Synthesis
International Scientific Conference of IT and Business-Related Research

STANDARD IMPLEMENTATION IN CLOUD FORENSICS

PRIMENA STANDARDA U CLOUD FORENZICI

Vladimir Dobrosavljević, Mladen Veinović, Ivan Barać
Singidunum University, Danijelova 32, Belgrade, Serbia

Abstract:
Everyday use of cloud services has exponentially increased primarily because of its popular price and because it is more convenient than the alternative physical computing services. Unfortunately, good marketing and lack of knowledge have lead many companies to enter the cloud without first performing a risk and security analysis. What happens when the cloud gets compromised is that you suffer a breach, and you find yourself in a position of having to conduct digital forensics and collect some data? What to do then? Is there an option to acquire data? Do you even know the location of your data? Can you tell if someone else has access to your data? Is the data located in the cloud service provider's data center or they have a data storage service with the 3rd party? It is recommended to consider these issues before the actual incident has happened. But what can you actually do? This paper shows the standards that can be implemented in Cloud forensics and procedures and contracts that will facilitate analysis on a daily basis.

Key words:
SaaS, PaaS, IaaS, SLA, SLO, ISO 27037.

Apstrakt:
Prisutan je porat u svakodnevnoj upotrebi usluga distriburanog internet računarstva (*Cloud services)* pre svega zbog popularne cene i brojnih pogodnosti u odnosu na alternativne usluge fizičkog računarstva. Nažalost, dobar marketing i nedostatak znanja primorali su mnoge kompanije da koriste ovakve usluge bez prethodno sprovedene procene rizika i bezbednosti. Ukoliko je virtuleno okruženje (oblak) kompromitovano, vi snosite štetu, i primorani ste da spovedete digitalnu forenzičku istragu i povratite podatake. Šta raditi u tom slučaju? Postoji li način da se povrate podaci? Da li znate gde se nalaze vaši podaci? Da li znate da li još neko ima pristup vašim podacima? Da li se podaci nalaze u bazi podataka u virtulenom okruženju (oblaku) pružaoca usluga ili uslugu čuvanja podataka pruža treća strana? Poželjno je pozabaviti se ovim pitanjima pre nego što do problema zaista dođe. Šta zapravo možemo uraditi? Ovaj rad upućuje na standarde koje možemo primeniti u Cloud forenzici (*Cloud forensics)* kao i na procedure koje bi olakšale redovno sprovođenje analize.

Ključne reči:
Softver kao usluga (SaaS), Platforma kao usluga (PaaS), Infrastruktura kao usluga (IaaS), SLA, SLO, ISO 27037.

1. INTRODUCTION

Cloud computing has become a dominant know- how in information technology, but with its many exciting features and low price for both enterprises and governments come unique and very serious security challenges.

Cloud itself presents a multi-tenant environment and highly virtualized environment, where processes for conducting forensic investigations are not fully developed and implemented.

In this paper, we shall focus on the analysis of the issues related to cloud forensics, connecting international standards with cloud forensics, and focusing on the current integration of cloud forensics into service level agreements (SLAs).

2. FORENSIC REQUIREMENTS

Law enforcement agencies and government agencies will require more proactive and reactive forensic support. The Cloud Service Providers will be obliged to log all the activities and have forensic support for all services offered and used by the customer. Different service distribution models (Software as a Service - SaaS, Platform as a Service - PaaS, Infrastructure as a Service - IaaS) offer basic terms of cloud forensics for everyday users.

a) **SaaS** model represents a model where the customization options and preferences of the customer are limited. The end-users do not have control over the physical infrastructure such as the network, servers and operating systems and do not have control over the source code of the application in use. All those things limit customer's ability to analyze log files and do forensics. Nowadays, SaaS solutions require that very detailed application logs are implemented on each application in cloud and rely on cloud service providers' support. Quite often, both sides must agree on the details about forensics, which is called Service Level Agreement (SLA).

b) **PaaS** model represents that the customer controls the entire development platform and all source code never leaves the development platform. Given these circumstances, the customer has a space to install any forensic tool and implement forensic options within his own application. Remote log collection servers can be installed and automatic logging option in applications can be implement creating a single repository of all logs and events, where multiple users can access and read logs, write-once, read-many (called WORM) principle. Although application logs cover all the logging needs of end user, some logs in PaaS deployment cloud model need to be done in cooperation with cloud service provider. Nevertheless, the end user is responsible for the functionality of the application, while the cloud service provider should guarantee that the application is

E-mail: dobrosavke@gmail.com
DOI: 10.15308/Synthesis-2015-139-142

available and operational. In that case, customer needs to create responsibility boundaries between end- users and cloud service providers when there is a need for forensic data. These responsibilities and boundaries must be documented in SLA between the end-user and cloud service provider.

SLAs may detail some procedures when accessing notification logs, identification logs, preservation logs, and access to all potential evidence sources (servers, switches, routers…).

c) **IaaS** deployment model, unlike SaaS and Paas, gives the user the greatest options for configuration along with great logging features and high level of control. Although end-user controls most of the components of the system including all log sources, some valuable information might only be reached from the inside of the cloud service provider infrastructure. This triggers the need to create a SLA between end users and cloud service providers and devote special attention to forensic data collection and logging.

3. SLA

As danger of compromising data becomes more critical for the business continuity, SLA needs to offer a window for forensic investigations. SLAs are agreements that have the legal power, which are validated by the signatures of end user and cloud service provider. More detailed sections of SLA are called objects – Service Level Objects – SLOs. In our case, forensics SLOs must be defined which determine the procedures that cloud service provider's needs to do in case of forensic data acquisition, including the methodology for evidence identification and evidence preservation of possible tampering with evidence and evidence damage.

Inside of cloud service provides infrastructure, each data node (server, router, switch...) can be a source of forensic data. However, the situation on the field is that the customers do not have access to all parts of the cloud infrastructure but cloud service provides for the needs of the forensic analysis allows end users a restricted evidence set. In a virtualized cloud environment, the hardest thing is to localize and identify all instances of data. For example, virtual instances of machines or applications used by a particular end user may migrate numerous numbers of times between various physical instances (servers) without or with small amount of recordkeeping. What kind of records do exist, and if they might be temporary and for how long can they be reachable. The access to the forensics data, evidence, may also be severely limited by price, degree of implemented technology (*e.g.*, available storage space and other storage options…), virtualization multi-tenancy, user's privacy implications and other conditions connected with the cloud service provider infrastructure.

All what has been noted so far recognizes the validity of SLA and it is very important to understand the sources of potential digital evidence and forensic data acquisition that will be available from cloud service providers, data size limit, and safe retention periods. All details within SLAs should be documented within SLOs.

4. ISO STANDARDS

There are many definitions of the Evidence Collection and Acquisition. Effective collection of digital evidence in an order for collection is provided by digital forensics. Evidence in question life expectancy represents the foundation for digital forensics. Nowadays, evidence mostly exists in the form of the volatile data located on the machines, and there is no reason to think that that data will be collected as digital evidence representing an important evidence for some case.

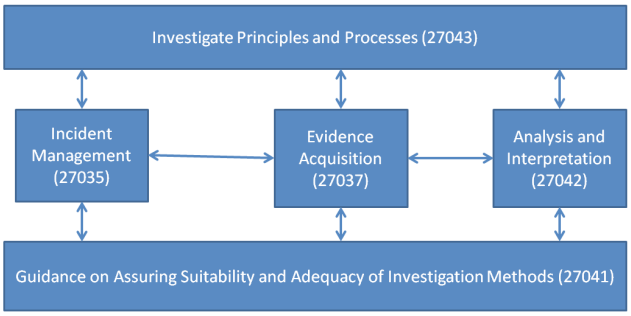

Figure 1: Implementation of ISO standards into the Digital Forensics process

ISO 27037 is the representative of an all-inclusive family of international standards which have a goal to create a common starting point in the forensic science. The main goal of ISO standards implementation in cloud forensics is to define processes and usability of evidence discovered during the forensic analysis in entity that is not under the same jurisdiction like the evidence requester. Thus, we can summarize that ISO standards do not need to replace local regulations or navigate national government's authority how to define and specify the digital forensic field of operations.

5. ISO 27037

ISO 27037 represents a relatively new standard (issued in October 2012) and the main goal is to set standards for good practice methods for forensic analysis and processing of digital evidence material. Although forensic analysts, forensic investigators, organizations and law enforcement agencies may use their own custom methods, custom processes and custom control processes, people assumed that standardization will lead to the creation of standardized if not identical procedures, making it easier to make comparison and contrast the results of such analysis even when performed by totally different persons or organizations.

One of the most important tasks in forensic data collection is the collection and preservation of forensics data in such a way that you can guaranty its integrity. Regular physical evidence or data is very important for the first and subsequent data collectors to link and connect all digital forensic evidence, making sure that the evidence is gathered and protected from tampering with the evidence. The main thing is that digital evidence must provide integrity and assurance that nothing suspicious has happened with the evidence. All this requires that information security controls are conducted and that the control results are met or exceeded.

Since ISO 27037 standard is the pioneer in digital forensics, it only addresses the initial steps of the digital forensics process: identifying, collecting, acquiring and preserving digital evidence. Other steps in digital forensics are dealt with in other standards that are still at the development phase.

The first step in the forensics process begins with the potential digital evidence identification, as shown in Figure 2. Formally, identification is the "process involving the lookup for digital evidence and recognition of digital evidence".

DOI: 10.15308/Synthesis-2015-139-142

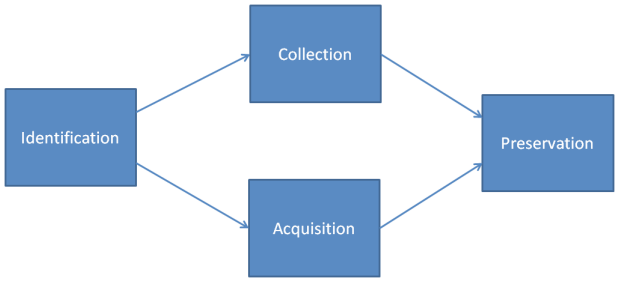

Figure 2: ISO 27037 procedure for Evidence Handling

Identification of digital evidence seems like a simple process, but it is actually quite opposite. There are a lot of small details and complexities that must be considered. For instance, representation of digital evidence can be both virtual and physical. Suppose we have digital evidence on an USB drive with some random info. The actual physical location of the evidence is the data center where USB drive resides, but the evidence is not the actual USB drive but the data loaded on it. Furthermore, the physical location can be easily changed since the USB drive can be attached to entirely new location and housed in a completely different data center. Another example is the data on the servers as a server may not have any attached disk cabinets and have its entire storage within a Storage Area Network (SAN) or Network Attached Storage (NAS).

After the process of identification and location of the potential digital evidence, it must either be collected or acquired:

- Collection – "Process of gathering digital material that might be considered to possess digital evidence."
- Acquisition – "Process of creating a copy of digital material within a defined set that might be considered to be digital evidence."

Collection process in a simple way of things represents standard law enforcement practice of taking items as evidence material under authority of a legal officer and taking them for a detailed analysis by forensic teams. This method has a 100% impact on the functional abilities of the subject of analysis. Acquisition is a more used method because it does not impact the subject of analysis and minimizes the impact on business continuity of an ongoing investigation. All this makes acquisition more preferable method than collection. However, collection is a must in some cases, especially when it comes to the cloud environment where everything is virtual, and can simply jump from one resource to another.

We must make a point that the subject of forensic analysis can easily be copied during the acquisition process and can easily make a forensic image. For example, forensic evidence can be acquired from any type of memory such as: hard drive, server's RAM memory… but can be acquired from users all in favor of the investigation. This leads to the conclusion that all the data acquired are very similar: they represent an identical copies of the subjects of forensic analysis and must be made using a standardized, documented process. The next thing we should do is to include the evidence copied that has not been tampered with or evidence that the integrity of the copy was not compromised. This makes acquisition more challenging and complex than collection because there need to be mechanisms for all the types of the forensic analysis subjects, and this represents a never-ending process as the technology keeps evolving on a daily basis.

Upon the process of collection or acquisition, we come upon the next challenge which represents data preservation. ISO 27037 has a definition of a preservation process that says "preservation is a process to keep and guarantee the integrity or/and original contents of the potential digital evidence". The most important part of the evidence handling is the preservation of evidences, because if we used the standard procedures for acquisition the evidence will be good for nothing if are not preserved on the proper way. Evidence preservation is a very important thing to assure credibility in a court of law. Although digital evidence is notoriously fragile, and must be handled with most attention, it can be easily changed or destroyed. Since the court processes can last very long data might be sitting in the forensic laboratories from six months to a year, potential digital evidence may lay untouched a very big period of time in safekeeping facilities before it is actually used in a legal process. All this indicates that evidence preservation must be considered with caution and with most care. Safekeeping facilities require access control policies to prevent/protect the potential evidence from tampering with, as well as the appropriate storage conditions.

6. DIFFERENCES BETWEEN CLOUD FORENSICS AND TRADITIONAL FORENSICS

Although cloud forensics and traditional forensics have the same basis "forensics", they are completely different. As regards the traditional forensics, cloud forensics has unique challenges, techniques and borders. Although most people do not differentiate between cloud and traditional forensics, there are unique things for each field of forensics.

The primary challenge in cloud forensics is how to identify the evidence. For instance, in IaaS cloud deployment environment, we can easily determine the data location on the servers if the data is located on the direct attached storage. However, along with a virtualization technology progress, more and more servers do not have direct attached storage units but mapped storage devices which have become much more complex, which is particularly visible in the virtualized cloud environment. For instance, a group of physical disk devices can be represented as a set of logical units (LUNs) and presented to a cloud user using iSCSI protocol (or to a server supporting a cloud user using any other protocol FCoE, NFS…), because they are cheaper, more reliable and have better performance than directly physical disk devices. These logical units may be easily moved from place to place using the storage migration techniques in a different case scenarios (perhaps storage instance "A" needs to be turned off for annual maintenance so the content of the storage A will be migrated to storage "B"). This is the entirely transparent process for end user and he is not aware of anything happening. From the forensic data acquisition point of view, identification process would have to be fully opened and frequent migration must be noted to assure that the correct data was acquired.

It is important to note that when data migration occurs it does not becomes permanently deleted and the remnants of the data can be used as potential evidence, because it is possible to recover the data from logical units on "A" within the scope of the investigation.

7. SUMMARY

In this paper, we described how we can use standardization and what mechanisms can be used in forensic investigation in cloud environments, described the basis of international standards that can be applied for cloud forensics, and summarized requirements that stand up to cloud forensics into service level agreements (SLAs) and compared cloud and traditional forensic techniques.

DOI: 10.15308/Synthesis-2015-139-142

As new technology gets adopted, security challenges arise from those adoptions and all challenges are followed with security analysis and digital forensics. Cloud, as one of the newest technologies, must be considered and forensic readiness must be provided.

At last, cloud end users must be aware that they need to make arrangements with cloud service providers to ensure data collection and acquisition so that cloud service providers can respond appropriately to forensic investigation requests because ends users can easily end up with data loss from hacking activities in the cloud.

When end users decide to transfer their sensitive data and services to the cloud, end users should form a SLA written in explicit language with SLOs marked as priority ones to ensure that they can rely on the cloud service providers when they need to perform some digital forensics activities.

Cloud service provides must think about comprehensive offer of their cloud services and must offer forensic capabilities because that will make end users more comfortable and will probably lead to revenue increase. As cloud is seen as a logarithmic expansion rate, and more and more companies move their businesses to the cloud, digital forensics will be a key feature for accepting the cloud as the best business critical solution.

Acknowledgements. I **would like to express my great appreciation to** *Singidunum University and especially, the professor Mladen Veinović, for his unselfish support and understanding.*

REFERENCES

Dykstra, J., & Sherman, A. (2011). Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies. *Proceedings of the 2011 ADSFL Conference on Digital Forensics, Security, and Law, pp. 25-31.*

Dykstra, J., & Sherman, A. (2012). Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing. *Digital Investigation,* 9(2012), 90-98

Grispos, G., Storer, T., & Glisson, W.B. (2014). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. *Cryptography and Security*. 4, 28-48. DOI. 10.4018/jdcf.2012040103

ISO. (2012). ISO/IEC 27037:2012 - Information technology -Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence. Retrieved from http://www.iso27001security.com/html/27037.html

National Institute of Standards and Technology. (2014). *NIST Cloud Computing Forensics Challenge*. Retrieved February 12, 2015, from http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

Willson, D. (2013). Legal Issues of Cloud Forensics. *Global Knowledge, Expert Reference Series of White Papers*, pp. 2-4.

DOI: 10.15308/Synthesis-2015-139-142