iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5028

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Privacy Aware Authentication Scheme for Cloud Computing Services

Sheethal.K[1], Madhushree SK[2], Sowmya. P [3], Gadug Sudhamsu[4]
[1, 2, 3]*Students,* [4]*Guide, Department of Computer science and Engineering Jain University, Bangaluru*

Abstract: In the proposed technique, the main idea is to provide the Privacy Aware Authentication (PAA) to the mobile cloud computing. For security PAA, Identity-based signature scheme is required. To improve the security level, we proposed a password-based authentication scheme and followed the encryption and decryption process which includes Attribute Based Encryption Scheme (ABE). It uses the private key only to access the file, after getting access for the file, user can download the particular file and it can be saved in the local system.

I. INTRODUCTION

Development of cloud computing is considered as one of the powerful network technologies. Cloud computing has the ability to provide cheap service to users in pay-as-you-go mode through resource visualization technology. Cloud service providers such as Baidu and google can provide cloud storage services. Mobile Cloud Computing is the new digital ecosystem that has emerged recently, where cloud computing platforms is integrated in mobile computing. Practical applications are being employed in mobile cloud computing service types and the distributed mobile cloud computing where different types of cloud services to users are being provided by many kinds of cloud service providers. In Mobile Cloud Computing service environment, the privacy Aware Authentication (PAA) scheme is very crucial for address security problem as it has the ability to identify the participants identity and in protecting their privacy. In past several years many Privacy Aware Authentication schemes have been proposed. However, due to serious security problem or unsatisfactory performances, most of them are not suitable for Mobile Cloud Computing Services. Therefore, as to ensure security and preserve the privacy in Mobile Cloud Computing environment it is necessary to design new Privacy Aware Authentication schemes. A large scale distributed network system like Mobile Cloud Computing is based on a number of servers in data centers. Based on the layer concept the models of cloud services can be categorized. As in the upper layers of this paradigm, they are stacked as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Due to the limitation of mobile device, the typical mobile cloud computing service can be functionally grouped into two categories:

A. Storage Service
B. Computing Service

Storage service aims to solve the problem of storage limitations on mobile devices. The applications need large data transmission between mobile client and server. Network availability, respond time, and these are the main concerns of this type of service. Mobile commerce, mobile healthcare, mobile learning, and mobile multimedia are typical applications belonging to this kind of service. Mobile commerce usually requires low network cost, but high availability and response time. The computing services transfer the heavy computing task from mobile device to the cloud and achieve the results. The applications offload the task and data to cloud, which is a suitable solution to address the issues of computational power and battery lifetime. Mobile designing, mobile online gaming, and mobile multimedia are common applications which require large processing resources. Some of them also need high quality of service for short response time and high throughout a mobile device. It is more robust for a service adaptor to have multiple choices than the centralized architecture.

III. RELATED WORK

According to the referred IEEE papers the works in the field of Mobile Computing Services based on authentication scheme.

1) A wide range of mobile devices has become increasingly ubiquitous and popular with rapid advances in wireless communication technologies. But the the main aspect to ensure the availability of various mobile services, there is a need to deploy multi-server architectures.
2) The aim in this paper is to solve the problem of Multi-Keyword Ranked Search Over Encrypted (MRSE) cloud data at the time of protecting exact method wise privacy in the cloud computing concept. But the disadvantage is that for obsoletes data utilization the sensitive data should be encrypted before outsourcing for privacy requirements.

3) In this context of authors view it is based on the illegal accessing must be restricted and the information from theft during transmission over the insecure internet must be prevented. As the disadvantage is that through the security analysis, we show that our scheme is secure against possible known attacks.

4) The work being carried out by authors on a secure biometrics-based multi-server authentication protocol using smartcards. With low communication cost, computational cost, and Provides high security along. As scheme is suitable for battery-limited mobile devices. Disadvantage was in some design flaws, such as wrong password, login and its consequences, and wrong password update during password change phase.

IV. METHODOLOGY

An identity-based signature scheme is being used in the proposed system of the Privacy Aware Authentication scheme for Mobile Cloud Computing. This scheme is used to improve the performance level. An efficient Privacy Aware Authentication for mobile cloud computing services uses bilinear pairing for better performance. First authentication scheme was proposed by Lamport for the single server environment in order to achieve Mutual Authentication (MA) in open networks. Several Password based authentication schemes are proposed to improve the security level.

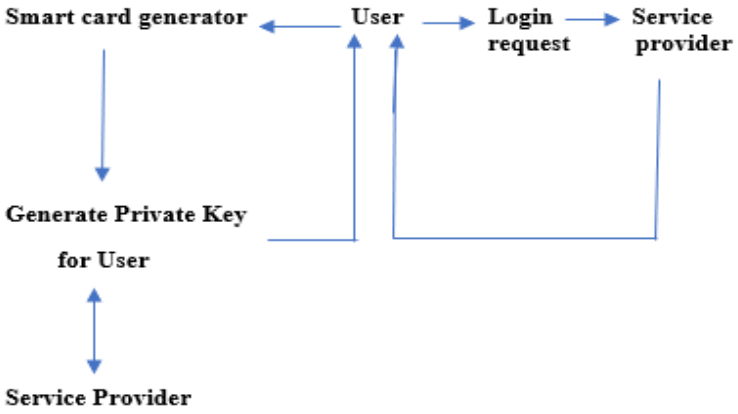


Figure.1 Flow Diagram for Proposed System.

A. User

After the registration process, the user can login into this system using the id and password. User can upload the files into the cloud and they can also view the files from the cloud using signature and keys. In the uploading phase user can select which file to be uploaded and then get the signature key using that key. The file will be encrypted and stored in the cloud. In viewing phase, user has to first select the file from the uploaded files and then they can send access permission to Cloud Service Provider for getting the key from the Cloud Service Provider and then give the private key after that the user can view the file.

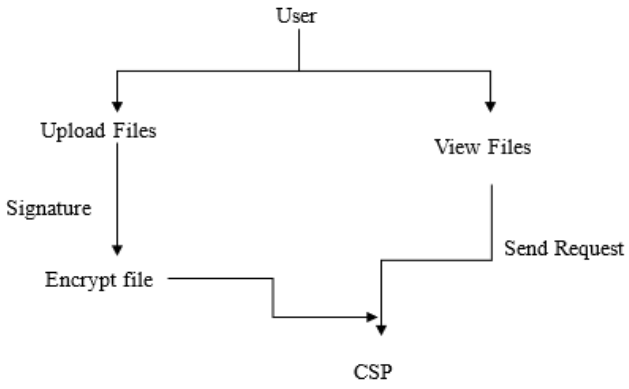


Figure.2 User Interaction.

B. Smart Card Generator

Smart Card Generator (SCG) work is to provide the private key to the users. In this process Smart Card Generator can get the signature from the user at the time of registration. After getting the signature, they generate a key using that signature. The Private Key is mainly to increase our security level.

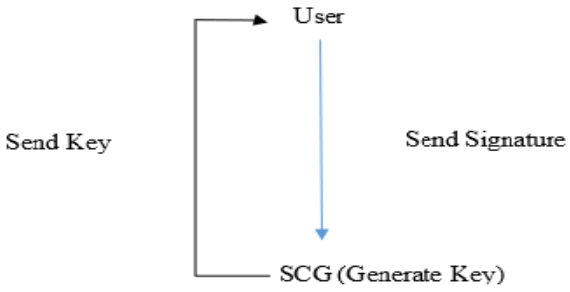


Figure.3 Smart Card Generator

C. Cloud Service Providers

In Cloud Service Provider (CSP) the user uploads their files using their signature, then they encrypt and store the files respectively. In this process, Cloud Service Provider will get the request from the user to access the file. For that request, they send the file signature key to the users for accessing the file.

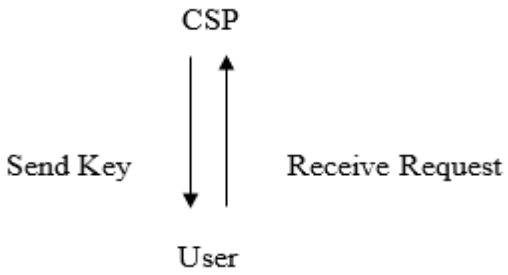


Figure 4. Cloud Service Provider Interaction.

V. ANALYSIS

The new Privacy Aware Authentication scheme for Mobile Cloud Computing services shows that the security analysis of our proposed Privacy Aware Authentication scheme can solve the security problem existing in Tsai and Lo's scheme. Besides, the performance analysis shows that our proposed Privacy Aware Authentication scheme has better performance criteria.

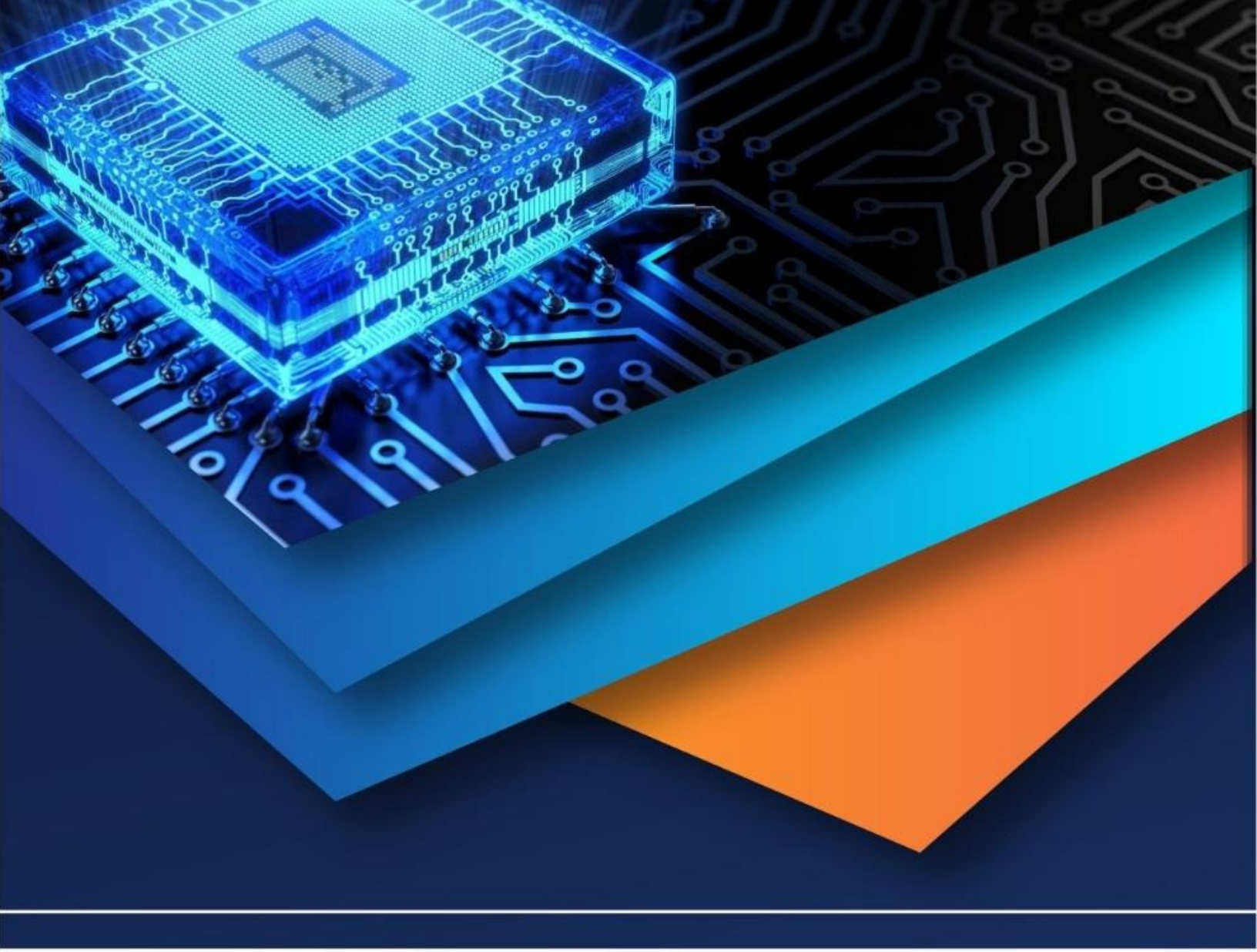
VI. CONCLUSION

In Mobile Cloud Computing environment due to the dynamic nature of mobile devises, traditional authentication schemes are not suitable for various other services. Tsai and Lo's proposed an efficient Privacy Aware Authentication scheme for the Mobile Cloud Computing services by using bilinear pairing to solve the security problem in Mobile Cloud Computing services. On analysis proposed Privacy Aware Authentication performs better than Tsai and Lo's Privacy Aware Authentication schemes.

REFERENCES

[1] He, S. Feudally, N. Kumar, and W. Wei, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptographyformulti-serverarchitectures," IEEETrans.Inf. Forens.Security, vol. 11, no. 9, pp. 2052–2064, Sep. 2016.
[2] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Dystric. Syst., vol. 27, no. 2, pp. 340–352, Feb. 2016.
[3] A. K. Das, "A secure and robust password-based remote user authentications Scheme using smartcards for the integrated EPR information system," J. Med. Syst., vol. 39, no. 3, pp. 1–14, 2015.

[4] V. Odell, A.K. Das, andA.Goswami, "Asecurebiometrics-basedmultiserverauthenticationprotocolusingsmartcards," IEEETrans.Inf. Forens. Security, vol. 10, no. 9, pp. 1953–1966, Sep. 2015
[5] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.
[6] L. Lamppost, "Password authentication with insecure communication," Common. ACM, vol. 24, no. 11, pp. 770–772, 1981.
[7] E.-J. Yoon, K.-Y. You, C. Kim, Y.-S. Hong, M. Jo, and H.-H. Chen, "A secure and efficient sip authentication scheme for converged VOIP networks," Compute. Common., vol. 33, no. 14, pp. 1674–1681, 2010.
[8] R. Arshad and N. Ikram, "Elliptic curve cryptography based mutual au-thematization scheme for session initiation protocol," Multimedia Tools Appl., vol. 66, no. 2, pp. 165–178, 2013
[9] S. H. Islam and G. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," Math. Compute. Modelling, vol. 57, no. 11, pp. 2703–2717, 2013.
[10] P. Guo, J. Wang, X. Gang, S. K. Chang, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," J. Internet Technol., vol. 15, no. 6, pp. 929–935, 2014
[11] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," J. Internet Technol., vol. 16, no. 1, pp. 171–178, 2015. [14] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using
[12] P. Guo, J. Wang, X. Gang, S. K. Chang, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," J. Internet Technol., vol. 15, no. 6, pp. 929–935, 2014
[13] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," J. Internet Technol., vol. 16, no. 1, pp. 171–178, 2015. [14] M.-S. Hwang and L.-H. Li.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY