Buletinul Ştiinţific al Universităţii "Politehnica" din Timişoara

Seria ELECTRONICĂ şi TELECOMUNICAŢII
TRANSACTIONS on ELECTRONICS and COMMUNICATIONS

Tom 58(72), Fascicola 1, 2013

Overview on Mobile Cloud Computing Security Issues

D. Popa[1] K. Boudaoud[2] M. Cremene[1] M. Borda[1]

Abstract – Mobile Cloud Computing, the combination of mobile devices with Cloud Computing services. It brings several advantages to the devices with low resources; advantages that lead to the development of rich functionality applications. The security issues in Mobile Cloud Computing can be classified as follows: mobile threats and cloud threats. The main purpose of these menaces is to steal personal data (e.g. credit card numbers, passwords, contact database, calendar, location) or to exploit mobile device resources. This paper is an overview on Mobile Cloud Computing security issues.

Keywords: Mobile Cloud Computing, Security Issues

I. INTRODUCTION

Just a short time ago a user was only expecting from her/his mobile phone to allow her/him to perform activities using just the device resources (e.g. to take pictures and save them locally on the device, or to read different types of files that were saved locally).
Today, the same user wants to be able to take advantage of powerful and complex applications that manipulate not only the mobile local resources but also external resources as computation power and storage place. To obtain these types of performances several improvements have been made in the domains of mobile hardware and network [1]. Even with those improvements mobile devices still have a lack of resources and energy, an unstable connectivity and introduce several security issues.
To resolve some of these issues, the concept of Mobile Cloud Computing has been proposed as a solution where the Cloud is used as a platform to execute mobile applications. Mobile Cloud Computing as a term was born shortly after the emergence of Cloud Computing model in 2007 [2]. Marketing research [3] stated that in 2015 there would be more than 240 million customers using Mobile Cloud Computing services while in 2008 there were only 42.8 million customers.
Thanks to the emergence of Mobile Cloud Computing different novel mobile applications models have been defined where the Cloud is used to overcome the limitations imposed by mobile devices such as processing power, memory capacity and display size.
Mobile devices are vulnerable to numerous security threats that aim the theft of users' data. Moreover Cloud Computing introduces several security, privacy and trust issues regarding the data stored in the Cloud. Consequently to maintain consumer's trust in mobile platforms more specifically in mobile cloud applications, it is important to secure data that will be used and processed by mobile cloud applications.
In this paper we present an overview of Mobile Cloud Computing security issues. The paper is organized as follow. Section II presents what Mobile Cloud Computing is, by showing several main characteristics described in various papers. In Section III, there is presented the overview on Mobile Cloud Computing security issues, namely the mobile threats and the Cloud threats. Finally, in section IV, several conclusions are presented.

II. WHAT IS MOBILE CLOUD COMPUTING?

In order to answer the question raised in the section title, it will be presented in the following, several definition and characteristics of Mobile Cloud Computing along with the mobile cloud applications models.

A. *Definitions*

Mobile Cloud Computing (Fig.1) is a new concept that can be described as the availability of Cloud Computing resources and services for mobile devices. As in the case of Cloud Computing, several definitions were proposed to define Mobile Cloud Computing.

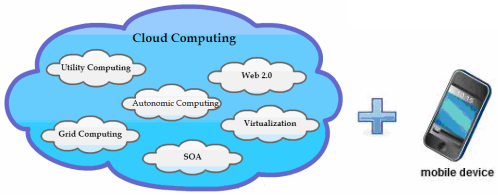

Fig.1 Mobile Cloud Computing

[1] Technical University of Cluj-Napoca, Communications Department,
Str. Dorobantilor. 71-73 CP. 400609 Cluj-Napoca, Romania, Daniela.Popa@com.utcluj.ro
[2]University of Nice Sophia Antipolis,
930 Route des Colles - BP 145- 06903 Sophia Antipolis

BUPT

As in the case of Cloud Computing, there are several opinions on what Mobile Cloud Computing is. There is not a consensual definition for Mobile Cloud Computing.

Mobile Cloud Computing is defined in [4] as follows:
"*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 smart-phone users but a much broader range of mobile subscribers.*"
Another definition given in [5]:
"*Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions, while preserving available sensing and interactivity capabilities of mobile devices.*"

The first definition emphasizes that Mobile Cloud Computing benefits from Cloud Computing features – storage and data processing, and also reveals a Mobile Cloud Computing characteristic – moving part of the computation and the storage away from mobile phones.
The second definition is more concise. It starts by saying what is Mobile Cloud Computing – a model; it also tells the purpose of using Mobile Cloud Computing – to overcome the mobile device challenges; it tells the way – using storage and computation resources offered by Cloud Computing model; it also specifies that is appropriate to take into account the context of the mobile operating conditions.

As a conclusion, we can say that Mobile Cloud Computing offers Cloud Computing resources such as storage and computations to the mobile devices with limited CPU speed, memory capacity and display size which allows the development, deployment and execution of powerful mobile applications.

III. MOBILE CLOUD COMPUTING - SECURITY

Mobile Cloud Computing exposes private data of the mobile user to different security risks. User's data can be stored on the mobile side or on the Cloud side, can be accessed by applications (or application components) running on the mobile device or in Cloud, or can be transmitted between the mobile device application components and Cloud application components.
This section presents in the first part the security issues related to Mobile Cloud Computing and highlights in the second part the state of the art work proposed to address these security issues.

As we have said previously, Mobile Cloud Computing is a combination of mobile and Cloud Computing. Thus, the security issues in Mobile Cloud Computing are due to the security threats against the Cloud, the mobile devices and the applications running on these devices. These threats can be classified as follows: mobile threats and cloud threats. The main purpose of these menaces is to steal personal data (e.g. credit card numbers, passwords, contact database, calendar, location) or to exploit mobile device resources.

A. Mobile Threats

A little while ago the malware development for mobile devices was seen as a myth due to their limitations in terms of hardware and software.

Table 1. Key Characterisitcs of Mobile Cloud Computing

Characteristics/ Papers	**Model**	**Combination**	**Outside device processing**	**Outside device storage**	**Elasticity**	**Remote access**
R.D.Caytiles [6]	X	X	X	X		
A. Khan [7]	X		X	X		X
S.K.Ko [8]		X				X
H.T.Dinh [9]		X	X	X		
AEPONA [5]	X		X	X	X	
MCCForum [4]	X		X	X		
J.H.Christensen [10]	X	X				
A.N.Khan [11]			X	X	X	X
H.Qi [12]	X	X	X	X		X
N.Fernando [13]	X	X	X	X	X	X

BUPT

Nowadays, the increasing use and development of mobile devices (e.g. smartphones) has lead to the evolution of mobile threats; from the first case of malware on mobile devices in 2004 targeting Symbian, to the code of DroidDream, DroidKungFu and Plankton discovered in 2011 in the official Android Market [14].

Recent studies [15], [16] have classified mobile attacks in several categories such as: application based attacks, web-based attacks, network based attacks and physical based attacks.

The application based attacks concern both offline and online applications. In these kinds of attacks are included: malware, spyware and privacy threats.

- Malware is software that performs a malicious behavior on a device without the user being aware of this behavior (e.g. sending unsolicited messages and increasing the phone's bill or allowing an attacker to have the control over the device).
- Spyware is software designed to collect private data without the user's knowledge (e.g. phone call history, text messages, camera pictures).
- Privacy Threats are caused by applications (malicious or not), that in order to run they need more sensitive data such as location (e.g. location based applications).

The web-based attacks are specific to online application and include: phishing scams, drive-by-downloads, or browser exploits.

- Phishing scams aim stealing information like account login and password.
- Drive-by-Downloads is a technique that allows the automatic download of applications when a user visits a certain web page.

In addition to these attacks, attackers use different techniques to obtain private data: repackaging, misleading disclosure and update.

- Repackaging was the most used technique in 2011 to infect applications running under Android [15]. In this kind of attack, an attacker takes a healthy application; modifies it with a malicious code and then republishes it. The main difference between the healthy and modified applications is that the last ones require more access control permissions such as to access the phone contacts or to send SMS messages.
- Misleading disclosure [15] is a technique used by an attacker to hide the undesirable functionality of an application, so that a user would not notice it and would agree to. The undesirable functionality is usually hidden in the applications terms and conditions. The attackers rely on the fact that usually the users do not pay attention to the applications terms and conditions while these are installed. Those applications are difficult to block or remove because they do not violate their own terms of service or any application market's user agreement.
- The update technique was recently used by malware writers as an attack method in Android Market [16]. Firstly, the malware writer publishes an uninfected application, than the application is updated with a malicious version. Using this technique, the attacker takes advantage of the users trust in the applications market. The number of infected devices increases; there are affected the users that only use the official market to download the applications. A consequence of this attack technique is a decrease of users' confidence in the application market. This may lower the market customers' number and therefore the market profits.

B. Cloud Threats

The Cloud acts as a big black box where nothing inside is visible to the clients. Therefore clients have no idea or control over what happens with their assets. Cloud Computing is about clients transferring the control of their resources (e.g data, applications) and responsibilities to one or more third parties (cloud services providers). This brings an increased risk to which client assets are greatly exposed.
Before Cloud's emergence, generally, the companies where keeping their data inside their perimeter and protecting them from any risks caused by malicious intruders. A malicious intruder was considered to be an outside attacker or a malicious employee. Now, if a company chooses to move its assets into the cloud, it is forced to trust the Cloud provider and the security solutions it offers when provided. However, even if the cloud provider is honest, it can have malicious employees (e.g system administrators) who can tamper with the virtual machines and violate confidentiality and integrity of client's assets.

In Cloud Computing the obligations in terms of security are divided between the cloud provider and the cloud user. In the case of SaaS, this means that the provider must ensure data and application security; so service levels, security, governance, compliance, and liability expectations of the service are contractually stipulated and enforced. In the case of PaaS or IaaS the security responsibility is shared between the consumer and the provider. The responsibility of the consumer's system administrators is to effectively manage the data security. The responsibility of the provider is to secure the underlying platform and infrastructure components and to ensure the basic services of availability and security [18].

Several analyses have been conducted to identify the main security issues regarding the Cloud Computing [17, 18, 19, 20, 21, 22, 23, 24, and 25]. Following these analyses, security issues have been classified in terms of concerns: domain concerns, services concerns, threats, actors concerns and properties concerns (Fig.2).

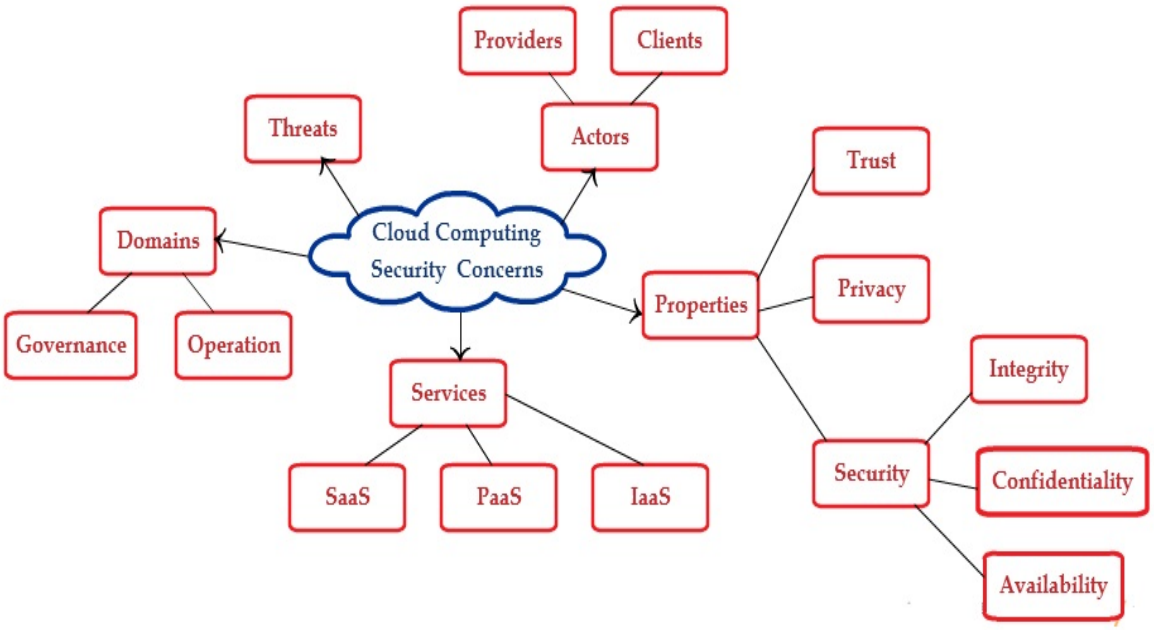

Fig.2 Cloud Computing terms of concerns

The domain concerns are divided in two types: 1) governance concerns and 2) operation concerns.

Governance addresses strategic and policy security issues within Cloud Computing [19]. The highlighted issues are: data ownership and data location. Data Ownership refers to the ownership of purchased digital data. Thanks to the Cloud it is possible to store purchased media files, such as audio, video or e-books remotely rather than locally. This can lead concerns regarding the true ownership of the data. If a user purchases media using a given service and the media itself is stored remotely there is a risk of losing access to the purchased media. The service used could go out of business, for example, or could deny access to the user for some other reasons [19]. Data location raises many issues because of the compliance problem of privacy laws that are different from a country to another. For example, the laws in European Union (EU) and South America are different from the laws in United States (US) regarding data privacy [18]. Under EU law [26] and South American law [27], personal data can be collected only under strict conditions and for a legitimate purpose. In the US, there is no all-encompassing law regulating the collection and processing of personal data [28].

Operation addresses technical security issues within Cloud Computing [19]; issues as: 1) the security of data stored into the Cloud, 2) the security of data transmitted between the Cloud services, 3) the security of data transmitted between the Cloud services and a mobile platform or 4) data access and integrity. If an application relies on remote data storage and Internet access in order to function then, any changes to these data can significantly affect the user.

Threats class identifies the main security issues an organization may face when it wants to move its assets into the Cloud. The main concerns mentioned are: data loss, unsecured applications interfaces, denial of services or malicious insider.

Actor class identifies the main security issues that may be caused by the Cloud provider, by the Cloud clients or by an outsider. Thereby, a Cloud provider may be affected by the malicious Cloud client's activities. The malicious Cloud clients can target honesty clients' data; they can legitimately be in the same physical machine as the target and they can gather information about the target. A Cloud client may be affected by the malicious Cloud provider. The malicious provider may log the client communication and read the unencrypted data; also it may peek into the virtual machines or make copies of the virtual machines assigned to run client assets. In this way a Cloud provider gain information about client data or behavior and sell the information or even use it itself. An outsider can affect a Cloud client. The outsider may listen to the network traffic or it may insert malicious traffic and lunch the denial of service attack.

Services class lists the security issues that may occur while using any of the Cloud provided services: SaaS, PaaS or IaaS. The fundamental security challenges are: data storage security, data transmission security, application security and security related to third-party resources [21].

The properties that bring out the security issues encountered in the Cloud are: the privacy, the security and the trust. Security in general, is related to the following aspects: data confidentiality, data integrity and data availability. Privacy is one of the significant concerns in Mobile Cloud Computing. For example,

BUPT

some smart phone applications use the Cloud to store user's data. The main risk in this context is that unauthorized people can access and get user's data. Another example concerns location-aware applications such as applications that finds nearby restaurants for the user; or applications that allows user's friends and family to receive updates regarding her/his location [29].

V. CONCLUSIONS

Mobile Cloud Computing is a model that can be described as the availability of Cloud Computing resources to mobile environments. From a security point of view, Mobile Cloud Computing introduces many security issues due to the fact that it combines mobile devices with Cloud services.

In this paper were presented the security issues that can jeopardize the Mobile Cloud users' private data or applications. The issues were divided in two types: mobile threats and Cloud threats. For each threats type were presented the security issues that may affect the data, the applications, the device (in the case of mobile threats) and the users' privacy. Also the paper presented an overview of the main Mobile Cloud Computing characteristics. Characteristics used to provide a definition for Mobile Cloud Computing.

ACKNOWLEDGMENT

This paper was supported by the project: Improvement of the doctoral studies quality in engineering science for development of the knowledge based society-QDOC" contract no. POSDRU/107/1.5/S/78534, project co-funded by the European Social Fund through the Sectorial Operational Prog. HR 2007-2013.

REFERENCES

[1] D. Kovachev, Yiwei Cao and Ralf Klamma. Mobile Cloud Computing: "A Comparison of application Models". In eprint arXiv: 1107.4940, July 2011.

[2] S.K.Sood, "A combined approach to ensure data security in cloud computing", in S.K. Sood/Journal of Network and Computer Applications Vol.35, pp. 1831–1838, 2012.

[3] S. Chetan, G. Kumar, K. Dinesh, K. Mathew and M.A. Abhimanyu "Cloud Computing for Mobile World", available online: http://chetan.ueuo.com/projects/CCMW.pdf, 2010.

[4] Mobile Cloud Computing Forum, available online: http://www.mobilecloudcomputingforum.com

[5] White Paper, "Mobile Cloud Computing Solution Brief," AEPONA, November 2010.

[6] R. D. Caytiles, S. Lee, "Security Considerations for Public Mobile Cloud Computing", International Journal of Advanced Science and Technology Vol. 44, July, 2012.

[7] A. Khan, K.K. Ahirwar, "Mobile Cloud Computing as a future of mobile multimedia database",, International Journal of Computer Science and Communication Vol. 2, No. 1, January-June, pp. 219-221, 2011.

[8] S.K. Ko, J.H. Lee, S.W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering, 2012.

[9] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", Accepted in Wireless Communications and Mobile Computing – Wiley, 2011, available online: http://onlinelibrary.wiley.com/doi/10.1002/wcm.1203/abstract

[10] J. H. Christensen, "Using RESTful web-services and cloud computing to create next generation mobile applications," in Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications (OOPSLA), pp. 627-634, October 2009.

[11] A. N. Khan, M.L. MatKiah, S. U. Khan, S. A. Madani, "Towards secure mobile cloud computing: A survey", Future Generation Computing Systems 2012, doi:10.1016/j.future.2012.08.003.

[12] H. Qi, A. Gani, "Research on Mobile Cloud Computing: Review, Trend and Perspectives".

[13] N. Fernando, S. W. Loke, W. Rahayu, "Mobile cloud computing: A survey", Future Generation Computer Systems, Vol. 29, pp. 84–106, 2013.

[14] C.A. Castillo, "White Paper: Android Malware Past, Present and Future", Mobile Security Working Group, McAfee, available online http://www.mcafee.com/us/resources/white-papers/wp-android-malware-past-present-future.pdf, 2011.

[15] Lookout Mobile Security, Lookout Mobile Threat Report, August 2011.

[16] C. Nachenberg, "A Window Into Mobile Device Security – Examining the security approaches employed in Apple's iOS and Google's Android", Symantec Security Response, available online: http://investor.symantec.com/files/doc_news/2012/symc_mobile_device_security_june2011.pdf, 2011.

[17] D. Catteddu, G. Hogben, "Benefits, risks and recommendations for information security", European Network and Information Security Agency, 2009.

[18] A. Archer "Boehm, Security guidance for critical areas of focus in cloud computing", Cloud Security Alliance, 2009.

[19] "Top threats to cloud computing", version 1.0, Cloud Security Alliance CSA, available online: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Retrieved March, 2010.

[20] "The Notorious Nine: Cloud Computing Top Threats in 2013", Cloud Security Alliance CSA, Top Threats Working Group, February 2013.

[21] L. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 2010.

[22] Open web application security project (OWSAP) Top 10, available online: https://www.owasp.org/index.php/Top_10_2010-Main, 2010.

[23] R. Choubey, R. Dubey, J. Bhattacharjee, "A survey on cloud computing security, challenges and threats", International Journal on Computer Science and Engineering Vol. 3, 2011.

[24] M. Pastaki Rad, A. Sajedi Badashian, G. Meydanipour, M. Ashurzad Delcheh, M. Alipour, H. Afzali, "A survey of cloud platforms and their future", Computational Science and Its Applications—ICCSA 2009, pp. 788–796, 2009.

[25] S. Srinivasamurthy, D. Liu, "Survey on cloud computing security", 2010.

[26] EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. L 281

[27] Personal Data Protection Act No. 25,326, (Arg.), available online www.privacyinternational.org/countries/argentina/argentine-dpa.html, Oct. 4, 2000.

[28] International Due Diligence: U.S. vs. European Privacy Laws Kroll an altegrity Company, available online: http://www.kroll.com/media/pdfs/International_Due_Diligence_US_vs_Euro_WP_040811P.pdf

[29] H. Zhangwei and X. Mingjun, "A Distributed Spatial Cloaking Protocol for Location Privacy," in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468, June 2010

BUPT