IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 5 Issue 6, June 2018
ISSN (Online) 2348 – 7968
www.ijiset.com

# Privacy Aware Authentication Scheme for Mobile Cloud Computing in an Efficient Manner

**Akshat Mehta [1], Latha A[2], Mulayam Singh Yadav[3], Pratik Kumar[4]**

[2]Assistant Professor, Department of Computer Science and Engineering, Sapthagiri College of Engineering,

[1, 3, 4]UG Students, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Bangalore.

*Abstract*— With the rapid growth in mobile applications and cloud computing technology, mobile cloud computing has been introduced to be an important technology for mobile services. Mobile devices such as smartphone, tablet, PC, laptop etc. are increasingly becoming an essential part of life. As it is the most effective and convenient communication tools. To use the cloud services, the communications between mobile devices and clouds are held through wireless medium. Day to day usage of mobile cloud computing attracted attackers to break the data security in the cloud. Thus, some new classes of security and privacy challenges are introduced. This paper reveals the overview and study to provide the privacy aware authentication (PAA) to the mobile cloud computing.

## INTRODUCTION

Mobile cloud computing (MCC) refers to the framework where both the storing of data and processing of data happens outside of the mobile device. Mobile cloud applications moves the computing power and storing of data away from the mobile devices and put it into a very powerful and centralized computing platforms located in clouds, which are then retrieve from the wireless connection network.

To protect the data on the cloud from any attack at user's end as well as in mobile device, it is very important to protect the data from the threats of device. For example: data theft via hacker, virus and malware attacks. Wireless devices and the misuse of access rights from information security point of view in the cloud. Some common information security issues of cloud computing are System security of server and database, Networking security, User authentication, Data protection, System and Storage protection. The best way to protect the data in the cloud is to have a mixture of encryption, data loss prevention techniques, integrity protection, authentication, and authorization techniques.

With the increase of MCC service's types, the distributed MCC is also employed in many practical applications, where many other kinds of Cloud Service Providers are able to provide different types of services to users. All the messages are broadcasted by using the wireless technology in Mobile Cloud Computing services environment. The attacker could control the communication channel easily, i.e. he/she may be able to delay, intercept, and modify the transmitted data. More techniques were used previously to provide security to the data stored in cloud like secure socket layer encryption, intrusion detection system, multi tenancy based access control etc. In our paper, privacy-aware authentication (PAA) scheme is proposed. PAA scheme is very crucial for addressing security related problems which were present in MCC services environment because PAA scheme is able to identify the participant's identities and protect their privacy. In past several years, many PAA scheme have been proposed. However, most of them are not appropriate to be used by MCC services because they suffers from very serious security problems or have disappointing performance. Therefore, it is very important and necessary to design a new PAA schemes to ensure the security issues and to preserve privacy of users in MCC services.

## I. LITERATURE SURVEY

Rapid growth in wireless communication technologies have cover the way for a wide range of mobile devices to become increasingly universal and popular. Mobile devices allow the person anytime, anywhere access to the Internet. The fast growth and advance of several types of mobile services that are used by various users has made the traditional single-server architecture of its functional requirements inefficient. There is a need to deploy multi-server architectures to make ensure the availability of various mobile devices. The anonymous mobile user authentication (AMUA) protocol without online registration using the self-certified public key cryptography (SCPKC) for multi-server architectures to ensure the security of various mobile service applications was proposed in the past. However, the past AMUA solutions are the most that suffer from malicious attacks or have unacceptable computation and communication costs. We propose a new AMUA protocol that uses the SCPKC for multi-server architectures to address these drawbacks. In differ to the existing AMUA protocol, the cost offer by our proposed AMUA protocol is lower computation and communication costs.

Cloud computing is an evolving paradigm with tremendous momentum, but its unique aspects exacerbate security and privacy challenges. This article traverses the obstruction and solutions to providing a trustworthy cloud computing environment.

Cloud computing provide the convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly supplied and released with least management effort or service provider interaction. This cloud is still in evolving paradigm and this model promotes availability and is made of five essential characteristics that are on demand self-service, broad network access, resource pooling, rapid elasticity, and measured three service models, and four deployment models.

## II. EXISTING SYSTEM

Existing System provides security to the cloud computing services from the unauthorized users. Earlier, for mobile cloud computing services Tsai and Lo's scheme exists. The communication path uses mutual authentication to communicate with each other within the system, for example communication between the cloud services provider and the users. In existing system, a private key is generated by using bilinear pairing with hashing technique. But the disadvantage is that it consumes more time in securing the communication. In the new computing technology, ensuring security and providing privacy to the services is difficult because of the unreserved wireless communications. The existing system does not able to secure the services from service provider impersonate attacks which means the attacker can fetched the user's real identity during the execution.

## III. PROPOSED SYSTEM

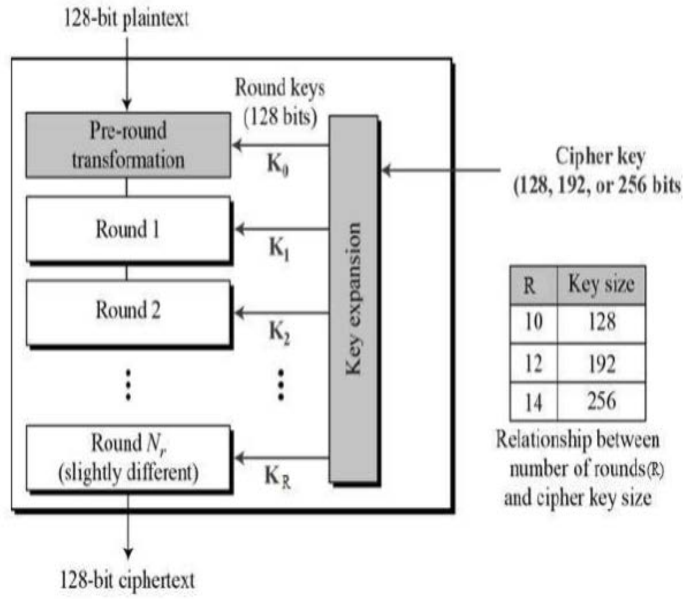
In our paper, the proposed scheme depends on identify based signatures strategy. This scheme is used to improve the performance of the proposed system. Our proposed scheme is able to solve the security issues related to the Tsai and Lo's scheme. From the performance analysis point of view, performance of our proposed scheme is better as compared to the previous schemes. We noticed that the previous scheme is insecure against the service provider impersonate attacks. The major contributions of our paper is summarized as follows:

1] We analyse the previous scheme and shows that their scheme is insecure against the service provider impersonate attacks.

2] Our proposed scheme defeats the weakness exists in previous scheme.

3] Finally, our proposed scheme provides more security and privacy to the mobile cloud computing services and also has a better performance than the previous schemes.

We are using AES algorithm for encrypting and decrypting the data. Nowadays the AES algorithm is more popular and it is globally accepted. Rather than bits, AES performs all its computations on bytes. AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.



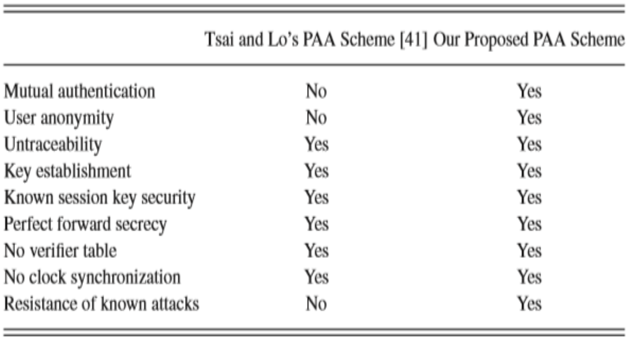
| R | Key size |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |

Fig 3.1- AES Algorithm

## IV. RESULT

In this paper, we have seen that our PAA scheme is better and efficient than previously existing schemes. In our proposed PAA scheme, as you can see, it is more secure against the attacks and it is more efficient as we don't have to register to the cloud again and again. Only one time we have to register in the registration phase and then we can use the services of the cloud.

TABLE I
SECURITY COMPARISONS OF TWO PAA SCHEMES



| | Tsai and Lo's PAA Scheme [41] | Our Proposed PAA Scheme |
|---|---|---|
| Mutual authentication | No | Yes |
| User anonymity | No | Yes |
| Untraceability | Yes | Yes |
| Key establishment | Yes | Yes |
| Known session key security | Yes | Yes |
| Perfect forward secrecy | Yes | Yes |
| No verifier table | Yes | Yes |
| No clock synchronization | Yes | Yes |
| Resistance of known attacks | No | Yes |

## V. CONCLUSIONS

Privacy Aware Authentication schemes are not suitable for various services that are present in the cloud environment. To solve the security and privacy problem in MCC environment, Tsai and Lo proposed an efficient PAA scheme for the MCC services. Security and privacy analysis shows that our proposed PAA scheme can solve the security problem that were existing in Tsai and Lo's PAA scheme. Analysis shows that our proposed PAA scheme has better performance than previously existing PAA scheme.

## REFERENCES

[1] M. Satyanarayanan, "Fundamental challenges in mobile computing," in Proc. 15th Annu. ACM Symp. Princ. Distrib. Comput., 1996, pp. 1–7.

[2] A. Lin and N.-C. Chen, "Cloud computing as an innovation: Percepetion, attitude, and adoption," Int. J. Inf. Manag., vol. 32, no. 6, pp. 533–540, 2012.

[3] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340–352, Feb. 2016.

[4] M.Armbrustetal.,"Aviewofcloudcomputing,"Commun.ACM,vol.53, no. 4, pp. 50–58, 2010.

[5] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[6] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[7] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.

[8] E.-J. Yoon, K.-Y. Yoo, C. Kim, Y.-S. Hong, M. Jo, and H.-H. Chen, "A secure and efficient sip authentication scheme for converged VOIP networks," Comput. Commun., vol. 33, no. 14, pp. 1674–1681, 2010.