MANTECH Publications

International Journal of Computer Science and Soft Computing
Volume 1 Issue 1

Security Requirements and Threats User Awareness during Computation Offloading On Cloud Using Mobile

Aradhana[1], Samarendra Mohan Ghosh[2]

Department of CSE

Dr. C. V. Raman University Bilaspur, C.G.

***Corresponding Authors' email id**: aradhana236@gmail.com*

Abstract

Offloading the computation from mobile to cloud bring significant security concern. Secure execution of computation requires strategic planning and awareness of growing the security threats and measures. In this paper we list various security threats and measures to securing computation offloading using mobile.

***Keywords:** Computation offloading; xDSL; Wi-Fi, SaaS; PaaS; IaaS, MCC*

INTRODUCTION

Complexity of execution demands resources. It is to be multimedia base application like 4D animated series are being growing demanded on mobile phones. Even requirements of software and hardware upgrade every months. So that mobile devices have poor resources, less secure. Resource poorness is major obstacle for advance applications. The concept of computation offloading is new ability to gain high computation speedups with small communication delays.

In last few years, this idea has received more interest because of the significant rise in the sophistication of mobile applications, the availability of powerful clouds and the improved connectivity options for mobile devices. By identifying the offloadable tasks at runtime, recent work [3, 2, 4, and 6] has aimed to generalize this approach to benefit more mobile applications. The computational offloading approaches new and attractive interaction of computation, it arises significant challenges in terms of data and code security during the offloading.

OVERVIEW OF CLOUD AND COMPUTATION OFFLOADING

Cloud computing migrates the computation and the resources from one location onto recourses. The cloud system resource is open, as neither the application nor the user knows the location of the resource. According to Buyya et al. [7] the cloud computing has the following definition "Cloud is a parallel and distributed computing system consisting of a collection of interconnected and virtualized computers that are dynamically Copyright (c) IARIA, 2015. ISBN: 978-1-61208-388-9 103 CLOUD COMPUTING 2015 : The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization provisioned and presented as one or more unified computing resources based on Service-Level Agreements (SLA) established through negotiation between the service provider and consumers [8]."

Vaquero et al. stated that "clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services) [9]", where the resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization.

CLOUD SERVICE MODELS

There are three cloud models:-Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1].

Infrastructure as a Service (IaaS): IT provides the work environment. One IaaS example is Amazon Elastic Compute Cloud (EC2).

Software as a Service (SaaS): This facility provides application software as per the demand of user requirement e.g. SaaS are Flickr, Google Docs, Siri, Amazon and Cloud Drive.

Platform as a Service (PaaS): It provides infrastructure for new applications e.g. of PaaS are Google App Engine, Amazon Web services.

CLOUD DEPLOYMENT MODEL

Cloud computing model are three type private cloud, public cloud and hybrid cloud, according to the different deployment models [6].

Private Cloud: It is developed for particular organization and security can be created easily.

Public Cloud: It runs on the Internet with high security complex. It is virtualized data centres outside .All the demands of user available in the public Internet.

Hybrid Cloud: It builds with two or more clouds are called hybrid cloud. Hybrid clouds have the property of both public and private clouds.

A new type of cloud deployment models offers Cloud Computing resources and services to mobile devices called Mobile Cloud Computing. Khan et al. defined mobile cloud computing as "an integration of cloud computing technology with mobile devices to make the mobile devices resource-full in terms of computational power, memory, storage, energy, and context awareness [10]".

However, in cloud computing the security situation is very different as the hardware, software and application data can be deployed and stored by the cloud providers. Therefore, to solve security problems that are occur in cloud computing there are some risk management frameworks can be used to secure the data transmitted, ensure the integrity of the applications and increase trust between users and service providers, etc. [11].

SECURITY THREATS ON CLOUD ENVIRONMENT

Security concern of cloud is fall on two broad categories first is security issue faced by cloud providers and second is their end users. So that the responsibility is shared and implement the security on both ends. This environment has many advantages but It has also some drawbacks and security issues .It can arise during offloading the computation (SaaS) services. Here we describe some security threats facing cloud users. Cloud Security Alliance (CSA) did survey on related issue and find the following threats:

1) Tracing and hacking our sensitive information by attackers.
2) Unauthorized use of network used by
3) Data leakage in cloud environment
4) Lacking of skilled hands and experts
5) Data loss on cloud environment
6) Data Segregation from other recourses
7) Security culture among different providers
8) Evolving threats may target clouds.
9) Hardware and software modification
10) Interruptions on software
11) Software theft

12) Misuse of infrastructure

13) Privacy concerns

Cloud provides us distributed environment .It proposes unique security challenges, dependent on the level at which the user operates, application, virtual or physical (Table 1)[19].

SECURITY MEASURES ON COMPUTATION DURING OFFLOADING

Mobile devices are affected by numerous attacks. It is targeting the various resources like Software, hardware, operating systems, applications software, communication links, back-end systems, and users. All these threat are concern the security of mobile computation.

1. The storage of a mobile device is usually made of an on-board memory and a plugged-in memory. The on-board memory stores the code and data of the running software. The plugged-in memory includes non-volatile flash storage and subscriber identity module (SIM) card storage.

2. Attackers can obtain access to the code and data stored in on-board memory via JTAG functionalities [17] or through directly tapping into the circuit board.

3. The security measures in protecting on-board memory include disabling JTAG functions and

4. Implementing secure storage and secure access to user I/O facilities

5. Attackers can obtain access to the code and data stored in plugged-in memory via forensic analysis [16]. The protection measures rely on the encryption of either the data or the memory. The security of encryption keys needs Trusted Platform Module (TPM), which is either a stand-alone chip in the device or a part of the functionality of the SIM card.

6. Securing MOS is the fundamental measure to ensure the confidentiality and the integrity of running mobile applications in the cloud. The security of MOSs can be achieved with kernel hardening, security control over applications, and secure updating and installation.

Table 1 User-specific security requirements and threats

Level	Service level	Users	Security requirements	Threats
Application level	Software as a Service (SaS)	End client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use	• Privacy in multitenant environment	• Interception
			• Data protection from exposure (remnants)	• Modification of data at rest and in transit
			• Access control	• Data interruption (deletion)
			• Communication protection	• Privacy breach
			• Software security	• Impersonation
			• Service availability	• Session hijacking
				• Traffic flow analysis
				• Exposure in network
Virtual level	Platform as a Service (PaS) Infrastructure as a Service (IaS)	Developer–moderator applies to a person or organization thatdeploys software on a cloud infrastructure	• Access control	• Programming flaws
			• Application security	• Software modification
			• Data security, (data in transit, data at rest, remanence)	• Software interruption (deletion)
			• Cloud management control security	• Impersonation
			• Secure images	• Session hijacking
			• Virtual cloud protection	• Traffic flow analysis
			• Communication security	• Exposure in network
				• Defacement
				• Connection flooding
				• DDOS
				• Impersonation
				• Disrupting communications
Physical level	Physical datacenter	Owner applies to a person or orginization that owns the infrastructure upon which clouds are deployed	• Legal not abusive use of cloud computing	• Network attacks
			• Hardware security	• Connection flooding
			• Hardware reliability	• DDOS
			• Network protection	• Hardware interruption
			• Network resources protection	• Hardware theft
				• Hardware modification
				• Misuse of infrastructure

7. In Android, each application runs in a process isolated from other processes through virtualization of the phone so that a compromising process will not endanger other processes or the operating system. Most modern MOSs supports updating the system remotely to update or patch drivers, the OS modules and the installed applications.

8. In Android, a list of privileges comes with each application to be installed. Accepting the list is the only way to install the application. However, the privileges in the list usually give the application access to personal data without any additional mechanisms to actually inspect how the application uses the data. A category of security measures have been proposed to disable unwanted privileges [12] or assign only needed permissions at run time [15].

9. Another category of security measures is to profile and track the information flow of applications and discover the critical points in time when applications access sensitive information or are about to expose such information [13, 24].

The Security Objectives of Cloud Computing Environment

1) Must ensure the availability of information is protected with secure algorithm.

2) To maintain the integrity of computation (information and services) offloading.

3) Prevent the information loss on communication link.

4) Prevent the information from unauthorized access.

5) TO identify the authorised user.

6) To provide the computation flow control with secure manner.

7) To maintain the security when adding the recourses on Physical Level.

REASONS FOR BUILDING TRUST IN COMPUTATIONAL OFFLOADING

For building the secure framework , we measures the following three parameters of security in mobile cloud computing ,(1) authentication of end users ,(2) security in code offloading, and (3) security in data management on cloud. The security of these three parameter not only provide the

authenticity, integrity and confidentiality to mobile computing in the cloud, but also provide flexibility, mobility, scalability and performance

For computation offloading, the code and data collected by mobile devices is executed and stored on cloud services. The agents of mobile application could be instantiation on the cloud environment and to supplement the functionalities of the device. During the offloading confidentiality and authenticity of this execution is a concern much attention.

A secure computational offloading framework is proposed to address this concern. For providing the security on computation by owner provides the encryption keys as aforementioned. The critical part of computation is encrypted with keys used by the owner. Hence, access to critical data needs the authorization of the owners. The limitation of encryption/decryption method of information on cloud computing is key management from both ends information for that we send and store the key in the cloud the key. The problem in this technique is key outflow from channel or cloud so that information is not confidential .We analyze that code obfuscation method is better than encryption because it also transform the information in intellectual form without using key. Code obfuscation provide information to better security and information will be more complex than encryption, including improved software security, tamper prevention, and intellectual property protection. As obfuscation results more complex and become more obfuscate and mitigation and detection are not impossible.

CONCLUSIONS

In this paper, we focus the three parameters of security which affecting the computational on mobile cloud computing. We first list various threats found during mobile computing models in the cloud. Finally we summarized the proposed mechanisms that ensure providing the better security on mobile cloud computation offloading using code obfuscation method rather than encryption/decryption methods also discuss the limitation of encryption /decryption during offloading. We observe that securing the information using Obfuscation method is more robust.com complex and difficult than encryption/decryption method.

REFERENCES

I. R. K. Balan, D. Gergle, M. Satyanarayanan, and J. Herbsleb. Simplifying cyber foraging for mobile devices. In ACM MobiSys, 2007.

II. B. Chun, S. Ihm, P. Maniatis, M. Naik, and A. Patti. Clonecloud: elastic execution between mobile device and cloud. In EuroSys, pages 301–314, 2011.

III. E. Cuervo, A. Balasubramanian, D.-k. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl. Maui: making smartphones last longer with code offload. In ACM MobiSys, 2010

IV. M. S. Gordon, D. A. Jamshidi, S. Mahlke, Z. M. Mao, and X. Chen. COMET: code offload by migrating execution transparently. In USENIX OSDI, pages 93–106, 2012.

V. F. Xie, Y. Peng, W. Zhao, D. Chen, X. Wang, and X. Huo, "A risk management framework for cloud computing," in Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on, 2012, vol. 1, pp. 476–480.

VI. W. Liu, "Research on cloud computing security problem and strategy," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, 2012, pp. 1216–1219.

VII. H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual , pp. 393–398.

VIII. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, Jun. 2009, pp. 599–616.

IX. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A

break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, 2009, pp. 50–55.

X. A. U. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A Survey of Mobile Cloud Computing Application Models," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, 2014, pp. 393–413

XI. K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security Issues for Cloud Computing:," International Journal of Information Security and Privacy, vol. 4, no. 2, 2010, pp. 36–48.

XII. Enck, W., Ongtang, M., McDaniel, P.: On lightweight mobile phone application certification.In: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS'09, Chicago, pp. 235–245. ACM, New York (2009). doi:10.1145/1653662.1653691.

XIII. Enck, W., Gilbert, P., Chun, B.G., Cox, L.P., Jung, J., McDaniel, P., Sheth, A.N.: TaintDroid:an information-flow tracking system for realtime privacy monitoring on smartphones. In: Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation,OSDI'10, Vancouver, pp. 1–6. USENIX Association, Berkeley (2010).

XIV. Hornyack, P., Han, S., Jung, J., Schechter, S., Wetherall, D.: These aren't the droids you'relooking for: retrofitting Android to protect data from imperious applications. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS'11, Chicago,pp. 639–652. ACM, New York (2011). doi:10.1145/2046707.2046780.

XV. W. Liu, "Research on cloud computing security problem and strategy," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, 2012, pp. 1216–1219.

XVI. Walls, R.J., Learned-Miller, E., Levine, B.N.: Forensic triage for mobile phones with DEC0DE.In: Proceedings of the 20th USENIX Conference on Security, SEC'11, San Francisco,pp. 1–14. USENIX Association, Berkeley (2011).

XVII. Jack, B.: blackhat.com, exploiting embedded systems. http://goo.gl/oz7Vs (2006).

XVIII. Drimer, S., Murdoch, S.J., Anderson, R.: Thinking inside the box: system-level failures of tamper proofing. In: Proceedings of the 2008 IEEE Symposium on Security and Privacy, SP'08, Oakland, pp. 281–295. IEEE Computer Society, Washington, DC (2008). doi:10.1109/SP.2008.

XIX. Zissis, D. Lekkas / Future Generation Computer Systems Addressing cloud computing security issues. Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece.