American Journal of Networks and Communications
2019; 8(1): 23-31
http://www.sciencepublishinggroup.com/j/ajnc
doi: 10.11648/j.ajnc.20190801.13
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

Forensics and Digital Criminal Investigation Challenges in Cloud Computing and Virtualization

Pedro Ramos Brandao

Interdisciplinary Centre for History, Cultures, and Societies, Evora University, Evora, Portugal

Email address:
pb@pbrandao.net

To cite this article:
Pedro Ramos Brandão. Forensics and Digital Criminal Investigation Challenges in Cloud Computing and Virtualization. *American Journal of Networks and Communications*. Vol. 8, No. 1, 2019, pp. 23-31. doi: 10.11648/j.ajnc.20190801.13

Received: May 15, 2019; **Accepted**: June 17, 2019; **Published**: July 9, 2019

Abstract: I'll address the fundamentals of Cloud Computing and Virtualization. The types of cloud computing deployment models and their relationship with the responsibility of the users are developed. The fundamentals of digital criminal investigation applied to Cloud Computing are discussed, and the most significant challenges are presented to criminal investigation and forensic sciences in this type and digital environment. The implications of Virtualization used in Cloud Computing in Criminal Investigation and Forensic Science are discussed. The paradigm case of Nested Virtualization technology is presented as an obstacle to Criminal investigation and forensic investigation. In cases of criminal investigations in traditional environments, it is common practice for computer expertise to turn off the equipment and make a copy of the disks that will be analysed later in the laboratory. This is unfeasible in a cloud computing environment, due to the large storage capacity, legal issues, geographic distribution and data control, which may vary depending on the model of service contracted. In addition, lack of physical access to data collection and lack of control over the system make information acquisition a challenging task for cloud expertise. Therefore, forensic computing has been restructured, bringing new techniques, solutions and research methods, giving rise to cloud forensics or expertise in the cloud. Thus, the so-called Forensic as a Service (FaaS) is dedicated to solving the security challenges inherent in the cloud environment. In this paper we will analyse some of these challenges.

Keywords: Digital Forensic Science, Virtualization, Cloud Computing, Digital Criminal Investigation

1. Introduction

The distributed computing system called Cloud Computing is changing the way information platforms and information itself is created and used. Investment in Cloud Computing is growing five times more than in traditional computing systems, particularly in the areas of on-premises networks and information and technology services. This type of distributed computing is an evolution of the technology in the model of multiple stakeholders, independent of the location, elastic, measured as a function of the consumption of the computational resources used. These computing resources include networks, servers, processors, memory, hosting systems, specific applications, and security services. Cloud computing technology enables users (individual or business) to scale-up and scale their computing needs at low cost with a high level of efficiency, and sometimes without the complexity of the standard technological requirements of any structure.

Until now, forensic tools were quickly developed for use in investigations because encryption is not widespread as it is today. Now, forensic analysis faces new technologies in virtualized operating systems, different file formats, growing data sizes, ample storage devices, and also cloud computing that by themselves defy all the basics of digital forensics.

Traditional digital forensic methods are often criticised when applied to cloud computing in their admissibility of evidence in court due to various technical issues. Examples of such problems are decentralization of data, segregation of customer data, jurisdictional areas, loss of metadata in the chain of custody, etc.

Apart from this, there is still a question of pure inability to obtain data through legal expertise. Virtualization, used in Cloud Computing, in its latest versions can prevent access to data, such as using data on a virtual server hosted on a

Virtual Nesting system, if someone erases the disk and the virtual machine in nesting, data will not be recoverable.

If it is necessary to comply with the stipulated in Point 1 of Article 15 of the Portuguese Cybercrime Law, and if we have to develop the research in a Cloud Computing structure severe problems and obstacles to the execution of this diligence will be found. And this happens because virtualization and cloud computing have established a new paradigm over traditional computing and computing. In this work I will develop the particularities of Cloud Computing that can interfere with forensic investigations, the main challenges created by Cloud Computing for Forensic Sciences will be explained. Cloud computing today is based on virtualization, this alone brings enormous difficulties to forensic investigation, so we will analyse the significant challenges that virtualization poses to digital forensic science. Finally, we will give a practical example of a forensic examination in specific server virtualization environments. And this is a technical and not a legal aspect. Therefore, we will not address problems such as the transnational obtaining of evidence and sovereignty issues, but rather the difficulty of finding data that is "spread" by several data centres due to the characteristics of the distributed questionnaires, the question of cross-border data jurisdiction is not addressed because it is not, in essence, a technical matter.

2. Fundamentals of Cloud Computing

2.1. The Architecture

Cloud computing anticipates substantial isolation of the applications and information, infrastructure and mechanisms that we use to support it so that the one can dynamically allocate the available resources whenever requested. Most of the time, cloud computing is directly linked to virtualization technologies (the definition of which is a computer-generated abstraction), specifically for the ease of configuring and making available the integration, scalability, mobility, and dynamic storage of the resources used.

For computer forensics, it is relevant to understand the impact that the distributed computing architecture and the consequent dispersion of the information, used in Cloud Computing, brings to the collection of evidence, since, for example, data can be distributed by several countries [1].

2.2. Main Features

The abstraction of infrastructure:

The computing, network and storage infrastructure is isolated from information and application resources. For the point of view of the application and the services made available no matter where and by what means the data is processed, transmitted or stored.

Resources democratization:

A logical consequence of the abstraction of infrastructure, the democratization of resources, be they infrastructures, applications or information, allows them to be made available as a pool to those who have the authorization to access them.

Architecture-Oriented Services:

The abstraction of infrastructure and the democratization of resources lead to services oriented to architecture, where resources can be accessed and used in a standardized way. Thus, the focus is on the delivery of services and not on infrastructure management.

Elasticity/ Dynamics:

High levels of automation and virtualization, in conjunction with faster and more reliable connectivity, allow resource allocation to be expanded or retracted to meet the requested capacity. Thus, the resources can be better utilized and the levels of services more easily achieved.

Consumption utility and storage:

The four characteristics, previously explained, combined allow the visibility at the atomic level of the resources, by service providers. This visibility allows for models of cost and usage (the contractor of service can consume it at will, but will pay for everything provided and consumed) are implemented. And this leads to improved environmental management, with increased scale and predictable costs [1].

2.3. Models of Service Provision (Figure 1)

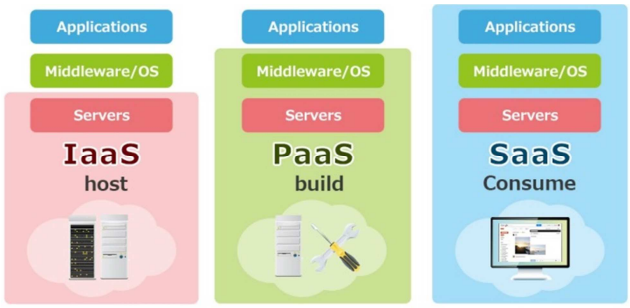

Figure 1. *Cloud Computing Services Delivery Models.*

2.3.1. Software as a Service (SaaS)

What is offered in this model are applications that run on the cloud infrastructure and can be accessed by thin clients, such as browsers. The user/ consumer does not manage or control the infrastructure used by applications (network, storage devices, operating systems, etc.), or even application settings (except for a few specific configurations).

Key points:

a. The service provider supplies applications. The user does not manage or control the underlying cloud infrastructure or individual application capabilities.
b. Services offered include: Enterprise services such as workflow management, groupware and collaborative, supply chain, communications, digital signature, customer relationship management (CRM), desktop software, financial management, geospatial, and search.
c. Web 2.0 applications such as metadata management, social networking, blogs, wiki services, and portal services.
d. Not suitable for real-time applications or for those where data is not allowed to be hosted externally.

e. Examples: Office 365, Salesforce.com, Gmail.

2.3.2. Infrastructure as a Service (IaaS)

Consumers use the cloud infrastructure to make their applications available that must be developed in languages supported by the service provider. The user/ consumer does not manage or controls the infrastructure used by the applications (network, storage devices, operating systems, etc.), but has full control and responsibility for the apps available.

Key Points:

a) It allows a cloud user to deploy consumer-created or acquired applications using programming languages and tools supported by the service provider.

b) The user:

i. has control over the deployed applications and, possibly, application hosting environment configurations.

ii. It does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

c) Not particularly useful when:

i. The application must be portable.

ii. Proprietary programming languages are used.

iii. The hardware and software must be customized to improve the performance of the application [2].

2.3.3. Infrastructure as a Service (IaaS)

What is offered to the consumer in this model is the rental of processing, storage devices, networks and other resources considered essential. The consumer can run any software (such as various operating systems and applications) and he is responsible for it.

Key Points:

a) The user can deploy and run arbitrary software, which can include operating systems and applications.

b) The user does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of some networking components, e.g., host firewalls.

c) Services offered by this delivery model include server hosting, Web servers, storage, computing hardware, operating systems, virtual instances, load balancing, Internet access, and bandwidth provisioning.

2.4. Implementation Models (Figure 2)

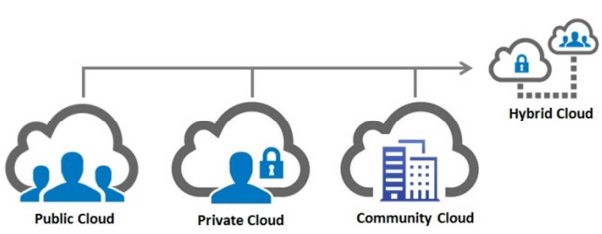

Figure 2. *Cloud Computing Implementation Models.*

2.4.1. Private Cloud Computing

Also known as Internal Cloud. Its main characteristic is that it is offered by the organization itself, or by the service provider that the organization indicates, that will consume the resources. And a dedicated operating environment that adds the features and characteristics of cloud computing where it is available. The physical infrastructure is the organization's infrastructure and may be located in your datacentre or service provider's datacentre as determined. In this way, the users of the services are considered reliable (staff/ employees, third parties and others that have some contractual relationship with the organization). Untrusted users are those who are not logical extensions of the organization, even if they somehow consume the services of the organization [2].

2.4.2. Public Cloud Computing

Service providers offer them. The operating environment offered, encompassing all the features of cloud computing, can be dedicated or shared. Consumers of services are considered unreliable.

2.4.3. Hybrid Cloud Computing

This system is widely used nowadays because it divides levels of security and privacy. A part of the network is in Private Cloud Computing, that is, within the perimeter of physical security of the company, another part of the network is in a system of Public Cloud Computing, that is, an external provider of cloud computing. Nevertheless, both methods are interconnected and synchronized [2].

2.4.4. Community Cloud

It is a particular type, and sometimes it is not considered in the groups of implementation models; hence it adds parts of the previously mentioned models:

a) The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

b) It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

2.5. Reference Model

The CSA describes a reference model for cloud computing that illustrates how service delivery models are orchestrated and layered. The highest layer (SaaS) depends on the next lower layer, which supports it. The lowest layer, IaaS, serves as the basis for the others. It shall be taken into account that this is a reference model that fulfils its role of clarifying the relationships of the cloud computing service delivery models and the orchestration models of an entire IT structure [2].

2.6. Security Architecture

The security architecture will depend on the combination of the availability model and the mode of contracted consumptions. The availability model will define which

controls are to be implemented and how this implementation should occur since there are specific controls for each layer of the reference model. An example of this is that in the IaaS model there must be physical level controls (alarms, guards, etc.), whereas in SaaS they are the controls as a firewall for web applications. The mode of consumption indicates who will be responsible for administering the controls. Thus, for example, in the case of the private modality, the contractor will be responsible for the administration of the security architecture. In the public mode, the cloud computing service provider is responsible for administering security architecture [2].

3. Civil Liability by Availability and Implementation Model

About issues of responsibility and ownership of systems in Cloud Computing, it is necessary to pay close attention to the availability models.

If we want to analyse forensic network equipment such as switches or routers used by someone using Cloud Computing at the Software-as-Service Model level, we can never implement this investigation at the level of the suspect user; infrastructure provider, even though he is not suspected of any wrongdoing.

The same applies in the case of a suspect making use of Cloud Computing at the Platform-as-service Model level since he does not have access to the configurations of the intermediate network equipment.

In the case of a suspect use of the Software-as-Service Model and whose objective is to investigate the configurations and logs of a client application of its electronic mail, it can be directly applied to that user, since it is responsible for the content of use of this layer in the said model [2].

In legal terms, it is very important to understand the responsibility and manipulation capacity of a suspect of a crime, because the responsibility varies depending on the type and model of service (Figure 3).

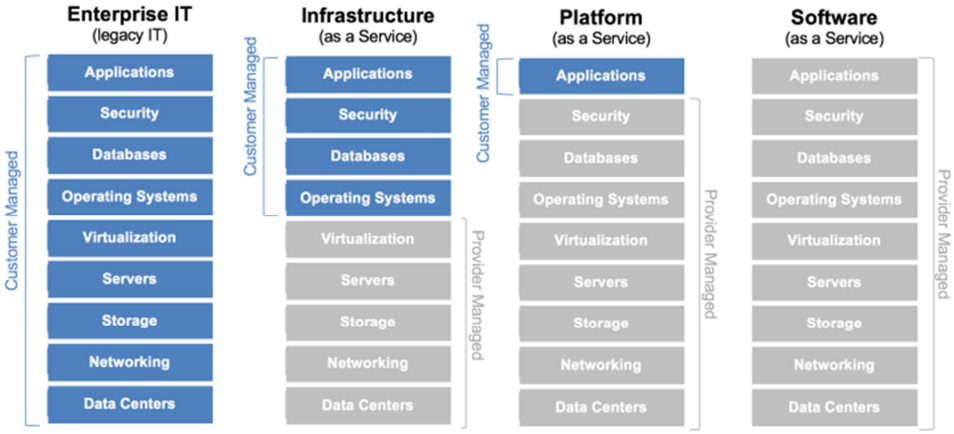

Figure 3. *The heads of each service according to the Models, and costumer layer responsibility.*

4. Cloud Forensics: Fundamentals

We can define cloud forensics as the application of digital forensics to Cloud Computing. It is, therefore, a cross-cutting area of digital forensic science. NIST recently created a workgroup for this area and defined it as follows: "Cloud Computing forensics is the application of scientific principles, technological practices and derived and proven methods to process past Cloud Computing events through identification, collection, preservation, examination, and reporting of digital data for facilitating the reconstruction of these events." [3]

The exceptional nature of cloud computing technological environments, such as shared computing, data duplication due to georeferencing and principles of distributed computing, jurisdiction, and a high degree of virtualization with the use of multiple computational layers, making these layers of complexity for forensic science applied to cloud computing. It makes it possible to follow a chain of events in this environment. Unlike a classical computing scenario. We cannot apply the forensic process used in traditional computing and networking systems in cloud computing. Forensic science involved in Cloud Computing (Cloud Forensics) contemplates three dimensions: technical, organizational and legal. [4]

This paper will focus more on the technical aspect.

The technical dimension covers the procedures and tools needed to develop the forensic process in a cloud computing environment. Includes: data collection, online forensic procedures, segregation of evidence, and proactive measures.

The organizational dimension slows down all regulatory aspects, including CSPs, clients, legal advisors, incident handling, etc.

The legal dimension deals with regulations and laws that ensure the legality of forensic actions in a cloud computing environment, such as jurisdiction over the location of data, etc. [4]

4.1. The Forensic Process in Cloud Computing

The forensic process begins after an incident, such as an

action after activity. And it follows a set of predefined steps. In Cloud Computing this process can be grouped into three areas: Client Forensics, Cloud (server) Forensics and Network Forensics.

4.2. Forensic Procedures at the Client Level (Client Is Understood Here as Client Operating System in Counterpoint with Server System)

Digital crimes are usually initiated on the client side of computer systems; however, digital objects are always left on the client side and not served. The collection and identification of evidence on the client side is a significant part of this process. Evidence such as log history, data dates, registry data, log access, logs of conversations, the persistence of authentications, cookies, can be found easily on the client used by the suspect. [6] It is critical that evidence be collected as soon as possible in its sterile state so that it can effectively be used as evidence, which in the environment, for example, virtualization (as we will see later), is extraordinarily difficult, even at the customer level, because we are talking about a virtual computer. In the case of traditional clients, there may also be events that lead to the destruction of evidence, mainly if the user is a computer professional.

The proliferation of customer endpoints on mobile devices makes this work even more difficult for evidence/ evidence collection. [4]

For forensic science applied to cloud computing, it is essential that such evidence is collected promptly to ensure its integrity and to enable the eventual creation of a timeline of events.

4.3. Forensic Procedures at the Cloud Level (Server)

Much of the evidence to be collected in forensic cases lie at the heart of the server, and they are a significant part of clarifying what is being investigated. These digital pieces of evidence are log systems, log applications, user authentication, access to information, database logs, etc. The physical inaccessibility of access to these systems is a huge problem, the lack of knowledge of the storage location (the characteristic of the distributed systems) is a gold problem, all this makes it difficult to collect evidence in Cloud Computing. In cloud computing systems with virtualization, it is common for a user's data to be stored in different places and simultaneously in several areas, that is, in several simultaneous data centres. [7]

Virtualization is another problem; instances of virtual machines can have a high factor of movement between hypervisor servers, even keeping it running. Switching virtual machines from one server to another is effortless. That is, it is elementary to transfer virtual servers from one data centre to another located on another continent; this can lead to problems of cross-border jurisdiction.

4.4. Forensic Procedures at the Network Level

Forensic procedures at the network level typically deal with the analysis of network traffic logs. These procedures are theoretically possible in cloud computing environments. The TCP / IP protocol, through its layers, can provide different information about the traffic between virtual servers. The problem is those server providers that own the infrastructure, as a rule, do not keep logs of the network activities of their clients' virtual servers. Network analysis in Cloud computing is therefore much more difficult, in some cases impossible, in the case of virtual networks based on new synthetic switches (as we will see later). [8]

5. Critical Challenges for Forensic Investigators in a Cloud Computing Environment (Tools and Methodologies)

There are numerous difficulties and challenges in digital forensics applied to Cloud Computing. Most of the tools used in digital forensic investigations are geared to offline inquiries, with the assumption that the storage of the data under study is under full control by the investigators.

Tools and methodologies that can assist in extracting and analysing possible acceptable evidence in legal procedures are limited and significantly dependent on the service model or deployment model adopted in cloud infrastructure and on how a cloud service provider manages these models [9].

Traditionally in digital forensic investigation, investigators identify a crime as follows:

a. If an individual makes a complaint,
b. Detection of anomalies in intrusion detection systems,
c. Auditing a computer system or network.

Identifying a crime in a cloud computing system is very difficult to do in the way it is done in other digital systems.

The complexity of forensic investigations in cloud computing environments is usually related to the following challenges:

a. Access to evidence through logs.

The distributive nature of Cloud Computing makes data identification very difficult. The availability of logs is dependent on the Cloud Computing implementation model. In Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) is extraordinarily difficult because access is minimal, identification is easier on Infrastructure-as-a-Service (IaaS), but access is not total either. Cloud Computing systems are volatile by nature, so researchers always need to access logs, it happens that most Server Provider never keep records of their clients' activities [8];

b. Volatile data.

Everything in Cloud Computing is volatile, volatile data in Cloud Computing means that as soon as the virtual machine is shut down, all data is lost. Not even the traditional RAM parsing processes are feasible because most virtual machines use the dynamic RAM method, which does not allow any data maintenance or capture. This volatility in Cloud Computing is a direct consequence of using virtualization;

c. Lack of system control.

Cloud Computing systems are based on demand-based access to a set of resources that are always in a pool, sometimes shared, and made available through virtual devices, the exact location of these resources is never known to users, and researchers. Only the service providers understand the precise location of the resources. Cloud Computing users and researchers have no control over real systems, which puts a lot of problems for forensic investigators when they want to collect evidence;

d. Lack of information on the part of the client.

In Cloud Computing everything is under the control of the Cloud service provider (CSP), and Cloud Computing users can have some interaction with the CSP. Some lack of transparency on the part of the CSP combined with little international regulation leads to the loss of valuable information in the case of a forensic investigation. This issue applies to the three Cloud Computing implementation models [10];

e. Data integrity.

Researchers need to maintain the integrity of the evidence to preserve the integrity of the original Cloud data, and this is extraordinarily difficult. It is complicated to keep your Cloud Computing data untouchable. Even because this goes against the technological nature of distributed computing systems, maintaining data integrity is the most challenging part of a forensic investigation process in Cloud Computing because the original data cannot be changed so that it can be presented in court as evidence. It is complicated to stop data change or keep a file unchanged in a cloud computing system, by the technical nature of the system the data is always being changed or at least receiving network information, which changes the metadata immediately. The sophisticated redundancy and anti-disaster systems inherent in cloud computing systems mean that data is always being changed even if users are not accessing it [11].

f. The isolation of instances in Cloud Computing.

When there is a crime researcher need to isolate the instances that are in Cloud Computing to preserve the integrity of the data. Now separating cases in Cloud Computing is a complicated thing and cannot be applied quickly, such as turning off a computer and isolating the hard drive. And this is impossible in Cloud Computing. It is a technically complex process and requires several phases to be accomplished and, in some cases, impossible, such as isolating a virtual machine that is operating under the system of nesting virtualization (which we will address at the front) [12].

g. Few existing cloud forensics tools.

Current Cloud Computing is a set of modern and very sophisticated technologies. Forensic sciences are not yet equipped with the tools to do everything they do in regular digital research, and many tools are missing for forensic investigation in Cloud Computing. For example, the software is often used to make hard copies of hard disks, and these tools are not used to make copies of virtual disks, which are those that exist in Cloud Computing [13].

h. Correlation of evidence through multiple sources.

In Cloud Computing a resource is shared by several users; consequently, the evidence is spread across several resources, which brings several problems to researchers. For again it makes it challenging to maintain data integrity because the nature of Cloud Computing is the sharing of resources.

6. Virtualization and Forensic Science

6.1. Definition

Virtualization is the creation of abstraction of something that exists physically, such as an operating system, a server, hosting devices or network devices, etc. The virtualization of a server changes the rules of the traditional model of physical system operation, in which a physical server plays the role of a host server, where a hypervisor is installed and where several virtual machines are installed. Virtualization enables the creation of multiple virtualized resources from physical resources. This form of virtualization maximizes resource utilization. Virtualization, as already mentioned, is not CC, but substantially facilitates the establishment and management of Cloud Computing (CC). Virtualization can be defined as an abstract layer and can exist as part or all of the IT Stack. In other words, virtualization can be represented as the process of implementing a set of technologies capable of camouflaging the physical characteristics of the resources of the servers, network resources, and hosting resources, as usually systems, applications or end users interact with those resources [14].

6.2. Virtualization in Technical Terms

Server virtualization is the primary domain of virtualization where a (physical) server is converted to a virtual server. The term "physical server" is often used by virtualization vendors to describe the difference between a virtual server and a physical server [12]. The physical server refers to the hardware that does the actual computing processing imposed by the software, such as the operating system and applications. A virtual server cannot operate without a physical server. With server virtualization, multiple physical servers can be converted to virtual servers and placed on a physical server, which is called the host. Virtual servers, in turn, are called the guests. Figure 4 and Figure 5, represent the difference between a traditional server architecture and a virtual server architecture.

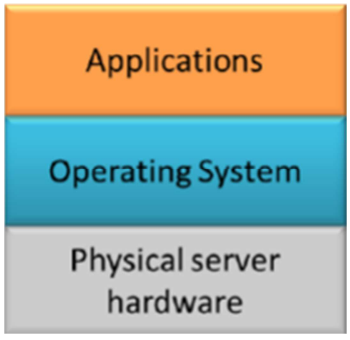

Figure 4. *Traditional Architecture.*

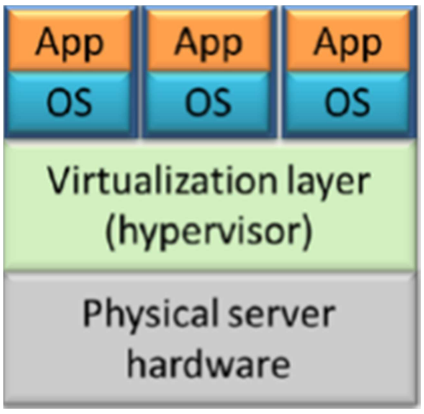

Figure 5. *Virtual Architecture.*

Both traditional and virtual architecture showcase your server architecture. In the lower layer, both architectures are composed of a set of hardware computing, such as a central processing unit (CPU), memory, a network card (NIC), and a local hard disk. The hardware is placed inside a "box" or enclosure and is called a physical server, in which the software, an operating system (OS) and applications, is installed at the top. However, OS or application installation on a traditional server architecture is very vulnerable to changes or failures in the hardware layer. Changes to hardware or hardware configuration failures can immediately result in an OS malfunction, which means that the physical server needs to be repaired with the same hardware configuration or require a reinstallation of OS and applications. With server virtualization, a virtualization layer is placed above the physical server hardware and under the OS and application layers. The virtualization layer makes it possible to install multiple sets of OS instances and applications on a physical server. Each OS set has applications and functions similar to the traditional server architecture, with the difference of running multiple instances on a physical server instead of just one instance. Besides, the virtualization layer isolates each set from each other, which causes one instance to be unaffected by failures or changes to other instances or hardware. All instances "judge" to be the only instance on the physical server, and are not aware of other virtual instances. These instances are called virtual machines or virtual servers. As shown in Figure 5, virtualization decouples the software server (OS and applications) from a given set of hardware, which makes it independent of a specific hardware configuration that is required to function. In this way, a virtual machine can operate on physical servers that use different hardware configurations. Another feature of server virtualization is that a traditional physical server with a specific configuration of an OS and applications can be converted to a virtual server or virtual machine. Some authors define a virtual machine as the efficient and isolated duplication of an actual device. By real machine is meant a traditional server architecture, with a single OS and applications. However, the use of virtual machines with server virtualization goes beyond the duplication of a real device [14].

6.3. Virtual Machine

A virtual machine is the virtual representation of a physical server or computer, composed of an OS and one or more applications. We can represent a virtual machine as shown in Figure 6. A virtual machine is typically composed of a single file or group of data that can be read and run by the virtualization layer. Each virtual machine is an independent operating environment that behaves as if it were a separate computer. Different virtual machines are therefore not "aware" of each other. They are built in such a way that they are isolated, which means that they are not aware of other virtual machines being present on the same physical server. A virtual machine uses emulation to mimic a complete set of hardware, such as CPU, memory, network card, etc. And this is done through a set of drivers, which are compatible with different types of equipment. The drivers are built on a virtual machine so that they can be used in various hardware configurations. With this type of drivers, a virtual machine generates a virtual version of the physical hardware and creates a virtual CPU, a virtual memory, a virtual network interface card (NIC), a virtual hard disk, and other types of hardware that may be required. When a virtual machine is started, a certain amount of CPU, memory, and disk space processor capacity are automatically assigned by the virtualization or hypervisor layer. To implement a virtual machine, a virtualization layer (hypervisor) is added to a physical server to support the desired architecture. In doing so, the virtual machine can bypass hardware compatibility and resource limitations [14].

Figure 6. *Graphical representation of a Virtual Machine.*

7. Challenges Posed by Virtualization to Forensic Science

7.1. Main Problems

Virtually the entire Cloud Computing framework is based on virtual servers and virtual networks. Cloud Computing and Virtualization are two different technologies, but nowadays, Cloud Computing systems work with a virtualization-supported infrastructure architecture. [14] Cloud Computing can be described as a collection of services dynamically available to a customer and presented as a service-end product with no underlying mechanical exposure. Currently, the most practical and most used way to offer this collection and services is through virtualization [15]. Virtualization involves the insertion of an abstraction layer between hardware and software. A server provides this

abstract bed with the hypervisor function, that is, the hypervisor provides virtual machines. Virtual machines have their operating system that runs independently of the operating system of the hypervisor, and may even be isolated from the host system, and have a virtual network that also gives support independent of the physical network that supports the hypervisor server [16]. Network traffic between virtual machines and other virtual machines or between other networks can be done without any knowledge of the host server and any registration in this system. Developing digital or forensic criminal investigations in these environments is extraordinarily tricky [17]. Investigators can access the hypervisor and have no access to the virtual machines, on the other hand, the owner of a virtual machine can secondly delete a virtual machine and leave no record of it, as well as all the network traffic that it virtual machine has generated [18].

7.2. Another Problems

Figure 7. *Graphical representation of a Hypervisor, within the description of virtual machines, which are mere computational abstractions that share Hypervisor hardware.*

Another complex problem for digital and forensic criminal investigation is that, for example, in Microsoft's virtualization system (Hyper-V). There are two types of virtual machines, first-generation virtual machines, that share among them the hardware of the hypervisor requiring the drivers of the hardware vendors installed in it, and therefore make the communication through known driver generating some logs on them. Allowing to the investigators, in the end, to obtain some information on the computation and net activity of that machine virtual; and second-generation virtual machines do not use the conventional drivers provided by hardware manufacturers, create so-called synthetic drivers, purely mathematical objects that simulate the taxi driver, and serve to communicate with hardware in a non-transparent way. In the latter case, it is not possible for the researchers to obtain information and activity regarding the device of the hypervisor [19]. And that is an issue for research [20]. On the other hand, even if you do not turn off the virtual machines, which we remind you are a small file, they have a so-called snapshot technology that allows you to roll back to the system. That is, I can create a virtual machine on a hypervisor, at first use create a snapshot of the entire system, then establish an encrypted communication with a weapons purchase site, buy the weapons, and then roll back to the initial picture and I turn off the snapshot, all the information about the crime of buying weapons literally disappears. It is effortless to perceive the problem that is generated for a digital criminal investigation [20].

Finally, we approach what for us is one of the biggest challenges posed by the simultaneous use of Cloud Computing and Virtualization: Nested Virtualization [21]. The 2016 version of Windows Server from Microsoft introduces several useful new features, including features designed specifically for the Hyper-V virtualization platform. Nested Virtualization is a new feature included with Hyper-V 2016, released with Windows Server 2016 and Windows 10; therefore, it is available on workstations and also on servers. This technology can now be used in virtual servers allocated in Cloud Computing, such as Azure [22]. Nested virtualization is the ability to produce virtualization within virtualization, that is before we had a physical hypervisor that created virtual machines, we can now produce virtual machines to parts of other virtual machines, as explained in Figure 8.

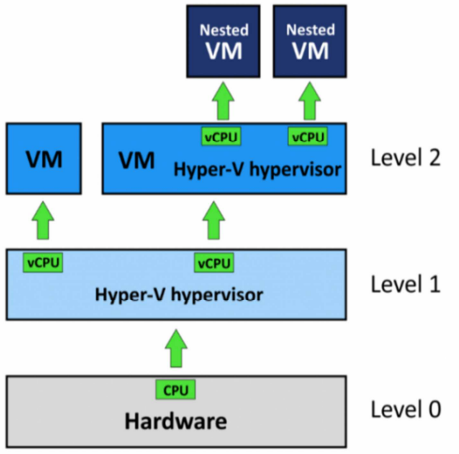

Figure 8. *Nested Virtualization, that which is above Level 2 is Nested Virtualization.*

This technology allows you to create virtual computer networks completely isolated from physical systems and even second-tier virtualization. Any digital crime practiced through a virtual machine produced by Nested Virtualization is not subject to the digital or forensic criminal investigation, in case the criminal or hypothetical criminal is a professional

with knowledge of this technology. After deleting a virtual machine from Nested Virtualization, it is not possible to obtain any data about it. On the other hand, all the network traffic it generates cannot be identified or captured [23]. If the criminal or hypothetical criminal uses a VPN in a virtual machine of Nested Virtualization does not leave any vestige in the network where this virtual machine is nor in the other systems including the Internet [24]. That is, any criminal investigation of that digital object is not possible.

And this, for us, is the greatest of all the challenges that can be posed to criminal and forensic investigation in digital terms.

8. Conclusion

We can conclude that the Cloud Computing environment by its ubiquitous nature brings new challenges to digital forensic science and digital criminal investigation.

Difficulties in accessing virtual machine logs or applications stored in virtual structures, data volatility, data dispersion due to the nature of distributed computing, the inability to control systems, the relative responsibility of users to the model Cloud Computing implementation, failing to ensure the integrity of the data to be collected are real challenges that criminal investigators encounter in these environments.

On the other hand, the intrinsic characteristics of virtualization entail even more complex challenges, such as the inability to manipulate virtual machines and the ease of volatilizing these virtual objects.

Finally, the new capability to implement Nested Virtualization in Cloud Computing may even render all digital criminal investigation in virtual machines based on this technology impossible, including the inability to access all computing and network data that have been used in these virtual machines, in practice this technology can provide total anonymity.

References

[1] P. R. Brandão, “Cloud Computing: Fundamentals,” *International Journal of Computer Science and Technology,* vol. 2, 31 03 2018.

[2] P. R. Brandão, “Computer Forensics in Cloud Computing Systems,” *Budapest International Research in Exact Sciences,* vol. 1, Nr. 1, 02 02 2019.

[3] NIST, "NIST Cloud Computing Forensic Science Challenges (Draft NISTIR 8006): 2014," NIST, EUA, 2014.

[4] R. K., Cloud Forensics, Springer, 2011.

[5] D. M., "Forensics investigation challenges in cloud computing environments.," in *International Conference on Cyber Security. Cyber Warfare and Digital Forensics*, IEEE, 2012.

[6] G. H., "Forensics investigations in cloud environments," in *International Conference on Computer Science and Information Processing*, IEEE, 2012.

[7] H. B., “Security challenges for IaaS cloud computing,” in *44th Hawaii International Conference on System Sciences*, Hawaii, 2012.

[8] B. D., “Technical issues of forensics investigations in cloud computing environments,” in *Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, 2011.

[9] A. Fahdi, “Challenges to digital forensics,” in *Information Security for South Africa*, Johannesburg, 2013.

[10] G. G., “The Challenges of Cloud Computing,” *Digital Forensics,* pp. 28-48, 2012.

[11] McKemmish, “What is Forensic Computing,” *Australian Institute of Criminology,* 1999.

[12] S. Stravos, “Cloud Forensics,” in *Advanced Information technology Laboratory*, Springer, 2014, pp. 271-284.

[13] Z. S., “Cloud Forensics,” in *3th International Conference on Emerging Intelligence data and Web Technologies*, 2012.

[14] P. R. Brandão, “Virtualização: Fundamentals,” *Kriativ-tech,* vol. 1, Nr. 6, 2018.

[15] D. Bem, “Computer Forensics Analysis in a Virtual Environment,” *International Journal of Digital Evidence,* vol. 6, Nr. 2, 2007.

[16] Q. L., “An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds,” *Security & Privacy. IEEE,* vol. 8, Nr. 6, pp. 56-62, 2010.

[17] A. Gavrilovska, "Abstract High-Performance Hypervisor," HPVCVirt 2007, Portugal, 2007.

[18] Vaughan-Nichols, “New Approach to Virtualization Is a Lightweight,” *Computer,* pp. 12-14, November 2006.

[19] Y. Zhang, “Research on the Technology of Secure Computer Forensics,” in *Intelligent Information Technology and Security Informatics*, 2010.

[20] K. Nance, “Investigating the Implications of Virtual Machines Introspection for Digital Forensics,” in *International Conference on Availability, Reliability, and Security*, 2009.

[21] W. Lam, "You are here: Home / NESTED VIRTUALIZATION," Virtually Ghetto, [Online]. Available: https://www.virtuallyghetto.com/nested-virtualization. [Accessed in 10-05-2019].

[22] S. Cooley, “Run Hyper-V in a Virtual Machine with Nested Virtualization,” Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization. [Accessed in 10-05-2019].

[23] B. Lee, “How to set up Hyper-V Nested Virtualization in Windows Server 2016,” Vembu, [Online]. Available: https://www.vembu.com/blog/setting-hyper-v-nested-virtualization-windows-server-2016/. [accessed in 10-05-2019].

[24] E. Wright, “A QUICK GUIDE TO NESTED VIRTUALIZATION,” Turbonomic, [Online]. Available: https://blog.turbonomic.com/blog/on-technology/a-quick-guide-to-nested-virtualization. [accessed in 10-05-2019].