International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

Mobile Cloud Computing With A Private Authentication Scheme

Mrs. Kavitha K K[1], B L Gopinath[2], C U Kushalappa[3], Dilip Kumar H[4]
[1]Assistant professor, Department of Information Science, New Horizon College of Engineering, Bengaluru, Karnataka(India)
[2,3,4]Student, Department of Information Science, New Horizon College of Engineering, Bengaluru, Karnataka(India)

Abstract—This paper describes an authentication scheme to manage various environments of the distributed mobile cloud services. Multiple services provided by the various mobile cloud service providers can be accessed by a mobile user using only a single unique private key. Different algorithms are used for providing mutual authentication and also for key exchange. User anonymity and user untracebility is considered and maintained, which increases the security strength. The bilinear pairing cryptosystem and dynamic nonce generation are the techniques used for maintaining the security strength and is not subjected to time synchronisation problem and it can be easily implemented in a distributed cloud computing environment. The scheme reduces the memory space used on the corresponding service providers. This project aims at combining both the techniques.
Keywords—smart card generator (SCG), mutual authentication, ID based cryptosystem, bilinear pairing cryptosystem, identity provider(IdP).

I. INTRODUCTION

The development of mobile cloud computing [4]–[7] has become an important research field in mobile-oriented world, providing new supplements, consumption, and delivery models for IT services. In mobile cloud computing, mobile users can access computation results, resources, applications, and services that are stored, implemented, and deployed in cloud computing environments by using mobile devices through an insecure wireless local area network (WLAN) or 3G/4G telecommunication networks. Cloud computing is a computing environment centered on users and can use programs or documents stored respectively in servers by operating on an applied software like a Web browser through diverse devices, a user authentication is needed in order to use the cloud computing service. Users in the Cloud Computing environment have to finish the user authentication process which is required by the service provider whenever they use a new Cloud service. The Web browser or the cloud service application will then mutually authenticate both the cloud service provider and the user. Once the authentication is done, the user can access the resources and available services from the cloud service provider. In order to prevent unauthorized access, cloud providers should support a secure authentication scheme for users using mobile devices. In our scheme we are providing bilinear pairing based authentication. Bilinear pairing is an effective method to reduce the complexity of the discrete logarithm problem, it also provides a good setting for the bilinear Diffie Hellman problem. The main benefit of bilinear pairing cryptosystem is that it provides same security level with less computation costs and limited system requirements. A smart card generator is used to provide cards to the users and the service providers who register themselves with the smart card generator. These cards are used by service providers and the users to authenticate each other before messages are transmitted between them.

II. RELATED WORK

In [1] author The paper presents a remote user authentication scheme using the properties of bilinear pairings. In this scheme, the remote system receives a user login request and allows the user to login to the remote system only if the login request is valid. The scheme strictly prohibits the scenario of many logged in users with the same login-ID, and provides an option to the registered users to change

their password flexibly without any involvement from the remote system. In this system the user is assigned a unique smart card, which is personalized by certain parameters during the user registration process. Usage of smart card makes the scheme secure and also prevents the users from the distribution of their login-IDs, which effectively prevents the scenario of many logged in users with the same login-ID. This system uses two algorithms such as discrete logarithm problem and computation diffie-hellman problem[11]. There are three phases in this system, the setup phase, the registration phase and the authentication phase. In setup phase, the remote system selects a key as it's private key and generates a public key from that and publishes the system parameters. In registration phase, when the user wants to register with the remote system, the user submits his ID and password to the remote system and it computes a smart card from those credentials. Then the smart card is sent to the user through a secure channel. In authentication phase, the smart card is placed in the terminal(input device) when the registered user wants to log into the remote system. The login request is sent directly by the smart card. Once the remote system receives the login request, it accepts it only after verifying it. But there are a few drawbacks in this system. The password can be easily changed or hacked by others when they have the user's ID. It is vulnerable to offline guessing attack and does not guarantee bilateral verification.

In [2] author proposes a scheme which is designed in such a way that it could ensure all sorts of facilities needed for a remote user authentication procedure and could resist all the types of known attacks. To prove the efficiency of their scheme, they also present a detailed validation, security, and performance analysis, describes access control of the remote user as a method where the remote server confirms the validity of the user before giving him any opportunity to communicate with the server. This communication method is widely used in e-commerce, e-transactions, e-banking, etc. As the development of communication technologies and use of distributed networking, remote user authentication has become a critical issue. In most of the cases, it is also needed to make sure that the communication is happening between the right entity and user and thus user needs to verify the legitimacy of the remote server. They improved the above system in many ways ,such as ,(a) Minimum processing and transmission requirement. (b) Robust password changing phase such that the smart card can verify the user legitimacy before changing its content and allowing the user to change their password. (c) Bilateral verification, in where both the server and the user can verify each other's legitimacy. (d) Resistance against all the known attacks based on bilinear pairings. (e) No storage table in the RS containing any particular secret information for a particular user. But its choices are frequently more expensive due to cprocessing, memory, and transmission costs.

In [3] author propose a strongly secure remote user authentication and key agreement scheme to solve the security weaknesses such as, Security proof shows that this scheme can achieve mutual authentication and key agreement, and provide perfect forward secrecy. Further security analysis shows that this scheme can provide user anonymity, insider attack resistance and leakage of the session temporary secrets resistance. The proposed scheme possesses low computation cost and low power consumption. Thus it is more suitable for mobile client-server environment. The remote user authentication based on ID and the key agreement schemes are subjected to an inherent design weakness, i.e., all users private keys are known to the server, and this scheme cannot provide insider attack resistance or mutual authentication. To improve security, the author has proposed a novel remote user authentication and key agreement scheme. Security analysis shows that this scheme does not suffer from the security weaknesses mentioned above. Security proof for the scheme's basic security properties including mutual authentication and key agreement is also provided. Comparison with several latest schemes has shown that this scheme is more secure, practical and suitable for mobile client-server environment.

III. PROPOSED SYSTEM

This paper assumes that the distributed mobile cloud service environment is supported by a trusted smart card generator (SCG) service. Three roles take part in the proposed scheme: mobile users, distinct mobile cloud service providers, and a trusted SCG service..The proposed scheme includes three phases: system set up, registration, and authentication. During the system set up phase, the SCG first selects a random number as its master private key, computes the corresponding public key, and generates all public parameters. Then, the SCG publishes its public key and public parameters. After the system set up phase is accomplished, the registration phase is executed between the SCG and each one of the mobile users (or service providers) who wishes to join and utilize the authentication service. Mobile user and service providers are required to register with the SCG by sending their identities. Upon receiving these identities, the SCG computes and generates corresponding private keys for these users and service providers before dispatching these keys back to corresponding users and service providers securely. In accordance with the design of ID based cryptosystem[10], the identities of mobile users and service providers are also served as their corresponding public keys. Finally, the authentication phase is executed between mobile user and service provider when a user is requesting for a mobile service. During this phase, a mobile user and the targeted service provider are able to authenticate each other without the involvement of the SCG. A session key is also generated during authentication to encrypt/decrypt subsequent messages sent between the user and the service provider after authentication..

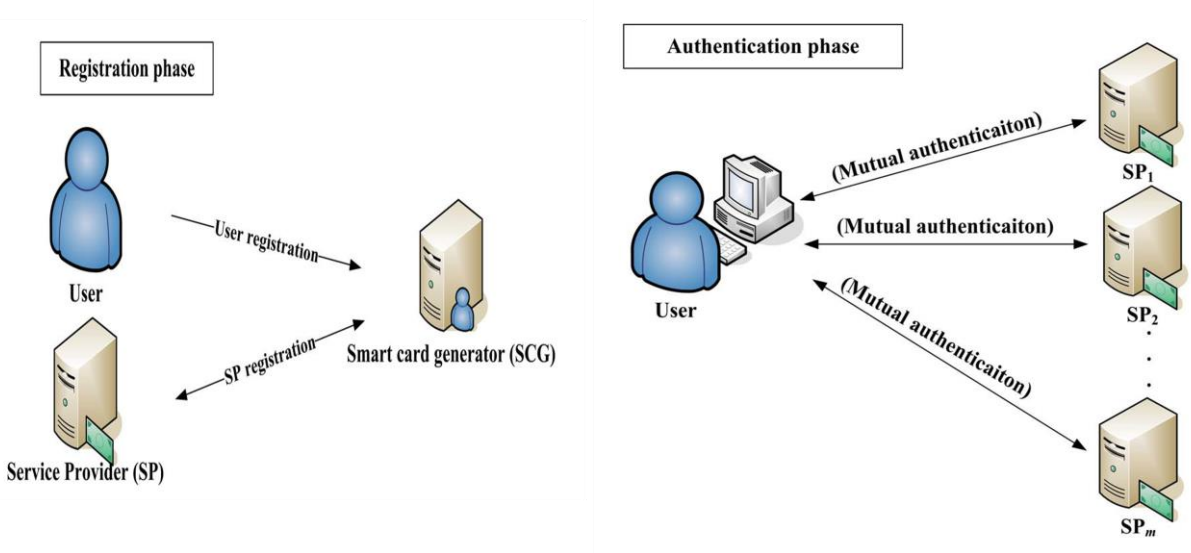

Fig. 3. Framework of proposed authentication scheme.

Fig. 1 illustrates the proposed system framework. A user can anonymously access multiple mobile cloud computing services from different service providers without the involvement of the SCG during user authentication phase. The SCG is only responsible for generating public parameters, as well as all private keys for service providers and users.

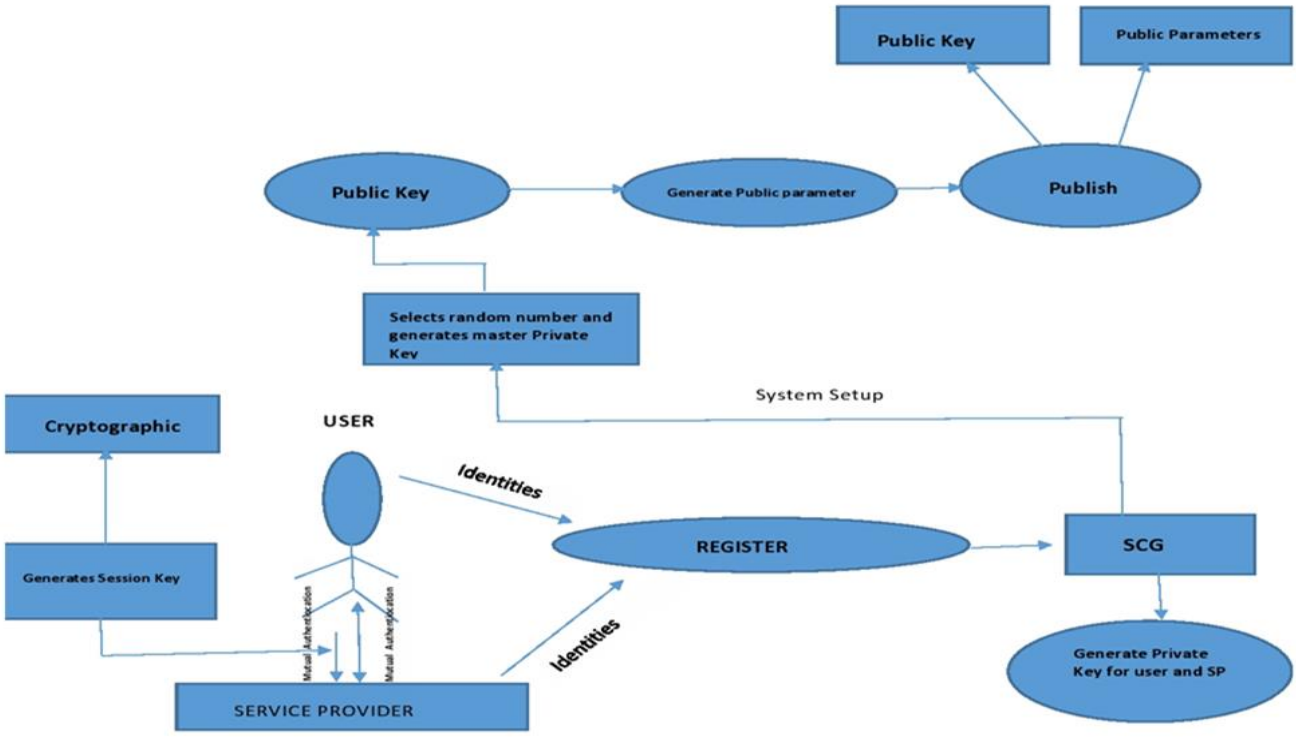

Fig. 2. System Architecture

Fig. 2 illustrates the proposed system architecture. The complete transitions starting from the user or service provider registration to the authentication of the user along with the smart card generation process is depicted in this figure.

IV. CONCLUSION

This paper has proposed a new anonymous authentication scheme for distributed mobile cloud services environment. The proposed scheme allows a mobile user to access multiple services from different mobile cloud service providers using only one single private key. The proposed scheme supports mutual authentication, key exchange, user anonymity, and user untraceability. Security analyses have shown that the proposed authentication scheme withstands all major security threats and meets general security requirements. In addition, no verification table is required to be implemented at service providers or the trusted SCG service. In the proposed scheme, the trusted SCG service is not involved in individual user authentication process. With the proposed design, the scheme reduces authentication process time which includes communication and computation between the various cloud service providers and traditional trusted third party service. As the security strength of the proposed scheme is based on nonce and bilinear pairing, the scheme itself is not subject to time synchronization problem and can be easily implemented in distributed mobile cloud computing environment.

REFERENCES

1. Manik Lal Das, Ashutosh Saxena, Ved P. Gulati,Deepak B. Phatak, "A novel remote user authentication scheme using bilinear pairings" Elsevier, Computers & Security, 2006.
2. Al-Sakib Khan Pathan and Choong Seon Hong "Bilinear-Pairing-Based Remote User Authentication Schemes Using Smart Cards " ICUIMC'09, January 2009.
3. Haiyan Sun, Qiaoyan Wen, Hua Zhang and Zhengping Jin, "A novel remote user authentication and key agreement scheme for mobile client-server environment", July 2013.
4. 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.
5. G. Le, K. Xu, M. Song, and J. Song, "A survey on research on mobile cloud computing," in Proc. 10th IEEE/ACIS/Int. Conf. Comput. Inf. Sci., 2011, pp. 387–392.

6. 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. 619–622.
7. W. G. Song and X. L. Su, "Review of mobile cloud computing," in Proc. IEEE 3rd ICCSN, 2011, pp. 4–7.
8. H. W. Lim and M. Robshaw, "On identity-based cryptography and grid computing," in Proc. ICCS, 2004, pp. 474–477.
9. H. W. Lim and M. Robshaw, "A dynamic key infrastructure for GRID," in Proc. EGC, 2005, pp. 255–264.
10. Boneh D, Franklin M. Identity-based encryption from the Weil pairing. In: Advances in cryptology e Crypto'01, LNCS, vol. 2139. Springer-Verlag; 2001. p. 213e29.
11. Frey G, Ruck H. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves.Mathematics of Computation 1994;62:865e74.

