MOBILE CLOUD COMPUTING: SECURITY AND PRIVACY CHALLENGES

By Marc-Landry DJAMOU
Candidate for the Executive Master in Cybersecurity

Advisor : Professor Bernardo PALAZZI

Contents

Executive Summary

Mobile devices such as smartphones have replaced Personal Computers (PCs) to become the primary computing devices for many users due to the rapid advance of mobile computing technology and wireless networks. However, smartphones have limited capabilities that can be effectively mitigated through the use of cloud computing. This combination of mobile computing, cloud computing and wireless networks, has given rise to a new paradigm: Mobile Cloud Computing (MCC).

Mobile Cloud Computing integrates mobile computing and cloud computing aiming to extend mobile devices capabilities. This brings great research and business opportunity for applications developers, mobile networks operators (MNOs), cloud service providers (CSPs) and smartphones manufacturers.

Unfortunately, being in a very nascent stage, mobile cloud computing has some privacy and security issues which deter the users from adopting this technology. This paper addresses the security and privacy challenges in mobile cloud computing with a special focus on enhancing the end-user cybersecurity awareness. Our approach is as follows; we will first give a succinct overview of mobile cloud computing, then present the security and privacy requirements for mobile cloud computing, outline the security and privacy threats for each component of this technology and, finally, make suggestions to mitigate these vulnerabilities. In addition, we will provide a cybersecurity checklist for mobile cloud users in order to enhance their cybersecurity awareness through self-assessment as well as initiate some guidance for applications developers, MNOs and CSPs.

Keywords: *mobile cloud computing, cloud computing, wireless networks, security and privacy, mobile devices, end-users.*

I. Introduction

Smartphones are becoming an essential part of human life as the most effective and convenient communication tools. Users now prefer smartphones compared to the traditional cell phones and personal computers. As per the Mobility Report of November, 2015 from Ericsson, by 2021, the number of smartphones users will reach 6.4 billion [1]. The rapid expansion of mobile computing becomes a powerful trend in the development of Information Technology (IT) in general. However, the users of mobile devices face many challenges in their storage and processing capabilities. The limited resources significantly impede the improvement of quality of services. Nevertheless, these limited capabilities are mitigated by integrating mobile computing into cloud computing and hence a new paradigm of computing called mobile cloud computing (MCC) emerges.

Mobile Cloud Computing (MCC) combines cloud computing, mobile computing and wireless networks to bring rich computational resources to mobile users. The ultimate goal of Mobile Cloud Computing is to enrich mobile users' experience. Mobile Cloud Computing provides also business opportunities for mobile network operators as well as cloud providers.

However, mobile cloud computing suffers from several security and privacy challenges that deter mobile users from effectively adopting this new and interesting technology.

This paper addresses the security and privacy challenges in mobile cloud computing with a special focus on mobile users' cybersecurity awareness. The remainder of this paper is organized as follows: section II provides a brief overview of MCC; section III considers the security and privacy requirements in mobile cloud computing; section IV details the security and privacy threats in mobile cloud computing for mobile users and suggest some solutions to mitigate these issues and finally propose a security and privacy checklist for mobile users and section V concludes the paper.

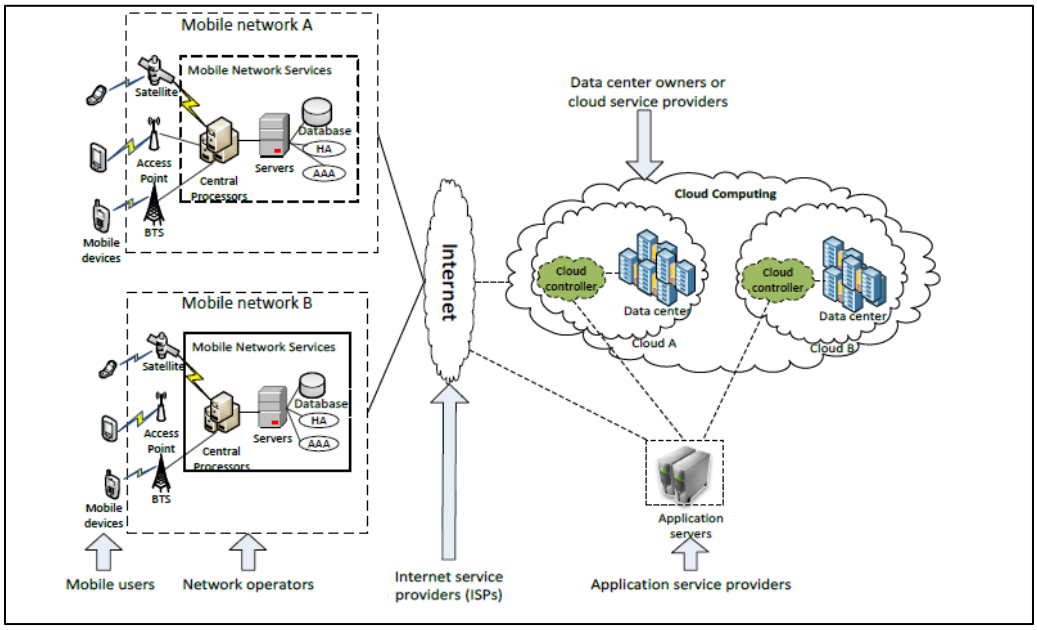
II. Overview of Mobile Cloud Computing (MCC)

1. Definition

The term "mobile cloud computing" was introduced in 2009 after the concept of "cloud computing" had been launched in mid-2007. The Mobile Cloud Computing Forum defines MCC as follows [2]: "Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers". To simplify we have this expression:

MCC = mobile devices + wireless networks + cloud computing

2. Architecture [3]



This MCC architecture shows that mobile devices are connected to the mobile networks via base stations (e.g., base transceiver station (BTS), access point, or satellite) that establish and control the connections (air interface) and functional interfaces between the networks and mobile devices. Users have access to internet through mobile networks and then benefit from the wide range of advantages offered by the cloud (storage, processing servers, and virtualization)

III. Security and privacy requirements for MCC

The security and privacy requirements for MCC may be categorized in the following way [4]:

- **Confidentiality**: In MCC, confidentiality is a fundamental requirement that refers to keep mobile users' data secret either in transit or at rest. Users do not want their personal data use or access by unauthorized parties.
- **Integrity**: In MCC, the data storage and processing reside on the service provider's end. Here, the integrity needs to ensure the accuracy and consistency of users' data. In other words, the integrity prevents data tampering by any unauthorized users or systems.
- **Availability**: For MCC, the availability ensures that all services (Mobile networks and cloud) remain constantly available for users. Ensuring availability includes preventing different kinds of availability attacks, which may delay, alter or interrupt the availability of services.

IV. Contributions

A. Security and privacy threats to mobile cloud computing

Security and privacy in MCC are intrinsically linked since security vulnerabilities in the mobile cloud computing paradigm will surely lead to a privacy breach. Security and privacy risks in mobile cloud computing are inherited from cloud computing threats. Moreover mobile cloud computing users are exposed to additional threats related to mobile devices and mobile networks. In this section, we will present the threats to each component of the mobile cloud computing paradigm: mobile devices, mobile networks and cloud computing.

1. Mobile devices

In today's "always-stay-connected" world, smartphones are used for wider range of activities such as banking, storing sensitive and valuable data. This extended range of functionalities leads to new security threats.

a. Physical threats[5]

Smartphones run programs and store sensitive and valuable data; thus these devices are targeted by adversaries who want to steal them in order to access sensitive data, e.g., personal messages in online social networking application, access the contacts list and get the smartphone itself as a valuable device. Further, the loss of mobile devices may lead to data loss and breach of personal data for their users and for companies as well [6]. For instance, McAfee reports that [7] "Four in 10 organizations have had mobile devices lost or stolen and half of lost/stolen devices contained business critical data". Therefore physical threats to mobile devices should be taken very seriously.

b. Malware[7]

Malicious Software (Malware) always operates in a way that is unknown to the user. By this means the malware gets the illegal access to the personal information and can even lead to certain actions without user's interaction. Because of this, the user of the mobile terminal could suffer from many risks such as information leakage. This illegal software installed not by the user is used for all attacks coming from the outside taking advantage of the vulnerabilities in smartphone's system. The current platforms ask users to make the decision about access. For example, iOS asks users to give minimum permissions to the application at the installation time, and later it asks whether an application may access other feature such as location, and Android asks them to grant all the

permissions before at the installation time. Unfortunately, such permission-granting create some critical threats to mobile users. The majority of these permissions is often ignored or not understood by users and permission prompts are disruptive to the user's experience. As a consequence users unintentionally grant applications more permissions than necessary and become vulnerable to applications that use the permissions in malicious or questionable ways (i.e., secretly sending SMS messages or leaking location information). The major ones of malware are Trojans, Worms, Virus and Spyware.

c. Mobile applications vulnerabilities [8]

Most applications installed on the user's mobile device are third party applications. These applications if they are not checked and patched regularly could be vulnerable to malicious attacks such us code injections, which in turn could lead to sensitive data leakage and even cause more damage to mobile users. Moreover, security teams for both Google and Apple have been quietly removing an undisclosed but increasing number of applications from their stores, but they haven't revealed a list of the removed applications or offered any reason for their removal.

d. Others

Besides the aforementioned security issues in the mobile terminal, mobile users may be contributing to other security issues. First of all, there is the lack of security awareness and good security hygiene from the mobile users. For instance, they could install unlicensed applications on their smartphones without a prior assessment of the risks these applications could pose to the valuable information stored on their devices.

2. Mobile networks [9]

Mobile network-based security threats usually target the Radio Access Network (RAN) which is the interface between mobile devices and the cloud. This interface is generally composed of Radio Base station (RBS) and Base Station Controller (BSC) in the case of 2G networks, or NodeB/eNodeB in the case of 3G/4G mobile networks for example. This may also refer to traditional Wi-Fi. Major Attacks in this category include Wi-Fi sniffing, Denial of Service (DoS) attacks, man-in-the-middle attack, and Distributed Denial of Service using compromised mobile devices (Botnets).

3. Cloud computing

Threats to the cloud can be grouped regarding the impact they have on Confidentiality, Integrity and Availability (CIA triad) of users data. The cloud platform is susceptible to being attacked because of its high concentration of information resources of users. First of all, major threats to confidentiality are achieved by insiders and external attackers. The ultimate goal of the malicious attacker is to steal valuable information or sabotage service. These attacks perhaps come from malicious outside, legal cloud computing user, or inside staff of the cloud computing operators. Second, data integrity in the cloud is an imperative because it is frequently targeted by malicious attackers. For instance, the implementation of poor access control procedures creates risks to data integrity since any individual who can manage to break into the system can tamper with the data or even worst delete the data. Third, Availability is really vital given how dependent on users have become to cloud services. This tenet is also targeted by attackers who are seeking to interrupt the service to users. For example, Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks will destroy the platform availability and

close the service of the cloud to legitimate cloud users. When users deliver all their data to the cloud service providers without selecting the expensive backup and disaster recovery service, they will have to cope with the risks of the data loss. Further, the fact that cloud service providers store users data all over the world and that users do not know exactly where their data is located poses serious concerns regarding privacy.

B. Suggestions

1. Mobile devices

The outlined threats to mobile devices especially smartphones will negatively impact mobile users if they are not addressed seriously. First of all, users need to be educated about security, not at the security experts level but at least they should get the basics. They should never leave their devices unattended. However, devices can be lost, misplaced or stolen so users should activate lock screen and protect their phones with strong passwords such as 10+ characters passwords with uppercase, lowercase letters, numbers and special characters. Further, they should use biometrics authentication on their devices. Second, users should install only applications available on stores like App store and Play store; they should be careful about the permissions they will grant to the applications as well as grant only minimum permissions to the applications in order to ensure their security and protect their privacy; it is vital for users to do some research before installing any application on their phone. Additionally, they should always update their applications and uninstall the ones that they don't use anymore. Third, they should install anti-malware on their phones and keep them up to date. Beware also of phishing attacks and do not trust spam emails, link from an advertisers, messages from friend's social account that could probably be hacked etc., because by clicking on a link it

will redirect you to an infected website. Thus it is very important to not click on short, suspicious links for which you did not request. Attackers can use phishing techniques to steal your money, your identity and open credit card accounts in your name and much more. Even the strongest antivirus will not protect you from phishing and all malicious software. They should be sure that they are connected only to secure wireless connection, which means to not use free or public Wi-Fi, especially when they are accessing and/or transmitting sensitive data because information sent via public networks can be easily accessed by attackers since they are sent in plain text.

2. Mobile networks [10]

The threats to mobile networks can be mitigated by engaging mobile networks operators to enhance the security of their networks. However, as this paper is mainly focuses on the end-users, therefore the suggested solutions are to help them prevent some attacks mentioned previously. The mobile users should maintain a good security hygiene of their devices; this security hygiene starts by keeping their operating systems and applications up to date and by being cautious and skeptical regarding applications and links suspicious or not that they receive on their devices, that will prevent some attacks such as Distributed Denial of Service (DDoS) on mobile networks using compromised mobile devices to launch botnets attacks. For threats such as man-in-the-middle attacks, eavesdropping and Wi-Fi-sniffing, the suggested mitigations in the literature advise the implementation of encryption to the air interface, authentication and digital signatures by the mobile networks operators in order to ensure the privacy and security of the mobile users. Additionally, for Denial of service Attacks it is required that the mobile networks operators strictly apply the security best practices such as patches installation,

vulnerability scanning, intrusion detection and prevention systems, authentication etc. Finally, with the upcoming 5G (5th Generation of mobile networks), some researchers are investigating the C-RAN and chances are that it will both enhance the end-to-end security and quality of service (QoS) in mobile networks thus impacting the mobile cloud computing users [11].

3. Cloud Computing

Like mobile networks operators, cloud service providers (CSP) have to implement the security best practices in order to ensure the confidentiality, integrity, and the availability of the mobile users' data. These best practices include keeping systems patched, implementing prevention and detection techniques to mitigate DoS attacks, also the implementation of strong authentication mechanisms incorporating multi-factor authentication (MFA) to avoid some malicious activities from intruders. The users data should be encrypted at rest, in process and in transit to ensure both the integrity and the confidentiality of the data. Moreover, cloud services providers should clearly inform the mobile users concerning the exact location(s) of their data as well as the mechanisms put in place to protect them. Mobile users for their part, should always maintain a good cybersecurity hygiene i.e. install patches of firmware and applications. Regarding security savvy end-users, there is a data integrity mechanism called the Merkle Tree, which they could use to verify the integrity of the data they stored in the cloud.

C. Security and privacy checklist for mobile cloud computing users

This section will provide a security and privacy checklist for mobile cloud users. Our expectation is that based on this checklist mobile users would instill mobile networks

operators, cloud service providers and also applications developers to provide a sort of minimum accepted service level based on users' security and privacy requirements. This checklist also responds to the security and privacy requirements in mobile cloud computing: Confidentiality, Integrity, and Availability described in section III.

We also think that this checklist would have a great impact on the way things are approached in the realm of mobile cloud computing because it will develop users' cybersecurity awareness. Obviously, this list of questions is not exhaustive; it is based on some telecommunications engineers and cybersecurity experts' experiences on the matter.

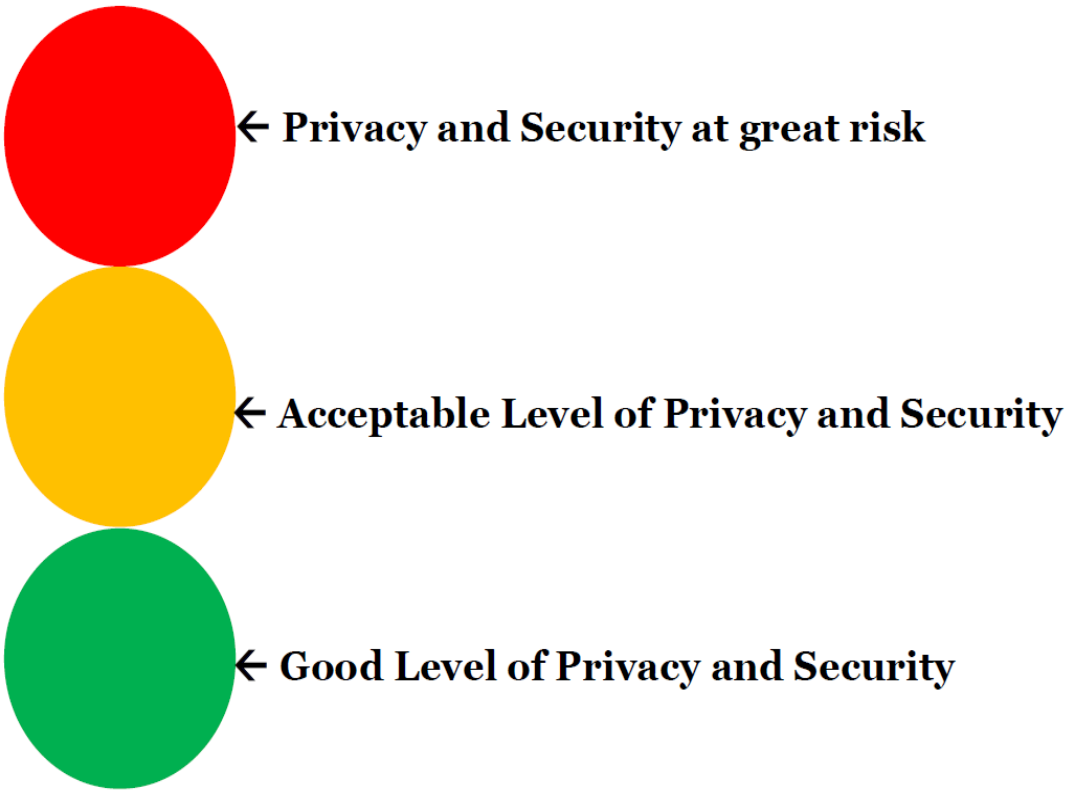
Mobile Devices	YES	NO	DON'T KNOW
1-Is your smartphone access protected with 10+ characters password and biometrics?			
2-Do you share your passwords with relatives?			
3- Is your smartphone firmware up to date?			
4- Are your mobile applications up to date?			
5- Do you have anti-malware software on your smartphone?			
6- Do you use 2-factor/Multi-factor authentication for your applications dealing with sensitive data (i.e. email, banking etc.)			

7- Do you install licensed applications and download them from trusted sources?			
8- Do you verify and understand the permissions asked by the applications before granting them?			
9- Are your location based services only activated while using General Positioning System (GPS) applications?			
10- Do you read the application description or research information on the application before installing it?			
Mobile Networks	YES	NO	DON'T KNOW
11- Are your messages transmitted through the Air interface protected by the use of encryption?			
12- Do you use only secure trusted wireless networks to access internet?			
13-Do your service provider maintain a very good coverage and availability even in bad weathers (storm, rain etc?)			
Cloud Computing	YES	NO	DON'T KNOW
14- Is your Cloud service provider certified ISO 27001/27002/27018?			

15- Do you know the exact location(s) where your cloud service provider stores your data?			
16- Are integrity verification mechanisms such as Merkle Tree implemented for the user to verify data integrity?			
17- Is the data encrypted at rest, in process and in transit?			
18- Is a Disaster recovery/Business continuity plan set up to ensure availability in the case of natural disasters or man-made sabotages?			
19- Do you have a cloud privacy policy in simple terms addressing how your data will be handled by the cloud service provider?			

Regarding the checklist response analysis, it is important to have "Yes" on each question to ensure a good level of privacy and security (**Green light**). In our analysis, in those cases where the respondent replies with "No" or "Don't know"; he/she should clearly be cautious and skeptical, and review if there is alternative features that covers this aspect of the service. However, we determine that for users to enjoy mobile cloud computing services with security and privacy, they should always avoid the **red bubble** as described in the classification table below:

At least one question addressing any of these aspects is not marked "YES"	At least one question addressing any of these aspects is not marked "YES"	All questions are marked "YES"
(1) 2/Multi-Factor authentication	(1) Anti-malware software	
(2) Firmware and applications updates	(2) Locations based services	
(3) Encryption of users data (transit/at rest)	(3) Privacy policy in simple terms	
(4) Data integrity verification mechanisms	(4) Disaster recovery plan	
(5) Permissions.		



V. Conclusion

Mobile Cloud computing is a very interesting technology that has changed the way users behave; they don't need to have traditional Personal Computers (PCs) to perform multiple activities such as online banking, storing videos and photos etc. However, privacy and security constitute a challenge for mobile users because they would like to benefit from advantages offered by mobile cloud computing while preserving the confidentiality, integrity and availability of their data.

This paper outlines the security and privacy requirements of mobile cloud computing. It also provides a cybersecurity checklist for mobile users. This checklist is for mobile users' self-assessment before opting for mobile cloud computing services. Additionally, this checklist will enhance mobile users' cybersecurity awareness and foster the establishment of thresholds regarding users' privacy and security to be met by mobile networks operators, cloud service providers and applications developers, which hopefully would make a more privacy and security oriented technology.

This study could be extended to other mobile devices such as medical devices that are really sensitive to confidentiality and integrity since when we talk about health accuracy and consistency are crucial because a simple modification of health data can cause people death.

References

[1] https://www.ericsson.com/assets/local/news/2016/03/ericsson-mobility-report-nov-2015.pdf

[2] http://www.mobilecloudcomputingforum.com/

[3] http://onlinelibrary.wiley.com/doi/10.1002/wcm.1203/abstract A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches, by Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang

[4] Security and privacy challenges in mobile cloud computing: Survey and way ahead, by Muhammad Baqer Mollaha, Md. Abul Kalam Azada, Athanasios Vasilakosb

[5] Survey: Data Protection in Smartphones Against Physical Threats, by Ildar Muslukhov

[6] Smartphone Security Threats, by Esmeralda Kadëna

[7] https://www.mcafee.com/us/about/news/2011/q2/20110523-01.aspx

[8] A Critical Overview of Latest Challenges and Solutions of Mobile Cloud Computing, by Hesham Allam, Nasser Nassiri, Amala Rajan, Jinesh Ahmad

[9] 5G Security: Analysis of Threats and Solutions, by Ijaz Ahmad, Tanesh Kumary, Madhusanka Liyanagez, Jude Okwuibex, Mika Ylianttila{, Andrei Gurtov

[10] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf Guide to LTE Security

[11] Dynamic Operations of Cloud Radio Access Networks (C-RAN) for Mobile Cloud Computing Systems, by Yegui Cai, F. Richard Yu, *Senior Member, IEEE*, and Shengrong Bu, *Member, IEEE*