference on Advance Computing (IACC), pp. 70–75. IEEE (2013)
7. Santos, N., Gummadi, K.P., Rodrigues, R.: Towards trusted cloud computing. HotCloud **09** (9), 3 (2009)
8. Choudhury, A. J., Kumar, P., Sain, M., et al.: A strong user authentication framework for cloud computing. In: Proceeding of the IEEE Asia-Pacific on Services Computing Conference (APSCC), pp. 110–115. IEEE (2011)
9. Nimmy, K., Sethumadhavan, M.: Novel mutual authentication protocol for cloud computing using secret sharing and steganography. In: Proceedings of the Fifth International Conference on Applications of Digital Information and Web Technologies (ICADIWT), pp. 101–106. IEEE (2014)
10. Vorugunti, C., Sarvabhatla, M., Murugan, G.: A secure mutual authentication protocol for cloud computing using secret sharing and steganography. In: Proceedings of the Cloud Computing in Emerging Markets (CCEM), 2014 IEEE International Conference, pp. 1–8. IEEE (2014)
11. Moghaddam, F.F., Moghaddam, S.G., Rouzbeh, S., et al.: A scalable and efficient user authentication scheme for cloud computing environments. In: Proceedings on Region 10 Symposium, pp. 508–513. IEEE (2014)
12. Chen, T.H., Yeh, H., Shih, W. K.: An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. In: Proceedings of the 5th FTRA International Conference on Multimedia and Ubiquitous Engineering (MUE), pp. 155–159. IEEE (2011)
13. Yang, J.H., Lin, P.Y.: An ID-based user authentication scheme for cloud computing. In: Proceedings of the Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 98–101. IEEE (2014)
14. Mnif, A., Cheikhrouhou, O., Jemaa, M. B.: An ID-based user authentication scheme for wireless sensor networks using ECC. In: ICM 2011 Proceeding, pp. 1–9. IEEE (2011)
15. Liao, Y.P., Hsiao, C.M.: The improvement of ID-based remote user authentication scheme using bilinear pairings. In: Proceedings of the International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 865–869. IEEE (2011)
16. Huang, H.F., Lin, P.H.: Enhancement of dynamic ID based user authentication for multi-server environment. In: Proceedings of the Sixth International Conference on Genetic and Evolutionary Computing (ICGEC), pp. 55–58. IEEE (2012)
17. Zhang, M., Zhang, Y.: Certificateless anonymous user authentication protocol for cloud computing. In: Proceedings of 2015 International Conference on Intelligent Transportation, Big Data and Smart City (ICITBS), pp. 200–203. IEEE (2015)
18. Tsai, J.L., Lo, N.W.: A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst. J. **9**(3), 805–815 (2015)
19. Chen, X.F., Feng, D.G.: Direct anonymous attestation based on bilinear maps. J. Softw. **21** (8), 2070–2078 (2010)