Privacy Aware Authentication Scheme for Distributed Mobile Cloud Computing

Mrs. Chaitali P. Kathar, Prof. Vidya Dhamdhere
Dept: Computer Engineering, Pune University, G.H.R.C.E.M, Wagholi, Pune, Maharashtra, India.
Email: chaitalikathar@gmail.com

Abstract— ***As mobile users generally access different types of mobile cloud computing services from a variety of service providers, it is extremely tedious for users to register different user accounts on each service provider and maintain corresponding private keys or passwords for authentication usage. In this paper, I propose a encryption method call Attribute encryption method. Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of required resources, but the data is outsourced or stored to some cloud servers, and various privacy concerns emerge from it. This paper focuses on data privacy, anonymity, access control. Attribute based encryption technique attached attributes along with the data and only attributes are encrypted the data is kept as it is. Attribute based encryption technique increased the security, performance and reduce the time of proposed system.***

Keywords— **Authentication scheme, Attribute Based Encryption, Anonymity, mobile cloud computing services.**

I. Introduction

Combination of cloud computing, mobile computing and wireless networks is called as Mobile Cloud Computing (MCC) to bring rich computational resources for mobile users, network operators, as well as cloud computing providers. The goal behind the use of MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience. The impact of mobile cloud computing [8]–[9] is very important research field in mobile-oriented world, providing new supplements, consumption, and delivery models for IT services. MCC gives the better business opportunities for mobile network operators as well as cloud providers. More comprehensively, MCC can be defined as ”a rich mobile computing technology that leverages untied elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle.

However, there are three concerns to be resolved along with the authentication scheme . First of all, in this scheme computing efficiency is seriously considered, since mobile devices have only relatively limited computing capability in comparison with laptop computers. Second, sufficient security strength should be supported; since all messages are transmitted via an insecure WLAN or telecommunication networks, an adversary can easily obtain, interrupt, or modify transmitting messages before they reach the desired recipient. In addition, privacy protection on user accounts is a rising issue as identity masquerade and identity tracing have become common attacks in wireless mobile environments. As mobile users generally access [1]

Traditional single sign-on (SSO) schemes [1]–[12] such as Passport and OpenID are one possible solution for key management issue. In such systems, users can access multiple mobile cloud computing services using only one secret key or password. However, most of SSO systems require a trusted third party to participate in each user authentication session. OpenID is an example of a decentralized SSO mechanism, which has been widely adopted by many Internet service providers such as Yahoo and Google, with over 50 000 websites currently using OpenID as their authentication scheme. OpenID involves three roles: users, relying partners (RP) or service providers (SP), and identity providers (IdP). In OpenID, an IdP can be also an SP and vice versa.

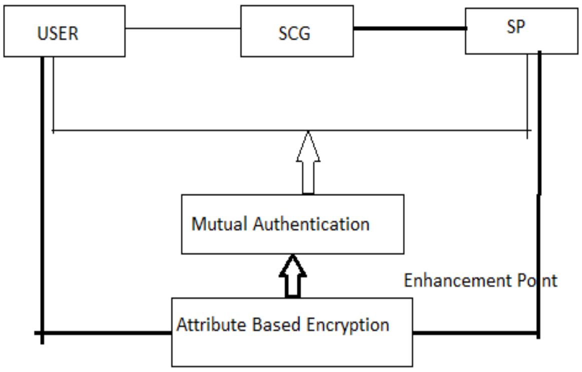
II. Material and Methodology

A. Existing System

In the Existing System in this paper is based on securing the unauthorised access of services from the non-registered users. In this paper RSA algorithm is modified with bilinear pairing and dynamic nonce generation technics to reduce the computation cost. But bilinear pairing scheme contains special hash functions and hash function is probabilistic and inefficient. And in the existing system when mobile user sends the request to service providers it will receive by all the authorized service provider. After receiving the request only valid or nearest service provider will fulfill that request and send response to user.

B. Proposed System Architecture

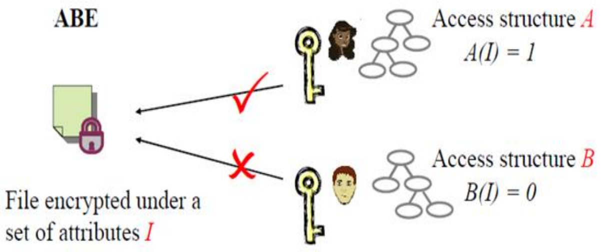
In the existing system the communication is done using mutual authentication. And for key generation bilinear paring with hashing technic is used but it is very time consuming to encrypt the whole data to secure the communication. So in this paper proposed the new technic which reduces the time of key generation along with that provide privileges to each user with the help of privilege tree.



C. Technique

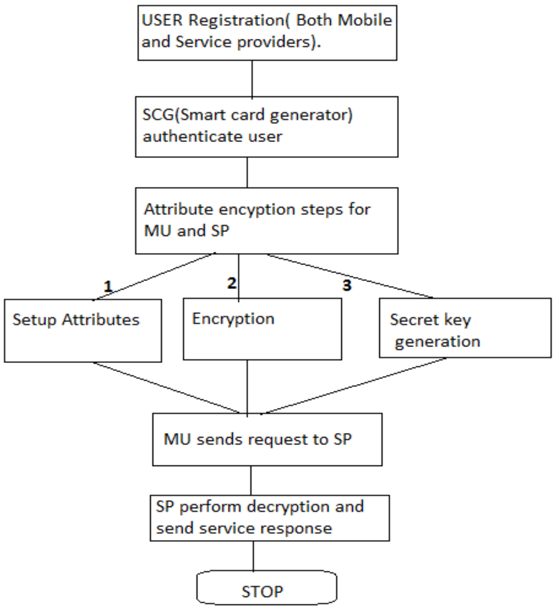
Attribute Based Encryption

ABE is a public key cryptography primitive for one-to-many communications. [2] In ABE, data are associated with attributes for each of which a public key component is defined. The encryptor associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes, i.e., interior nodes of the access tree are threshold gates and leaf nodes are associated with attributes. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure. ABE scheme is composed of four algorithms which can be defined as follows:



- Setup Attributes
- Encryption
- Secret key generation
- Decryption

D. Process Flow

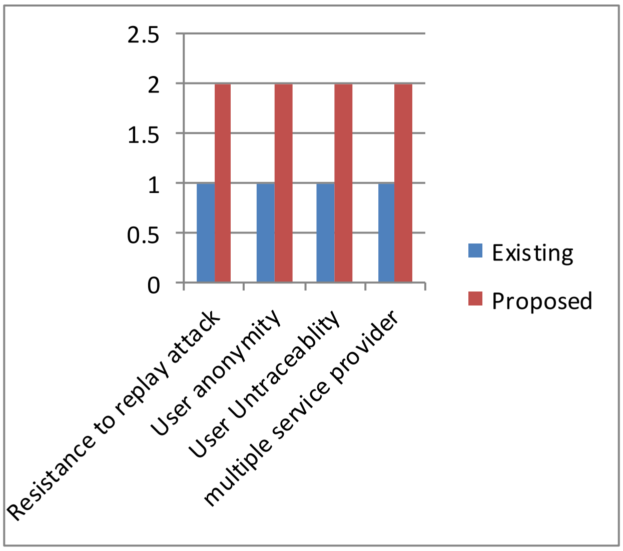

USER Registration(Both Mobile and Service providers).
SCG(Smart card generator) authenticate user
Attribute encyption steps for MU and SP
1
2
3
Setup Attributes
Encryption
Secret key generation
MU sends request to SP
SP perform decryption and send service response
STOP

E. Efficiency of Proposed System

1. The proposed algorithm has proved the best result in terms of execution cost.
2. No data loss.
3. Time complexity to execute the task is very low.
4. Proposed system is more efficient than existing system.
5. Proposed system inherits data dynamics.
6. Our scheme endorses scalable and competent authentication in cloud computing.
7. Proposed scheme are more sheltered and highly competent.

III. Results and Tables

As mention above proposed system is very efficient than the existing system. The technique which is used in existing system is very time consuming and contains high pairing operation with hashing. But in our proposed system which uses attribute based encryption saves the key generation time as well as searching time due to this performance is increased. Proposed system also preserve the user real identity.



Comparison with Existing System.

IV. Conclusion

The use of attribute based encryption technique increase the performance of the system. Attribute encryption technique provides the user anonymity which means the identity of user did not reveal. ABS also saves the time which is required in bilinear pairing for the creation of key. ABS creates a standard master key or secret key for communication and the data whatever send from the user is not encrypted only the attribute associated with that data is encrypt so it improves speed of operations. And also Searching of services is also based on attributes which gives faster results than the existing system.

In future there can be more advanced technique can be used other than attribute based encryption technique that is KP-ABE, CP-ABE etc.

Acknowledgement

I would like to thanks all researchers for making their resources available. I would like to thanks to all the faculty members and Department of Computer Engineering GHRCEM, Pune, India for the guidance and cooperation.

References

i. *Jia-Lun Tsai and Nai-wei Lo"A Privacy Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", IEEE system journal, Vol 9, No. 3, September 2015.*

ii. *Taeho Jung, Xiang- Yang li,Senior member,IEEE ,Zhiguo Wan andnMeng Wang, member, IEEE, "Control Cloud Data Access Privilege and*

Anonymity with Fully Anonymous Attribute Based Encryption.", IEEE transaction on Information Forensics and Security, Vol 10,No.1, January 2015.

iii. *Hengshu Zhu, Hui Xiong, Senior Member, IEEE, Yong Ge, and Enhong Chen, Senior Member, IEEE "Discovery of Ranking Fraud for Mobile Apps", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 27, NO. 1, JANUARY 2015.*

iv. *Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.*

v. *Wilko Henecka, Matthew Roughan "Privacy-Preserving Fraud Detection Across Multiple Phone Record Databases", DOI 10.1109/TDSC.2014.2382573, IEEE Transactions on Dependable and Secure Computing.*

vi. *Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE,Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 1, JANUARY 2015.*

vii. *X. F. Qiu, J.W. Liu, and P. C. Zhao, Secure cloud computing architecture on mobile Internet,in Proc. 2nd Int. Conf. AIMSEC, 2011, pp. 619622.*

viii. *N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Future Gen. Comput. Sys., vol. 29, no. 1, pp. 84–106, Jan. 2013.*

ix. *W. G. Song and X. L. Su, Review of mobile cloud computing, in Proc.IEEE 3rd ICCSN, 2011,pp. 14.*

x. *ABI Research Report, Mobile Cloud Applications. [Online]. Available: http://www.abiresearch.com/research/1003385-Mobile+Cloud+Computing*

xi. *HAOJIN ZHU1 (Member, IEEE), SUGUO DU2, MUYUAN LI1 (Student Member, IEEE), AND ZHAOYU GAO1 (Student Member, IEEE) "Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks"15 July 2013*