# Towards Mobile Cloud Security Performance: A Cross-Border Approach

Theodoros Mavroeidakos[1], Dimitrios Kallergis[2], Dimitrios D. Vergados[2], Christos Douligeris[2]
[1] School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece
[2] Department of Informatics, University of Piraeus, Piraeus, Greece
[1]el10807@central.ntua.gr, [2]{d.kallergis, vergados, cdoulig}@unipi.gr

***Abstract*—The concept of security performance emerges as the core attribute when cloud-based systems need to process data flows through different countries. To effectively address the cloud security issues through a territorial perspective, it is crucial to focus on the initial objectives of the Terms of Service as issued by the cloud service operator or provider. In this paper, a cloud-based service scenario where sensitive data are transferred and managed in a cross-border manner is assessed. The threats definition process considers the adoption of mobile devices. The paper focuses on the security assessment process and on information reconnaissance which in turn leads to the cloud defence boundary's exploitation. Also, the issue of how the service level objectives (SLOs) may affect security and privacy issues in a cloud-based environment is addressed.**

***Keywords*—cloud security; mobile cloud computing; cloud performance**

## I. INTRODUCTION

Nowadays, cloud computing (CC) services not only deal with critical software implementations but they also permeate in multiple activities of the civil society. Nevertheless, security performance challenges and trust issues still deter organizations and companies from adopting and enhancing their production networks by exploiting the benefits of CC. Because of CC's ubiquitous nature, security performance issues are becoming issues of paramount importance and capture the interest of the general public as personally identifiable information (PII) is aggregated in data centres which are physically located in various parts of the world. Even though many organisations, companies and individuals have the impression that their information is isolated in a single geographical region, this is not often the case. A common cloud-based system accommodates robust security mechanisms, but it is a fact-of-life that due to its services' infrastructure the scenario of aggregating data in cross-border entities is also likely to happen. Thus, the context of security needs to be achieved in a different way. Through another perspective, on-going regulation and legislation processes at regional and national levels have not yet filled the gap towards an integrated security scheme focused on cloud-based services. The challenge of defining unified terms for security engagement in service-oriented architectures, such as the Cloud, is of great importance because of the Cloud's penetrating nature in multiple socio-economic activities.

The service level agreement (SLA), which is in most cases part of the contract between the cloud service operator or provider (CSP) and the customer, can form the basis for any attempt to approach the former challenge. An SLA consists of commonly agreed measurable features - the service level objectives (SLOs). In a cloud environment, the SLOs should be defined to also take into account the security issues and the likely vulnerabilities of the underlying infrastructure [3]. To this end, the CSP adapts the SLA which regulates the service delivery in order to cope with issues such as service availability, integrity and scalability [4]. With reference to a CC environment's security and privacy, the security objectives persistence is also influenced by legal jurisdictions. The Data flow across borders, in particular that of sensitive data, brings out significant law and regulatory challenges for cloud providers and consumers. Although any enactment of a law requires a certain period of time, the rapid adaptation of cloud-based systems and the challenge they pose have urged new legal responses [5]. Currently, at the international [6] and European levels [3], there exist several efforts on standardising the SLAs. These efforts define *rules and codes of conduct* within the business-to-customer (B2C) relationship.

Since in the last years the majority of users have switched into mobile devices (MDs), a significant amount of sensitive information is managed by MDs. Thus, in this paper the assessed CC infrastructure adopts mobile devices for the end service.

Our work aims at addressing the issue of cloud security performance and, in particular, the significance of the SLOs during a cross-border data flow. Our objective is to assess a custom scenario which describes the interaction of a local data processor entity and a CSP which is located abroad.

This paper is organised as follows: Section II presents the related work, section III depicts the customised infrastructure apparatus, while section IV illustrates the methodology followed. Section V presents the results and section VI concludes the paper.

## II. RELATED WORK

Mazhar et al. argue in [1] that from a service model's point of view, three levels of challenges exist: *(a)* communication, *(b)* architectural and *(c)* contractual. The Cloud Standards Customer Council suggests that the deployment model, the

978-1-5090-1990-8/16/$31.00 ©2016 IEEE

service model and also their characteristics should be taken into consideration during the SLA definition [2]. As described in [3], the appropriate SLOs should be defined in the SLA and agreed between the CSP and the clients to take into account the security issues and vulnerabilities of the underlying infrastructure. Zissis and Lekkas [4] pose that a considerable amount of security and policy issues should be addressed in a CC environment; an issue which is exacerbated by the diversity of the technologies that coexist and also by the offered capabilities such as the availability, the integrity and the scalability. In essence, the CSP adapts the SLA which in turn governs the service delivery in order to address these issues.

Additional security concerns have been identified in a mobile cloud computing (MCC) environment, where MDs, which act as thin clients, form the basis of cloud-based applications [7]. In an MCC environment, several security issues arise due to the inherent weaknesses of the communication medium as well as due to the low level of security that the MDs support [8] [9] [10]. Moreover, since in many cases the MDs are strictly dependent on the wireless access points, they are also affected by attacks that target them.

With regards to a CC environment protection, the determination of the security objectives which are defined in the SLA has also been influenced by legal jurisdictions. In 2012, the European Commission (EU) introduced the defining concepts of CC to the European Parliament [11]. The European Commission Directorate General closed the gap between the legal community and the industry by establishing the Cloud Select Industry Group (C-SIG) in 2013. C-SIG consists of contributors such as the Cloud Security Alliance (CSA), the European Network and Information Security Agency (ENISA), IBM and Microsoft. By conducting the Commission's European Cloud Strategy, C-SIG introduced the SLA standardization guidelines in 2014. Moreover, the European Telecommunications Standards Institute (ETSI) launched the Cloud Standards Coordination in order to support critical areas such as security for CC environments. The National Institute of Standards and Technology (NIST) orchestrates the SLA into the CC architecture [12] and it has introduced the usage of the SLA metrics to assess its objectives [13]. NIST has introduced the SLA management and provisioning into the security reference of CC [14]. In the Asia region, the Asia Cloud Computing Association (ACCA) works on issues related to the adoption of CC through several Working Groups.

## III. Infrastructure Apparatus

### A. Cross-Border Scenario

To address the significance of the security SLOs during a cross-border transfer of sensitive data, we illustrate a custom scenario. This scenario describes the collaboration which takes place between a data controller and an out of the country CSP. The processing and management of the data will be performed by the CSP under the responsibility of the data controller. This type of responsibility should be officially defined in the SLA.

### B. Scenario Analysis

For the context of this work, a custom CC environment is implemented according to the SLA which is defined with regards to the legal jurisdictions. The SLOs are formed by national or regional legislation. Thus, the SLA is driven by the creation and the management of both the organizational and the operational level of this environment. To fully evaluate the SLOs, we assess the security level of the CC environment. To this end, it is crucial to follow the legal regulations that supervise the legality of the data transaction as well as the adequacy of the provided security level by the CSP during the transfer and the management of the data.

Figure 1 illustrates the CC implementation activities which are required to deploy the end service.

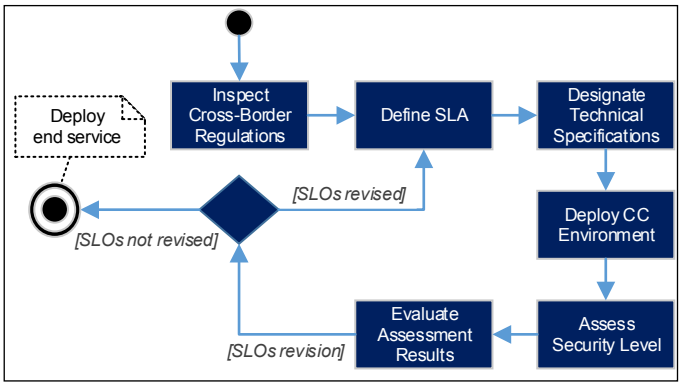


Figure 1. Activity diagram towards the end service

### C. Deploy the CC environment

We use OpenStack [15], an open-source software platform for IaaS implementation, to develop the CC infrastructure according to the SLOs. The CC environment consists of the *controller*, *network*, *compute*, *object* and *block* nodes.

The controller nodes host the main components of the environment services and they are responsible for the configuration process towards the delivery of the end service. The network nodes control the bidirectional flow of data between the OpenStack instances (i.e. the virtual machines) and the internet. The CC core component operates on the compute nodes and performs resource allocation to respectively deploy the instances. The block nodes offer block storage for the end service operation, whilst the object nodes are used for the images' storage.

The CC environment's intranets comprise the management and tunnelling networks. The CC nodes are interconnected through these networks. An external network is also accommodated so as to publicly deploy the OpenStack instances. The end service delivery becomes operational by deploying these instances on the compute nodes.

## IV. Methodology

### A. Scope of the Assessment

The scope of the assessment is to define the information the attacker has to acquire to exploit the initial defence cloud boundary. We consider an application with a sensitive data

context; e.g. governmental, health care or tax-related. Thus, different types of network attackers' actions lead to various potential threats against these data. The aggregation of the assessment results leads to the vulnerabilities definition that can be leveraged for the environment exploitation. The assessment phases are the following: *(a)* information gathering, *(b)* determination of network range, *(c)* identification of active machines, *(d)* finding of open ports and access points, *(e)* OS fingerprinting, *(f)* enumeration of services and *(g)* network mapping. Many computing entities with different characteristics interact in the OpenStack environment towards an end-to-end service delivery. Therefore, different vulnerabilities exist on the various computing entities. This particular knowledge, combined with the captured network traffic, creates attack vectors from the attacker perspective which can be used for exploitation. Table I categorises the security threats of a cloud-based system.

TABLE I. CLOUD THREATS

| Attack Spectrum | Type of Attack | Attacks | Exploitation of Cloud Infrastructure |
|---|---|---|---|
| *General Attacks* | Information Disclosure | Man-in the Middle, Sniffing, Spoofing, Session-Hijacking, Cross-Site Scripting, Authentication Attack | OSI model vulnerabilities |
| | Denial of Services | Distributed DoS | O.S., Intrusion Detection Systems, Service Delivery Systems |
| | | Economic DoS | Overall Infrastructure |
| *Cloud-Specific Attacks* | Resource Isolation Failure | Hypervisor Attack, Side Channel Attack | Virtualized Resources |
| | Insider Threat | Malicious Insider | Different parts of the infrastructure |
| | Power Failure | Power Attack | O.S., Virtualized Resources Isolation, Hypervisor |
| | Malware | Malware-Injection Attack | Virtualized Resources |
| | | Malicious Probes | Intrusion Detection Systems, Intrusion Prevention Systems |

### B. Assessment Tools

For the context of this work, we orchestrate a wide spectrum of tools and methods to accurately assess the CC environment vulnerabilities and also to detect the attack vectors. We also perform a study research on the Exploit Database [16] which discovers the environment's vulnerabilities. This research is based on the results produced by the tools used during the assessment.

The assessment is performed using various tools such as Nessus [17], OpenVAS [18], Metasploit [17], Nmap [18], Spiderfoot [19], Tcpdump [20] Wireshark [20] and AnDOSid [21]. *Nessus* performs advanced port scanning, service enumeration and analysis, as well as vulnerability detection. *OpenVAS* executes advanced scanning and also classifies the discovered vulnerabilities according to the common vulnerability scoring system [22]. *Metasploit* performs a feasible vulnerability detection. *Nmap* and *Spiderfoot* are used for port scanning as well as for service enumeration. Shell and nse scripts are also used to automate the procedures and operations of the Nmap. Additionally, *Tcpdump* performs packet capture and *Wireshark* is used for packet inspection. *AnDOSid* stress tests the end service's operation using MDs.

### C. The Inside Perimeter and the Controller Node

On the internal networks side, the captured by *tcpdump* network traffic reveals that the attacker acquires access to critical data, such as information about the CC environment operation and the clients' PII. This event leads to the environment identification and to the network mapping which is used for the computing entities communication. Going further, the attacker can also obtain knowledge about the end service deployment and its vital components by simply using the OpenStack's documentation. The attacker can also manage to identify the OpenStack controller and the network nodes using the overall results gathered by the tools. It must be noticed here that the controller's ntp-service version adds a critical vulnerability to the system; the *ntp mon_getlist* vulnerability allows ntp reflection and consequently a DoS attack to a spoofed IP address inside the CC environment. This IP address could belong to a computing entity of interest and, thus, the entity services would be unavailable during the attack. Furthermore, the information regarding the nodes ntp service that is gathered by the *nse script* of Nmap, namely the *ntp_monlist.nse*, leads to the OpenStack controller node identification as the core computing entity of the environment. This event occurs due to the fact that since the OpenStack controller is the ntp server any instance synchronizes to it.

Moreover, the cloud administration dashboard environment consists of a vector of attack which resides on the controller. An attack that threats the dashboard is the password attack using a brute force method. This attack can be enhanced by password profiling using the tool CeWL [23] and by mutation of the created wordlist using John the Ripper [24]. Furthermore, a successful DoS attack on the OpenStack instances of the *autoscaling group* is also feasible by TCP flooding methods using the hping3 tool [25]. This attack leads to services exhaustion and to the unavailability of the end service. Additionally, information-assisted attacks which associate to virtual machine breakouts and side channel

attacks cannot be achieved as already discussed, whilst the attacker gathers information regarding the target from different sources by knowing the type of the CC environment. The majority of the described attacks are feasible in conjunction to insider threats.

### D. The Outside Perimeter and the Mobile Devices

On the external interface, TLS is utilised to achieve end-to-end encryption between the clients (e.g. the MDs) and the end service.

In more detail, *GoldenEye* [26] is used to perform a DoS attack against the IP address of the *Virtual LoadBalancer* that hosts the OpenStack instances. Each OpenStack instance delivers the end service through a web server. The result is to exhaust the resources of the autoscaling group, which accommodates the OpenStack instances, and to put considerable overheadon the LoadBalancer. The environment scaling mechanisms, such as the *policies* and the *triggers*, also assist the attack. However, the autoscaling group operates through an *availability zone*. Due to multiple availability zones having been established, the end service remains accessible and the threat is mitigated.

Furthermore, in the presented scenario, for the purpose of the MCC assessment a mobile application is created to enable the users to acquire access to the resources of the cloud environment besides the usage of a browser. The assessment approach followed is based on the reverse engineering of the mobile application to create a *rogue client* and then to obtain access to the resources of a legitimate user. It is derived that this above case only exists for MDs and their authentication process in particular.

During the security assessment, the usage of mobile applications as a means to carry out a DoS attack is taken into consideration. For the context of this attack, AnDOSid was used in order to perform an HTTP POST flood attack against the *Virtual LoadBalancer*. The effect was that the cloud defence mechanism of the availability zones is triggered. As a result, the DOS attack on the outside perimeter by the sMDs affects the operation of the end service by adding an overhead of delay to its delivery.

## V. Results

The SLA has the ability to offer protection by defining associated objectives to certain security issues. From the security point of view, the SLA achieves a differentiation between the responsibilities and the liabilities among the collaborative parties that exist during the CC operation. This differentiation is compulsory in order to achieve transparency between the parties in collaboration.

Moreover, cross-border regulations take into consideration the type of data that are transferred and processed. Despite the fact that the legacy environments were orchestrated by homogenous systems, the cloud computing environment consists of heterogeneous systems and technologies. To this end, the cloud computing paradigm introduces new capabilities which are highly associated with new vectors of attacks and risks which have not taken into consideration by the regulations.

Furthermore, to achieve a higher level end service security, it is necessary not only to define SLOs such as *reliability*, *authentication*, *cryptography*, *security incident management*, *logging*, *monitoring*, *auditing* and *vulnerability management* but also to continuously evaluate these SLOs with appropriate metrics during the end service delivery. Going further, data security is affected by objectives such as *transparency*, *responsibility*, *integrity* and *confidentiality*. In our work, the SLA is partially defined with respect to the expected end-service utilization by the MDs. The assessment which was performed on the CSP's inside perimeter, identified vulnerabilities that affect the reliability, the authentication, the monitoring and the service incident management. This assessment consists a part of the SLA; this part may be used to mitigate the identified vulnerabilities.

The evaluation results show that the majority of the services cannot be exploited due to a specific SLO; the *vulnerability*, which is responsible for the installation and configuration of the secure versions. Additionally, a system's security assessment is required in order to satisfy the incident management. In this vein, the security threats are identified and restricted to minimize their effects on data and operational information.

Moreover, the DoS attack performed on the outside and the inside perimeters also affected several SLOs; the *reliability*, the *incident management* and the *responsibility*. These SLOs were affected due to the absence of cloud security mechanisms during the attack.

The network traffic capture affected the SLOs named *integrity*, *confidentiality* and *monitoring*. During this event, the capture is not acknowledged by the monitoring; therefore, the PIIs are exposed to the attacker. It is evident that the security mechanisms of this CC environment lack the capability to protect it against network traffic capture attacks.

In addition to this, the security challenges of MCC are not completely addressed through the SLA of this CC environment when the MDs behave as thin clients. Nevertheless, in the case of an MCC environment implemented following the guidelines of [27] or [28], a suitable SLA capable to address the presented security challenges and issues can be defined.

Furthermore, the SLA does not foresee methods and protocols to make the CSP capable of facing DoS and DDoS attacks by MDs. The only countermeasures against these attacks are the cloud defence mechanisms. Additionally, the SLA lacks mobile application guidelines for the communication between the mobile application and the CC environment and as proved the client validation has to be improved.

## VI. Conclusions and Future Work

In this paper, we focused on how the motivation for security performance in cloud-based services meets new challenges when a cross-border data flow exists. Our study path was affected by on-going works at European and

international levels that focus on service level objectives as partial commitments of the SLAs. The used methodology aimed to assess a cloud-based service using mobile devices as end-points and to define the information the attacker has to acquire for exploiting the initial defence Cloud boundary. The assessment results aggregation led to the vulnerabilities definition that can be leveraged for the cloud environment exploitation.

Since the CC paradigm introduces a new suite of threats which are not included in the current legislative framework, one can conclude that the existing regulations are not adequate to craft an SLA with a high level of security. Nevertheless, by following the legislation, the CSP operates legally but with limited security concerns and constraints.

However, it should be observed that the most crucial and weak factor of a CC environment which leads to multiple attacks is the human factor; the insider threat. The majority of the performed attacks are feasible due to the insider threat according to which CSP employees acquire unauthorized access. Accordingly, the SLA should provide security with respect to the human factor. Moreover, the SLA can be assisted by a code of conduct that would define the authorised employee behaviour.

Furthermore, work needs to be done on governmental or regional legislation so as to strengthen the cross-border transfer of PII. Currently, the legislation lacks the necessary security guidelines to cover the existing threats of a CC environment. Also, security concerns at the organizational level should be addressed through the SLA definition.

To ease the MCC market adaptation, a unified contract (UC) between the mobile operator (MO) and the clients should be agreed. The UC should also orchestrate the standard contract for the mobile services delivery and the SLA. To this end, any MD could operate as a computing entity of the MCC and in turn it could optimize the quality of services and address the security issues of this environment. In addition, the MO would operate as a mobile cloud provider by appropriately modifying its infrastructure and the MDs' operational principles.

## ACKNOWLEDGMENT

The publication of this paper has been partly supported by the University of Piraeus Research Center (UPRC).

## REFERENCES

[1] Mazhar A., Samee U.K. and Vasilakos A., (2015). *Security in Cloud Computing: Opportunities and challenges*. Information Sciences, 305, 1 June, pp.357-383.

[2] Cloud Standards Customer Council, (2012). *Practical Guide to Cloud Service Level Agreements.* 10 April, pp.7-41.

[3] European Commission (2014). *Cloud Service Level Agreement Standardisation Guideline.* Digital Agenda for Europe: A Europe 2020 Initiative, 24 June, Brussels, Belgium.

[4] Zissis D. and Lekkas D., (2012). *Addressing cloud computing security issues*. Future Generation Computer Systems, 28(3), pp.583-592.

[5] Staiger, D. N. (2015). *Cross-border data flow in the cloud between the EU and the US*. In: Cheung A. and Weber R., (eds.). Privacy and legal issues in cloud computing, Edward Elgar, pp.96-117.

[6] International Standards Organisation (2015). *ISO/IEC CD 19086*. Cloud computing--Service level agreement (SLA) framework and Technology.

[7] Fernando N., Loke S. W. and Rahayu W., (2013). *Mobile cloud computing:A survey*. Future Generation Computer Systems, 29(1), pp.84-106.

[8] Zohreh S., Saeid A., Abdullah G. and Rajkumar B., (2014). *Heterogeneity in Mobile Cloud Computing Taxonomy and Open Challenges*. IEEE Communications Surveys & Tutorials, 17 May, pp. 369-392.

[9] Kulkarni P. and Khanai, R. (2015). *Addressing mobile Cloud Computing security issues: A survey*. IEEE International Conference on Communications and Signal Processing (ICCSP), 2-4 April, Melmaruvathur, India, pp. 1463-1467.

[10] Alizadeh M., Abolfazli S., Zamanid M., Baharunb S., Sakuraia K., (2015). *Authentication in mobile cloud computing: A survey.* Journal of Network and Computer Applications.

[11] European Commission, (2012). *Unleashing the Potential of Cloud Computing in Europe*. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012DC0529

[12] Fang L., Jin T., Jian M., Robert B., John M., Lee B. and Dawn L., (2011). *NIST Cloud Computing Reference Architecture*. National Institute of Standards and Technology, Special Publication (NIST-SP) 500-292, pp.1-35.

[13] Cloud Computing Reference Architecture and Taxonomy Working Group, (2015). *Cloud Computing Service Metrics Description.* National Institute of Standards and Technology, DRAFT, Special Publication (NIST-SP) 500-307, pp. 1-30.

[14] Cloud Computing Security Working Group, (2013). *NIST Cloud Computing Reference Architecture*. National institute of Standards and Technology, Special Publication (NIST-SP) 500-299, pp.18-192.

[15] OpenStack, 11th release Kilo. [online] Available at: https://www.openstack.org/software/kilo/

[16] Exploit Database. [online] Available at: https://www.exploit-db.com/

[17] Gusev M., Ristov S. and Donevski A., (2013). *Security Vulnerabilities from Inside and Outside the Eucalyptus Cloud*. ACM, New York.

[18] Jhala N. Y., (2014). *Network Scanning & Vulnerability Assessment with Report Generation* Master of Technology in Computer Science and Engineering, Department of Computer Science and Engineering, Nirma University.

[19] Spiderfoot. [online] Available at: http://www.spiderfoot.net

[20] P. Asrodia and H. Patel, (2012). *Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis*. International Journal of Electrical, Electronics and Computer Engineering, 1(1), 5 May, pp. 55-58.

[21] Huawei Enterprise ICT Solutions, (2013). *Huawei 2013 Security Research Report*.

[22] Common Vulnerability Scoring System. [online] Available at: https://www.first.org/cvss

[23] CeWL. [online] Available at: https://digi.ninja/projects/cewl.php

[24] John the Ripper. [online] Available at: http://www.openwall.com/john/doc/

[25] Srivastava A. and Chaudhary D., (2014). *Simulation of DOS, DDOS attacks & Design Test its Countermeasures*.International Journal of Scientific & Engineering Research, 5(1), January 2014, pp. 1801-1807.

[26] GoldenEye. [online] Available at: https://github.com/jseidl/GoldenEye

[27] Satyanarayanan M., Bahl P., Caceres R., and Davies N., (2009). *The Case for VM-Based Cloudlets in Mobile Computing*. IEEE Pervasive Computing, 8(4), October 2009, pp. 14-23.

[28] Huerta-Canepa G. and Lee D., (2010). *A Virtual Cloud Computing Provider for Mobile Devices*. 8th Annual International Conference on Mobile Systems, Applications and Services. 15-18 June, San Francisco, USA, pp. 1–5.