SECURE AUTHENTICATION SCHEME FOR MOBILE CLOUD SERVICES

AN ABSTRACT

Submitted by

MUNIVEL E

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

ANNA UNIVERSITY

CHENNAI 600 025

AUGUST 2020

ABSTRACT

Password attack is one of the severe threats to mobile users. As per the recent Lookout report, password attack in mobile device is increasing 85% year to year and going to become a significant threat to the mobile users. Phishing like social engineering attack attempts to get the users' password by disguising as trusted service provider. Most of the mobile users are using the Internet services outside of the traditional firewall. Cloud-based services are one of the primary targets of this attack in the mobile cloud computing. Also, most of the mobile users are using the cloud storage in their device.

To secure against this password attack in the mobile cloud environments, proposed new authentication scheme to design without sharing the password in any form of the existing methods like Hash value, Encrypted key or a digital signature to verify the identity of mobile user and the cloud service provider during the authentication process. In this scheme, proposed to use zero-knowledge proof technique to satisfy the authentication process.

Moreover, to allows to change the mobile device and to change the any parameter of identity at any time, proposed an enhanced authentication protocol in the mobile cloud computing using multi identity with the option to change the device due to any other factors at any time securely. The second scheme is proposed to design a portable authentication scheme with multi-identity to secure the user password from the password attack and to provide the identity and key change at any time. This authentication scheme is not sending the password in any form of the methods like Hash value, Encrypted key or a digital signature to verify the identity of mobile user to and the cloud service provider. In this scheme, the enhanced zero-knowledge proof technique used to satisfy the authentication process.

To use the mobile cloud technique efficiently, proposed to design a secure authentication framework for computational offloading service in the mobile cloud environments. The new framework is offloading the resource intensive tasks into the cloud server to achieve energy efficiency and to improve the end device performance with security.

Also, to deal with the challenges of using the service specific applications like cloud infrastructure based virtual learning services in the mobile device, proposed secure virtual training environment service with the enhanced password security. This proposed framework in the cloud service is delivering the group of virtual machines to the cloud user.

The proposed authentication schemes and the application frameworks will provide security to the mobile cloud authentication, as well as achieve mutual authentication between the authentication entities. The effectiveness of the proposed schemes would be verified using the protocol verification tool called Scyther. This verification tools is developed by the University of Oxford and it is having the unique features like supports of unbounded, parallel execution and also auto terminate the code once verified. At last, the proposed schemes are compared with the recent similar schemes and prove that the schemes are resistance against major password attacks. Also, proves that the proposed authentication schemes are cost efficient and robust.