ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (162-166), Month: April - June 2019, Available at: www.researchpublish.com

Analysis and Design of Scheme for Secure Access of Software Services in Mobile Cloud Computing (MCC)

[1]Miss. M. S. Chinchamalatpure, [2]Dr. S.S. Sherekar, [3]Dr. V. M. Thakare

SGBAU, Amravati, India

megha.chinchamalatpure@gmail.com, ss_sherekar@rediffmail.com, vilthakare@yahoo.com

Abstract: **Cloud computing has been started to play a key role in the new computation era. Cloud computing can be used a wide range of applications, from personal to organizational services, various infrastructure, software, and platform services. In the mobile cloud computing it's requires a mutually-authenticated environment for mobile devices and cloud servers for the security purposes. This paper focused on five different techniques such as Context-aware Authentication System, Context-aware software architecture, Mobile Cloud Authenticator (MCA), Multi-factor Authentication protocol, Distributed Application processing Frameworks(DAPF's)But some problems have arisen in each scheme so as to overcome the problems that are given in analysis and discussion to improve "A Message Digest Secure Authentication Scheme in Mobile Cloud Computing". Software scheme is proposed using the analysis of the various software services.**

Keywords**: Mobile cloud computing security, Authentication, Pervasive Computing, Distributed System.**

I. INTRODUCTION

Cloud computing has serve to a new development, collaboration, storage and management. The research focus of this paper in mobile cloud computing is used for data processing. The widespread use of the mobile cloud computing is security, privacy and integrity. Authentication is the important role of mitigate security and privacy issue in the Mobile Cloud Computing. Cloud computing is a model for enabling convenient, on demand network access to a shred pool of configurable computing resources. 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. Security plays a major role in the cloud computing. 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 Context-aware authentication system, Context-aware authentication architecture, Mobile cloud authenticator(MCA),Multi-factor authentication protocol, Distributed Application processing framework(DAPF's). But some problems are include in each scheme so to overcome the problems that are given in analysis and discussion, improve "" 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:

Context-aware authentication system is cost-effective and easy to implement. The information is sent when the user makes an authentication request that render our system more practical [1]. Context-aware software architecture is services deployed in mobile and dynamic network environments. This scheme based on service replication scheme with the self configuration approach for the activation/hibernation of the replicas of the software services depending on the relevant context information from the mobile system[2]. Multi-factor authentication protocol analyzed security and privacy of these algorithms [3].Mobile Cloud Authenticator (MCA) is used for authenticating the mobile users. In the Mobile Cloud Authenticator is used three entities cloud users, mobile network and cloud [4]. Distributed Application Processing Frameworks (DAPFs) analyze the offloading scope, migration granularity, portioning approach and migration pattern [5].

This paper introduces five different schemes such as Context-Aware Authentication System, Context-Aware Software Architecture, Mobile Cloud Authenticator (MCA), Multi-Factor Authentication protocol, Distributed Application Processing Frameworks (DAPF's) **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. Kamal Benzekki et al. [1] have proposed Context-Aware Authentication System to use resources that are commonly found in the user device of the user in different situation and events. User is immersed in the pervasive space. It performs task and activities. Gabriel Guerrero-Contreras et al. [2] has worked on Context-Aware Software Architecture is proposed services in mobile and dynamic network environments. This architecture is made up of four elements Communication middleware, Monitoring subsystem, Context manager Service and Replica manager service. Mojtaba Alizadeh et al. [3] has analyzed a Multi-factor authentication protocol for security and privacy algorithm. In MCC, the mobile devices are connected to the cloud computing infrastructure, and process authentication. A. Cecil Donald et al. [4] has discussed the Mobile Cloud Authenticator (MCA) for authenticating the mobile cloud computing environment. The MCA holds the Unified Cloud Authenticator (UCA). UCA is comprised Authentication Server (AS). Muhammad Shiraz et al. [5] have proposed Distributed Application Processing Frameworks (DAPF's) for the SMD's in MCC domain. DAPFs is developing, implementing, and executing computational intensive mobile application within MCC domain.

IV. EXISTING METHODOLOGIES

Mobile users have made up of the Miniature nature, Compact Design, High Quality Graphics. Many mobile cloud computing schemes have been implemented over the last several decades. There are different methodologies that are implemented for different software services i. e Context-Aware Authentication System, Context-Aware Software Architecture, Multi-factor authentication protocol, Mobile Cloud Authenticator (MCA), Distributed Application Processing Frameworks (DAPF's).

Context-Aware Authentication System: Context-Aware Authentication System is a cost-effective and easy to implement. This schemes use the resources to found in the user device in different situation and events. Where user immersed in the pervasive space. In this scheme access the resources such as: GPS Position, Time Zone, Installed Applications, Running Processes/tasks, and Device Characteristics [1].

A Context-Aware Software Architecture: A Context-Aware Software Architecture is proposed to support the availability of the services deployed in mobile and dynamic network environments. This scheme is based on service replication with the approach for the activation/hibernation of the replicas of the service depending on the relevant context information from the mobile system. This scheme is made up of four elements such as: Communication Middleware, Monitoring System, Context Manager Service and Replica Manager Service [2].

Multi-Factor Authentication Protocol:

A multi-factor authentication protocol is important role of security and privacy of the algorithms. This schemes analyzed authentication to mitigate security and privacy issues in the mobile cloud computing. Multi-factor authentication protocol introduces opportunities as a new computing to mitigate the security and privacy [3].

Mobile Cloud Authenticator (MCA):

These schemes discussed overall framework of MCA and UCA. Mobile cloud authenticator (MCA) is proposed authenticating the mobile users in mobile cloud. In this schemes MCA is consist of three major entities cloud users, mobile network and cloud. In this framework Unified Cloud Authenticator (UCA) is placed between the mobile network and cloud service provider (CSP). UCA contains the authentication server, hashing machine, connection manager, user manager and service manager. In the UCA schemes there are three phases registration phase, authentication phase and verification phase. [4]

Distributed application Processing Frameworks (DAPF's):

These schemes propose the thematic taxonomy of SMD's in MCC domain. Distributed Application processing frameworks in developing, implementing and executing computational intensive mobile application within MCC domain. These schemes accomplish process offloading in diverse modes [5].

V. ANALYSIS AND DISCUSSION

Context aware authentication system is cost-effective and easy to implement. The context is relevant for the adaptive process of services and information. Context Aware authentication system is password based authentication method [1]. Context aware software architecture proposed services deployed in mobile and dynamic network environments. This scheme is based on activation/hibernation of the replicas of the service on relevant context information from the mobile system [2]. A multi-factor authentication protocol is based on privacy, security, performance and energy. This implementation method is based on knowledge, possession and biometric. Feasibility of implementation multi-factor authentication protocol [3]. Mobile cloud authenticator (MCA) proposed users, mobile networks, unified cloud authenticator (UCA) and cloud service provider. This schemes working on registration phase, authentication phase, verification phase [4]. Distributed Application processing frameworks (DAPF's) basis of virtual machine migration, entire application migration and application portioning. This schemes proposed thematic taxonomy and analyses the implications and critical aspects of offloading frameworks [5].

TABLE 1: Comparisons between different authentication schemes

Authentication Scheme	Advantages	Disadvantages
Context-aware Authentication System	Increase data processing speed, It is easy to implement.	It utilizes the large storage space in cloud.
Context-aware software architecture	Reuse of the services of dynamic aspects. Processing the web services.	Multi-casting context information around is increasing computation and communication.
Multi-Factor Authentication protocol	Key exchange scheme in security manner.	The drawback of this method store the error correction based partial encryption key.
Mobile Cloud Authenticator (MCA)	Secure authentication process and it prevents the third parties.	Limited storage capacity.
Distributed Application Processing Frameworks (DAPF's)	It support more application types. More performance optimizations.	Performance analysis on the thread level is hard. The shuffling phase introduces overheads.

VI. PROPOSED METHODOLOGY

Mobile Cloud Computing environment, if a mobile device is registered with a particular cloud service provider, both mobile device and cloud server must authenticate each other in a uniform way in order to secure communication with a single authentication technique. Authentication scheme is important and discuss the various methods based on different

parameters i.e. mobile cloud security, data privacy, continuous user authentication. A single and authentication process preventing the third parties from mobile devices and cloud service provider. There are still problems which troubles in this field of new mobile cloud computing services method called as "A Message Digest Secure Authentication Scheme". Software services for mobile cloud computing is proposed here to overcome the problems of this model. We focused on the following research. We use of user ID and password based authentication in addition to improve the security between mobile device and cloud service provider. The proposed authentication scheme reduces the vulnerability of system to attacks.

The Mobile devices authentication (MDA) is applicable to a verity of different mobile devices with MDA if the mobile devices is stolen, the authentication information of the user can remain to be safe. When the user change their registered mobile devices, they can still access the cloud using other mobile after a few encrypted files(such as hashed user and cloud certificates, and policies) are ported. MDA is composed of two phases: Registration and authentication phase. The details of these phases are presented as follows,

Registration Phase:

The registration process of a mobile device or a cloud user is one time and it is used for account with user id, password and other unique information such as credit card for accessing cloud services. We have considered standard mobile devices and cloud server registration process. Cloud server will perform the following operations,

- Mobile device stores the user ID, hash{password}and users mobile device information.
- Generates the message digest MD_{user} which consist of cloud certificate.
- Generates the message digest MD_{cloud} which consist of cloud certificate.
- Cloud sends an encrypted message to registered mobile device during registration process.

The proposed authentication scheme is applicable once the MD_{user} and $MD_{cloud,}$ are transferred to the mobile device during the registration process.

Authentication Phase:

- The cloud user has two messages digest MD_{user}, and MD_{cloud} in the mobile device.
- User knows user ID and password to access cloud services.

The mobile and cloud server need to authenticate each other in order to start transferring actual data processing request and response.

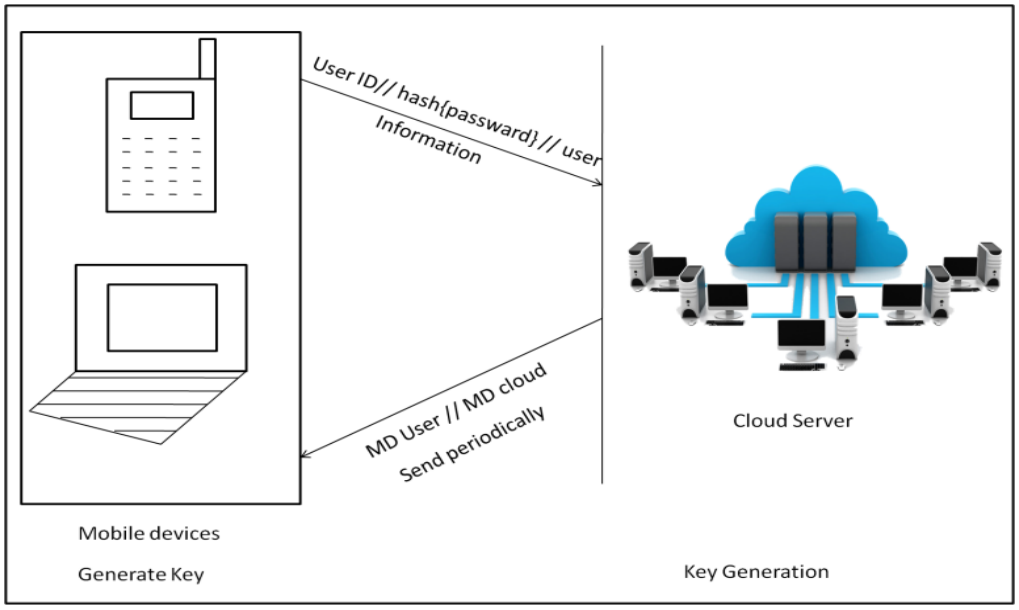

Figure 1:- Proposed registration process of mobile device with cloud server

Outcome and Possible Result

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. In order to perform the improve the usability of the authentication system. In the proposed system mobile device and cloud server are running. We focused on evaluating vulnerability of certain parameters such as, userID, hash{password},MD_{user}, MD_{cloud}, which are used in authentication scheme. If the vulnerability is high, i.e. these parameters are compromised at any level of communication between mobile device and cloud server during authentication process.

VII. CONCLUSION

This paper focused on the study of various authentication schemes. We proposed the design of message digest secure authentication scheme in mobile cloud computing. MDA is completely based on technique employing simple userID, password and hashing.

Future Scope

From observations of the proposed method the future work will enhance authentication process. In the future, firstly, we are about to concentrate on developing this system. Next step is testing performance of it. Lastly, to make a better system, we will fix all factors that affect validity and performance of our system.

REFERENCES

[1] Kamal Benzekki, Abdeslam EI Fergougui, Abdelbaki EIBelrhiti EIALaoui "A Context-Aware Authentication System for Mobile Cloud Computing", *ScienceDirect procedia computer science*, 2018.

[2] Gabriel Guerrero-Contreras, Jose Luis Garrido, Sara Balderas-Diaz, and Carlos Rodriguez-Dominguez "A Context-Aware Architecture Supporting Service Availability in Mobile Cloud Computing", *IEEE Transaction ON Services Computing, Vol.10. No.6 November/December 2017*

[3] Mojtaba Alizadeh, Wan Haslina Hassan, Touraj Khodadadi Member, *IEEE*, "Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing", *IEEE TRANSACTIONS OPEN ACCESS JOURNAl*, Vol. 5, April 2017.

[4] A. Cecil Donald, L. Arockiam "A Secure Authentication Scheme for MobiCloud", *IEEE ICEEOT*, 2016.

[5] Muhammad Shiraz, Abdullah Gani, Senior Member, IEEE Rajkumar Buyya, Senior member, IEEE "A Review on Distributed Application Processing Frameworks in Smart Mobile Devices For Mobile Cloud Computing", *IEEE Communications Surveys &Tutorials, Vol, 15, No.3 2013*.

Author's Profile:

	**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. He has also successfully completed the Software Development & Computerization of Finance, Library, Exam, Admission Process, and Revaluation Process of Amravati University. (e-mailid: vilthakare@yahoo.co.in)