Sécurité des Systèmes et Réseaux Travail Personnel de l'étudiant

2016/2017

Topic: Security and Privacy Challenges in Mobile Cloud Computing Survey and Way Ahead

KOUDANBE AMADOU Calvin

and

KOUYIM MELI Armandine Sorel

I. Introduction

1. Context

A mobile device is a handheld tablet or other device that is made for portability, and is therefore both compact and lightweight .new data storage, processing and display technologies have allows this new device to do nearly anything that had been traditionally done with larger personal computer. Since the mobile device has little memory storage and processor, it cannot be able to run Applications that need a considerable storage and computational power. To solve this problem the mobile cloud computing which is the combination of cloud computing, mobile computing and wireless communication to bring rich computational resources to the mobile users, network operators, as well as cloud computing is created. With mobile cloud computing user's data are stored and processed into cloud server and the communication is done device via wireless networks. The fact that the transmission is done via wireless commutation and the data stored in a distant server can affect the security and the privacy. It this why some research are made on security and privacy challenges in the MCC .this article talks about this challenges and some solutions.

2. Background

To understand the security and the challenges in MCC some notions need to be assimilate:

2.1 Definition and importance the mobile cloud computing

A mobile cloud computing which is the combination of cloud computing, mobile computing and wireless communication to bring rich computational resources to the mobile users, network operators, as well as cloud computing is created.

The MCC is used to show, process, transport and share the application and resources to a mobile user.

2.2 Some applications of the mobile devices

Some applications of cloud are: application processing, cloud storage, Cloud mobile media, data sharing, Mobile commerce system, Education and learning

2.3 Mobile cloud architecture

We have three architectures of mobile cloud available:

- **Client-server**

  Here a mobile devices and cloud are working as like as a client computer and a server cloud respectively. A mobile device give its request to a cloud which execute it and manage the computational intensive applications.

- **Had hoc**

  Here all mobile devices communicate to transmit data into cloud server.
- **Edge-cloud**

2.4 Different services offered by a mobile cloud computing

Different model exist to produce a cloud service to mobile user:

- **Mobile Network as a Service** (MNaaS) here service provider offer network infrastructure so that users can create their own network
- **Mobile Cloud Infrastructure as a Service** (MIaaS): In this service model, the service providers offer cloud infrastructure and storage to mobile users. Examples: iCloud (www.apple.com/icloud/) and Google drive
- **Mobile Data as a Service (MDaaS):**This model offered database to the mobile device for her data management, transaction and other operations
- **Mobile App as a Service (MAppaaS):**With this services user can downloads or built application in the cloud
- **Mobile Multimedia as a Service (MMaaS):** In this model, users can run and manage multimedia services (playing music, game) through wireless network.
- **Mobile Community as a Service (MCaaS)**

  This model give a possibility to a group of user to build and manage a social network

2.5 Challenges in mobile cloud computing

There many challenges in mobile cloud**: Limited** Resources of Mobile Devices**,** Heterogeneity**,** Elasticity**,** Application Services Issues Security, Privacy and Trust Challenges

3 Problem and research questions

3.1 problem

- Is it possible to reduce the security and privacy problem in mobile cloud computing?

3.2 Research questions

- What are the security and privacy challenges in mobile cloud computing?
- What are the solutions for the security and privacy challenges in mobile cloud computing?

I. Related works

Table 1: *comparison of related work on security and privacy challenges in MCC*

Works	**MCC overview**	**security**	**Privacy**	**Current solution**	**Open issue**
[39] A. N. Khan, M. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, pp. 1278-1299, 2013.	Yes	yes	No	yes	No
[43] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 61, pp. 59-80, 2016.	No	Authentication only	No	yes	No
[44] K. S. Tep, B. Martini, R. Hunt, and K.-K. R. Choo, "A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, 2015, pp. 1073-1080..	No	Yes	No	Yes	No
[45] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework," *Journal of Network and Computer Applications*, vol. 67, pp. 147-165, 2016.	No	Yes	No	Yes	No
[47] S. Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan, *et al.*, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *Journal of Network and Computer Applications*, vol. 74, pp. 98-120, 2016.	No	Yes	No	yes	No
[48] N. V. Juliadotter and K.-K. R. Choo, "Cloud attack and risk assessment taxonomy," *IEEE Cloud Computing*, vol. 2, pp. 14-20, 2015.	No	No	No	yes	No
article	Yes	Yes	Yes	yes	Yes

Works	Proposed solution	Techniques Used	Service offered	Problem Solve
[80] H. S. Alqahtani and G. Kouadri-Mostefaou, "Multi-clouds Mobile Computing for the Secure Storage of Data," in *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, 2014, pp. 495-496.	Multi-cloud server	Encryption, decryption and compression	Integrity	Data security
[81] A.-k. A. Abdalla and A.-S. K. Pathan, "On Protecting Data Storage in Mobile Cloud Computing Paradigm," *IETE Technical Review*, vol. 31, pp. 82-91, 2014.	fragmentation	Fragmentation and merge	Integrity	Data security
[86] K. Gai, M. Qiu, H. Zhao, and J. Xiong, "Privacy-aware adaptive data encryption strategy of big data in cloud computing," in *Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference on*, 2016, pp. 273-278.	Dynamique data encryption, strategy (D2ES)	Selective encryption strategi under timing constraints	Data confidentiality	Data security
[105] N. Dhanya and G. Kousalya, "Adaptive and Secure Application Partitioning for Offloading in Mobile Cloud Computing," in *Security in Computing and Communications*, ed: Springer, 2015, pp. 45-53.	Adaptive application partitioning And secure offloading Algorithms in MCC	Application Partitioning dynamically change the remote execution allocation	Secure offloading	Offloading and partitioning
[106] Y. Xia, Y. Liu, C. Tan, M. Ma, H. Guan, B. Zang, *et al.*, "TinMan: eliminating confidential mobile data exposure with security oriented offloading," in *Proceedings of the Tenth European Conference on Computer Systems*, 2015, p. 27.	TinMan	Trusted node, SSL session injection and TCP payloads replacement	Data confidentiality and Secure offloading	Offloading and partitioning
[107] A. N. Khan, M. M. Kiah, M. Ali, and S. Shamshirband, "A Cloud-Manager-Based Re-Encryption Scheme for Mobile Users in Cloud Environment: a Hybrid Approach," *Journal of Grid Computing*, vol. 13, pp. 651-675, 2015.	Cryptographic method	cloud-manager-based re-encryption scheme (CMReS)	Secure offloading and Privacy protection	Offloading and partitioning
[111] S. Y. Vaezpour, R. Zhang, K. Wu, J. Wang, and G. C. Shoja, "A New Approach to Mitigating Security Risks of Phone Clone Co-location Over Mobile Clouds," *Journal of Network and Computer Applications*, 2016.	SWAP	Protecting data leakage	Dynamic allocation and migration of phone clone	Virtualization

[112] Z. Hao, Y. Tang, Y. Zhang, E. Novak, N. Carter, and Q. Li, "SMOC: A secure mobile cloud computing platform," in *Computer Communications (INFOCOM), 2015 IEEE Conference on*, 2015, pp. 2668-2676.	SMOC	Secure application	Hardware virtualization , a proposed file System	Virtualization
[117] D. Popa, M. Cremene, M. Borda, and K. Boudaoud, "A security framework for mobile cloud applications," in *Roedunet International Conference (RoEduNet), 2013 11th*, 2013, pp. 1-4.	SMC, a security framework for mobile clod applications	Web API security	Strong authentication, web signature, web encryption, public key infrastructure, transport layer handshake protocol	mobile application security
[120] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 127-134.	Secure elastic application model	Trusted manager	Authentication secure communication and migration	mobile application security
[155] Y. Zhang, S. Su, Y. Wang, W. Chen, and F. Yang, "Privacy-assured substructure similarity query over encrypted graph-structured data in cloud," *Security and Communication Networks*, vol. 7, pp. 1933-1944, 2014.	PASSQA(privacy assures substrure similarity query)	Secure index construction trapdoor rand query processing	Data query privacy	Privacy solution
[164] A. N. Khan, M. M. Kiah, S. A. Madani, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile cloud Computing," *The Journal of Supercomputing*, vol. 66, pp. 1687-1706, 2013.	Identity privacy protection approach	Dynamic credential generation	Identity privacy	Privacy solution

Table 2: comparison of some related works of security

II. Methodology employed

To approach this survey, our authors firstly give an overview on MCC by given his definition, its importance, its requirement(Confidentiality, Integrity, Availability, Authentication and access control) and the different services offered by a MCC .Secondly, they enumerate all the challenges in MCC(Limited Resources

of Mobile Devices, Heterogeneity, Elasticity, Application Services Issues, Security, Privacy and Trust Challenges) .finally they identifies all the challenges related to the security and the privacy in MCC and for a specific challenge, they proposed some solutions.

III. Results found and Perspectives

1. Results found

After analyzing this work we can remind two main results: the different privacy and security challenges in MCC and the solutions for this challenges

1.1 Security and privacy challenges in MCC

The different security and privacy challenges in MCC are:

- Identity privacy
- Location privacy
- Data privacy
- Mobile device security
- Mobile cloud application security
- Virtualization security
- Data security

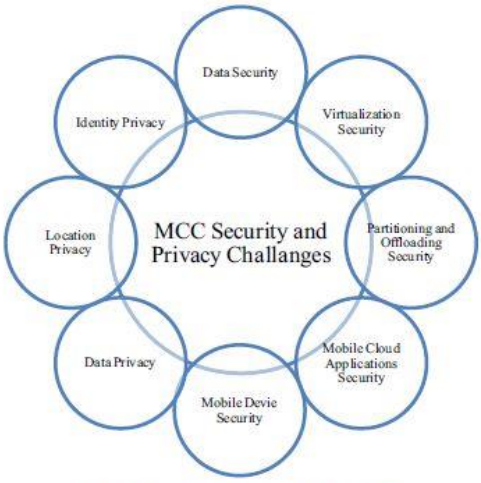

Fig. 1. Main security and privacy challenges in MCC.

1.2 Solutions for different challenges

1- Data security solution

✓ **The Dynamic Data Encryption Strategy (D2ES).**

Here the author proposes a solution based on multi cloud fata encryption and data compression solution; in this solution data are divides in segment itch of them is encrypted and compressed the user can store one segment in its own storage. This technique is use so that if there is an unauthorized access to one segment, another segment could not be accessed.

- ✓ **the propose proactive dynamic secure data scheme (P2DS)**

In this approach the data is fragment and store in to multi servers. The data is merge when the user want to use it.

2- Security solutions for partitioning and offloading

- ✓ **Data portioning concept**

In this method, data are divided in two part! Sensitive part and non-sensitive part; the sensitive part is treated in the mobile device and the no sensitive part is run on the cloud. The sensibility of a data is defined by the use, in this solution the mobile user benefices of offloading and the privacy of sensitive data is preserve

- ✓ **Secured offloading algorithm**

This method is use the data portioning concept and add to it an interconnection between the mobile phone and the cloud to ensure the update of the data in the mobile phone

- ✓ **The cryptographic method for secured offloading of mobile device (cloud manager base re-encryption scheme) CNReS**

In this approach the encryption, decryption and re-encryption operation are distributed amount mobile device, manger and cloud. This solution preserve user privacy

3- Solutions for virtualization related challenges

- ✓ **The SWAP solution**

This method proposed two solution: the first is to secure clone allocation to reduce the leakage of data from virtual machine. The second is the migration of clone phone if the threat become high

- ✓ **Data isolation process**

4- Solutions for mobile Security

- ✓ Anti-malwares solution

There are several security applications available for mobile devices with different features like detect and prevent mobile malwares, control unauthorized access and protect privacy. Some on-device security applications are 360 Degree Mobile Security (www.360safe.com), Avast Mobile Security (www.avast.com/free-mobile-security), Norton Mobile Security(www.mobilesecurity.norton.com/), Kaspersky Mobile Security(www.kaspersky.com/android-security), ESET Mobile Security (www.eset.com/us/home/products/mobile-security-android/),
Lookout Mobile Security (www.lookout.com/android) and so on.

5- Security solutions for privacy

- ✓ **The chameleon hash signature algorithm**

Authors in (Zhang and Zhao, 2015) propose an identity privacy public auditing protocol that is based on the chameleon hash signature algorithm. In this protocol, the user randomly generates a pseudo-key pair and compute data tag with this pseudo-key pair to hide user identity. Thus, the cloud server cannot differentiate the actual origin of the outsourced data.

- ✓ ***The PASSQ***

The authors in (Zhang et al., 2014) propose privacy assured substructure similarity query (PASSQ). This proposed solution contains three algorithms such as secure index construction, trapdoor generation and query processing. The secure index converts original into encrypted form to conceal the information. And last two algorithms are used to perform privacy assured similarity calculation and trapdoor generation respectively.

2. Perspectives

Although, more solutions have been proposed to solve the problem of security and privacy in cloud computing, we always find ourselves with a certain problem such as the security of the cloned phones and the mobile performance overhead due to the introduction of the computational and communicational.

That give to authors some reflection on how can the cloned phone be secured and to research a solution that can take the performance of the mobile phone in consideration.

IV. Most important publications for this work.

For this work there were not most important publications because all the publications are equally mentioned.

REFERENCES

[1] Muhammad Baqer Mollah,Md. Abul Kalam Azad and Athanasios Vasilakos, Security and Privacy Challenges in Mobile Cloud Computing: Survey and Way Ahead, *Journal of ComputerApplications*,http://dx.doi.org/10.1016/j.jnca.2017.02.001

[2] https://en.m.wikipedia.org/wiki/Mobile_Cloud_Compuiting date mise à jour: 28/02/2017; consulté le 06/03/2017