Authentication Issues In Mobile Cloud Computing

Ebin Johnson Mathew
Department of Master of Computer Applications
Aml Jyothi College OF Engineering
Kottayam, Kerala
ebinjohnsonmathew@mca.ajce.in

Sona Maria Sebastian
Asst.Professor Department of Master of Computer Applications
Aml Jyothi College OF Engineering
Kottayam, Kerala
sonamariasebastian@ajce.ac.in

***Abstract*—Mobile cloud computing is a popular topic in today's globe. It helps to improve the performance of mobile devices by utilizing cloud services. Security, particularly authentication in MCC, may be an important need for safeguarding cloud-based computations and communication. Wireless media is used to transmit data between the client and the cloud. As a result, MCC models emphasize fundamental security problems in a range of disciplines, including as authentication, privacy, and trust. Mobile device and cloud computing convergence has mostly led in MCC security threats. This article focuses on the principles of assessing various authentication techniques as well as the security issues that have evolved as a result of the combination of mobile and cloud computing technologies. Existing MCC approaches, according to this study, ignore cloud-to-client authentication issues.**

Keywords—Mobile Cloud Computing, Security, Authentication, Privacy

I. INTRODUCTION

Mobile Cloud Computing (MCC) integrates Cloud computing into the cellular surroundings, a aggregate of technology that permit people to get entry to community assets whenever, whenever, and whichever they pick. MCC is an infrastructure that stores and methods statistics out of doors of mobile gadgets. cell cloud packages eliminate laptop energy and statistics storage from cellular telephones and install them within the Cloud, making the app and mobile pc to be had to greater mobile subscribers than phone users. Low bandwidth, availability, heterogeneity, pc output, information access, security, privateness, and believe are simply a number of the few technological challenges Cloud computing and mobile network integration are going through, all of that have been announced through the dramatic growth in telephone use in latest years. person authentication in Mobile Cloud Computing is a method of verifying the identification of a cell person to make sure that the person is loyal to having access to mobile cloud services. Verification as an indispensable a part of security features at MCC is important to protect users from existing protection and privacy troubles by way of preventing unauthorized get entry to to mobile cloud consumer data.

A number of the most crucial protection threats to cellular customers are facts leakage, denial of service, malfunction of devices and theft or lack of the tool . furthermore, safety threats found in cellular devices can

take place as assaults through the offerings presented through the wireless networks, which includes community profiling, data

II. EASE OF USE

A. Cloud Computing

Mobile cloud computing is a hybrid of mobile internet and cloud computing that indicates the future trends in cloud computing development. Cloud computing is a type of computing in which resources that are dynamically scalable and sometimes virtualized are made available as a service through the internet. Cloud computing is also known as distributed computing via the network, which refers to the ability to run an application or programme on a large number of machines at the same time. Cloud services deliver software and hardware to individuals and organizations from distant locations maintained by a third party. Cloud computing aims to increase capacity and capabilities at runtime without investing in new equipment, licensing new software, or training new staff. Infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) are some examples of services. Cloud computing has several advantages, including the fact that it is less expensive than purchasing software and hardware and that it can be accessed from any computer or device with an Internet connection. The device does not need a huge internal storage system that is compatible with the vast majority of PCs and operating systems. Furthermore, mobile gadgets (e.g., smartphones, tablets, PCs, and so on) are becoming an increasingly important element of everyday life. When compared to typical information-processing devices such as PCs and laptops, these mobile devices still lack resources. Mobile cloud computing offers a solution to these difficulties (MCC). Mobile cloud computing refers to the cloud infrastructure in which computation and storage are performed remote from mobile devices.

B. MOBILE CLOUD COMPUTING

DOI: 10.5281/zenodo.6361875

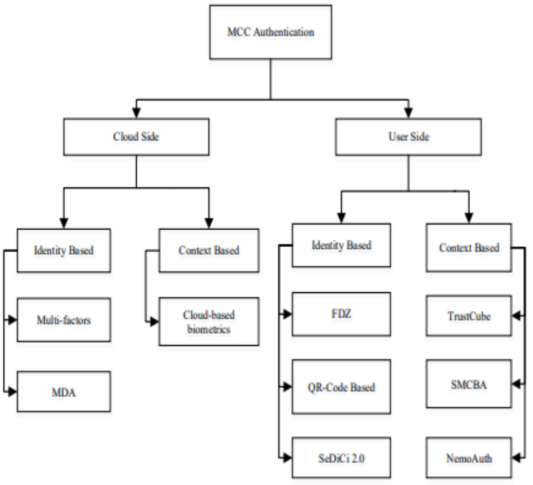
Mobile Cloud Computing is a combination of mobile technology and cloud computing infrastructure in which data and hence related processing take place on the cloud but can be accessed via a mobile device, thus the phrase "mobile cloud computing. To protect networks from various security risks, user authentication is critical. The successful implementation of MCC necessitates the deployment of robust and effective authentication systems that enable users to access cloud-based services for their mobile devices from anywhere, at any time, and from any mobile device at a cheap computational cost based on intrinsic resources. MCC authentication differs from standard mobile device authentication in that the mobile device connects to the Internet to accomplish authentication in the MCC environment. Furthermore, employing an appropriate algorithm, the resource-intensive components of the authentication method may be sent and processed in cloud servers.

III. MCC AUTHENTICATION ISSUES

A. *AUTHENICATION ON CLOUD SIDE*

The majority of the authentication procedures in cloud-side authentication are handled by the cloud server. Because cloud servers have infinite resources, cloud-based authentication solutions are more flexible, efficient, and customizable than previous authentication methods. Although cloud-based authentication provides certain advantages in terms of efficiency and utility, it also poses significant security and privacy concerns. The user's private authentication information, such as passwords and fingerprints, is very vulnerable.

Fig:1 MCC Authentication on cloud side



In contrast to identity-based approaches, context-based methods authenticate users by assessing numerous passive user information and requiring minimum user engagement. However, the accuracy is lower than that of the identity-based technique since the authentication mechanism is dependent on the precision of the pattern analysis results.

B. *AUTHENTICATION ON CLIENT SIDE*

In user-side authentication approaches, mobile devices handle the majority of the authentication stages. Transferring resource-intensive processing tasks to the cloud is one of the main MCC goals, as opposed to processing the authentication mechanism inside mobile devices in user-side authentication methods, which makes user-side approaches less efficient and secure for cloud-connected mobile devices when compared to cloud-side methods.

The different types of methods are:

- User identity based
- Context based methods

Identification-based approaches in the cloud employ user identity information to authenticate the user, although in this case, the mobile device processes and analyses user characteristics to ensure user authentication rather than cloud servers. During the authentication method, user sensitive information such as biometrics is saved locally on the mobile device, raising privacy and security concerns.

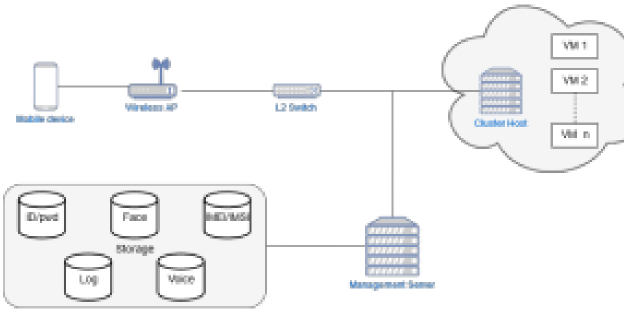
The only distinction between context-based user-side approaches and their cloud-based counterparts is that the mobile device analyses and evaluates user data rather than the cloud server. Context-based authentication systems, in general, need more computing resources than identity-based methods, resulting in performance concerns due to mobile device resource constraints. As a result, context-based user-side authentication is less suitable in MCC than cloud-based approaches. Furthermore, unlike the more secure cloud environment, mobile devices store a range of sensitive user data, putting users' privacy at risk if the device is stolen.

IV. IMPROVING THE AUTHORIZATION SECURITY USING MULTI-FACTOR AUTHENTICATION

As the name implies, authentication is conducted on the cloud server, which is deemed more flexible, efficient, and customizable than other techniques owing to the (potentially) endless resources of cloud servers. Such authentication can be identity- or context-based; in identity-based methods, several credentials such as a unique ID, password, and biometrics can be used; their combination results in two-factor authentication (easier) or even multi-factor authentication (safer).

The capabilities and constraints of mobile devices provide certain obstacles for establishing an effective and efficient authentication system. So combination of two factors for client side and cloud side increases the strength of security. Various authentication methods, such as ID/Password, IMEI, IMSI, and voice recognition, are used for two factor.

Fig2-Multi-Factor Authentication



Steps in the user-side authentication technique are executed in mobile devices, which now widely support such an approach due to significant performance improvements. Also, user-side authentication methods can be identify- or context-based; like identity-based methods in the cloud, it uses user identity information to authenticate the user, but here it is the mobile device that processes and analyses user attributes to check user authentication rather than cloud servers.

A. Security Of Multi-factor Authentication

To maintain security, several authentication elements such as a basic ID/password, a mobile phone number, and various bio-information about individuals are merged. In comparison to previous authentication techniques, this approach improves performance. In security and privacy evaluation, the privacy problems associated with biometric factors are addressed to some extent. Biometric data is highly sensitive information that should be kept private, and a suitable encryption scheme may be used to protect the data's privacy.

B. Comparison with other models

This section compares the algorithms evaluated in MCC. We examine three mobile device attributes: I security, (ii) privacy, and (iii) MCC adaptability.

Method of Authentication	**Key Feature**	**Security**	**Privacy**	**MCC adaptability**
Multi-Factor	Uses various factors like ID/password, speech recognition, IMEI/IMSI	High Quality	High Quality	Adequate
FDZ	Fuzzy vault, digital signature authentication, and zero-knowledge authentication	Fair	Moderate	Weak
Control-Based Biometrics	Biometric factor is user hand-writing	Very Low	Fair	Weak
QR-Code Based	The user's photo, ID, and password are converted to QR codes to save network traffic.	Fair	Fair	Good
SeDiCi 2.0	A zero-knowledge proof approach is used to secure user passwords.	Moderate	Fair	Moderate

V. CONCLUSION

A comparative evaluation of authentication strategies in MCC is presented in this review. The present authentication techniques in MCC are also assessed and analyzed. Compare the analysed algorithms in MCC based on three mobile device features such as security, privacy, and adaptation to the MCC environment. The assessment findings reveal that various crucial elements, such as user preferences, mobility, heterogeneity, mobile device features, and MCC-friendliness, must be taken into account when creating future authentication systems for MCC. The findings also indicate that hybrid adaptive approaches are the most suited authentication mechanism in MCC. The MCC authentication and authorization concerns were covered in this study, ranging from Cloud computing questions to particular MCC scenarios. We next explained the method we devised to address the security challenges that cloud-based apps confront. Additional work includes measuring and evaluating the suggested solution's performance, as well as improving it by integrating stronger mechanisms such as trustworthiness. Authentication is the most important procedure in MCC for maintaining end-user security and privacy. Although authentication is not a new concept in computing, it is still in its infancy in MCC owing to the specific characteristics, requirements, possibilities, and constraints that exist in mobile cloud environments.

VI. REFRENCES

1. A Review on Authentication Techniques in Mobile Cloud Computing ,International Journal of Engineering Research & Technology (IJERT)

DOI: 10.5281/zenodo.6361875

2. Rassan, Iehab AL, and Hanan AlShaher. "Securing mobile cloud computing using biometric authentication (SMCBA)." 2014 International conference on computational science and computational intelligence. Vol. 1. IEEE, 2014.
3. Schwab, David, and Li Yang. "Entity authentication in a mobile cloud environment." Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop. 2013.
4. Raut, Priyanka D., and Dinesh S. Datar. "REVIEW PAPER ON MOBILE CLOUD COMPUTING SECURITY." Compusoft 4.5 (2015): 1822
5. Authentication and Authorization Issues in Mobile Cloud Computing: A Case Study
   V. Carchiolo , A. Longheu , M. Malgeri , S. Ianniello, M. Marroccia and A. Randazzo