PERSONALIZED SECURITY MECHANISM FOR MOBILE CLOUD APPLICATIONS

D. POPA[1] K. BOUDAOUD[2] M. CREMENE[1] M. BORDA[1]
[1]*Communications Department, Technical University of Cluj-Napoca, Romania*
Str. Dorobantilor. 71-73, Tel/Fax: +40(0)264401575, {Daniela.Popa, cremene, Monica.Borda}@com.utcluj.ro
[2]*I3S-CNRS Laboratory, University of Nice Sophia Antipolis, France*
930 Route des Colles - BP 145- 06903, Tel(Fax): +33(0)492965172(55), karima.boudaoud@unice.fr

Abstract: Mobile Cloud Computing is a model that brings several advantages to the applications developed for mobile devices. In this paper, we focus on securing data used and processed by component-based mobile cloud applications. We first show some criteria that may affect the security properties (e.g. integrity, confidentiality and authenticity) applied to a component-based mobile cloud application data. Then, we describe a security solution that takes into account these criteria.

Keywords: *Mobile Cloud Computing, Applications, Security*

I. INTRODUCTION

Mobile Cloud Computing is a model [1] that proposes the use of Cloud Computing in combination with mobile devices. This combination brings several advantages for the mobile world. The advantages are due to the fact that Cloud Computing provides on-demand computing services. Furthermore, the services provided can be employed by different types of client platforms (e.g., smart-phones, laptops).

Mobile devices have downsides regarding the hardware resources, energy reserves, connectivity and security. When using services provided by Cloud Computing, mobile phones are overcoming some of the limitations and becoming more powerful. Nowadays mobile phones can see, hear, and sense their environment [2]. The complex applications developed for mobile phones also enable users to both keep in touch with others and to manage everyday tasks. They easily provide to the users a variety of complex features and characteristics such as: managing personal health, games, editing, making reservations and paying tickets [3].

New techniques like augmented execution, elasticity and mobility [4], are used to ameliorate the mobile cloud applications models. These techniques attempt to improve the application models so that they can take advantages from both mobile device and Cloud resources. A comparison between the novel applications models is made in [4]. The idea behind the new applications models is to separate an application into components. A component may run in the Cloud, on the mobile device or it can migrate. This separation can be made at code development level, like in elastic applications model proposed in [5], or at architectural level, like in rich applications model proposed in [6].

What about the security?

As we said before Mobile Cloud Computing is a combination between mobile devices and Cloud services. Thereby the security threats fall into one of these three categories: mobile threats [7], Cloud threats [8] and threats at the communication channels level.

What interests us is the security of data transmission, more specifically, the security of private data transmitted between the components of the same mobile cloud application. In our work, we focus on the adaptation of security according to end-user needs and mobile devices constraints. Furthermore, we assume that there is no need to apply the same security level (i.e. same security properties) for all data transmitted between the mobile cloud application's components.

Usually, security solutions proposed by service and Cloud providers to secure data transmission consist of security protocols such as SSL/HTTPS [9]. These protocols have the advantages of being simple and providing security properties as a block. However their main disadvantage is that they are high-energy consuming and thus, they affect the mobile devices battery lifetime as proved in [10]. The fact that the security properties are provided as a block represent a disadvantage for the user's expectations as the security protocols do not take into account the users requirements regarding the security level they would like for their private data. If a user asks for the integrity property regarding her/his data, a protocol such as HTTPS will ensure integrity, confidentiality and authenticity even if not required by the end-user. From an application point of view, this kind of security protocols do not adapt the security properties according to the sensitivity level required for each data transmitted between a mobile and a Cloud and between the components of a same mobile cloud application. If we take the example of an e-Health application, a password data is more sensitive than body characteristics data. Thus, security solutions developed for mobile cloud applications must adapt to the data sensitivity.

In this paper we discuss some criteria that may affect the security properties applied to component-based mobile cloud application data. Then, we give an overview about the security solution that we propose to secure mobile cloud applications, i.e. to secure data transmitted between the components (running on a mobile or in a Cloud) of a same

Manuscript received March 21, 2013; revised May 27, 2013

application. Our solution provides a way to apply different security properties according to data sensitivity, human requirements and technical constraints.

This paper is organized as follow. Section II describes the criteria that influence the security properties applied to data. In Section III, we detail our proposed solution. Section IV contains several existing solutions to address the security issues in Mobile Cloud Computing. Finally some conclusions are presented.

II. CRITERIA

The lack of resources is one of the biggest disadvantages of mobile phones. Therefore, a security solution must consider mobile device constraints. In addition, as said previously, mobile owners (mobile end-users), running mobile applications have different expectations regarding security of their private data. In this section we discuss several criteria that must be taken into account when designing a security solution for mobile cloud applications and more generally for today mobile applications.

A. Human constraints

For each individual, personal data are important. The degree of importance may vary from a person to another person. This degree can differ according to each person perceptions regarding privacy and also according to each person status (citizen, politician, actor, government employee etc.). For example, a politician may need a higher security level for her/his data than a non-politician person.

User's requirements are not taken into consideration by various traditional security solutions. Actually, most of the time, these solutions, do not fit with the users expectations. Even if this was more or less acceptable until now, today it is an important issue that cannot be ignored as end-users are more and more concerned about security of their private data. Thus, a security solution must allow an end-user to express her/his needs regarding the security level of her/his data and more generally of the applications she/he uses and run on her/his mobile and also regarding the device energy consumption (i.e. an end-user may requires for a security solution that does not consume all the battery of her/his mobile when using a specific mobile cloud application). Furthermore a security solution has to be adapted to the user profile (non-security expert or security expert).

B. Technical constraints

In our work, we consider different kinds of technical constraints: components location, user context and mobile device capabilities.

In a component-based mobile cloud application, each component runs in a specific location. It can be on the mobile device or in Cloud. Moreover, some components can migrate between the mobile device and Cloud. When a component changes a location, the security level may also change. It should be strengthened, if the components migrate from the mobile device to the Cloud, or it may be weakened if the migration is from the Cloud to the mobile device. Actually, these changes depend on the components that communicates between each other and on their location.

Concerning the user context, we refer to the area where the end-user is when executing an application: private or public area (e.g. home, office, public space such as airport, commercial center, etc.). The user context may change very often, particularly in the future, which will influence considerably the security level applied to the data transmitted between the components of a mobile cloud application.

Regarding mobile devices constraints, for devices like mobile phones, with limited resources and energy, it is important to provide security solutions that consume fewer resources without compromising and reducing the security level of data to secure.

The energy consumed by the cryptographic algorithms (encryption, decryption, hash functions, etc.) used to traditionally secure data (in transit and data at rest) depends on the algorithm type. Asymmetric ciphering algorithms consume more resources than symmetric ones, which in their turns are more consuming than hash functions.

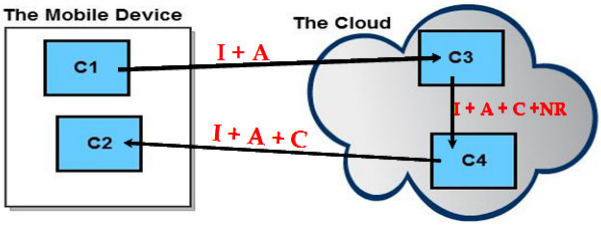

Figure 1. Different security levels

C. Data sensitivity constraints

Data may have different levels of sensitivity depending on user needs or user context. Moreover, in our opinion data are even more sensitive if their loss or theft causes important damages regarding the income and integrity of a user. For example the password data of a user or her/his bank account is more sensitive than her/his preferred color.

Each sensitivity level requires an adequate security level, where each security level implies providing the right security properties (integrity, confidentiality, etc.). Thus in a mobile cloud application, data transmitted between components may have different security levels and require different security properties (as shown in Figure 1).

III. THE PROPOSED ARCHITECTURE

The security framework, that we propose has to fulfill the following features: to secure data communication between the components of a same application (i.e. between components running on the mobile side and those running in a Cloud and between the components running only in Cloud). Our architecture has to be able to adapt the security services according to the following constraints: data sensitivity, human requirements and technical constraints.

Three sensibility levels (high, medium and low) were assigned to data. For each sensibility level the equivalent protection level required and the security level applied are different; as exemplified in Table I.

TABLE I. DATA SENSIBILITY, PROTECTION AND SECURITY LEVELS

Sensitivity Level	Protection Level Required	Security Level
High	Mandatory	Elevated
Medium	Desirable	Average
Low	Optionally	Little

As security properties we have the following: integrity, confidentiality, authenticity and non-repudiation. The

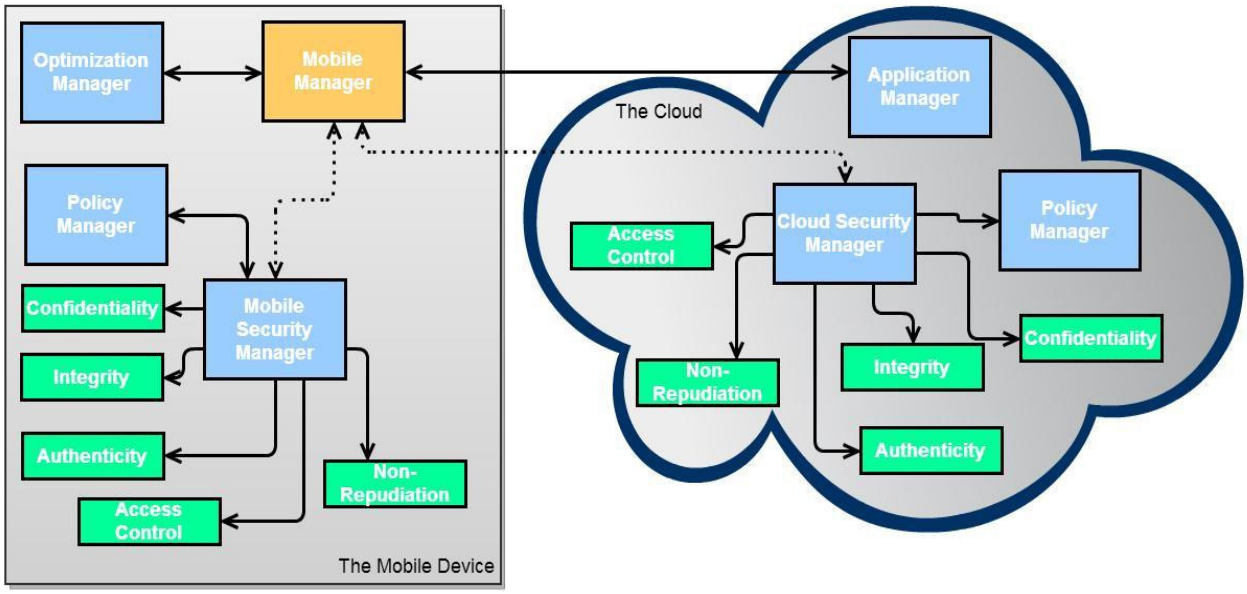

Figure 2. Secure Mobile-Cloud framework

combination between those security properties shows the security levels that can be applied to an application data; as presented in Table II (A - Authenticity, C – Confidentiality, I – Integrity, NR – Non-Repudiation).

For one security level there may be several components combinations. There may be various implementations of the security component. This is because in implementation it can be used different encryption or hash algorithms.

TABLE II. COMPONENTS COMBINATIONS

Security Level	Combination 1	Combination 2
Elevated	A + I + C	A + I + C+ NR
Average	A + I	A+ I+ C
Little	Not-Exist	A + I

TABLE III. DESCRIPTION OF THE MANAGERS

Manager	Description
Mobile Manager	It collects data and events that occurs on the mobile side and sends them to the appropriate manager to be analyzed.
Mobile Security Manager Cloud Security Manager	Both ensure the composition of the security components. The Mobile Security Manager ensures security composition on the mobile side and the Cloud Security Manager does it on the Cloud side.
Optimization Manager	It sends the information collected from sensors (e.g. network sensor, energy sensor) to the mobile manager.
Application Manager	It checks the application integrity at setup.
Policy Manager	It determinates which security components are

The proposed security framework has to answer to the following questions: 1) which security components combination is applied to each data type; 2) which implemented version of a security component is used to secure data; 3) where are the security components executed, in Cloud or on the mobile device (see Figure 3).

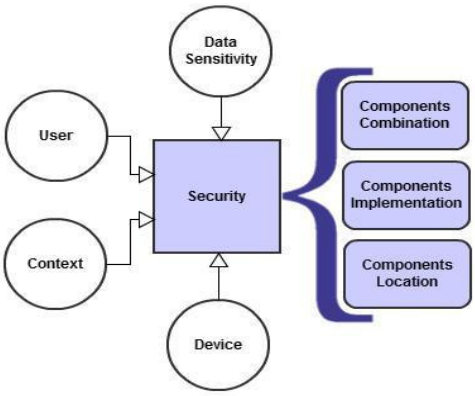

Figure 3. Security framework – answers needed

An end-user may express her/his wishes regarding the security level applied to her/his data employed into an application. Also, the user may choose the energy consumption for her/his battery. All this options are made available to the user through a user interface.

The security architecture we propose is called Security Mobile-Cloud framework (SMC) and it is briefly described in [11]. As it is shown in Figure 2, SMC framework has components running in a Cloud and on a mobile device. A short description of each component is given in Table III.

The security components are deployed on the mobile device as simple components and in the Cloud as services. The deployment of the security components may change to adapt to the user choices and context, data sensitivity and devices resources.

The Mobile Security Manager and Cloud Security Manager ensure data security by applying the right security

properties through composition of security components. However, the Security Mobile Manager has more responsibilities:

1. It checks the sensitivity of received data and stores it with a sensitivity attribute (low, medium or high).
2. It checks the user preferences regarding the security level and the saving of mobile resources.
3. It determinates the required security level for received data and the characteristics of the adequate cryptographic algorithms to use.
4. It identifies the user context and checks mobile device resources e.g. battery level.

According to the results obtained in the previous steps it determinates which security manager will be in charge of securing data: the Mobile or Cloud Security Manager.

IV. RELATED WORK

There is a variety of proposed solutions for the security issues related to Mobile Cloud Computing. The existing security solutions treat independently the different types of mobile cloud security problems. They can be classified in solutions for: security issues on mobile devices, security issues in Cloud and security issues concerning data transmission.

Solutions for security issues on mobile devices are proposed by the mobile platforms. They have implemented five types of security features: traditional access control, application provenance, encryption, isolation and permission-based access control [7]. These features will secure data on the mobile device, however, when the data will be sent and stored in the Cloud, it will become out of the user control.

Zhang et al [5] proposed a solution to secure an elastic mobile application which is executed in a Cloud environment. An elastic application can consist of one or more 'weblets'; 'weblets' are independent software modules. Each 'weblet' runs on a mobile device or in Cloud, and can migrate between them according to the changes that may appear on the mobile device. This solution is provided for a specific application model, i.e. elastic applications and it covers the secure installation of elastic application, authentication, secure migration, and authorization of wablets. Solutions to ensure the confidentiality and integrity of the user's data stored in Cloud are proposed in [12] and [13]; a solution for data access is provided in [14].

Data exchange between the mobile devices and the Cloud has to be secured by the mobile cloud application providers. A solution frequently used is the SSL protocol, but as it has been proved in [10] using SSL increases the energy consumption of mobile devices. Another solution proposed is LECCSAM [10]. LECCSAM is an architecture based on security components that aims to optimize the mobile device energy consumption. LECCSAM is not adapted to the mobile cloud applications.

V. CONCLUSONS

In this paper, we are not willing to criticize the existing security solutions for mobile cloud applications. Our objective is to propose an alternative solution to secure data communication between the components of a same mobile cloud application in order to adapt to different kinds of criteria: human and technical ones. Regarding the implementation of the security solution that we propose, we have implemented in Java all the security components and the Security Manager on the mobile (Android) and the Cloud side. We are still working on the implementation of the other components and of a friendly user interface. For future work we plan to evaluate the performances of our solution regarding adaptation of the security composition, dynamic deployment of the security components and energy consumption.

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] H. Liang1, D. Huang and D. Peng, "On Economic Mobile Cloud Computing Model", in Mobile Computing, Applications, and Services Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 76, 2012, pp 329-341.
[2] R. Ballagas, J. Borchers, M. Rohs and J. G. Sheridan, "The Smart Phone: A Ubiquitous Input Device", in IEEE Pervasive Computing , vol. 5, no. 1, pp. 70-77, 2006.
[3] Hoang T. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", http://www.eecis.udel.edu/~cshen/859/papers/survey_MCC.pdf.
[4] D. Kovachev, Y. Cao and R. Klamma, "Mobile Cloud Computing: A Comparison of application Models", eprint arXiv:1107.4940, Jul. 2011.
[5] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing Elastic Applications on Mobile Devices", In CCSW'09, November, 2009, Chicago, Illinois, USA.
[6] V. March, Y. Gu, E. Leonardi, G. Goh, M. Kirchberg, B. S. Lee, "µCloud: Towards a New Paradigm of Rich Mobile Applications", in the 8th International Conference on Mobile Web Information Systems (MobiWIS), June, 2011.
[7] Lookout Mobile Security, "Lookout Mobile Threat Report", Aug. 2011.
[8] Cloud Security Alliance, "Top Threats to Cloud Computing V 1.0", March 2010.
[9] D. Huang, Z. Zhou, Le Xu, "Secure Data Processing Framework for Mobile Cloud Computing", Workshop on Cloud Computing, INFOCOM 2011
[10] M. Kamel, K. Boudaoud, S. Resondry, M. Riveill, "Low-Energy Consuming and User-centric Security Management Architecture Adapted to Mobile Environments" In Proceedings of the 12th IFIP/IEEE International Symposium on Integrated Network Management (IM'2011), Dublin, Ireland, May, 23 - 27, 2011
[11] D. Popa, K. Boudaoud, M. Cremene, M. Borda , " A Security Framework for Mobile Cloud Applications", in Proceedings ROEduNet 11 th International Conference, Sinaia, January 17-19, 2013.
[12] W. Ren, L. Yu, R. Gao, F. Xiong, "Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing", in Journal of Tsinghua Science and Technology vol. 16 pp. 520–528, 2011.
[13] J. Yang, H. Wang, J. Wang, C. Tan and D. Yu1, "Provable data possession of resource constrained mobile devices in cloud computing", in Journal of Networks vol. 6 pp. 1033–1040, 2011.
[14] Z. Song, J. Molina, S. Lee, S. Kotani, and R. Masuoka, "TrustCube: An Infrastructure that Builds Trust in Client", in Proceedings of the 1st International Conference on Future of Trust in Computing, 2009.