International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

# Secure Authentication Scheme for Distributed Cloud Computing

**Brundha Elci J[1], Manisha K R[2], D M Pooja[3], Divya H D[4]**

*[1]Assistant professor, [234]UG Students*
*Department of CSE,*
*Vemana Institute of Technology, Bangalore-560034, India*

***Abstract*** *— **Recent usage of internet in mobile devices has adversely increasing. In the existing system , for one mobile user authentication session only the targeted cloud service provider needs to interact with the service requestor (user) and there is no support for user anonymity and user untraceability and it is vulnerable to time synchronization problem and forgery attack. The proposed system provides security and convenience for mobile users to access distributed mobile cloud computing services from multiple service providers using only a single private key that is generated by trusted third party smart card generator (SCG).The smart card generator act as the secure key distributor for distributed cloud service providers and mobile clients. The security strength of the proposed scheme is based on bilinear pairing in an elliptic curve cryptosystem (ECC).In addition, the system provides mutual authentication, key exchange, user anonymity, user untraceability. The secured authentication scheme provides both security and efficiency for distributed cloud computing services.***

***Keywords****—Authentication scheme, bilinear pairing, user anonymity and user untraceability*

## I. INTRODUCTION

Now-a-days the low power handled mobile devices make our life more comfortable that with the fast evolution of mobile communication technologies and internet, mobile users are accessing remote services at home over the internet. Cloud Computing is a construct used for the delivery of hosted services placed at different locations over the internet. It enables the various cloud computing companies to analyse and compute resources, such as a virtual machine (VMs) storage or an application, as a utilization of electricity rather than having to build and maintain computing infrastructures in house. The term Mobile Cloud Computing (MCC) can be defined as collection of cloud computing, mobile computing and various wireless networks used to carry out rich computational resources for mobile users, network operators, as well as cloud computing service providers. The ultimate goal of MCC is to provide rich mobile applications on an execution on mobile devices, with a rich user experience**.** 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) which is installed on mobile device. The Web browser or the cloud service application will then mutually authenticate both the cloud service provider and the client. After authentication phase, the user can access the resources and response services back from the cloud service provider. Authentication scheme is a fundamental and important concept used in network security, because it is usually used to protect sensitive and secure information or restrict the access of precious resources for legal privileged users only. In general, authentication scheme can be achieved using two main purposes. An authentication scheme must provide mutual authentication between user and service provider. That is, not only a legal user is able to authenticate the remote server, but also the server can also authenticate the user. After authenticating both between user and server side, a session key is generated by the agent to encrypt/decrypt all communicating messages between the user and the server. That is, all messages forwarded after authentication process has to be read only by the bonafied user and the server.

In order to prevent illegal access, cloud providers should ensure a secure authentication for users using mobile devices. However, there are concerns to be resolved along with the authentication scheme. Firstly, computing efficiency of the scheme should be seriously considered, since there exists less computing capability of mobile devices over laptop computers. Secondly, sufficient security strength should be supported since all messages are to be transmitted via an insecure WLAN or telecommunication networks, in which an adversary can be easily obtained to interrupt, or modify transmitting messages before they reach the desired recipient. In addition, security on user accounts is a rising issue as identity deception and identity tracing have become common attacks in wireless mobile environments.

It is undergoing various threats such as forgery attack and deny of service attack. So therefore system should support user anonymity and user untraceability to overcome this entire problem.

## II. LITERATURE SURVEY

The author [1] says Cloud Computing makes data truly mobile and a user can simply access a chosen cloud with any internet accessible device. Using ECC dynamic Id based remote mutual authentication scheme for remote devices which solves insider attack and impersonation attack. Yang and Chang's authentication mechanism consists of three phases namely: initialization, user registration and mutual authentication with session key authentication phase. It is described as follows

**1. Initialization**: During this phase user register his/her identity with authentication servers. The following steps are taking place which is explained below.

- *When the user register's his/her identities with authentication servers.*
- *The server uses elliptic curve algorithm to perform encryption and decryption.*
- *It computes public/private key pair but publishes message as private key for security purposes*.

**2. User registration phase:** Interaction between user and authentication server.

- *Firstly User chooses his/her id and password, submits to the authentication server.*
- *Authentication server generates a authentication key and stores on a smart card then sends the smart card to user over a secure channel.*
- *User verifies this smart card using the same id and password which he/she used for registration. If it is correct user accept this smart card otherwise rejects the smart card.*

**3. Mutual authentication with key agreement** When user wants services from remote server the following steps are taking place .They are

- *User uses id and password to login to obtain the services from remote servers. Remote servers checks for authentication key and then provides services to users.*
- *The author provides ID-based authentication with higher security for cloud computing but also drawback from paper is, it undergoes various threats. and vulnerable to offline password guessing attack and forgery attack.*

Author [2] proposed, the user anonymity, user untraceability and also to defend against major security threats for the service is deployed and the system is proposed to overcome the issue of this is explained. This paper first presents a security mode for anonymous authentication and then proposes a new anonymous authentication scheme using smart card. By using smart card we can support user anonymity.

DETAILS OF EACH PHASE ARE DESCRIBED AS FOLLOWS.

**1. Parameter Generation phase**: During this phase server generate the parameters which are required for encryption/decryption using elliptic curve algorithm. First it generates private key and then computes as its public key, where it is the length of the private key. Next, publishes as its public parameters.

**2. Registration phase**: During this phase, assume that smart card has been configured with public parameters stored in its memory before the card is given to a user. . When the user wants to register on must insert his/her smartcard into the card reader and give his/her fingerprint information to the smart card for successful registration, where a built-in fingerprint scan component is assumed to be embedded in the card reader. Registration phase take place in the following four scheme.

- *Firstly User registers with his/her identity, inputs his/her chosen password and fingerprint.*
- *After that, sends via a secure channel. Authentication server upon receiving, computes the identities and then sends back via a secure channel. When user receives, stores into the smart card.*

**3**. **Pre-Computation Phase:** The smart card generates random number and stores into its memory. This phase take place after generation of session key which is established between the user and server because the smart card will reselect the random number and compute after this.

**4**. **Login phase**: User can login using his /her password and fingerprint to access the server.
It takes place in the following steps:

- *Users have to insert his /her smart card into card reader and then input his identity, password and fingerprint.*
- *Upon receiving the user identity server computers, verifies whether registration is valid and then provides services.*


 

Even though it has various advantages such as fingerprint recognition but the authentication protocol off-line. al. does not provide user anonymity and untraceability this is major disadvantage of this paper. Author[3] proposes a novel ECC-based authentication protocol for portable communication systems. The proposed protocol resists Denial of Service attacks and requires less computation cost when authenticating a communication session.

1. **Setup phase**: First of all, HLR(Home Location Register) chooses two private keys x and xv, and then computes their corresponding public keys respectively. Next, HLR shares public key with VLR(Visited Location Register).

2. **Online authentication phase**: For each online authentication session, MS(Mobile Station) precomputes one-way hash function and stores them in its database.

- *MS sends a login request to VLR and further sends randomly generated key to MS.*
- *MS retrieves hash value from its SIM card, and then computes it.*
- *Further, MS sends to VLR. VLR first uses private key to retrieve data from the service provider.*
- *VLR computes and then verifies whether the two computed values are the same. If the verification establishes, it computes. Otherwise, VLR denies the login request.*

3. **Offline authentication phase**: MS retrieves hash functions from its database and sends to VLR. Upon receiving, VLR decrypts the encrypted message and computes the one-way hash function. Next, VLR verifies whether the computed value is the same as the stored value in its database. If the condition holds, VLR Replaces retrieved value, and computes the session key. In this paper, cloud providers should support a secure authentication scheme for users using mobile devices in order to prevent illegal access.

## III. EXISTING SYSTEM

In Existing System, there is no support for user anonymity and user untraceability and it is vulnerable to time synchronization problem and forgery attack. In one mobile user authentication session, only the targeted cloud service provider needs to interact with the service requestor (user).Since most authentication schemes based on ECC or bilinear pairing are designed for client server distribution .They are not suitable to be directly adopted into distributed services environment.

## IV. PROPOSED SYSTEM

Using single session key provided by smart card generator reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party(SCG) .The proposed scheme provides user anonymity and user untraceability to preserve user privacy. It overcomes time synchronization problem and can be easily implemented in distributed mobile cloud computing environment.

.

## V SYSTEM DESIGN

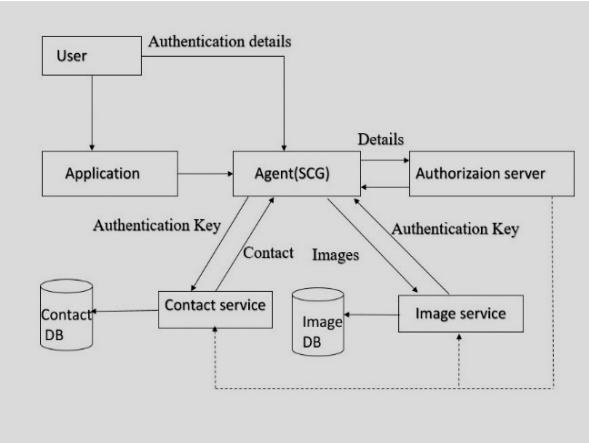


*Fig.1Framework of user authentication with multiple service providers*

The above Fig 1 shows various process taking place between users and multiple service providers to obtain single private key generated by smart card generator using this user can access multiple service providers. It provides both security and allows user s to access disturbed cloud computing.

## VI. CONCLUSION

In our approach user make uses of single private key which is generated by smart card generator(SCG) to access multiple service providers and the smart card generator is used only during registration phase not in authentication phase due to this it reduces the processing time required for computational and communication between user and service providers. The proposed system supports new user anonymous authentication scheme for distributed mobile cloud services environment. For authentication , bilinear pairing in an Elliptic curve(ECC) has been used in developing an ID-based cryptosystem which 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 therefore user 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 it can be easily implemented in distributed mobile cloud computing environment. It overcomes many problems such as time synchronization, key management issue, forgery attack.

Therefore, using of mutual authentication and single private key in distributed cloud computing allows user to access multiple service providers which is secured and easy to access instead of registering for each service providers. The secured authentication scheme provides both security and efficiency for distributed mobile cloud computing services.

## REFERENCES

[1] T. H. Chen, H. L. Yeh, and W. K. Shih, "An advanced ECC dynamic ID-based remote mutual authentication scheme for cloud computing," in Proc.5th FTRA Int. Confe. Multimedia Ubiquitous Eng., 2011, pp. 155–159.
[2] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel anonymous authentication scheme using smart cards," IEEE Trans. Ind. Informat., vol. 9, no. 4,pp. 2004–2013, Nov. 2013.
[3] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure delegation-based authentication protocol for wireless roaming service," IEEE Commun. Lett., vol. 16,


 