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

BOIMADI NICOLE & DONGMO DIFFO JOEL

March 23, 2017

Part I
Introduction

1 context

Information and Communication Technology (ICT) is an expretion that refers to the field of telematics (computer techniques, audiovisual, multimedia, internet, telecommunications) that allows communication, Access to information sources, storage, manipulation, production and transmission of information in all forms (text, music, sound, image, video, ...). Nowadays mobile devices (smartphones, tablets) no longer only in the traditional (call, sms) but are the most used tools for ICT. Given the growing number of mobile phones and the increasing demand for software, mobile computing is failing to fully satisfy the large number of users and their computing needs, Mobile cloud computing (MCC) is presented as cloud computing services, offered either in a mobile telephony environment or in a mobile embedded system environment. Claude computing integrates mobile computing and is widely used by mobile users thanks to the services offered such as storing, free on-demand, computing power. This raises the problems of data security and confidentiality.

2 background

2.1 Mobile Cloud Definitions

A technology that combines mobile computing with claude computing and wireless network technology. Like the computer users, the MCC offers the possibility for the mobile user to use in the claude.

2.2 Partitioning and Offloading

The mobile devices are stopped by the consumption of given during the execution of the applications for that the discharge on the claude comes to overcome this problem. The discharge is divided into three stages: partitioning, migration and execution. Although execution and processing are transferred from mobile devices to clouds, mobile devices can decide how to run and how much the calculation must be unloaded to the cloud based on its resources.

2.3 Mobile Cloud Applications

applications is divided into three types : client based, client-cloud based and cloud based models.

- In client based major execution of an application is held on mobile device.
- In client-cloud an application is partitioned into components and these components are executed by mobile device as well as remote cloud.
- In cloud based models cloud is part and parcel of an application where the application runs, processes, and stores.

2.4 Mobile Cloud Architectures

Three kinds of MCC architectures are available. These are mobile client-server, ad hoc and mobile edge-cloud architectures.

- In Client-server architecture the mobile is worcking like client and the server is the claude. Although the mobile client-server architecture can support to mobile users, it has some limitations like latency due to round trip delay, jitter and bulk data transfer within the wireless network[1].
- Ad hoc architecture is be the solution For the chalenge of client-server architector. In there architecture the mobile devices form themselves an ad hoc network by using modern wireless technologies to provide cloud services each other. latency intensive services face end-to-end communications delay, bandwidth problems and costly data services.
- In the mobile edge-cloud architectures, the computational tasks are processed in both cloud and nearby mobile devices or local cloud server[1].

2.5 Mobile Cloud Service Models

MCC provide many services, these are :

- **Mobile Network as a Service (MNaaS)** these model provider offer network infrastructure so that users can create their own network, control the traffics, and connect to the servers. Example: OpenStack Networking

- **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)** In this service model, the service providers supply database related services in order that mobile users can do their data management, transaction and other data related operations. Example: Oracle's mobile cloud data as a service (www.oracle.com/cloud/daas.html)
- **Mobile App as a Service (MappaaS)** In this service model, the users can use, access and execute cloud based mobile applications through wireless network in anywhere and anytime. Example: Applications in Google Play Store (www.play.google.com/store/apps).
- **Mobile Multimedia as a Service (MmaaS)** In this service model, the users can run and manage the multimedia services such as playing movies or games through the wireless network in rich hardware equipment.
- **Mobile Community as a Service (McaaS)** In this service model, a group of mobile users can build and manage a mobile social network or community where the users can get provided social network or community services.

3 Problem and research questions

3.1 problem

Can we have solutions to the problem of security and confidentiality to which the MCC faces?

3.2 Research questions

- What are the issues related to MCC security and confidentiality?
- What solutions link to these problems?

Part II
Related works

There is another section dealing with the same subject as Article [1]. The table below illustrates some of them.

dommaine⇒ ⇓related works	MCC overview	security	privacy	current solutions	Open Issues
[39]	yes	yes	no	yes	no
[43]	no	yes	no	yes	no
[44]	no	yes	no	yes	no
[45]	no	yes	no	yes	yes
[47]	no	yes	no	yes	no
[48]	no	yes	yes	yes	no
[1]	yes	yes	yes	yes	yes

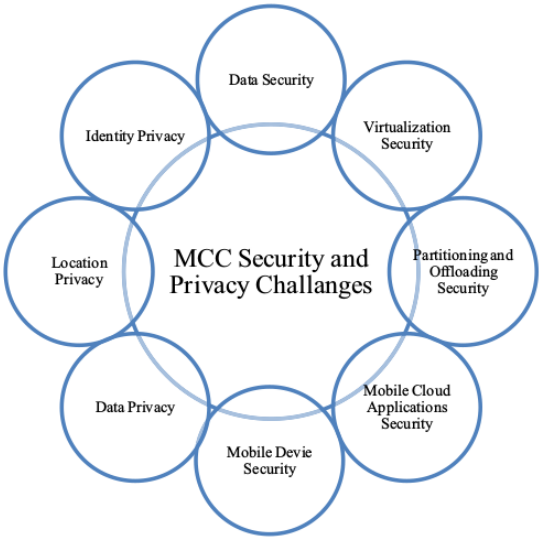
Part III

Methodology employed

The author began with a study of the functioning of the mobile claude computing, then the challenges facing the MCC which are among others:

Limited Resources of Mobile Devices; Heterogeneity; Elasticity; Application Services Issues; Security, Privacy and Trust Challenges.

He then turned his attention to the problems of data Security, Privacy and Trust Challenges. In this part of the problem he also resurrected the different challenges which are illustrated in the following figure.



He has gone through the studies carried out by other authors in which these problems are solved in order to identify all the solutions made and to make a comparative study of the level of efficiency.

Part IV
Results found and Perspectives

Results found

Several solutions have been proposed by different authors. The tables below show a few.

- **Data Security Solutions**

works	Proposed Schemes	Security Features	Technical Approaches	scalability
[2, 3]	Multi-clouds for secure storage of data	Data Confidentiality	Distributed multi-cloud storage, cryptography and data compression	high
[4]	Secure data storage and sharing in mobile media cloud	Authentication and Data Confidentiality	Scalable watermarking and Reed-Solemon coding	high
[5]	A public auditing protocol for secure data storage and sharing	Data Integrity, Identity Privacy Protection	Asymmetric group key agreement and proxy re-signature	medium
[6]	Cloud Data Auditing with practical Key Update and Zero Knowledge Privacy	Data Integrity	zero knowledge proof systems, proxy re-signatures and homorphic linear authenticators	high
[7]	Dynamic hash table based public auditing	Data Integrity and data privacy	Two-dimensional data structure, homomorphic authentication	moderate
[8]	Proactive dynamic secure data scheme (P2DS)	Access Control	Attribute based access control mechanism	high

- **Security Solutions for Partitioning and Offloading**

works	Proposed Schemes	Security Features	Technical Approaches	scalability
[9]	adaptive application partitioning and secure offloading in MCC	Secure Application Offloading	Application partitioning, dynamically changed the remote execution allocation	high
[10]	Cloud-manager-based re-encryption scheme	Secure Offloading and Privacy Protection	Both cloud and manager based re-encryption schemes	high
[11]	Security analysis of offloading under timing attacks	Defend Timing Attack	Modified cryptographic system	low
[12]	Secure mobile application offloading mechanism	Secure Offloading	Profiling and decision making algorithm	high
[13]	Privacy preserving mobile application offloading	Secure Offloading	Adaptive data partitioning	high

- **Security Solutions for Mobile Cloud Applications**

works	Proposed Schemes	Security Features	Technical Approaches	scalability
[14]	SMC, a security framework for mobile clod applications	Ensure secure data communication within applications components and application integrity	Trusted managers, verification application signature	moderate
[15]	A protocol for security mobile applications	Application security	Attribute based encryption, group keying mechanism and re-encryption	high
[16]	Secure elastic application model	Authentication, secure communication and migration	Trusted managers	high
[17]	Secure communication model for highly scalable mobile application in cloud	Secure communication withing application components	Key management in mobile device, cloud based re-encryption approach	high
[18]	STOVE model	Secure application execution	Trusted party, strong isolation and verification	high

- **Security Solutions for Privacy**

works	Proposed Schemes	Security Features	Technical Approaches	scalability
[19]	Efficient privacy preserving approach for outsourced data	Data Privacy	Probabilistic pubic key encryption and ranked keyword searching algorithm	high
[20]	A lightweight data privacy preserving method	Data Privacy	Pseudo-random permutation method	moderate
[21]	A privacy preserving public auditing protocol	Privacy Preserving audit	chameleon hashing algorithm	high
[22]	PASSQ, privacy assured subs tructure similarity query	Data Query Privacy	Secure index construction, trapdoor generation and query processing	moderate
[23]	Data query privacy preserving for mobile mashups	Data Query Privacy	Dynamically created VMs as proxies, live migration of application level VMs	low
[24]	LPPs, location privacy preservation scheme	Location Privacy	Distributed cache proxy servers	high
[25]	preserving location based information survey applications	Location Privacy	System level cloning of mobile devices	moderate
[26]	Identity privacy protection approach	Identity Privacy	Dynamic credential generations	high

For more flashing and more results on these solutions and that of the challenges that we could not enumerated in document consulted [1].

Perspectives

Telephone cloning is an essential part of MCC virtualization where mobile peripheries are deployed on the claude for data trunking and application. This cloning represents huge masses for the security and confidentiality of the data. Yet at present the current work can be carried out in this field.

The user submits migrated their data and application on the claude (storage and power constraint). This migration therefore imposes technical challenges. Like a flexible framework allowing the mobile user to migrate their data and application safely.

Part V
Most important publications for this work.

References

[1] Muhammad Baqer Mollah, Md. Abul Kalam Azad, Athanasios Vasilakos: Security and Privacy Challenges in Mobile Cloud Computing : Survey and Way Ahead. Journal of Network and Computer Applications, 2017

[2] 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.

[3] 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.

[4] H. Wang, S. Wu, M. Chen, and W. Wang, "Security protection between users and the mobile media cloud," Communications Magazine, IEEE, vol. 52, pp. 73-79, 2014.

[5] Y. Yu, Y. Mu, J. Ni, J. Deng, and K. Huang, "Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage," in Network and System Security, ed: Springer, 2014, pp. 28-40.

[6] Y. Yu, Y. Li, M. H. Au, W. Susilo, K.-K. R. Choo, and X. Zhang, "Public cloud data auditing with practical key update and zero knowledge privacy," in Australasian Conference on Information Security and Privacy, 2016, pp. 389-405.

[7] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, et al., "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, 2015.

[8] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, and H. Zhao, "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry," Future Generation Computer Systems, 2016.

[9] 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.

[10] 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.

[11] T. Meng, Q. Wang, and K. Wolter, "Model-based quantitative security analysis of mobile offloading systems under timing attacks," in Analytical and Stochastic Modelling Techniques and Applications, ed: Springer, 2015, pp. 143-157.

[12] S. A. Saab, F. Saab, A. Kayssi, A. Chehab, and I. H. Elhajj, "Partial mobile application offloading to the cloud for energy-efficiency with security measures," Sustainable Computing: Informatics and Systems, vol. 8, pp. 38-46, 2015.

[13] Y. Duan, M. Zhang, H. Yin, and Y. Tang, "Privacy-preserving offloading of mobile app to the public cloud," in 7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 15), 2015.

[14] 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.

[15] P. K. Tysowski and M. A. Hasan, "Hybrid Attribute-and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds," Cloud Computing, IEEE Transactions on, vol. 1, pp. 172-186, 2013.

[16] 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.

[17] P. Tysowski and M. A. Hasan, "Towards secure communication for highly scalable mobile applications in cloud computing systems," Centre for Applied Cryptographic Research, University of Waterloo, Tech. Rep. CACR, vol. 33, p. 2011, 2011.

[18] J. Tan, R. Gandhi, and P. Narasimhan, "STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications," in Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on, 2014, pp. 644-649.

[19] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," Journal of Network and Computer Applications, vol. 64, pp. 12-22, 2016.

[20] M. Bahrami and M. Singhal, "A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing," in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015 3rd IEEE International Conference on, 2015, pp. 189-198.

[21] J. Zhang and X. Zhao, "Efficient chameleon hashing-based privacy-preserving auditing in cloud storage," Cluster Computing, pp. 1-10, 2015.

[22] 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.

[23] R. Owens and W. Wang, "Preserving Data Query Privacy in Mobile Mashups through Mobile Cloud Computing," in Computer Communications and Networks (ICCCN), 2013 22nd International Conference on, 2013, pp. 1-5.

[24] M. Chen, W. Li, Z. Li, S. Lu, and D. Chen, "Preserving location privacy based on distributed cache pushing," in Wireless Communications and Networking Conference (WCNC), 2014 IEEE, 2014, pp. 3456-3461.

[25] H. Zhang, N. Yu, and Y. Wen, "Mobile cloud computing based privacy protection in location-based information survey applications," Security and Communication Networks, vol. 8, pp. 1006-1025, 2015.

[26] 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.