University of Ngaoundere
Faculty of sciences
Department of Mathematics and computer sciences

Université de Ngaoundéré
Faculté de sciences
Département de Mathématique et informatique

TPE
SECURITY SYSTEM AND NETWORK

Theme N°13: **Security and Privacy Challenges in Mobile Cloud Computing: Survey and Way Ahead.**

Baqer Mollah, Muhammad, Kalam Azada, Md. Abul, Vasilakos, Athanasios
2017 (English) In: Journal of Network and Computer Applications, ISSN 1084-8045, E-ISSN 1095-8592

Summarized by

Name and Surname	Level	Register
AWÉ SAMALNA DENIS	M1SLED	07L251FS
SAMDALLE AMARIA	M1SLED	09B051FS

Under the coordination to :
Dr.-Ing. Franklin TCHAKOUNTE
University of Ngaoundere

Academic Year : 2016-2017

Report

1. Introduction

*1.1.*Context

Nowadays, the use of handheld gives us a future of business solution in information and communication technology (ICT). More than the three four of the world population are users of mobile devices. In the midst of final word, smartphones and tablets over and about make ring to his corresponding, users can also benefits more and more of internet services as emailing, internet browsing, running a wide range of applications, file sharing, reading or editing documents, entertaining, etc. A Mobile Cloud Computing is defined as integrated of mobile computing in the cloud computing for mobile devices [3]. The widespread fast-development of the last one makes some researchers quiet to his constraint resources useful about satisfaction of subscriber's operator of telephony. Now, a new paradigm as Mobile cloud computing is become to solve more of problems. It considered as services of cloud computing offered for a mobile phone environment and mobile embedded system environment, which the users can benefits to some facilities as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. Anyway, there are many applications for a mobile users proper for the cloud computing: application processing, cloud storage, data sharing, cloud mobile media, cloud based next generation cellular network, mobile commerce system, education and learning, mobile social networks, gaming, human-centric mobile cloud, cloud assisted Internet of Things, etc. Nevertheless, the advanced studies of connection protocols used in mobile clouds, using of cloud services will become too easy. In 2012, Zhang and his partners are defined six elements as features for MCC such as breaking through hardware limitations, having suitable data access, intelligent load balancing, efficient task processing, cost effective on demand service and removing the regional boundary. This survey paper presents in details the security and privacy challenges that arise due to the integration of mobile computing and cloud computing.

1.2. Background

After analyzing definitions of MCC acronym in [8] set an example and the definition writes by [10], we withhold that, MCC is a combination of mobile computing, cloud computing, and wireless technology where the mobile users utilize different cloud based services as like as personal computer users.

Whether offloading intensive computations, or data storage, using the cloud for mobile devices do pose questions of security and trust issues. Because of the low capacity of mobile device storage, many users are starting to store data such as contacts, calendars and SMS on clouds.

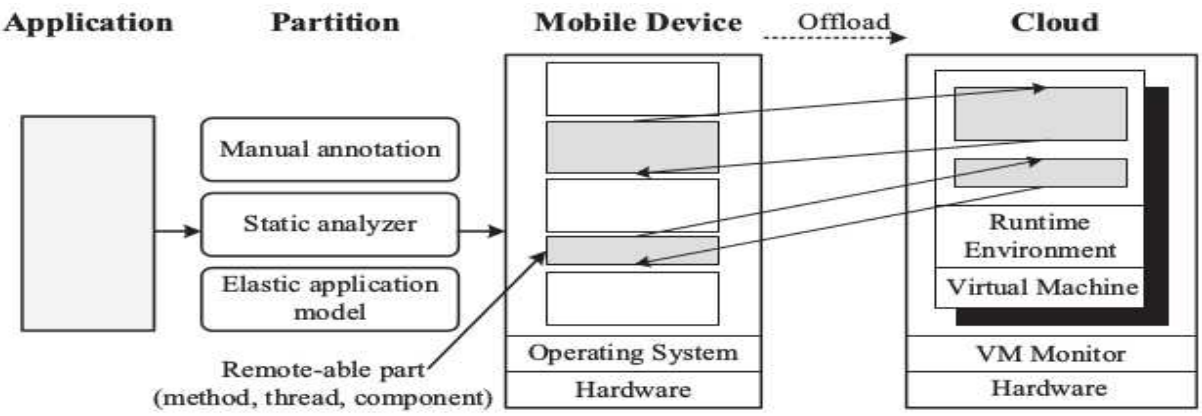

Figure 1: The computational offloading process for mobile devices to cloud

About Mobile cloud applications, these applications offer cloud based services with rich user experience. The application of this environment is divided into a client based, client-cloud based and clouds based model. Thus, we can have a problem to offload to the cloud for execution.

According to Mobile cloud architectures, there are three kinds of MCC architectures : mobile client-server, ad hoc and mobile edge-cloud architectures. A mobile client-server has some limitations like latency due to round trip delay, jitter and bulk data transfer within the wireless network, needs of infrastructure and wireless access to provide services. Even if the wireless accesses to the cloud service is difficult, the ad hoc architecture most be used to solve the problem. At the moment, there are problems of latency intensive services face end-to-end communications delay, bandwidth problems and costly data services even if the mobile applications are offloaded the computational processing task from mobile device to cloud.

MCC has following service models to provide cloud services to mobile users: Mobile Network as a Service (MNaaS), Mobile Cloud Infrastructure as a Service (MIaaS), Mobile Data as a Service (MDaaS), Mobile App as a Service (MAppaaS), Mobile Multimedia as a Service (MMaaS), Mobile Community as a Service (MCaaS).

*1.3.*Problem and research questions

According the section 1.2 some issues and challenges are briefly described: limited resources of mobile devices, stability, availability, costs of network access, scarcity of channel bandwidth, heterogeneity, process offloading, mobility management, context-processing, cloud policies for mobile users, elasticity, application services issues, energy efficiency, ensuring Quality of Service (QoS), security, trust, privacy challenges etc.

Among these, security and privacy are becoming more challenging issues than others due to several reasons like insecure open air transmission medium, resource-constraint mobile devices, distributed cloud storage and processing, and heterogeneous environments.

2. Related works (only a comparative table)

Tableau 1: Comparison of related works towards secure offloading

Authors	Year	Proposed Schemes	Security features	Technical approaches	Scalability
Al-Mutawa, M., Mishra, S.	2014	Privacy preserving computational offloading	Privacy protection	Data partition	High
Dhanya, N., Kousalya, G.	2015	Adaptive application partitioning and secure offloading in MCC	Secure application offloading	Application partitioning, dynamically changed the remote execution allocation	High
Khan, A.N., Kiah, M.M., Ali, M., Shamshirband, S.	2015	Cloud-Manager-based re-encryption scheme (CMReS)	Secure offloading and Privacy protection	Both cloud and manager based re-encryption schemes	High
Saab, S.A., Saab, F., Kayssi, A., Chehab, A., Elhajj, I.H.	2015	Secure mobile application offloading mechanism	Secure offloading	Profiling and decision making algorithm	High
Duan, Y., Zhang, M., Yin, H., Tang, Y.	2015	Privacy preserving mobile application offloading	Secure Offloading	Adaptive data partitioning	High

Tableau 2: Comparison of related works for cloud based mobile application security

Authors	Year	Proposed Schemes	Security features	Technical approaches	Scalability
Tysowski, P., Hasan, M.A.	2011	Secure communication model for highly scalable mobile application in cloud	Secure communication within application components	Key management in mobile device, cloud based re-encryption approach	High
Popa, D., Cremene, M., Borda, M., Boudaoud,K.,	2013	SMC, a security framework for mobile cloud applications	Ensure secure data communication within applications components and application integrity	Trusted managers, application signature verification	Moderate
Tysowski,P.K., Hasan, M.A.	2013	A protocol for secure mobile applications	Application security	Attribute based encryption, group keying mechanism and re-encryption	High
Zhong, H., Xiao, J.,	2014	MAACA, Mobile Application Assessment Cloud Architecture	Application security Assessment	Trusted managers/components	Moderate
Tang, L., Ouyang, L., Tsai, W.-T	2015	Strong API security for securing MCC	Web API security	Strong authentication, web signature, web encryption, public key infrastructure, transport layer handshake protocol	Moderate

3. Methodology employed

This survey paper presents in details the security and privacy challenges that arise due to the integration of mobile computing and cloud computing. The challenges that are concentrating in this scientific paper are describe on Figure 2 below. We then discuss on some recent solutions and countermeasures techniques. However, some of these security and privacy challenges are yet to be solved and under research activity. In Table 1 and Table 2, we try to condense our contribution and excerpt a comparison with other recent works.

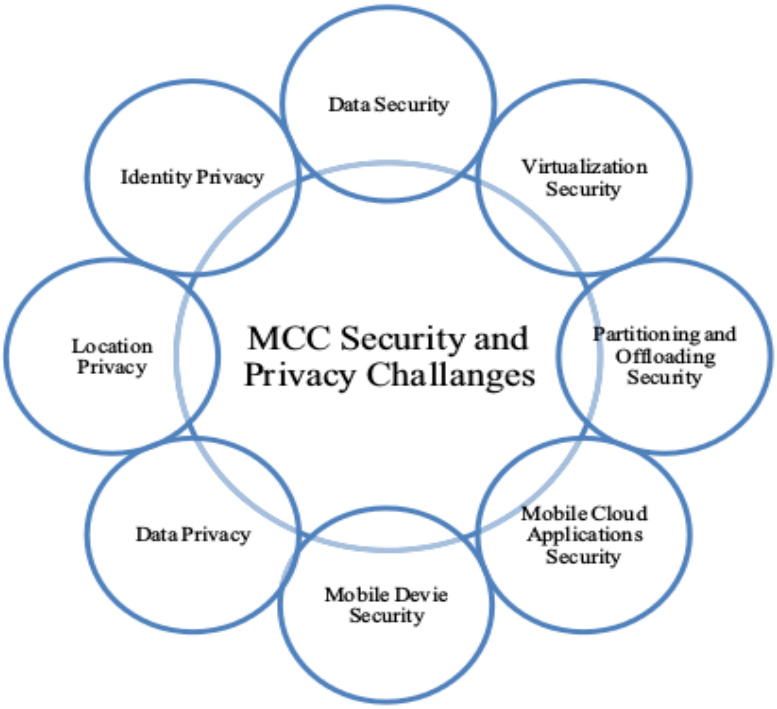

Figure 2: Main security and piracy challenges in MCC

4. Results found and perspectives

4.1.Current security solutions

4.1.1. Data security solutions

To warrant data security in the MCC, the author suggests us to use a framework in [1] which is established on distributed multi-cloud storage, data encryption and data compression techniques. [13] propose another a security approach as secure sharing, scalable water marking and Reed-Solemon coding, data security scheme by homomorphic encryption, a cryptographic method, a public auditing protocol, a remote data auditing method based on algebraic signature, a public auditing scheme based on dynamic hash table, proactive dynamic secure data scheme, cipher text-policy attribute based encryption (CP-ABE) to protect from unauthorized access, IntercroSsed Secure Big Multimedia Model to ensure secure assesses within different cloud platforms, an efficient multi-keyword ranked search approach, search over encrypted data and secure updates, secure infrastructure, novel data encryption approach named Dynamic Data Encryption Strategy.

4.1.2. Security solutions for partitioning and offloading

To ensure the data partitioning and offloading, the author proposes an adaptive application partitioning and secure offloading algorithm in MCC, TinMan, cryptographic method, defend against timing attacks during offloading process, a secure and energy efficient mobile application offloading mechanism,

4.1.3. Security solutions for virtualization related challenges

To secure for virtualization, the author propose a security aware provisioning and migration scheme for phone clones (SWAP), a secure mobile cloud platform (SMOC), using of secure framework for cloud infrastructure, defend against co-resident attacks, hardware assisted secure VMs (H-SVM), lightweight security approach to secure VMs deployment

4.1.4. Security solutions for mobile cloud applications

To secure mobile cloud applications, propose Secure Mobile Cloud (SMC), a hybrid attribute and re-encryption based protocol, secure elastic mobile application model for cloud computing, three key distribution schemes such as identity-based encryption, multi-level key management and data re-encryption, and a cloud based re-encryption scheme, a model STOVE (Strict, Observable, Verifiable Data and Execution), Mobile Application Assessment Cloud Architecture (MAACA),

4.1.5. Secure mobile cloud architectures

For secure mobile cloud architectures, propose a secure architecture for MCC, context-aware security architecture for MCC, a service to mobile users, a security framework for RESTful MCC services, a security framework for CloneCloud based MCC architecture.

4.1.6. Authentication to mobile cloud

To ensure an authentication, propose a privacy-aware authentication scheme, proposes and implements a biometric based authentication approach, bio-hashing techniques, authentication approach, MDLA (Message Digest and Location based Authentication), an authentication approach for cloudlets based architecture, mobile cloud authenticator (MCA).

4.1.7. Security solutions for mobile devices

*To ensure mobile devices, there are several solutions approaches in security applications. We're s*olutions for physical threats, *s*olutions for malwares, *a*vailable on-device security applications, Malware detection techniques, *cloud based solutions*, Mobile devices storages issues, Authentication to mobile devices

4.1.8. Security solutions for privacy

*To ensure the piracy, this survey proposes set of solutions : a p*robabilistic public key encryption technique and ranked keyword searching algorithm, lightweight cryptographic method, a private cloud, an identity privacy preserving public auditing protocol, two data query privacy preserving approaches for MCC, privacy assured substructure similarity query (PASSQ*),* an approach to preserve data query privacy for mobile mashups in MCC, K-anonymity *for* protect*ed* location privacy, a caching aware dummy selection algorithm (CaDSA), a fine-grained location access control tool, LPPS (location privacy preservation scheme) to protect location privacy of mobile users, a privacy protection in location based information survey applications (LB-ISA), an improved identity management protocol (I2DM), a consolidated identity management (CIDM) architecture, dynamic credential generation instead of digital credential method.

4.2. Perspectives

The field of MCC defines new categories *of challenges: to ensure a handling* for the integration of mobile device and cloud as data, application, virtualization and remote execution, *develop an* easy management *for* an integrated solution, ensure security while performing data communication between mobile device and cloud, security and privacy for phone clone, *develop a flexible frame*work *for migration user* data and application from mobile devices to phone clones.

5. Most important publications for this work

[1] Al-Mutawa, M., Mishra, S., 2014. **Data partitioning: an approach to preserving data privacy in computation offload in pervasive computing systems**. In: Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks, pp.51–60.

[2] N. K. Chaubey, D. M. Tank, **"Security, Privacy and Challenges in Mobile Cloud Computing (MCC):- A Critical Study**", International Journal of Innovative Research in Computer and Communication Engineering and Comparison (IJIRCCEC), Vol. 4, Issue 2, February 2016

[3] Popa, D., Cremene, M., Borda, M., Boudaoud, K., 2013**. A security framework for mobile cloud applications**. In: Roedunet International Conference (RoEduNet), 2013 11th, pp. 1-4.

[4] S. Malik, M. M. Chaturvedi, "**Privacy and Security in Mobile Cloud Computing: Review**", International Journal of Computer Applications (0975 – 8887), Volume 80, No 11, October 2013

[5] Tang, L., Ouyang, L., Tsai, W.-T., 2015. **Multi-factor web API security for securing Mobile Cloud**. In: Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on, pp. 2163-2168.

[6] Tysowski, P., Hasan, M.A., 2011. **Towards secure communication for highly scalable mobile applications in cloud computing systems**. Cent. Appl. Cryptogr. Res. Univ. Waterloo Tech. Rep. CACR 33, 2011.

[7] Tysowski, P.K., Hasan, M.A., 2013. **Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds**. Cloud Comput. IEEE Trans. 1, 172–186.
[8] Wang, H., Wu, S., Chen, M., Wang, W., 2014. **Security protection between users and the mobile media cloud**. Commun. Mag., IEEE 52, 73–79.
[9] Yu, Y., Li, Y., Au, M.H., Susilo, W., Choo, K.-K.R., Zhang, X., 2016. **Public cloud data auditing with practical key update and zero knowledge privacy**. In: Australasian Conference on Information Security and Privacy, pp. 389–405.
[10] Zhong, H., Xiao, J., 2014. **Design for a cloud-based hybrid Android application security assessment framework**. In: Reliability, Maintainability and Safety (ICRMS), 2014 International Conference on, pp. 539–546.