UNIVERSITÉ DE NGAOUNDERE

Faculté des Sciences

Département de Mathématiques

Et Informatique

THE UNIVERSITY OF NGAOUNDERE

Faculty of Science

Department of Mathematics

And Computer Science

Article 13 :

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

By

Yera Pagore Athanase	**08M521FS**
Tala Kuate Cédric	**16B086FS**

Directed by

Dr. – Ing Franklin Tchakounté

Academic year: 2016-2017

Table of content

1. Introduction

1.1 Context

Now a days the development of mobile devices such as smart phones, tablets, PDA is increasing at a very high speed. The hardware and software designs are more sophisticated and attractive. This increases the number of their user days after days. Mobile devices are used for many different purposes from simple calling, sending and receiving messages, sending and receiving emails, playing music, watching video, editing documents to the execution of applications. Due to their usage for more and more consuming tasks in term of storage, energy as well as computing power, it raises from one hand the problem limited storage capacity of the mobile devices, energy constraint and the other hand the problem of the limited computational power of the mobile devices. Regarding those limitations, the cloud computing provides a suitable alternative to overcome those problems.

The mobile cloud computing consists to use the unlimited resources of the cloud in term of computation power as well as storage capacity to run some application that couldn't be run on a mobile device. The mobile cloud computing can be seen as a service of cloud computing which is offered in mobile phone as well as embedded system environments. As it can provides cloud services, mobile cloud computing becomes more and more popular to the users of mobiles devices, and their number increases every day which makes the field of cloud services potentially more beneficial with the time. However, the services provided by the cloud can be available for mobile devices just through wireless channel such as WIFI. For mobile cloud computing at least six essential features are needed 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. Those features have some issues and challenges which act as a break in the fast development of mobile cloud computing such as 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., But among these issues and challenges, the security and privacy are the most important due to some elements involved in mobile cloud computing such as : the wireless transmission medium, the resources constraints of the mobiles devices, the distributed property of cloud storage as well as processing, and the heterogeneity of the environments.

The paper submitted to our study presents in details the security and privacy challenges that arise due to the integration of mobile computing and cloud computing. The challenges highlighted in this paper are: data security, virtualization security, identity privacy, location privacy, data privacy, partitioning and offloading security, mobile devices security and mobile cloud applications security. Our work will be subdivided as follows: the section I introduces our work by giving the context and the background of study, the problem statement and the research questions of the paper. Section II deals with the related works, in section III, we present the methodology employed, in section IV are presented the results and perspectives and in section V we will give the most important publications for this work.

1.2 Background

This paper has as canvas the followings parts: the mobile cloud definitions, partitioning and offloading, mobile cloud application, mobile cloud architectures, mobile cloud services and challenges.

From mobile cloud definitions, we can summarize that mobile cloud computing 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.

Partitioning and offloading illustrates how, due to the increasing of the computing power needed by the mobile applications and their energy and storage constraints, applications can be partitioned and offloaded or sent to the cloud for their execution. The mobile device will decide how much computational power is needed and then send a part of the application on the cloud for it execution.

Mobile cloud applications presents how an application should be divided, what are the parts that shall be kept at the mobile side and those than could be send on the cloud. Here are presented three kinds of applications: client based, client-cloud based and cloud based models.

In mobile cloud architectures are presented the three available kinds of mobile cloud computing architectures: mobile client-server, ad hoc and mobile edge-cloud architectures.

In mobiles cloud services models are presented the different services models the mobile cloud computing propose to provide cloud services to mobile users. Those models are: 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).

In challenges are presented the different difficulties faced by the mobile cloud computing like: limited resources of mobile devices, heterogeneity of the communication medium, the elasticity and scalability, application services issues, and the security, privacy and trust challenges that make it more complicated compare to conventional cloud computing.

1.3 Problem and research questions

The problems or challenges faced in mobile cloud computing are many due to wireless communication medium used to for the exchange within the mobile devices and the cloud. In this paper an emphasis is done on the security and privacy challenges. Those challenges are classified under the followings categories: data security, virtualization security, identity privacy, location privacy, data privacy, partitioning and offloading security, mobile devices security and mobile cloud applications security.

The research questions emerging to this paper are the followings:

- How can we provide the security and the privacy of client's data as well as on the mobile devices, the cloud and during the communication via wireless medium?
- What are the different work that have been done on that issue?
- What are the proposed or existing solutions, their advantages and limitations?

2. Related works

This paper is specially based on many works related to mobile cloud computing. Those works are summarized in the following tables where an emphasis is done on the security features and the scalability they treat.

Works	Proposed Schemes	Security Features	Technical Approaches	Scalability
[80, 81]	Multi-clouds for secure storage of data	Data Confidentiality	Distributed multi-cloud storage, cryptography and data compression	High
[82]	Secure data storage and sharing in mobile media cloud	Authentication and Data Confidentiality	Scalable watermarking and Reed-Solemon coding	High
[83, 84]	Data storage security	Data Confidentiality	Homomorphic encryption	Low
[85]	BSS, Block based sharing scheme	Data Confidentiality	Block based cryptographic system	High
[86]	Dynamic Data Encryption Strategy(D2ES)	Data Confidentiality	Selective encryption strategy under timing constraints	Moderate

[87]	Extended Proxy-Assisted Approach	Data Confidentiality	Attribute based Encryption	High
[88]	A public auditing protocol for secure data storage and sharing	Data Confidentiality	Asymmetric group key agreement and proxy re-signature	Medium
[89]	Remote data auditing for secure data storage	Data Integrity, Identity	Algebraic signature and new data structure model named divide and conquer table (DCT)	High
[90]	Cloud Data Auditing with Practical Key Update and Zero Knowledge Privacy	Privacy Protection	zero knowledge proof systems, proxy re-signatures and homorphic linear authenticators	High
[91]	Dynamic hash table based public auditing	Data Integrity	Two-dimensional data structure, homomorphic authentication	Moderate
[92]	Proactive dynamic secure data scheme (P2DS)	Data Integrity	Attribute based access control mechanism	High
[93]	Secure and lightweight ciphertext-policy attribute based encryption (SL-CP-ABE)	Data Integrity and Data	Ciphertext-policy attribute based encryption (CP-ABE) algorithm	High
[94]	CP-ABE-CSCTSK (CP-ABE-constant size ciphertext and secret keys)	Privacy	Ciphertext-policy attribute based encryption (CP-ABE algorithm	Medium
[95]	IntercroSsed Secure Big MultimediaModel (2SBM)	Access Control	Semantic-Based Access Control	High
[96]	Efficient multi-keyword ranked search (EMRS)	Access Control	Relevance score, secure k-nearest neighbor technique, an efficient index and blind storage system	High
[97]	Fine-grained Database Field Search	Access Control	Attribute based encryption	Moderate
[98]	Personalized search over encrypted data and secure updates (PSU)	Access Control	Bloom filter, k-nearest neighbor technique, modified attribute based keyword search and vector-space based search technique	High
[99]	Attribute based data sharing in MCC	Secure Data Searching	Ciphertext-policy attribute based encryption and symmetric encryption	High
[100]	Secure real time video sharing and searching in MCC	Secure Data Searching	Advanced Encryption Standard, Searchable Symmetric	High
[101]	Conditional proxy re-encryption (CPRE)	Secure Data Searching	Encryption, CP-ABE and Digital Signature Cipher-policy Attribute based encryption	Moderate
[102]	Secure data sharing and seraching at the edge of cloud network	Secure Data Sharing	Secret key encryption, Public key encryption, Searchable secret key encryption and Digital signature	High
[103]	Secure Data Sharing in Clouds (SeDaSC)	Secure Data Sharing and	Advanced Encryption Standard and symmetric encryption	High

3. Methodology employed

In this paper, the authors present a comprehensive survey of security and privacy challenges, and their security solutions of MCC. To achieve their work, they did an investigation to have an overview of the existing related works in the field of mobile cloud computing. After they did a comparative study of these related works based on different security and privacy requirements. The methodology employed here is a qualitative method. The authors' interest is to gain a rich and complex understanding of the existing solution for the security and privacy concerns in a mobile cloud computing in the aim to propose a suitable way or solution to that issue. According to the nature of the study, a descriptive and analytical methods are used because the authors did a description of the existing works dealing with the security and privacy of mobile cloud computing and the also make an analysis of these works in the aim to compare them on some specific bases. According to the purpose of the study, the methodology employed can be classified as fundamental research.

4. Results found and Perspectives

The results of this paper are the different solutions found concerning the security and privacy challenges in mobile cloud computing that have been proposed recently in different journals and conference proceedings. Those solutions are given for each category of security and privacy challenge identified in mobile cloud computing such as: data security challenges, partitioning and offloading security challenges, virtualization security challenges, mobile cloud applications security challenges, mobile devices security challenges, privacy challenges.

According to data security solutions, the different proposed schemes are:

Multi-clouds for secure storage of data, Secure data storage and sharing in mobile media cloud

Data storage security, BSS, Block based sharing scheme, Dynamic Data Encryption Strategy (D2ES)

Extended Proxy-Assisted Approach, A public auditing protocol for secure data storage and sharing

Remote data auditing for secure data storage, Cloud Data Auditing with Practical Key Update and Zero Knowledge Privacy, Dynamic hash table based public auditing, Proactive dynamic secure data scheme (P2DS), Secure and lightweight ciphertext-policy attribute based encryption (SL-CP-ABE), CP-ABE-CSCTSK (CP-ABE- constant size ciphertext and secret keys), IntercroSsed Secure Big Multimedia

Model (2SBM), Efficient multi-keyword ranked search (EMRS), Fine-grained Database Field Search, Personalized search over encrypted data and secure updates (PSU), Attribute based data sharing in MCC, Secure real time video sharing and searching in MCC, Conditional proxy re-encryption (CPRE), Secure data sharing and searching at the edge of cloud network, and Secure Data Sharing in Clouds (SeDaSC).

According to the security solutions for partitioning and offloading the proposed schemes are: privacy preserving computational offloading, Adaptive application partitioning and secure offloading in MCC, TinMan, Cloud-manager-based re-encryption scheme (CMReS), Security analysis of offloading under timing attacks, Secure mobile application offloading mechanism and Privacy preserving mobile application offloading.

According to the security solutions for virtualization related challenges, the proposed schemes are: SWAP, a security aware provisioning and migration approach, SMOC, secure mobile cloud platform, User security protection framework in cloud infrastructure, An approach to protect co resident attacks, H-SVM, Hardware assisted secure VM, and A security isolation and migration approach for VM deployment.

concerning the security solutions for mobile cloud applications, the proposed schemes are: SMC, a security framework for mobile clod applications, A protocol for secure mobile applications, Strong API security for securing MCC, Secure elastic application model, Secure communication model for highly scalable mobile application in cloud, STOVE model and MAACA (Mobile Application Assessment Cloud Architecture).

Concerning the secure mobile cloud architectures, many architectures are described here, such as:

- A secure architecture for MCC considered as modern mobile and cloud computing security threats, features of mobile Internet, and other secure cloud architectures. The whole architecture is divided into five parts.
- Another architecture, a context-aware security architecture for MCC that needs to be deployed at cloud end as an additional security layer.
- Another architecture consists of some components installed in both mobile device and cloud. This architecture is presented to guarantee the integrity of application and the communications among same application parts in both mobile and cloud ends.
- A security framework for RESTful MCC services is also proposed. This framework is based on existing security and key management protocols. This framework includes different modules and blocks such as web service servlet, HTTP listener, request handler, parser module, fuzzy logic module, augmented offloading module, orchestrator module, response composer, certificate generation and authorization modules.

Concerning the security solutions for privacy the proposed schemes are the followings: Efficient privacy preserving approach for outsourced data, A lightweight data privacy preserving method, An approach of privacy preserving data utilization, A privacy preserving public auditing protocol, PASSQ (privacy assured substructure similarity query), Data query privacy preserving for mobile mashups, CaDSA, (Caching aware dummy selection algorithm), LP-doctor, LPPS (location privacy preservation scheme), Preserving location based information survey applications I2DM (improved identity management protocol), CIDM (consolidated identity management protocol), Identity privacy protection approach.

As perspectives, despite several recent security and privacy related works were presented, in this paper, there arestill open issues which need to be solved for giving a secure and privacy preserved MCC environment. Firstly, acomprehensive and integrated security solution is needed to develop that enclose most of the major security requirements. An integrated solution will result in easy management, and provide desired security level. Some solutions are required which ensure security while performing offloading and remote processing. Moreover, the data recovery in case of data loss is also needed to focus. A flexible framework is needed that allows the mobile users to migrate their data and application to mobile clones easily and securely. The proposed security solutions should encounter both security requirements as well as performance.

5. Most important publications for this work.

The most important publications for this work are:

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.

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.

M. Louk and H. Lim, "Homomorphic encryption in mobile multi cloud computing," in Information Networking (ICOIN), 2015 International Conference on, 2015, pp. 493-497.

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.

J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud, "Network, IEEE, vol. 29, pp. 46-50, 2015.

M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things," IEEECloud Computing, vol. 4, pp. 34-42, 2017.

M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, et al., "SeDaSC: Secure Data Sharing in Clouds," IEEE Systems Journal, vol. 99, pp. 1-10, 2015.

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.

Y. Xia, Y. Liu, C. Tan, M. Ma, H. Guan, B. Zang, et al., "TinMan: eliminating confidential mobile data exposure with security orientedoffloading," in Proceedings of the Tenth European Conference on Computer Systems, 2015, p. 27.

H. Zhong and J. Xiao, "Design for a cloud-based hybrid Android application security assessment framework," in Reliability, Maintainability and Safety (ICRMS), 2014 International Conference on, 2014, pp. 539-546.

Q. Xiu-feng, L. Jian-Wei, and Z. Peng-Chuan, "Secure cloud computing architecture on mobile internet," in Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference on, 2011, pp. 619-622.