Analysis of Schemes for Secure Access of Software Services in Mobile Cloud Computing

Miss. M. S. Chinchamalatpure, Dr. Mrs. Swati Sherekar, Dr. V. M. Thakare

Abstract-Mobile cloud computing have been research area of software services with lots of secure schemes to design secure data distrib ution system. This paper focused on five different techniques such as type based proxy re-encryption scheme, robust anonymous authentication scheme for mcc, Attribute-Based Encryption (ABE) access control system for cloud, ExpSOS: secure outsourcing of exponentiation operation and Smart Card Generator (SCG) services. But some problems exist in each scheme. This paper proposes the methodology to overcome the problems that are given in analysis and discussion to improve "Multi user authentication scheme". In mobile cloud computing service software scheme is proposed using the analysis of the various software services

Keywords:Access control system, Authentication, Mobile cloud computing services, Security, Secure data distribution

I. INTRODUCTION

The development of mobile cloud computing has become an important research field in mobile-oriented world, providing new supplements, consumption and delivery models for IT services. Various kinds of cloud service models based on cloud computation have been emerged. When a user intends to access a mobile cloud computing service, he/she activates the service through a web browser or cloud service application installed on mobile device. Furthermore 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 providers and maintain corresponding private keys or password for authentication usage. Each cloud computing services have their own application with different behaviour to communicate with other nodes in the network.

This paper, discusses five different mobile cloud computing schemes such as Type based proxy re-encryption scheme (TB-PRE), Robust anonymous authentication scheme for mcc. Attribute-based encryption (ABE) access control system for cloud, ExpSOS: secure outsourcing of exponentiation operation, Smart card Generator (SCG) services. But some problems are include in each scheme so to overcome the problems that are given in analysis and discussion, improve "Multi user authentication scheme in mobile cloud computing services" software scheme is proposed using the analysis of the various software services**.**

II. BACKGROUND

Many studies on mobile cloud services have been done to develop the security scheme in recent past years. Such schemes are:

A new type-based proxy re-encryption scheme to design a secure and efficient data distribution system in MCC, which provides data privacy, data integrity, data authentication, and flexible data distribution with access control [1]. A new robust anonymous mutual authentication scheme utilizes both MU and service cloud with purpose of improves the legitimacy in secure and efficient way [2]. ExpSOS scheme has been proposed secure verification with probability approximately 1 to ensure that mobile end users can always receive valid result. This scheme improves the existing scheme in efficiency, security [3]. To improve the performance of mobile cloud service and different mobile operator mode using ABE access control scheme [4]. An efficient authentication scheme for distributed mobile cloud computing services from multiple service providers using a single private key on smart card generator (SCG) service [5].

This paper introduces five different scheme such as Type based proxy re-encryption scheme, robust anonymous Authentication scheme for mcc, Attribute-based encryption (ABE) access control system for cloud, ExpSOS: secure outsourcing of exponentiation operation, Smart card Generator (SCG) services.

The paper is organised as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses

previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on mobile cloud services. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III.PREVIOUS WORK DONE

In research literature, many computing models have been studied to provide various schemes and improve the performance in terms of capacity-throughput-delay tradeoffs, overhead and packet delivery ratio.

Jiang Zhang et al. [1] have worked on the several cryptographic primitives such as a new type based proxy re-encryption to design a secure and efficient data distribution system in MCC, which provides data integrity, data authentication and flexible data distribution with access control.

Prosanta Gope et al. [2] has proposed a new robust anonymous mutual authentication scheme for mobile cloud. This scheme proved legitimacy with both MU and service cloud.

Kai Zhou et al. [3] has worked on the analysis of ExpSOS provides a secure verification scheme with probability approximately 1 to ensure that the mobile end users can always receive valid result.

TU Shanshan et al. [4] has presents the analysis of ABE access control scheme on mobile cloud to improve the performance of mobile cloud service.

Jia-Lun Tsai et al. [5] have shown the scheme of smart card generator provides security and convenience for mobile users to access multiple mobile cloud computing services from multiple service providers using only a single private key.

IV. EXISTING METHODOLOGIES

Many mobile cloud computing schemes have been implemented over the last several decades. There are different methodologies that are implemented for different mobility models i.e Type based proxy re-encryption scheme (TB-PRE), Robust anonymous authentication scheme for mcc, Attribute-based encryption (ABE) access control system for cloud, ExpSOS: secure outsourcing of exponentiation operation, Smart card Generator (SCG) services.

4.1 A New Type-based Proxy Re-encryption: TB-PRE in designing a concrete secure data distribution system in MCC. An efficient TB-PRE scheme, and then carefully combine it with several other Cryptographic primitives such as signatures to obtain a secure and efficient data distribution System with fine-grained access control in MCC. Since use TB-PRE as a building Block, one can instantiate system with other TB-PRE schemes. Present new re-encryption schemes that realize a stronger notion of security and demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of experimental file system demonstrate that proxy re-encryption [1].

4.2 Robust Anonymous Mutual Authentication Scheme: new robust anonymous mutual authentication scheme for mobile cloud environment. Through this scheme, author need to prove both the MU and the service cloud and their legitimacy, it eventually helps the legitimate mobile cloud user to enjoy *n* times all the ubiquitous services in a secure and efficient way, where the value of *n* may differ based on the principal for paid. The security of the proposed scheme is thoroughly analysed using both formal as well as informal security analysis. Furthermore, functionality and performance comparisons using the testbed simulation among the proposed scheme and other existing relevant schemes reveal that the proposed scheme outperforms other existing schemes [2].

4.3 ExpSOS: Secure Outsourcing of Exponentiation Operation:

A Secure Outsourcing Scheme for general Exponential (ExpSOS) operations. The proposed Exp- SOS is based on a secure disguising procedure that maps the integers in the group R_N to the larger group R*L* so that the cloud will carry out the computation in R*L* while still keeps *N* secure. ExpSOS also provides a secure verification scheme with probability approximately 1 to ensure that the mobile end users can out the computation in R*L* while still keeps *N* secure. ExpSOS also provides a secure verification scheme with probability approximately 1 to ensure that the mobile end users can always receive valid results. The comprehensive analysis as well as the simulation results in real mobile device

demonstrates that our proposed ExpSOS can significantly improve the existing schemes in efficiency, security, and result verifiability [3].

4.4 Attribute-Based Encryption (ABE) Access Control System: Attribute-Based Encryption (ABE) access control systems for the cloud including MCC are carried out on encryption/decryption task partitioning, i.e., how to divide an access control system into the cloud partition(s) and the local partitions. One common feature of these works is the fact that they all assume that there is perfect network connection and sufficient bandwidth between a mobile device and the remote cloud Virtual machine (VM) [4].

4.5 Smart card generator service: An efficient authentication scheme for distributed mobile cloud computing services. It provides security and convenience for mobile users to access multiple mobile cloud computing services from multiple service providers using only a single private key. Smart card generator service and cloud computing service based on bilinear pairing cryptosystem and dynamic nonce generation [5].

V. ANALYSIS AND DISCUSSION

TB-PRE scheme performance between the scheme and choice of parameters and on a Lenovo X1 Carbon laptop (equipped with a Win 10 system, 2.5 GHz Intel i7 CPU and 8 GB memory). The evaluation of the proposed present an efficient data distribution system in MCC, which allows mobile users to securely store data in the cloud storage, and flexible share the data with friends. The leverage several cryptographic primitives to achieve data privacy, data integrity, dynamical data modification and deletion, and flexible data distribution. An efficient type-based proxy re encryption (TB-PRE), which allows a mobile user with single Secret key [1]. Robust Anonymous Mutual Authentication Scheme performed security issues in the MCC environment. The communication overhead is concerned, during the authentication process the proposed scheme requires the communication overhead as $\sum^{2}_{i=1}|MAi| = 576$ bits, which is less as compared to that for the other schemes. [2]. ExpSOS: Secure and Verifiable Outsourcing of Exponentiation scheme shows that the verification scheme can also be applied to outsourcing of scalar multiplication [3]. ABE access control system shows the analysis of ABE algorithm has been evaluated in the previous work, which is similar in the new framework and just to improve the mobile user experience**.** The access control architecture is called "Cloudlet+ Cloud", and "Cloud Only" denotes those conventional architectures. The evaluation assumes that the CPU power (MIPS) of the remote server, is twice as big as the CPU power of the mobile device and also the size is fixed throughout the whole evaluation [4]. Smart card generator (SCG) schemes achieve user-to-service-providerauthentication, service-provider-to-user authentication, and key agreement. This scheme analysis to preserve user privacy [5].

TABLE 1: Comparisons between different authentication scheme

Authentication Scheme	Advantages	Disadvantages
	TB-PRE to enforce access control for mobile devices in cloud computing.User has to keep a single secret key and does not suffer from the escrow problem.	Mobile cloud computing is the unpredictable internet connectivity. Low storage and less energy
Robust Anonymous Mutual Authentication Scheme	User anonymity is ensured in this scheme. This Scheme was completely insecure for its incapability of password dependent goal.	It needs more processing time for to implement. Nothing mentioned about advanced security metrics e.g. end-to-end security evaluation.
ExpSOS: Secure and Verifiable of exponentiation operation scheme	This proposed method is very efficient and scalable in mobile cloud computing. Cloud provides low cost and good reliability.	The drawback of this method it needs more storage and time for to implement. The performance decreases as the no of users increases.
ABE Access Control System Scheme	This method improves the portability and it is visualized & dynamic. Mobility communication .	This method is not well suited for complex nature of user mobility model.

Smart card generator (SCG) service scheme.	Mobile user to access multiple services different mobile cloud using only one single private key.	SCG is not involved in individual user authentication process.

VI.PROPOSED METHODOLOGY

Authentication scheme is important and discuss the various methods based on different parameters i.e. mutual authentication, security, key exchange, user anonymity formobile cloud computing services. There are still problems which troubles in this field of new mobile cloud computing services method called as "Multiuser Authentication Scheme". Software services for mobile cloud computing is proposed here to overcome the problems of this model. The proposed authentication scheme is mainly for distributed cloud computing service environment. The trusted SCG is responsible for generating and distributing the private keys to the users and service providers securely. If service provider SP_j or user U_i joins the system, the SCG is not required to update its master key or corresponding public key. When a user obtains private key, it can authenticate and communicate with the other legal entity by using private key without help of SCG.

The proposed scheme includes three phases:

System set up phase: 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.

Registration phase: A user must register with an IdP in advance to obtain an OpenID identifier. When user logs in to websites that have adopted OpenID. Once the IdP confirms the legal status of the logging in users, the IdP redirects user session back to the targeted SP with credential. SP receive the message from IdP. If it is valid, then the SP authenticates the user. 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. The no. of mobile user and service providers are required to register with the SCG (Agent) by sending their identities. Upon receiving these identities, the SCG (Agent) computes and generates corresponding private keys for these users and service providers before dispatching these keys it store on authenticated database back to corresponding users and service providers securely. In accordance with the design of identity-based cryptosystem, the identities of mobile users and service providers are also served as their corresponding public keys.

Authentication phase: 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.

Diagrammatic representation of proposed method is shown as follows:

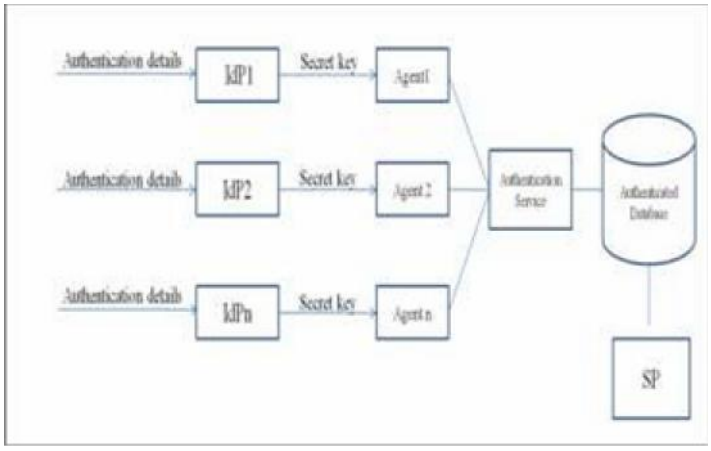

Figure 1(a): Registration phase

VII. OUTCOME AND POSSIBLE RESULTS

In this way the proposed scheme is perform to exclude the necessity for the trusted third party to be involved in regular user authentication session such that the total user authentication processing time can be reduced. This scheme requires less computing resources on both the mobile users devices and service providers. Through an IDbased cryptosystem, a user is required only one private key to access multiple services from distinct mobile cloud service providers, provided that the user knows all the identities of the service providers.

VIII. CONCLUSION

This paper focused on the study of various authentication scheme i.e. type based proxy re-encryption scheme, robust anonymous authentication scheme for mcc, Attribute-based encryption (ABE) access control system for cloud, ExpSOS: secure outsourcing of exponentiation operation, Smart card Generator (SCG) services. But some problems are include in each scheme so to overcome the problems that are given in analysis and discussion, improve "Multi user authentication scheme in mobile cloud computing services" software scheme is propose here the trusted SCG service is not involved in individual user authentication process. With this design, this scheme reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service.

IX. FUTURE SCOPE

From observations of the proposed method the future work will enhance authentication process prediction with the help of more close form of mathematical expression.

ACKNOWLEDGEMENT

Authors wish to express their sincere thanks to Dr. V. M. Thakre, head, Post Graduate Department of Computer Science and Engineering for providing constructive and generous guidance.

REFRENCES

[1] Jiang Zhang, Zhenfeng Zhang, Hui Guo, "Towards Secure Data Distribution System in Mobile Cloud Computing", *IEEE Transaction ON MOBILE CLOUD COMPUTING*

[2] Prosanta Gope, Ashok Kumar Das, ,"Robust Anonymous mutual Authentication Scheme for n-Times Ubiquitous Mobile Cloud Computing Services", *IEEE INTERNET OF THINGS JOURNAL*, Vol. 4, No. 5, OCTOBER, 2017

[3] Kai Zhou, Student Member,*IEEE*, M.H. Afifi, and Jian Ren, Senior Member, *IEEE*, "ExpSOS: Secure and Verifiable Outsorcing of Exponentiation Operations for Mobile Cloud Computing", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, Vol. 12, No. 11, NEVEMBER2017.

[4] TU Shanshan, HUANG Yongfeng, "Towards Efficient and Secure Access Control System for Mobile Cloud Computing", *IEEE CHAINA COMMUNICATION*, *DECEMBER* 2015.

[5]Jia-Lun Tsai, Nai-Wei Lo,"A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", *IEEE SYSTEM JOURNAL*, Vol. 9, No.3, SEPTEMBER 2015.

	**Megha S. Chinchamalatpure** has completed B.E. Degree in Information technology from Sant Gadge Baba Amravati University, Amravati, and Maharashtra. She is persuing Master's Degree in Computer Science and Information Technology from P.G. Department of Computer Science and Engineering, S.G.B.A.U. Amravati. (e-mail id: megha.chinchamalatpure@gmail.com)
	**Dr. Vilas M. Thakare** is Professor and Head in Post Graduate department of Computer Science and engg, Faculty of Engineering & Technology, SGB Amravati university, Amravati. He is also working as a coordinator on UGC sponsored scheme of e-learning and m-learning specially designed for teaching and research. He is Ph.D. in Computer Science/Engg. and completed M.E. in year 1989 and graduated in 1984-85. He has done his PhD in area of robotics, AI and computer architecture. His area of research is Computer Architectures, AI and IT. He has published more than 150 papers in International & National level Journals and also International Conferences and National level Conferences.(e-mailid: vilthakare@yahoo.co.in)