Designing Authentication Protocol for Micro data Center Architecture in Cloud

Vijender Kumar
M.Tech student, UIET, Kurukshetra University, 136119, Kurukshetra, Haryana, India

Naresh Kumar
Assistant professor, UIET Kurukshetra University, 136119, Kurukshetra, Haryana, India

Abstract – Mobile cloud computing is composed of two things: Mobile Computing and Cloud Computing which provides space to the mobile user to offload heavy task on the cloud which can help performing mobile device operations in the cloud. By using MCC mobile user loses its physical control. So it needs security, there is already a lot of security concern but no protocol has been found for the micro data centre architecture. Micro data centre is resource rich which is connected to the internet and easily available for nearby devices.

In this paper, we propose a authentication protocol for a micro data centre architecture, our protocol protects the data from any unauthorized user and secure it.

Index Terms – mobile cloud computing, micro data center.

1. INTRODUCTION

Accessing information at any time and any place, [1] mobile computing has made it easy. Mobile cloud computing has been defined in the Open Gardens blog on 5 March 2010 record [2] as "the availability of cloud computing services in a mobile environment. In recent years, applications developed for mobile devices have become plentiful including applications of various types such as fitness, news, amusement, Commercial, Social networking Cloud computing allows devices to avoid these constraints by letting more resource intensive tasks be performed on systems without these constraints and having the results sent to the device. Thus, cloud computing for mobile devices is a highly appealing and potentially lucrative trend. [3].

2. RELATED WORK

L. Lamport [7] proposed one of the most famous authentication schemes for remote users. The proposed scheme is secure even if the intruder has access to the system data or if the intruder alters the data communicated to the user and the system. However, in the given scheme, the server maintains the list of the hashed value of user's passwords hence; the system could be partially or completely compromised if the password table is stolen by the adversary

M.Asif and A. Ghafoor [11] It offloads all complex and computation-intensive operations, involved in the creation of digital certificate to the proxy server (PS). S.Dey et al. The proposed protocol utilize only existing hardware and platforms to avoid the possible attacks between a mobile device and the cloud during the authentication process. This property makes it possible to apply the given scheme to any of the mobile devices without making any charges.

S. Sharma *et al*. [12] SSL and digital certificate provides to enable external security. "antivirus". all networking activates are susceptible to one or other type of malicious attacks. As there is more use of websites that are sometimes accessing malicious code sites. Fair information practice principles(FIPP) which require rigorous control and procedures to protect the privacy of individual person data as well as organizations information. Encryption is the best way to maintain integrity and confidentiality of information

S.yang *et al*. [13] Focus on the problem of how to transfer some modules of a mobile application to the server so as to minimize the total execution time of the entire mobile application. Then, formulated the offloading problematic as a combinatorial optimization problem. put forward two algorithms to tackle the offloading problematic for a simple application chain and also for a general application.

The put forward algorithm was implemented and examined on the R-OSGi-based framework.

3. PORPOSED MODELLING

M.Felemabn et al. proposed a micro data centre architecture which is placed edge of the internet because of well connected to the internet. mobile user uses it for computational work because of the mobile user not able to process this programs due to lack of memory and ram problem[15]. micro data centre lies between cloud and mobile user so security is important in this case and a lot of attacks occurs:

i. MITM attacks: Intruder lies between the mobile user and the micro data centre. Intruder easily intercepts the messages because messages are not encrypted

ii. Non-repudiation attacks: owner can't deny what owner said. There is no way taking it back

iii. Phishing attacks: Intruder can act as an authorized user and can gain access to the cloud resources and services.

iv. Credential security: data user credentials such as user id and password or email id are store in the micro data centre and malicious user gain access data owner credential are to be at risk.

v. Password security: password is sent to the micro data centre which is not secure.

4. CONCLUSION

In this paper, we discuss the lot of work about mobile cloud computing which offloads the heavy task on the cloud and performs computational work and gives the results to the mobile user. But it used to cost more time and money and battery usage. Hence, the micro data centre is vital to deal with this problem. mDC presents all the time of the corner of the internet for a good connectivity and mobile user use mDC for direct communication while use cloud. and mDC work for mobile user as cloud and help to overcome the problem of computation time cost and battery.

REFERENCES

[1] Guan L, Ke X, Song M, et al. A survey of research on mobile cloud computing. *Proc - 2011 10th IEEE/ACIS Int Conf Comput Inf Sci ICIS 2011* 2011; 387–392.

[2] Mobile cloud applicationshttps://www.abiresearch.com/market-research/product/1004607-enterprise-mobile-cloud-computing/ (accessed 15 December 2017).

[3] Abolfazli S, Sanaei Z, Ahmed E, et al. Cloud-based augmentation for mobile devices: Motivation, taxonomies, and open challenges. *IEEE Commun Surv Tutorials* 2014; 16: 337–368.

[4] Qi H, Gani A. Research on Mobile Cloud Computing : Review, Trend and Perspectives. 2014; 195–202.

[5] Kovachev D, Klamma R. Beyond the client-server architectures: A survey of mobile cloud techniques. *2012 1st IEEE Int Conf Commun China Work ICCC 2012* 2012; 20–25.

[6] Gao J, Gruhn V, He J, et al. Mobile Cloud Computing Research - Issues, Challenges and Needs. *2013 IEEE Seventh Int Symp Serv Syst Eng* 2013; 442–453.

[7] Lamport L. Password authentication with insecure communication. *Commun ACM* 1981; 24: 770–772.

[8] Lee S, Ong I, Lim H, et al. Two Factor Authentication for Cloud Computing. *J Inf Commun Converg Eng* 2010; 8: 427–432.

[9] Chow R, Jakobsson M, Masuoka R, et al. Authentication in the Clouds : A Framework and its Application to Mobile Users. *ACM Work Cloud Comput Secur* 2010; 1–6.

[10] Yoo K-Y. A lightweight multi-user authentication scheme based on cellular automata in cloud environment. *2012 IEEE 1st Int Conf Cloud Netw* 2012; 1: 176–178.

[11] Asif M, Ghafoor A. Generic Lightweight Certificate Management Protocol (GLCMP). *2012 15th Int Multitopic Conf INMIC 2012* 2012; 489–495.

[12] Sharma PS. Mobile Cloud Computing : Its Challenges and Solutions. 2015; 4: 287–293.

[13] Yang S, Bei X, Zhang Y, et al. Application offloading based on R-OSGi in mobile cloud computing. *Proc - 2016 4th IEEE Int Conf Mob Cloud Comput Serv Eng MobileCloud 2016* 2016; 46–52.

[14] Allam H, Ahmad J, Nassiri N, et al. A Critical Overview of Latest Challenges and Solutions of Mobile Cloud Computing. *2017 Second Int Conf Fog Mob Edge Comput* 2017; 225–229.

[15] Felemban M, Basalamah S, Ghafoor A. A distributed cloud architecture for mobile multimedia services. *IEEE Netw* 2013; 27: 20–27.