Forensics challenges of cross-border use of cloud services under special consideration of ENISA's contributions

report for "IMT6003 - COINS Summer School" @ Metochi
by PhD Candidate Andrii Shalaginov
andrii.shalaginov@hig.no
Høgskolen i Gjøvik, Norway

August 13, 2015

Abstract

In this report we will cover existing challenges in forensics readiness related to the cross-border use of cloud computing services. At first, we will cover the most common ways of building the infrastructure. Then, we will discuss the place of Forensics and way how the can be achieved by means of Forensics Readiness. Furthermore, we point the challenges related to this in cloud computing. Finally, the paper will present how the mitigation can take place and what are the contributions of ENISA's excellence initiative in it.

Keywords: Cloud Computing, Cloud Forensics, Forensics Readiness

1 Introduction

Cloud Computing has become extensively used in the recent decade. It denotes usage not only shared data, yet also infrastructure, platform and software services. Therefore, it is important to make sure that the Confidentiality, Integrity and Availability are preserved from one side. From another side, the assurance of a proper investigation of incidence has to take place. In this work we consider how to make sure that any privacy-related issues are preserved and all forensically-relevant information are preserved as much as possible to facilitate investigation when necessary in a shortest possible period of time.

Last decade characterized an ICT by a strong development of network-based services that help to overcome limitation of physical premises and provide a strong means of security. However, flexibility and cross-border access place new tear of challenges related to analysis of threats to privacy and possible commuted illegal activities. Digital Forensics in general provide a practice to approach such issues in a conventional manner that will give a forensically-sound evidences [1]. Yet since Cloud Computing implies usage of network technologies, different set of skills and considerations is require to approach the Cloud Forensics. Ruan et al. in 2011 made a study of the Cloud Forensics are in the overview [1]. It was stated that the Cloud Forensics is a self-standing area, which nevertheless can be treated as a cross-discipline between the Digital Forensics, Network Forensics and Cloud Computing. Moreover, the cross-border access to the shared pool of resources requires new way of thinking rather than applying Digital Forensics Process: Collection, Examination, Analysis and Reporting as defined by NIST SP 800-86 [2] in 2006. The main difficulties arise when it is necessary to preserve an order of volatility during data acquiring.

[1] `http://digital-forensics.sans.org/`

Application of Cloud Computing within an organization can take many forms, there exist several guidelines of how the Could framework can be built and what are the main features to keep track on. In this work we analyse the documents issues by National Institute of Standards and Technology (NIST)[2] in USA and guidelines provided by the European Union Agency for Network and Information Security (ENISA)[3] in Europe. Primarily, the contribution of this report is overview of the challenges related to forensics in Cloud and how it can be mitigated by means of awareness-training within an organization. Continuous training is one of the main components of the IT Security. This report is organized as following. The Section 2 provides an overview of the Cloud Computing framework that can be used inside an organization to facilitate business needs. Further, Section 3 will give an overview of the most common security challenges and suggested mitigation given by the ENISA's guidelines. Final remarks and discussions are given in the Section 4.

2 Cloud Computing within an organization

In this Section we provide an overview and motivation behind application of Cloud in organization and how it affects the business model in cross-border coverage. Every modern business model implicitly or explicitly includes IT services as inseparable part. Depending on the internal needs and physical locations of departments, it always includes some kind of sharing resources, which can be characterized as a Cloud Computing. At this point we can refer to NIST SP 800-145 Definition of Cloud Computing published in 2011 [3] that covers following important definitions

Cloud service models presents how the infrastructure is used and what are the responsibilities of the parties:

- *Software as a Service (SaaS)* uses software located in provider's site infrastructure.
- *Platform as a Service (PaaS)* allows to deploy own platform in provider's environment.
- *Infrastructure as a Service (IaaS)* gives a exclusive virtual or physical access to resources.

Cloud deployment models gives an overview of the properties of infrastructure with respect to used technologies and operational roles:

- *Private cloud* denotes ad-hoc own cloud solution, usually within organization's premises.
- *Community cloud* usually is for collaboration between organizations.
- *Public cloud* opened for access and usage by general public.
- *Hybrid cloud* encompasses several of mentioned before models.

Depending on the needs, CIO may report to CEO particular set of properties of the required Cloud Platform. There have to be counted many aspects that influence business process such that characteristics of market, threats to business continuity and possible impact of adversaries. Cloud Computing data security is one of the most important decision-making aspects since in modern world information makes value and business [4]. Breach in any of the CIA TRIAD may result not only in simple financial losses, yet also in legal litigations. We can see that depending on the service model, an organization may get an inexpensive solution with almost none control over the data as depicted in the Figure 1.

[2] `http://www.nist.gov/`

[3] `https://www.enisa.europa.eu`

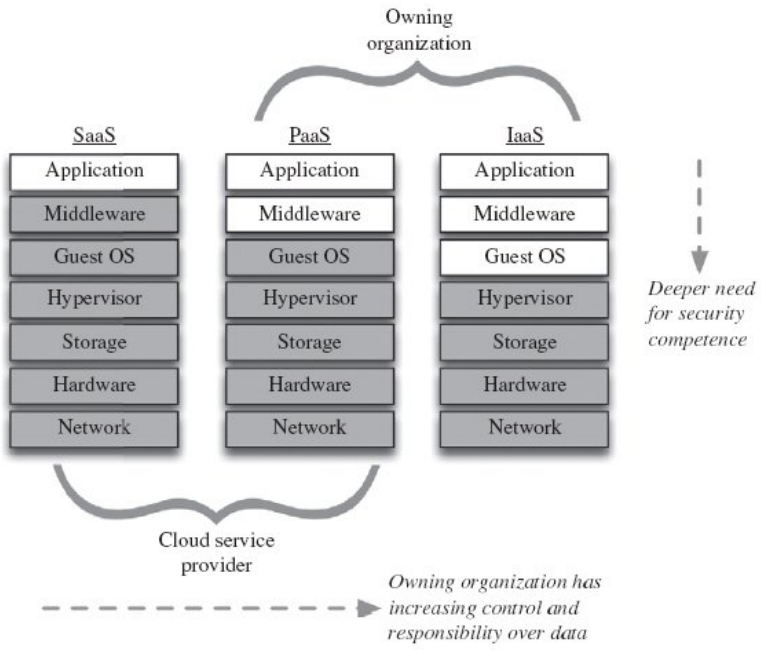

Figure 1: Dependence of security in organization based on different Cloud models [4]

We can consider an example of Cloud that facilitate Cyber Crime Investigations. Paterva[4] developed several intelligence solutions that offers a range of functionality for forensics investigation. Moreover, it might be possible to rent a virtual server to handle the cases information. However, there is an obvious threat to stored data since end user does not have a direct physical control over the stored information as indicated in the Figure 2. Therefore, our concern is inability to ensure forensics readiness when necessary over the borders and different policies adopted for customer and provider countries.

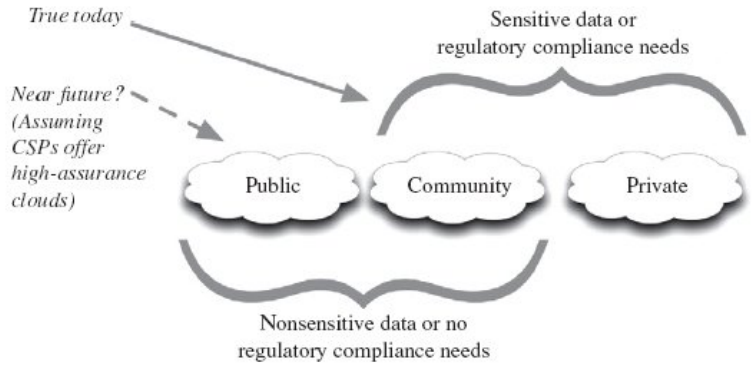

Figure 2: Data in different cloud deployment models [4]

Considering this grey-area of Cloud Computing, ENISA is heading an initiative on application of Cloud[5] since 2009 with a special focus on security. In particular, the risks of Cloud applications were analysed in the report [5]. Among other risks, there have been defined the lack of forensics readiness. In particular, risks R.30 and R.31 denotes that the security logs can be compromised due to range of reasons. There have also been a recommendations to improve

[4] https://www.paterva.com/web6/

[5] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

the evidence gathering and preservation mechanism when dealing with Cloud. So, we can say that the importance of the forensics readiness is high when using Cloud Computing since it may not only be useful for data security, yet also for possible criminal prosecution of adversaries in a less time and resources consuming manner.

3 Forensics Readiness Challenges and Possible Mitigations

Forensics readiness represent a set of practicalities that insure collection of useful data and decreasing the efforts and cost of forensic investigations as defined by Rawlington [6] in 2004. In this research, the author proposed ten steps that are necessary to ensure that forensics readies within an enterprise does not impact significantly business process. While from the other side the most important information is preserved in case if crime is committed. Keyun et al [1] in overview from 2011 showed that there exist three dimensions of cloud forensics: technical, organizational and legal due to the multi-jurisdictional and multi-tenancy operation over the borders. Berry et al in 2012 [7] presented a research on policy challenges of Cross-Border Cloud Computing. We have learnt that due to growing demand, multiple policies such that data privacy standards across Europe, US and Asia have to be adopted. Also there is a strong demand for guidelines on the international level as well as industry standards among the Governments. The importance of the legal compliance and regulations denotes the interaction within the Cloud that is deployed over different countries and physical locations. Based on the studied literature we can highlight the following forensics readiness challenges that can be found when making a decision regarding the structure of an organization's Cloud:

1. *Business continuity and data recovery* defines how the cloud forensics influences business processes and what the the benefits of following the readiness guidelines. The first step that describes implementation of forensics readiness according to Rowlingson [6] covers the purpose of evidences collection, possible threats to business when using Cloud. So, the aim is to understand where the forensics-readiness overhead will be useful for further mishandling analysis and incidence response. NIST Cloud Forensic Science Working Group in 2014 sketched the draft of possible challenges that forensics science faces in Cloud Computing [8]. The main problem is that the investigators has reduced capability of processing and control over the Cloud ecosystem. Potential overhead might be overseen under the need for artifices preservation on the Hypervisor or Virtual Machine Monitor layers. ENISA in the report from 2009 stated that Forensics Readiness is one of the key factors when deploying the Cloud.
2. *Logs and audit trails preservation and handling* is another valuable angle of Forensics Readiness in Cloud. From ENISA's study of risks in Cloud [5] we can see that one of the risks is "R.30 Loss or Compromise of Operational Logs", where a particular vulnerability "V19. Lack of Forensics Readiness" was identified. This vulnerability has the following properties: *"While the cloud has the potential to improve forensic readiness, many providers do not provide appropriate services and terms of use to enable this. For example, SaaS providers will typically not provide access to the IP logs of clients accessing content. IaaS providers may not provide forensic services such as recent VM and disk images"*. In addition to this, NIST studied the forensics challenges in Cloud Computing in 2014 [8] and selected following important log types: audit logs, security logs, and application logs. Another handbook produced by ENISA is Network Forensics [9], where the examples of log investigation and study are given with respect to incident response.

Finally in the teaching material by ENISA [10] targeted on Digital Forensics in general the recommendations for identifying auspicious activities by log examination were given.

3. *Assuring the compliance process* defines how the legal requirements have to be followed, in particular related to destroying evidences and private data handling. ENISA has published in 2013 [11] as practice guide for deploying Governmental Cloud securely. There have been touched challenges of cross-border cooperation with respect to EU legislations and country-specific regulations. As Rowlingson described in the first steps of forensics readiness [6], there have to be clear way for experts to perform investigations when regulatory and legal constraints are followed. It can be seen in the Figure 3 that there are many countries that have not deployed governmental cloud and do not have national cloud strategy. In overall, it can be a threat to a proper forensics readiness.

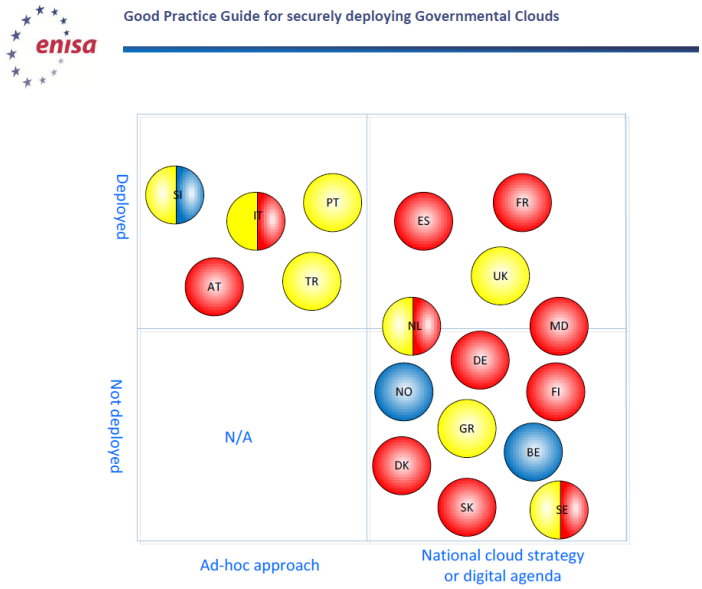

Figure 3: Representation of deployed models of cloud across EU [11]. Red means private Cloud, yellow means public and blue are community Clouds

So, the framework proposed by ENISA is structure via Plan-Do-Check-Act (PDCA) security paradigm of how the cross-border accreditation and certification of national programs can be performed.

4 Discussions & Conclusions

In this paper we discussed a challenges that can appear when dealing with Forensics Readiness in the Cloud Computing environments with respect to cross-border usage. At his point we looked into the Network and Information Security Agency (ENISA) recommendations and guidelines how this challenge can be mitigated. ENISA provides awareness training that helps to eliminate possible basic incompetence when dealing with forensics data collection in the network and cloud environments. Three main contributions are: awareness, guidelines and security framework for deploying governmental clouds. Using all this components, one can target establishing a proper Forensics Readiness routing as defined by Rowlingson [6]. Moreover, corresponding standards and regulations have to be considered when dealing with evidences preservation with regards to multi-jurisdiction and multi-tenancy in Cloud Computing.

References

[1] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in *Advances in Digital Forensics VII* (G. Peterson and S. Shenoi, eds.), vol. 361 of *IFIP Advances in Information and Communication Technology*, pp. 35–46, Springer Berlin Heidelberg, 2011. 1, 4

[2] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Sp 800-86. guide to integrating forensic techniques into incident response," tech. rep., Gaithersburg, MD, United States, 2006. 1

[3] P. M. Mell and T. Grance, "Sp 800-145. the nist definition of cloud computing," tech. rep., Gaithersburg, MD, United States, 2011. 2

[4] meshIP, "Cloud computing data security." `http://meship.com/Blog/2011/07/12/cloud-computing-data-security/`, July 2011. accessed: 04.08.2015. 2, 3

[5] ENISA, "Cloud computing. benefits, risks and recommendations for information security," `http://www.enisa.europa.eu/activities/cert/support/exercise/files/digital-forensics-handbook`: ENISA, September 2009. accessed: 03.08.2015. 3, 4

[6] R. Rowlingson, "A ten step process for forensic readiness," *International Journal of Digital Evidence*, vol. 2, no. 3, pp. 1–28, 2004. 4, 5

[7] R. Berry and M. Reisman, "Policy challenges of cross-border cloud computing," *Journal of International Commerce and Economics*, vol. 4, no. 2, pp. 1–38, 2012. 4

[8] M. Iorga and E. Simmon, "Draft nistir 8006. nist cloud computing. forensic science challenges," tech. rep., NIST, Gaithersburg, MD, United States, 2014. 4

[9] Sidiropoulos, "Network forensics. handbook, document for teachers," `http://www.enisa.europa.eu/activities/cert/training/training-resources/documents/network-forensics-handbook`: ENISA, February 2015. 4

[10] ENISA, "Digital forensics. handbook, document for teachers," `http://www.enisa.europa.eu/activities/cert/support/exercise/files/digital-forensics-handbook`: ENISA, September 2013. accessed: 03.08.2015. 5

[11] M. L. Thomas Haeberlen, Dimitra Liveri, "Good practice guide for securely deploying governmental clouds," `http://www.enisa.europa.eu/activities/cert/support/exercise/files/digital-forensics-handbook`: ENISA, September 2013. accessed: 03.08.2015. 5