Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.16 – 21

An Effective Authentication Scheme for Distributed Mobile Cloud Computing Services Using a Single Private Key

Mrs. Kavitha K K[1], Avinash B[2]

[1]Assistant professor, Department of Information Science, New Horizon College of Engineering, India

[2]Student, Department of Information Science, New Horizon College of Engineering, India

[1] kavithagowda09@gmail.com, [2] avinash.kb94@gmail.com

Abstract: Mobile cloud computing comprises of cloud computing, mobile computing and wireless network. Providing secure and convenience for the mobile users to access multiple cloud computing services is essential. This paper furnishes an effective way of providing the authentication for the mobile users to access multiple cloud computing services. The proposed scheme outfits a secure and expediency for mobile users to access several cloud computing services from multiple service providers using a single private key. Our proposed scheme is based on bilinear pairing cryptosystem. In addition, the scheme also supports mutual authentication, key exchange, user anonymity. To overcome the vulnerabilities of traditional methods, from system implementation point of view, the proposed scheme eliminates the usage of verification tables that are required to store the user credentials (user ID and password) which are the part of smart card generator service and cloud computing service provider.

Keywords—smart card generator (SCG), mutual authentication, ID based cryptosystem, bilinear pairing cryptosystem, identity provider (IdP).

I. INTRODUCTION

Due to abundant benefits and possibilities that are provided by Cloud computing there is a rapid growth of users in the recent years. As the report from Juniper Research estimates that the number of unique consumers accessing cloud-based services will exceed 3.6bn by 2018, rising from an estimated 2.4bn in 2013 [1]. This expeditious development has been revolutionized in number of areas. In early days of computing, huge scale machine and mainframe computers were used to implement various task and applications. Now a days, we are doing the same tasks, but in flexible, much cheaper, and are in portable manner, either by desktop computers or

mobile devices (such as, smart phones, tablets, etc.), with several type of services tied, so called Cloud Computing System (CCS). The user can use services and application on the cloud through internet.

However, In the recent years, there is a rapid growth in the mobile application due to increase in the popularity of smart phones. Mobile devices have started becoming abundant with application in various categories such as entertainment, health, games, business, social networking, travel and news [2]. The reason for this is that mobile computing is able to provide a tool to use the user when and where is needed, irrespective of user movements, hence supporting location independence. So the development mobile cloud computing become an important research in this mobile oriented world. The general purpose[3] of mobile cloud computing is, a public system is built need uses the cloud infrastructure, to contribute in improving mobile device performance efficiency.

In this paper, an effective authentication schema for the distributed mobile cloud computing is proposed. This schema uses a single private key for the authentication of multiple service providers [4]. Earlier, in one mobile user authentication only the target cloud service provider need to interact with the requestor(user). As the mobile user generally access different mobile cloud computing services, it is very tedious for user to register different user accounts on each service provider and to maintain them. The proposed schema is built upon bilinear pairing[5]. And therefore, requires less computation resources on both mobile devices and service provider. Through this, a user can get access to multiple service providers using a single private key, provided both mobile user and service provider should know the identities of each other.

II. RELATED WORK

Today, providing access to right user is the major concern. There should be a right mechanism that prevent the illegal access from unauthorized user. Authorization schema is the security mechanism for the network based services. Traditionally, authorization schema's user traditional public key cryptosystem such as RSA, which requires lengthy key size and utilizes the maximum of computational resources on the mobile devices. Since mobile devices be short of resources, traditional authentication schema are inappropriate to use. Therefore an efficient schema is required, which is beneficial for the mobile device.

In the recent years, many ID based cryptosystem [6] have been proposed. An ID based cryptosystem is the public key cryptosystem that resolve the issues with the traditional public key cryptosystem. In the proposed system, an ID based cryptosystem is based on bilinear pairing in an elliptic curve.

III. PROPOSED SYSTEM

In this paper, an user authentication schema is based on bilinear pairing for distributed mobile cloud computing. The proposed system supports mutual authentication, key exchange, and user untraceability.

The following are the benefits that are preserved by using this authentication scheme.

i. The key size provided by ECC is much smaller compared to the size provided by the traditional public key cryptosystem.

ii. Since the public key is used as a identity of the user, the computational cost to verify other public keys are eliminated and the storing space of other public key is not required.

iii. The user must access multiple service provider, it is important for the user to manage multiple keys provided by each service provider. This problem is resolved by sharing the same private key by all the service provider.

The trusted smart card generator (SCG) is used in the proposed system as the third party, that eliminates the use of identity provider (IdP), which is used by other system for the user authentication. There are three characters in the scheme: mobile user, mobile cloud service provider and trusted SCG service. In our

scheme, the user is assigned a smart card, which is being modified by some parameters during the user registration phase. The usage of this smart card makes the system make more protected by avoiding the user from distributing their login credentials. By this the scheme effectively prevents the situation of many logged in users with same login ID. Typically the registered user share his credentials so that other who know the login-ID and password can login successfully. In this scheme, the login request is created by the smart card using its stored secret component without any human intervention. It is extremely difficult to extract the secret component from the smart card, and thus the user cannot share it with others. Even if the legitimate user's password is shared with others, the other person cannot login to the system without the smart card. Once a valid user logs into the remote system, his smart card will be inside the terminal until the user logs out. If the user pulls out the card from the terminal after login the remote system, the login session will be immediately expired. Thus, the scheme can successfully prevent the scenario of many logged in users with the same login-ID.

The scheme consist of three phases: set up phase, registration phase, and authentication phase. In the rest of the paper, we give preliminaries of these three phases based on bilinear pairing cryptosystem [7].

Preliminaries

A. Bilinear pairing

Let G_1 the cyclic additive group generated by P, whose order is Q. G_2 be the multiplicative group of same order. A map $e : G_1 \times G_1 \rightarrow G_2$ is called bilinear mapping if it satisfies the following properties.

a. Bilinear: $e(aP, bQ)=e(P,Q)^{ab}$ for all $P,Q \in G_1$ and $a,b \in Zq^*$.

b. Non degenerate: there exist $P,Q \in G_1$ such that $e(P,Q) \neq 1$.

c. Computable: there exist an efficient algorithm to compute $e(P,Q)$ for all $P,Q \in G_1$.

In reality, G_1 is the group of points on an elliptic curve Zq^* and G_2 is the subgroup of multiplicative group of finite field $Z^*{}_q{}^k$ for some $k \in Z_q^*$.

B. Set up Phase

During set up phase, the smart card generator select the random number and computes its master private key (s). With this master private key it also generates public key and public parameters.

Suppose G_1 is an additive group and G_2 is the multiplicative group of order q and suppose P is the generator of G_1, then $e : G_1 \times G_1 \rightarrow G_2$ is called bilinear mapping, $H: \{0,1\}^* \rightarrow G_1$ is the cryptographic hash function. Selects a master private key s and computes public key as $Pub=sP$. Then publishes the public parameters (G_1, G_2, e, q, P, Pub, H) and keeps s secret.

C. Registration Phase

The registration phase is executed between the SCG and the mobile users. The mobile who wishes to join the network and utilize the service can join the network by sending the identities to the SCG. Even the SP's also requested to register with SCG in this phase. With the identities provided, the SCG generates the public key for each mobile user and SP, then dispatches it to corresponding user or SP securely.

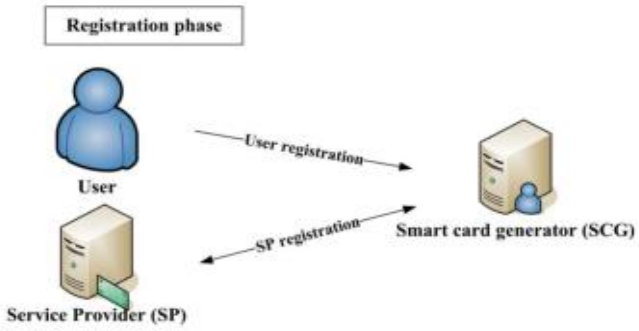

Fig 1. Registration Phase

This phase is executed by following steps when user wants to register.

i) Suppose a new user U_i wants to register with SCG.

ii) U_i submits the identity ID_i and password PW_i.

iii) On receiving the request, the SCG computes $Reg_{id} = s.H(ID_i) \mid H(PW_i)$.

iv) The SCG initializes the smart card with the parameter ID_i, Reg_{id}, $H(.)$ and send the smart card to the U_i over a secure channel.

D. Authentication Phase

This is executed when the user logs into the system. This phase is further divided into login phase and verification phase.

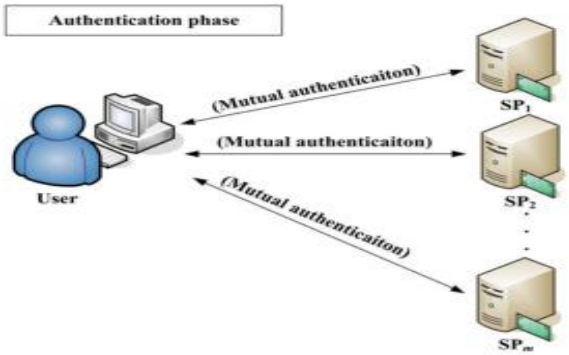

Fig 2. Authentication Phase

1) Login Phase

The user U_i insert the smart card in a terminal and enter ID_i and PW_i. The ID_i is identitical to one that is stored in smart card. If the credentials are same then sends the login request to the corresponding SP.

i) Computes $DID_i = T.Reg_{id}$, where T is the user system's timestamp.

ii) Computes $Vi = T.H(PW_i)$.

iii) Sends the login request (ID_i, $DIDi$,V_i,T) to the SP over a public channel.

2) Verification Phase

The SP receives the login message (ID_i, DID_i, V_i, T) at time $T^* (\geq T)$. Over receiving the login request the SP does the following operations.

i) Computes the time interval between T and T^*. If $(T^* - T) \leq \Delta T$ then SP proceeds to step ii. Otherwise rejects the login request. ΔT is the expected time interval between transmission delay.

ii) Checks whether $e(DID_i - V_i, P) = e(H(ID_i), Pub)$. If it is valid, the SP accept the request , else rejects it.

During this phase, the mobile user and service provider are able to authenticate without the intervention of SCG. And therefore reduces the time required by the trusted third party to verify the user. The session key is also generated during this phase to encrypt/decrypt the messages sent between user and service provider.

E. Password Change Phase

This phase is executed when the user wants to change the password. The proposed scheme allow this step to execute without the intervention of the SCG. The user insert the smart card into the terminal and keys ID_i and PW_i. If ID_i is matching with the value stored in smart card then allows the user to change or it terminates the operation. The phase works like this.

i) U_i enters the new password PW_i.

ii) The smart card calculates $Reg_{id}^* = Reg_{id} - H(PW_i) + H(PW_i^*) = s.H(ID_i) + H(PW_i^*)$.

iii) The password has been changed to the new password PW_i^* and the smart card restore the value of Reg_{id} with Reg_{id}^* value.

IV. RESILIENCE OF PROPOSED SYSTEM

A. Security

The proposed scheme can resist to the following attacks:

1) Replay Attack

Suppose an adversary tap the login request from the valid user, the SP receive the request at time T_{new}. The SP calculates the time interval $(T_{new} - T)$ and compares with expected time interval delay (ΔT) which exceed the value. And therefore the attack fails.

2) Forgery Attack

From the valid login message, an adversary can get only get ID_i, DID_i, V_i and T. from these values an adversary can't find any use full information. Though $DID_i = T. Reg_{id}$, this does not reveal any information needed since the Reg_{id} kept secret.

3) Insider Attack

In password based user request, the trusted third party maintains a separate table called verifier table for storing the user credentials. Since in our proposed scheme, the login request is based on user's password as well as the secret key *s*, and thus it eliminates the usage of verifier table.

V. CONCLUSION

The scheme prevents the adversary from forgery attacks by employing a dynamic login request in every login session. The use of smart card not only makes the scheme secure but also prevents the users from distribution of their login-IDs, which effectively prohibits the scenario of many logged in users with the same login-ID.

REFERENCES

[1] Steffen Sorrell, "Cloud Computing - Consumer Markets: Strategies & Forecasts 2015-2020", Juniper, Enabling Technologies, 04 November 2015.

[2] Ahmed Dheyaa Basha, Irfan Naufal Umar, Merza Abbas, "Mobile Applications as Cloud Computing:Implementation and Challenge", International Journal of Information and Electronics Engineering, Vol. 4, No. 1, January 2014.

[3] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu," Mobile cloud computing: A survey", Elsevier, 22 May 2012.

[4] Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication scheme for Distributed Mobile Cloud Computing Services", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 3, SEPTEMBER 2015.

[5] Al-Sakib Khan Pathan and Choong Seon Hong "Bilinear-Pairing-Based Remote User Authentication Schemes Using Smart Cards " ICUIMC'09, January 2009.

[6] T. H. Chen; H. l. Yeh; W. K. Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing" IEEE Conference Publications, 2011.

[7] Manik Lal Das, Ashutosh Saxena, Ved P. Gulati,Deepak B. Phatak, "A novel remote user authentication scheme using bilinear pairings" Elsevier, Computers & Security, 2006.

