A PRIVACY PRESERVATION IN CLOUD COMPUTING SCHEME FOR DISTRIBUTED MOBILE SERVICES

G.Sugathi[1], S.Kanaga Lakshmi[2]

[1]Student Member, Department of Computer Science and Engineering,

[2] Staff Member, Department of Computer Science and Engineering,

VPMM Engineering College, Krishnankovil, TamilNadu, India.

ABSTRACT- In modern societies, the number of mobile users has dramatically risen in recent years. In this Work, an efficient authentication scheme is proposed for distributed mobile cloud computing services. The proposed scheme provides security and convenience for mobile users to access multiple mobile cloud computing services from multiple service providers using only a single private key. The security strength of the proposed scheme is based on bilinear pairing cryptosystem and dynamic nonce generation. In addition, the scheme supports mutual authentication, key exchange, user anonymity, and user intractability. From system implementation point of view, verification tables are not required for the trusted smart card generator (SCG) service and cloud computing service providers when adopting the proposed scheme. In consequence, this scheme reduces the usage of memory space son these corresponding service providers. In one mobile user authentication session, only the targeted cloud service provider needs to interact with the service requestor (user). The trusted SCG serves as the secure key distributor for distributed cloud service providers and mobile clients. In the proposed scheme, the trusted SCG service is not involved in individual user authentication process. With this design, our scheme reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service. Formal security proof and performance analyses are conducted to show that the scheme is both secure and efficient.

Keywords

Authentication scheme, bilinear pairing, mobile cloud computing services, user anonymity, user untraceability

1. INTRODUCTION

The development of mobile cloud computing has become an important research field in mobile-oriented world, providing new supplements, consumption, and delivery models for IT services. As reported by ABI Research, more than 240 million business customers will be leveraging cloud computing services through mobile devices by 2015, driving revenues of $5.2 billion In mobile cloud computing, mobile users can access computation results, resources, applications, and services that are stored, implemented, and deployed in cloud computing environments by using mobile devices through an insecure wireless local area network (WLAN) or 3G/4G telecommunication networks. When a user intends to access a mobile cloud computing service, he/she activates the service through a Web browser or a cloud service application (i.e., App) installed on his/her mobile device.

The Web browser or the cloud service application will then mutually authenticate both the cloud service provider and the user. After authentication, the user can access the resources and available services from the cloud service provider. In order to prevent illegal access, cloud providers should support a secure authentication scheme for users using mobile devices. However, there are three concerns to be resolved along with the authentication scheme. First of all, computing efficiency of the scheme should be seriously considered, since mobile devices have only relatively limited computing capability in comparison with laptop computers. Second, sufficient security strength should be supported; since all messages are transmitted via an insecure WLAN or telecommunication networks, an adversary can easily obtain, interrupt, or modify transmitting messages before they reach the desired recipient. In addition, privacy protection on user accounts is a rising issue as identity masquerade and identity tracing have become common attacks in wireless mobile environments.

As mobile users generally access different types of mobile cloud computing services from a variety of service providers, it is extremely tedious for users to register different user accounts on each service provider and maintain corresponding private keys or passwords for authentication usage. In other words, key management issue for users has emerged for distributed mobile cloud environment. In consequence, mobile users will likely be interested in how to access various services from distinct mobile cloud service providers by using only one single private key or password.

Traditional single sign-on schemes such as Passport are one possible solution for key management issue. In such systems, users can access multiple mobile cloud computing services using only one secret key or password. However, most of systems require a trusted third party to participate in each user authentication session. Pined is an example of a decentralized mechanism, which has been widely adopted by many Internet service providers such as Google.

The most important issue is that a user needs to manage multiple private keys learned from each service provider. To resolve user key management issue, the simplest way is that all service providers share the same master private key. However, if an adversary attacks one of the service providers successfully, he/she can learn this master private key and masquerade as any one of the service providers to cheat users. In addition, a malicious adversary, who has obtained the master private key from a service provider, can learn session keys established between another service provider and a user if the applied authentication scheme does not support perfect forward secrecy.

A desirable user authentication scheme for mobile users in distributed cloud services environment should preserve the following benefits.

1) The authentication scheme is based on some efficient cryptosystems to support mutual authentication and user anonymity without using SSL.

2) A trusted third party is required for user registration and service provider registration, but it is not required to participate in each user authentication session later.

3) A user can access mobile services from multiple service providers with only one private key.

4) The authentication scheme does not require heavy computation Operations on users' mobile devices.

2. RELATED WORK

Authentication scheme is a basic security mechanism for all network-based services to prevent illegal access from unauthorized users or adversaries. Traditional authentication schemes are usually based on traditional public key cryptosystem. Traditional public key cryptosystems such as RSA require lengthy key size and consume computation resources heavily. Hence, most of traditional authentication schemes are unsuitable for mobile devices, which have limited computing resources. Elliptic curve cryptosystem (ECC), which was first introduced by Koblitz and Miller, offers the smallest key size per equivalent strength of any traditional public key cryptosystem, including RSA and Discrete Logarithm Problem (DLP). For example, a 256-bit ECC public key has the same security level as a 3072-bit RSA public key Such computational efficiency is beneficial for mobile devices. Recently, bilinear pairing in an elliptic curve has been used in developing an ID-based cryptosystem. Since then, several ID based cryptosystems have been proposed. An ID basedcryptosystem is one kind of public key cryptosystems that can solve the high cost issue of public key management and authentication derived from traditional public key cryptosystems.In an ID-based cryptosystem, the identity of a user is used as the public key of this user; a user therefore does not spend extra computational cost to verify public keys of others, and no extra storage space in the user's device is required to store public keys of others and their corresponding certificates. Several studies have applied ID-based cryptosystems in cloud and grid computing environments. Lim and Robshaw] first applied an ID-based cryptosystem to grid security in 2004, whereas in the same year, Mao proposed an identity-based noninteractive authentication framework for grids. In 2009, Li *et al.* developed a new ID-based authentication for cloud computing environment. However, the authentication protocolof Lin *et al.* does not provide user anonymity and untraceability. Since most authentication schemes based on ECC or bilinear pairing are designed for client–server environment, they are not suitable to be directly adopted into distributed services environment in which multiple service providers compete with each other and offer various kinds of services. The most important issue is that a user needs to manage multiple private keys learned from each service provider. To resolve user key management issue, the simplest way is that all service providers share the same master private key. However, if an adversary attacks one of the service providers successfully, he/she can learn this master private key and masquerade as any one of the service providers to cheat users. In addition, a malicious adversary, who has obtained the master private key from a service provider, can learn session keys established between another service provider and a user if the applied authentication scheme does not support perfect forward secrecy. After learning the session key, the malicious attacker can get sensitive information transmitted between another service provider and a user. Hence, this simple approach is also unsuitable for distributed mobile cloud environments.

An anonymous user authentication scheme based on bilinear pairing for distributed mobile cloud computing services is proposed in this paper. The proposed scheme supports mutual authentication, key exchange, and initiator (user) untraceability. The proposed scheme is carefully designed to exclude the necessity for the trusted third party to be involved in regular user authentication session such that the total user authentication processing time can be reduced. The proposed scheme is built upon bilinear pairing and random nonce; consequently, this scheme requires less computing resources on both the mobile users' devices and server providers. Through an IDbased cryptosystem, a user is required only one private key to access multiple services from distinct mobile cloud service providers, provided that the user knows all the identities of the service providers and vice versa. Formal security proof under random oracle model is conducted to show the security robustness of our scheme.

The distributed mobile cloud service environment is supported by a trusted smart card generator (SCG) service. Three roles take part in the proposed scheme: mobile users, distinct mobile cloud service providers, and a trusted SCG service. Notice that the trusted third party used
in the proposed scheme is named as the smart card generator (SCG) service rather than the IdP service, since our trusted third party issues one smart card to every registered user securely during user registration phase. We assume that there are many mobile users and service providers within distributed mobile cloud services environment, and a small portion of these mobile users and service providers are malicious. Mobileusers, service providers, and the trusted SCG are denoted by $V = \{Ui|\ i = 1, \ldots, n\}$, $W = \{SPj\ |j = 1, \ldots, m\}$, and SCG. A user can anonymously access multiple mobile cloud computing services from different service providers without the involvement of the SCG during user authentication phase. The SCG is only responsible for generating public parameters, as well as all private keys for service providers and users. The proposed scheme includes three phases: system set up, registration, and authentication. During the system set up phase, the SCG first selects a random number as its master private key, computes the corresponding public key, and generates all public parameters. Then, the SCG publishes its public key and public parameters. After accomplishing the system set up phase, the registration phase is executed between the SCG and each one of the mobile users (or service providers) who wishes to join and utilize the authentication service. Mobile user and service providers are required to register with the SCG by sending their identities. Upon receiving these identities, the SCG computes and generates corresponding private keys for these users and service providers before dispatching these keys back to corresponding users and service providers securely. In accordance with the design of identity-based cryptosystem, the identities of mobile users and service providers are also served as their corresponding public keys. Finally, the authentication phase is executed between mobile user and service provider This paper assumes that the distributed mobile cloud service environment is supported by a trusted smart card generator (SCG) service. Three roles take part in the proposed scheme: mobile users, distinct

mobile cloud service providers, and a trusted SCG service. Notice that the trusted third party used

in the proposed scheme is named as the smart card generator (SCG) service rather than the IdP service, since our trusted third party issues one smart card to every registered user securely during user registration phase. We assume that there are many mobile users and service providers within distributed

mobile cloud services environment, and a small portion of these mobile users and service providers are malicious. Mobileusers, service providers, and the trusted SCG are denoted by $V = \{Ui|\ i = 1, . . . , n\}$, $W = \{\mathrm{SP}j\ |j = 1, . . . , m\}$, and SCG. A user can anonymously access multiple mobile cloud computing services from different service providers without the involvement of the SCG during user authentication phase. The SCG is only responsible for generating public parameters, as well as all private keys for service providers and users. The proposed scheme includes three phases: system set up, registration, and authentication. During the system set up phase, the SCG first selects a random number as its master private key, computes the corresponding public key, and generates all public parameters. Then, the SCG publishes its public key and public parameters. After accomplishing the system set up phase, the registration phase is executed between the SCG and each one of the mobile users (or service providers) who wishes to join and utilize the authentication service. Mobile user and service providers are required to register with the SCG by sending their identities. Upon receiving these identities, the SCG computes and generates corresponding private keys for these users and service providers before dispatching these keys back to corresponding users and service providers securely. In accordance with the design of identity-based cryptosystem, the identities of mobile users and service providers are also served as their corresponding public keys. Finally, the authentication phase is executed between mobile user and service provider This paper assumes that the distributed mobile cloud service environment is supported by a trusted smart card generator (SCG) service. Three roles take part in the proposed scheme: mobile users, distinct mobile cloud service providers, and a trusted SCG service. Notice that the trusted third party used

in the proposed scheme is named as the smart card generator (SCG) service rather than the IdP service, since our trusted third party issues one smart card to every registered user securely during user registration phase. We assume that there are many mobile users and service providers within distributed

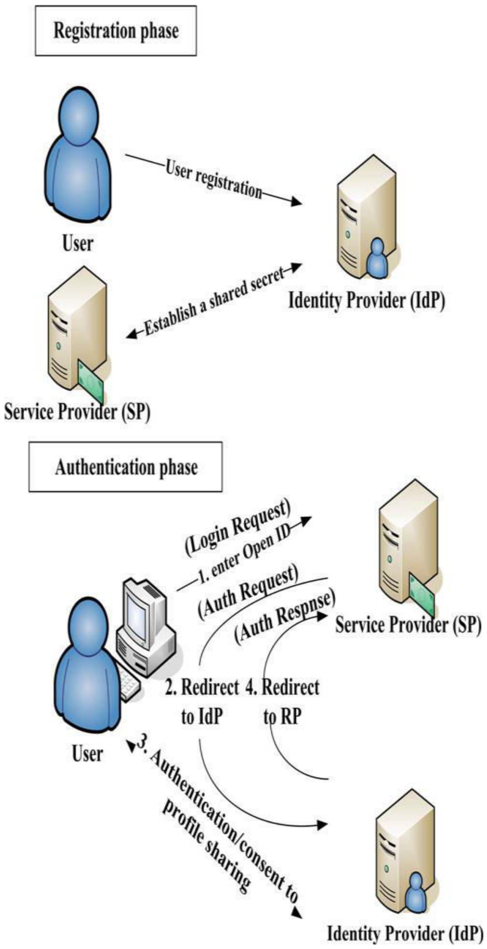
mobile cloud services environment, and a small portion of these mobile users and service providers are malicious. Mobileusers, service providers, and the trusted SCG are denoted by $V = \{Ui|\ i = 1, . . . , n\}$, $W = \{\mathrm{SP}j\ |j = 1, . . . , m\}$, and SCG. A user can anonymously access multiple mobile cloud computing services from different service providers without the involvement of the SCG during user authentication phase. The SCG is only responsible for generating public parameters, as well as all private keys for service providers and users. The proposed scheme includes three phases: system set up, registration, and authentication. During the system set up phase, the SCG first selects a random number as its master private key, computes the corresponding public key, and generates all public parameters. Then, the SCG publishes its public key and public parameters. After accomplishing the system set up phase, the registration phase is executed between the SCG and each one of the mobile users (or service providers) who wishes to join and utilize the authentication service. Mobile user and service providers are required to register with the SCG by sending their identities. Upon receiving these identities, the SCG computes and generates corresponding private keys for these users and service providers before dispatching these keys back to corresponding users and service providers securely. In accordance with the design of identity-based cryptosystem, the identities of mobile users and service providers are also served as their corresponding public keys. Finally, the authentication phase is executed between mobile user and service provider when a user is requesting for a mobile service. During this phase, a mobile user and the targeted service provider are able to authenticate each other without the involvement of the SCG. A session key is also generated during authentication to encrypt/decrypt subsequent messages sent between the user and the service provider after authentication.

3.1Security Model

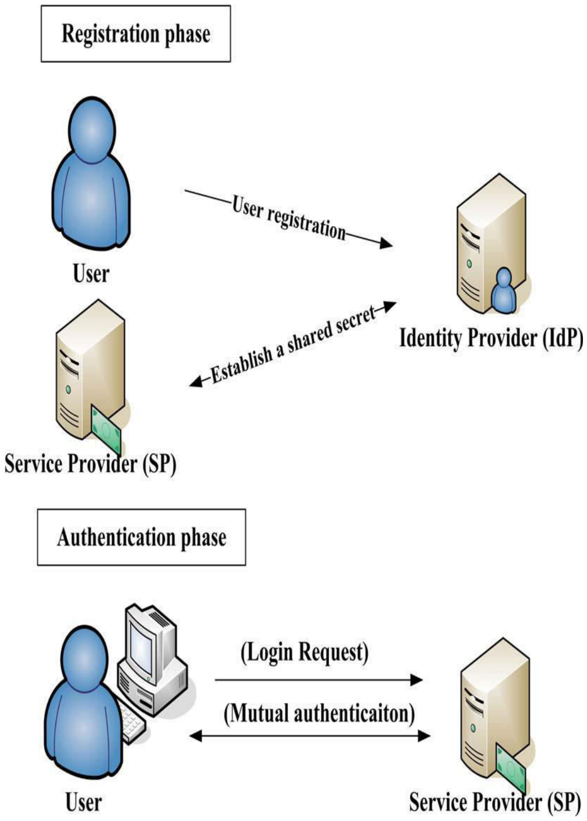
Let $Pi \in \{Ui, \mathrm{SP}j\}$ be an instance i of a participant P. Any instance of each entity is seen as an oracle in this security model, while it is also assumed that the probabilistic polynomial adversary A potentially controls all communications between the mobile user and the service provider. The capacities of the adversary are defined as follows

1) ***Extract***(ID*i*): This query allows the adversary *A* to obtain the private key corresponding to identity ID*i*.
2) ***Send***(*M,Pi*): This query models that an adversary *A* can send any message *M* to the oracle. Upon receiving the message *M*, the oracle returns the computation result to the adversary *A*.
3) ***Hi***(*m*): When an adversary *A* sends a message *m* to the hash query, the oracle returns *r* and then stores (*m, r*) in a hash list *LHi*, where *r* is a random number, and *LHi* is initially empty.
4) ***Reveal***(*Pi*): This query allows an adversary *A* to learn a session key *Kij* from an oracle if the oracle receives a Reveal query request from adversary *A*.
5) ***Corrupt***(*Pi*): This query allows an adversary *A* to corrupt the party *Pi* and obtain the private key of the corrupted party *Pi*.

The proposed authentication scheme for distributed mobile cloud service environment.The trusted SCG is responsible for generating and distributing the private keys to the users and service providers securely. If a service provider SP*j* or a user *Ui* joins the system, the SCG is not required to update its master key or corresponding public key. When a user obtains his/her private key, he/she can authenticate and communicate with the other legal entity by using his/her private key without the help of the SCG.



User Authentication Process Using Openid..



Desirable Authentication Scheme For Distributed Cloud Computing Environment.

3.2 SECURITY ANALYSIS

Security analysis for the proposed scheme is conducted here to show that the proposed scheme achieves user-to-serviceprovider authentication, service-provider-to-user authentication, and key agreement under random oracle in Theorems 1–3, respectively. User anonymity and user untraceability of the proposed scheme are also evaluated in Theorem 4. In order to clarify those hard mathematical problems used for securityanalysis, definitions of three mathematical problems . Let $G1$ be a cyclic additive group of prime order q.

Definition 1: Collusion Attack Algorithm with k-traitors (k-CAA problem): Given P, sP , $\{e1, e2, \ldots , ek \in Z* q\}$, and $\{(1/(s + e1))P, (1/(s + e2))P, \ldots , (1/(s + ek))P\}$ for an integer$k$ and $s \in Z* \ q$, $P \in G1$, it is infeasible to compute $(1/(s + e0))P$, where $e0 /\in \{e1, e2, \ldots , ek\}$.

Definition 2: Divisible computation Diffie–Hellman problem (DCDH problem): Given xP and yP for $x, y \in Z* \ q$, $P \in G1$, it is infeasible to compute $xy-1P$.

Definition 3: Computational Diffie–Hellman problem (CDH problem): Given aP and bP for a, $b \in Z* \ q$, $P \in G1$, it is infeasible to compute abP .

Let $Ek(M)/Dk(M)$ be a Xor operation to encrypt/decrypt a message M with key k. The Hash, Extract, Execute, Reveal, Send, Corrupt, and Test queries are used to simulate real attacks (refer to Tables II–IV). In the following, we show that the proposed scheme is secure under random oracle through Theorems 1–3. Theorem 4 is introduced to prove user anonymity and user untraceability of the proposed scheme. Note that the adversary B maintains four hash lists, namely, as $LH1$, $LH2$, $LH3$, and $LH4$, and all hash lists are initially empty.

Distributed mobile cloud services environment; however, it does not support user anonymity and user untraceability. Therefore, one of the design goals for the proposed scheme is to offer user anonymity and user untraceability to preserve user privacy. In order to evaluate security strength of a proposed authentication scheme, security analysis based on formal proof technique is usually conducted. From Table V, it is very obvious that only our scheme and the scheme proposed in have conducted formal proof process in terms of security strength. Existing schemes introduced in are also vulnerable to several security threats. For example, the schemes are vulnerable to replay attack, time synchronization problem, and forgery attack; the existing scheme is vulnerable to time synchronization problem and forgery attack is vulnerable to offline password guessing attack and forgery attack. Next, we analyze the computation costs of the proposed scheme. Let Tb be the time required to perform a bilinear pairing operation, and let Tm be the time required to perform a multiplication point operation. In general, the time required to perform a one-way hash function is much less than the time consumed for the two operations previously mentioned. Therefore, the time consumed by hash operations within our scheme is ignored in Table VI. As bitwise Exclusive-OR operation and bitwise concatenation operation both are much faster than one-way hash function operation, we also ignore time consumption from both operations within one user authentication session when drawing Table VI. Efficiency analysis of our scheme in terms of computation time is presented in Table VI. During the registration phase, the SCG requires only $1Tm$ to compute one private key for a mobile user Ui or a service provider SPj. During the user authentication phase, a user Ui requires $3Tm$ to authenticate the targeted service provider SPj provided that bPpub, bP , and $bH1(\mathrm{ID}i)P$ are precomputed before authentication. The targeted service provider SPj requires $2Tb + 4Tm$ to authenticate the corresponding user Ui**5.0**

4. Conclusion And Future Work

This paper has proposed a new anonymous authentication scheme for distributed mobile cloud services environment. The proposed scheme allows a mobile user to access multiple services from different mobile cloud service providers using only one single private key. The proposed scheme supports mutual authentication, key exchange, user anonymity, and user untraceability. Security analyses have shown that the proposed authentication scheme withstands all major security threats and meets general security requirements. In addition, no verification table is required to be implemented at service providers or the trusted SCG service. In the proposed scheme, the trusted SCG service is not involved in individual user authentication process. With this design, our scheme reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service. As security strength of the proposed scheme is based on nonce and bilinear pairing, the scheme itself is not subject to time synchronization problem and can be easily implemented in distributed mobile cloud computing environment.

5. REFERENCES

[1] Jia-Lun Tsai and Nai-Wei Lo, “A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services”, IEEE Systems,September,2015.

[2] M. Bellare, D. Pointcheval, and P. Rogaway, “Authenticated Key Agreement Secure Against Dictionary Attacks,” in Proc. EUROCRYPT, 2000, pp. 139–155.

[3] H. Sun, Q.Wen, H. Zhang, and Z. Jin, “A Novel Remote User Authentication And Key Agreement Scheme For Mobile Client–Server Environment,” Appl. Math. Inf. Sci., vol. 7, no. 4, pp. 1365–1374, 2013.

[4] J. L. Tsai, N. W. Lo, and T. C. Wu, “Secure Delegation-Based Authentication Protocol For Wireless Roaming Service,” IEEE Commun. Lett., vol. 16, no. 7, pp. 1100–1102, Jul. 2012.

[5] S. Pearson, “Taking Account Of Privacy When Designing Cloud Computing Services,” in Proc. CLOUD ICSEWorkshop Softw. Eng. Challenges Cloud Comput., 2009, pp. 44–52.

[6] V. S. Hughes, “Information Hiding, Anonymity And Privacy A Modular Approach,” J. Comput. Security, vol. 12, no. 1, pp. 3–36, Jan. 2004.

[7] H. Ahn, H. Chang, C. Jang, and E. Choi, “User Authentication Platform Using Provisioning In Cloud Computing Environment,” in Proc. ACN CCIS, 2011, vol. 199, pp. 132–138.

[8] M. Jakpbsson and D. Pointcheval, “Mutual Authentication For Low-Power Mobile Devices,” in Proc. FC, Feb. 19–22, 2001, pp. 178–195.

[9] Preeti Garg and Dr. Vineet Sharma, “Secure Data Storage In Mobile Cloud Computing,” IJARIIE-ISSN ,Vol-2 Issue-2 ,2016.

[10] W. Itani, A. Kayssi, and A. Chehab, “Privacy As A Service: Privacy-Aware Data Storage And Processing In Cloud Computing Architectures,” in Proc. IEEE Int. Conf. Dependable Auton. Secure Comput., 2009, pp. 711–716.