A Review on Authentication Techniques in Mobile Cloud Computing

Himadri Bhatt
M.E in Computer Engineering (Cyber Security)
Gujarat Technological University
Ahmedabad, Gujarat, India

Seema Joshi
Asst. Prof. Dept. of Cyber Security
Gujarat Technological University
Ahemedabad, Gujarat, India

***Abstract*— Mobile Cloud Computing (MCC) is a developing technology which attempts to mix the storage and processing resources of cloud environment with the dynamicity and accessibility of mobile devices. With the development of mobility and cloud computing, mobile cloud computing has introduced. The necessity of extendibility and on-demand self-service, it can provide the great infrastructure, platform and software services during a cloud to mobile clients through the mobile network. Therefore, cloud computing is predicted to bring an innovation in mobile computing, where the mobile devices can make use of clouds for processing, storage and other exhaustive operations. Security, particularly authentication in MCC may be a critical requirement in securing cloud based computations and communication. This review presents various authentication techniques in MCC and comparative analysis of authentication techniques based on security, privacy and adaptivity to MCC environment.**

Keywords—Cloud Computing, Mobile Cloud Computing, Cloud Security, Mobile Security

I. INTRODUCTION

User authentication in Mobile Cloud Computing is the process of validating the identity of the mobile user to ensure that the user is genuine to access mobile cloud resources [3]. Authentication as a critical aspect of security prosecution approaches in MCC is vital to protect users against existing security and privacy issues by preventing unauthorized access to the mobile cloud user information [4]. The security and privacy issues of mobile cloud users are the main hurdles to the successful and quick MCC deployment, which exist in three MCC components, namely cloud, wireless communication, and mobile device. Therefore, considering characteristics and computing limitations of mobile devices, effective and efficient MCC authentication solutions are expected to be lightweight with the least possible computing, memory, and storage. Some of the most important security threats to mobile users are information leakage, denial of service, malfunction of devices and theft or loss of the device [4]. Moreover, security threats found in mobile devices can manifest as attacks via the services offered through the wireless networks, including network profiling, information leakages by sniffing, session hijacking, and jamming [5].

The paper is divided into 6 Sections. Section 2 describes the basic concepts about cloud computing and mobile cloud computing. Section 3 represents various authentication approaches in mobile cloud computing. Section 4 describes comparison of evaluated authentication methods. Section 5 concludes about the paper.

II. EASE OF USE

A. Cloud Computing

The mobile cloud computing is a combination of the mobile internet and the cloud computing, which represents the future trends in the development of the cloud computing. Cloud computing may be a sort of computing during which dynamically scalable and sometimes virtualized resources are provided as a service over the web. Cloud computing is additionally called distributed computing over the network, i.e., the power to execute an application or a program on many computers at an equivalent time. Cloud services provide software and hardware from remote locations which are managed by third party to the individual or businesses [1].

The objectives of cloud computing are to extend capacity and capabilities at runtime without investing in new infrastructure, licensing new software, and training new employees. The services may be infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) [1].

There are many benefits of cloud computing such as it can be less expensive compared to buying software and hardware, it can be used from any computer or device with an Internet connection. The device does not need large internal storage system compatible with most computers and operating systems. Also, mobile devices (e.g., smartphone, tablet, PCs, etc.) are increasingly becoming an essential part of human life.

These mobile devices still lack in resources compared to a standard information-processing device like PCs and laptops. The solution to beat of those challenges is mobile cloud computing (MCC). Mobile cloud computing is that the cloud infrastructure where the computation and storage are moved faraway from mobile devices.

B. Mobile Cloud Computing

Mobile Cloud Computing may be a composition of mobile technology and cloud computing infrastructure where data and therefore the related processing will happen within the cloud only with the exception that they can be accessed through a mobile device and hence termed as mobile cloud computing [2].

In MCC, a shared pool of varied configurable cloud based computing resources is employed to improve mobile devices computing capabilities like executing resource thorough applications. The mobile devices are connected to the cloud-based resources dominantly through the risky channel of the Internet via the wireless medium, though Internet-free connection to nearby or private resources is also conceivable. Therefore, the remote computing and data transmission are completed in collaboration of mobile clients, cloud-based resources, and heterogeneous wireless technologies. The security issues as one of the important concerns in MCC.

The user authentication is very important to guard networks from different security threats. Successful adaptation of MCC highly requires robust and effective authentication solutions by which user can utilize the cloud based services for his or her mobile devices anywhere, anytime, from any mobile devices with low computing cost on the innate resources. The MCC authentication is different from a typical mobile device because in MCC environment, the mobile device connects to the Internet to perform authentication. Furthermore, the resource-thorough parts of authentication mechanism can be transferred and processed in cloud servers using a suitable algorithm.

III. AUTHENTICATION APPROACHES IN MCC

Classify authentication methods into two main categories, cloud-side and user-side authentication approaches. Each category is again divided into two sub-categories based on types of authentication credentials. The credentials is defined as a unique identifier that can be used for node authentication. There are two types of credentials based on this classification, identity-based and context-based credentials.

A. Cloud-side authentication methods

In cloud-side authentication, most of the authentication steps are processed in the cloud server. The cloud-based authentication methods are more flexible, efficient, and adjustable compared to other authentication methods because of using unlimited resources of cloud servers. Although, the cloud-based authentication introduces some benefits just in case of performance and usefulness, it introduces some security and privacy issues. The user's private authentication information like password and biometrics are highly exposed to risk. Therefore, robust authentication method may be a critical requirement for mobile cloud environment. Classify cloud side authentication methods into two groups of identity based and context based that are explained as follows.

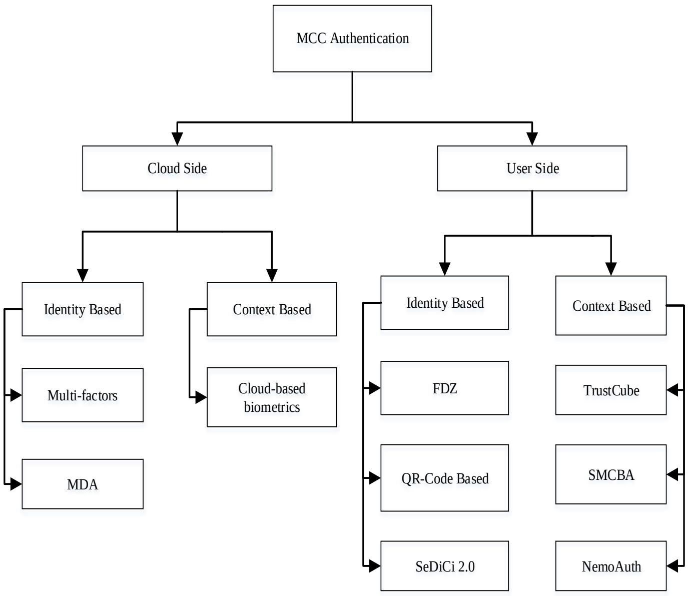

Fig. 1. MCC Authentications Approaches

1) Identity based authentication methods

In identity based authentication methods, users are authenticated through user identification attributes like unique ID, password and biometrics. However, the user attributes are usually fixed in this kind of authentication, which introduces some issues such as exposing private biometric information and user ID to different service providers leading to weakening their authentication power. Some of the most credible identity based authentication methods are describe below.

a) Multifactor based authentication

Different authentication features like basic ID/password, mobile number , various bio- information of users are combined to preserves security. This method improve the performance of authentication compare to other methods. However, the privacy issues of using biometric factors are neglected in security and privacy evaluation. The bio-information are very sensitive data that are recommended to be confidential and appropriate encryption algorithm can be applied to preserve the confidentiality of the data. Another security issue is that mutual authentication between MCC server and mobile users. The user can check authenticity of the MCC servers to prevent different attack such as man-in-middle, masquerading attack.

b) Message digest authentication

This method is based is designed based on existing mobile device hardware and platforms to protect mobile users against different potential security attacks. Digest authentication may be a method of authentication during which an invitation from a possible user is received by a network server then sent to a website controller. The domain controller sends a special key, called a digest session key, to the server that received the first request.

2) Context based authentication methods

In context based methods, the users are authenticated by analyzing multiple passive user information such as IP address, device location, and behavioral features of users. Analyzing the MCC user private information such as location, calling pattern, web searching patterns which can be used to improve the accuracy of context based methods, increases privacy issues.

a) Cloud-based biometric

Cloud based biometrics use user handwriting as an authentication factor to access the cloud securely. The mobile user writes his password manually using his smartphone touch screen and send the images to cloud server to be check the validity of password. The privacy risk for handwriting is lower than other biometrics, however the security using handwriting is low as well. if handwriting authentication fails, the system can ask for other methods.

B. User-side authentication methods

In user-side authentication methods, most of the authentication steps are processed in mobile devices. Transferring resource intensive processing tasks to the cloud as one of the main MCC goal contrast with the processing of the authentication mechanism inside the mobile devices in user side authentication methods, which makes the user side approaches less efficient and secure for cloud connected mobile devices compare to cloud side methods.

1) Identity based authentication methods

Similar to identity based methods in cloud side, authentication methods that use user identities. However, mobile devices processes and analyzer user attributes to check user authentication instead of cloud server. The private user identities such as biometrics are stored locally in the mobile device during authentication procedure in user side identity based authentication mechanism, which increase the privacy issues, especially in case of loss or stolen mobile device.

a) Fuzzy value, digital signature, and zero-knowledge combination

FDZ is based on zero knowledge proof authentication, digital signature and, and fuzzy value. Firstly, the secure encrypted channel between the mobile device and the server is created, then entity authentication will be processed. The authors used Diffie–Hellman key exchange protocol to create a shared Advanced Encryption Standard (AES) session key. In addition, RSA key pairs are used to protect the Diffie–Hellman key exchange against attacks especially man-in-themiddle attack, and fuzzy password are used to avoid some drawbacks of traditional password. This approach is resistant to some of the popular security treats and attacks such as impersonation, loss of device, man-in-the-middle, and reply attacks.

b) QR-code based

The QR code, which is typically a 2 dimensional code can be used for the authentication scheme in MCC. QR is a form of the matrix that allows quick decoding, utilizing a form of mass storage of high density and uses the reed-solomon error correction. In QR code based scheme, users are able to able to authorize a whole new set of information in contrast to information using a new form of data that has three types of QR code by changing the user's information to three different versions of QR code and keeping all the QR codes in a distributed format in the cloud server in circular method.

c) SeDiCi 2.0

The SeDiCi 2.0 protocol, which is another form of zero knowledge proof (ZKP) technique. This technique provides mutual authentication, which are supported to be more secure when it comes to phishing attack as compared to present system of using third party protocols. The main goal is to provide an improved solution for phishing attempts by offering mutual authentication, where users do not have to disclose their password at each of the websites that they visit. The user runs his authentication on the browser that domain is controlled trusted third party (TTP) and can login to the system if the name of a service is on the trusted list.

2) context based authentication methods

The context based methods in the user side analyze user behavior features, similar to the cloud side methods. The only difference between cloud side and user side context based authentication method is that the mobile device processes and evaluates user information instead of cloud server. Typically, a context based authentication needs more computational power compared to the identity based methods, and processing these kind of resource intensive mechanisms by mobile devices. Therefore, context-based user side authentication methods are less appropriate in MCC compared to cloud based methods, various kind of user's sensitive information are stored inside smartphones increases the user privacy risk due to device loss compare to more reliable cloud environment.

a) TrustCube

TrustCube is a cloud based authentication solution that is policy based and utilizes an open standard. In trustcube scheme the trusted network connect (TNC) protocol is used for authentication between the authentication server and the smartphone. TransCube supports a broad range of policies, including the platform, device's runtime environment and user. In TrustCube scheme, the Trusted Network Connect (TNC) protocol is used for authentication between the authentication server and the smartphone; the OpenID protocol is used to redirect service requests to the integrated authentication service. The Android is used for developing client agent because it can run a background monitoring service, and this ability is critical for data collection of implicit authentication.

b) Securing mobile cloud computing using biometric authentication (SMCBA)

SMCBA is a authentication algorithm based on fingerprint. In this method, the fingerprint image is captured by existing mobile device camera, which goes not need to implement sensors in the mobile device. The whole process of capturing and matching fingerprint is hosted on the cloud server to take all benefits from cloud. The main idea of this method is alike to other normal finger recognition methods that use mobile device camera to capture fingerprint.

c) NemoAuth

NemoAuth authentication is based on the mnemonic multimodal approach. NemoAuth utilizes different mobile device sensors such as gyroscopic, gravity, orientation, proximity, pressure, ambient light, temperature, touch screen, and moisture sensors as well as other facilities such as microphone and camera to measure and extract the biometric features of mobile device user. In general, the dynamic knowledge and biometric based approaches are combined to improve accuracy of authentication method in NemoAuth.

The main objective of the NemoAuth is to utilize different capabilities of the mobile device to improve the usability of authentication by using mnemonic images.

IV. COMPARISON OF EVALUATED ALGORITHM IN MCC

In this section, we present comparison of the evaluated algorithms in MCC. We evaluate based on the three mobile device characteristics: (i) Security (ii) Privacy (iii) adaptability to MCC environment.

Authentication Approaches	**Basic Concepts**	**Security**	**Privacy**	**Adaptability to MCC Environment**
Multi-Factor[8]	Using different authentication factors such as ID/Password, IMEI, IMSI and voice recognition	Good	Good	Moderate
MDA[9]	Message digest based algorithm	Good	Very Good	Good
Control-Based Biometrics[10]	User hand-writing as a biometric factor based authentication	Poor	Fair	Low
FDZ[11]	Authentication using digital signature, zero-knowledge authentication and fuzzy vault	Good	Good	Low
QR-Code Based[12]	The image, ID, and password of user are converted to QR code to reduce network traffic	Fair	Fair	Good
SeDiCi 2.0 [13]	Protecting user passwords using zero knowledge proof scheme	Good	Fair	Good
Trust Cube[14]	Trustcube is a cloud based authentication method that support using combination of different authentication methods	Poor	Good	Very Low
SMCBA[15]	Fingerprint recognition as an authentication factor for user authentication	Poor	Good	Low
NemoAuth[16]	The biometric knowledge like graphical password and biometric such as voice or face, are used together.	Poor	Good	Low

Fig. 2. Comparison of evaluated authentication methods

The results in this table advocate lack of adaptivity of current MCC authentication schemes for MCC ecosystem. Furthermore, most of these schemes are based on traditional methods that previous researchers recommended to be used in conventional mobile computing environment. In the other word, the proposed schemes hardly considered capabilities and limitations of mobile devices. The results of this comparison indicate that MCC-ready authentication methods are required to focus more on mobile-friendliness when exploiting cloud resources for mobile users.

V. CONCLUSIONS

In the core of MCC, authentication is the most critical process to preserve security and privacy of end- users. Although authentication is not new in computing, it is immature in MCC due to unique features, requirements, opportunities, and challenges existing in mobile cloud environments. Mobility, resource poverty, small form factor, and pervasive usability of mobile devices on one hand, and wireless communication, cloud resource provisioning, computation offloading, and heterogeneity on the other hand necessitate proposing authentication mechanisms that are developed for mobile users. In this review, we present a comparative study of authentication techniques in MCC. Furthermore, the existing authentication methods in MCC are evaluated and analyzed. Based on this, compare the evaluated algorithms in MCC based on three mobile device characteristics like security, privacy and adaptability to MCC environment. The results of the evaluation show that some important factors such as user preferences, mobility, heterogeneity, mobile device characteristics, and MCC-friendliness are highly critical to be considered when designing the future authentication mechanisms for MCC. The results also suggest that the most appropriate authentication method in MCC would be hybrid adaptive methods with varied degrees of fidelity that can be adopted depending on user location, Internet connectivity, native resource level, and remote resource proximity.

REFERENCES

[1] Taha, Ali Abdulridha, Diaa Salama Abd Elminaam, and Khalid M. Hosny. "An improved security schema for mobile cloud computing using hybrid cryptographic algorithms." *Far East Journal of Electronics and Communications* 18.4 (2018): 521-546.

[2] Raut, Priyanka D., and Dinesh S. Datar. "REVIEW PAPER ON MOBILE CLOUD COMPUTING SECURITY." Compusoft 4.5 (2015): 1822.

[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] Park, Ji Soo, Ki Jung Yi, and Jong Hyuk Park. "SSP-MCloud: A study on security service protocol for smartphone centric mobile cloud computing." IT Convergence and Services. Springer, Dordrecht, 2011. 165-172.

[5] Khan, Abdul Nasir, et al. "A study of incremental cryptography for security schemes in mobile cloud computing environments." 2013 IEEE Symposium on Wireless Technology & Applications (ISWTA). IEEE, 2013.

[6] Jalan, Shraddha A., and Vaishali B. Bhagat. "Mobile Cloud Computing An Efficient Technique For Mobile Users." International Journal of Computer Science and Mobile Computing 3.3 (2014): 145-154.

[7] Omri, Faten, et al. "Cloud-ready biometric system for mobile security access." International Conference on Networked Digital Technologies. Springer, Berlin, Heidelberg, 2012.

[8] Jeong, Young?Sik, Ji Soo Park, and Jong Hyuk Park. "An efficient authentication system of smart device using multi factors in mobile cloud service architecture." International Journal of Communication Systems 28.4 (2015): 659-674.

[9] Dey, Saurabh, Srinivas Sampalli, and Qiang Ye. "Message digest as authentication entity for mobile cloud computing." 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC). IEEE, 2013.

[10] Barra, Silvio, et al. "Cloud-based biometrics (biometrics as a service) for smart cities, nations, and beyond." IEEE Cloud Computing 5.5 (2018): 92-100.

[11] 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.

[12] Carchiolo, V., et al. "Authentication and Authorization Issues in Mobile Cloud Computing: A Case Study." (2019).

[13] Grzonkowski, S?awomir. "Sedici: an authentication service taking advantage of zero-knowledge proofs." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2010.

[14] Chow, Richard, et al. "Authentication in the clouds: a framework and its application to mobile users." Proceedings of the 2010 ACM workshop on Cloud computing security workshop. 2010.

[15] 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.

[16] Le, Zhengyi, Xinwen Zhang, and Zeyu Gao. "NemoAuth: a mnemonic multimodal approach to mobile user authentication." 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013). IEEE, 2013.