GSTF Journal on Computing (JOC)
DOI: 10.5176/2251-3043_4.4.361
ISSN:2251 - 3043 ; Volume 5, Issue 1; 2016 pp. 116-120

Cloud Computing and Digital Forensics Challenges

Samah Mansour
School of Computing and Information Systems
Grand Valley State University
1 Campus Dr.
C2-303 Mackinac Hall
Allendale, MI 49401-9403

(616) 331-8686
elsaidm@gvsu.edu

***Abstract*—Nowadays, the storage of computer data is moving rapidly toward cloud computing as an evolving information technology phenomenon. Instead of building, maintaining, and managing a physical Information technology infrastructure, the organizations start to replace the physical infrastructure with remote and virtual environments that are managed by third parties. This shift has a significant impact on forensics investigators, hardware and software vendors, IT experts, law enforcements and corporate audit departments since more crimes are committed with the involvement of computers. Digital forensics helps courts and law enforcement agencies to collect valuable evidence for investigations. This paper presents a general overview of cloud computing and digital forensics. Also, it discusses the major benefits and challenges of using cloud computing on digital forensics.**

Keywords: Digital forensics, Cloud Computing, Cloud Forensics

I. Introduction

Cloud computing becomes a new notable step in information technology. It has the potential to change how the organizations view their information technology. Through cloud computing, the organization will replace their physical IT infrastructure with remote services. These services are either managed by the organization itself or by a third party. It offers several promising technological and economic opportunities that have a potential to become an evolutionary point in the new era of computing environment. The evolution of this technology creates various challenges mostly in cybercrime investigations and digital forensics.

Digital forensics is a discipline that supports law enforcement agencies in finding legal evidence in the computing environment. Forensics examination of the commonly used computing devices such as cell phones and computers can lead to a wealth of evidences that can be unavailable through using the traditional investigation methods.

Although cloud computing has several benefits, it introduces a significant challenge to its users and law enforcements authorities. There are still speculations about its level of security.

This paper presents the fundamental and technical background about cloud computing and digital forensics. In addition, it discusses the positive and negative impact of cloud computing on digital forensics. The remainder of the paper is organized as follows. Section 2 introduces a general background about cloud computing. It describes the main characteristics and delivery and deployment models of cloud computing. Section 3 presents broad background about digital forensics and the technique that is followed by investigators. Section 4 discusses that relationship between cloud computing and digital forensics. It also discusses that main benefits and challenges of cloud computing on digital forensics. Section 5 concludes the paper.

II. What is cloud computing?

Cloud computing is a technology that provides services through the Internet. The Open Cloud Manifesto Consortium defines cloud as *"the ability of the consumer (end user, organization, or IT staff) to make the most of that power without having to manage the underlying complexity of the technology"* [8]. NIST identified five key characteristics of cloud computing, three delivery models, and four deployment models as shown in figure 1.

The five key characteristics are [11]:

1. On-demand self-service
2. Ubiquitous network access
3. Location independent resource pooling
4. Rapid elasticity
5. Pay per use.

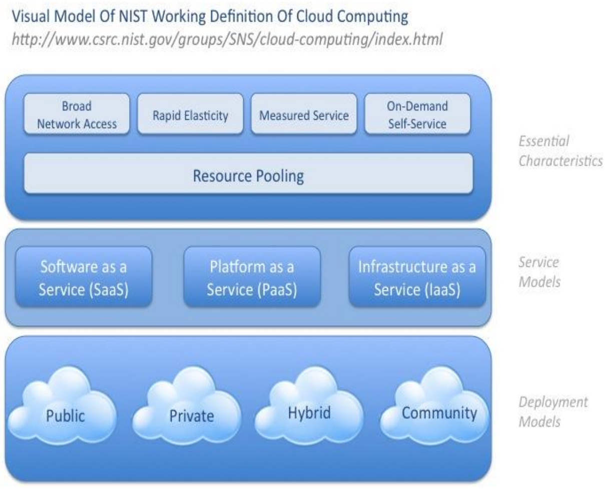
Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

Fig 1. Characteristics and Model of Cloud Computing

The three delivery models are [2]:

1. Software as a Service (SaaS): a client uses applications that are available from the cloud providers. Users interact with SaaS applications through using web browsers. Google Docs can be used as an example of SaaS.
2. Platform as a Service (PaaS): a client is provided by application programming interface (API) to create a host custom-built application. Google Apps Engine is an example of PaaS.
3. Infrastructure as a Service (IaaS): is the leasing of virtualized computing resources such as processing power, network capacity and storage.

The four deployment models are [11]:

1. Private cloud: the infrastructure is operated by the organization that owns the cloud.
2. Community cloud: the infrastructure is shared among several organizations to share resources.
3. Public cloud: the infrastructure is owned by an organization that will maintain the cloud facilities in one or more datacenters. The user can lease the computing resources from the providers.
4. Hybrid cloud: is a combination of two or more of the above mentioned deployment models. Hybrid cloud can be used to provide load balancing to multiple clouds.

Two popular cloud computing facilities are Amazon Elastic Compute Cloud (EC2) and Google App Engine. Amazon EC2 is part of a set of standalone services which include S3 for storage, EC2 for hosting and the simpleDB database. Google App Engine is an end-to-end service, which combines everything into one package to provide a PaaS facility. With Amazon EC2, users may rent virtual machine instances to run their own software and users can monitor and increase/decrease the number of VMs as demand changes.

III. WHAT IS DIGITAL FORENSICS?

One of the main questions that start to be raised during the past few years is why digital forensics. In general forensics is the science of using computer systems and techniques to gather potential legal evidence. With the rapid increase of using the Internet and cloud computing, the number of crimes that involve computers has grown [2]. Therefore, digital forensics tools and techniques have evolved to enable investigators to provide computer crimes data to courts. NIST defined digital forensics as “the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations” [11].

According to [1] digital forensics for cloud computing includes:

- Computer forensics: focus on data recovery
- Intrusion forensics: focus on intrusion detection and is concerned with tracking attacks and suspicious behaviors using computing systems
- Network forensics: focus on monitoring and analyzing network traffic. Most of the time combinations of intrusion and network forensics techniques are used to deal with attacks for which network traffic is significant.

Since digital forensics focus on collecting legal digital evidence, it faces several challenges that exist as a result of the nature of digital evidence. Those challenges are [15]:

- Massive quantity of evidence: there are thousands of files on a single computer
- Easily contaminated: rebooting the system may remove important traces of evidence
- Crime identification: a crime may be discovered after months or years
- A large number of potential suspects: this is due to the millions of the Internet users.

For the digital evidence to be considered in the court, they have to be authentic, reliable, complete, believable, and admissible [16]. Therefore, the forensics techniques must be applied in a consistent manner. The following section will describe the phases of the technique as introduced in figure 2 [9].

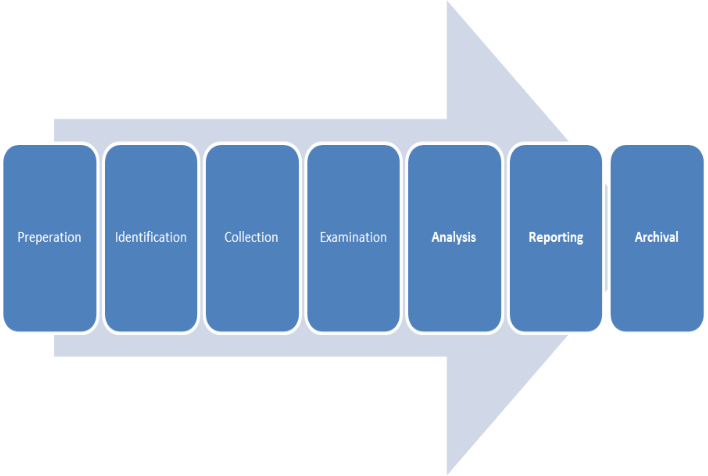

Fig 2. Forensics Technique

Preparation: this phase covers all of the activities that occur before working on a case. This phase includes activities for preserving evidence and to establish guidelines on how to manage evidence to ensure evidence is preserved throughout the entire investigation process.

Identification: this phase starts when a customer requests a digital forensics investigation. This phase involves understanding the purpose of the request and the scope of the investigation such as the type of case, subjects involved, and systems involved.

Collection: After identifying the case and the needed data, the collect phase will start to acquire data from all of the possible sources using procedures that preserve the integrity of the data. Data should be collected in a timely manner to avoid the loss of dynamic data.

Examination. The data that is collected should be examined using a combination of automated and manual methods to assess and extract data of particular interest for the specific situation, while preserving the integrity of the data.

Analysis. The results of the examination should be analyzed by using well-documented methods and techniques to derive useful information that addresses the questions that were the impetus for the collection and examination.

Reporting. The results of the analysis should be reported. In this stage, the results are presented to the person or group that requested digital forensics investigation. The reported items may include a description of the actions employed, a determination of any other actions that should be performed, such as forensic examination of additional data sources, securing identified vulnerabilities, and improving existing security controls; and recommendations for improvements to policies, guidelines, procedures, tools, and other aspects of the forensics process.

Archival: this phase focuses on the management of the storage of the case materials including the evidence once the case has been closed.

IV. Relationship between Digital Forensics and Cloud Computing

As we covered in the above sections, digital forensics is a rapidly growing field due to the enormous increase in using computing devices which some people may use them to commit crimes. According to [12], in 2013, 91% of the adult population owns some kind of cell phone. 56% of *all* American adults are now smartphone adopters. One-third (35%) have some other kind of cell phone that is not a smartphone. In addition, 81% of the population is using the Internet. It is estimated that six of every ten crimes will involve the use of a computing device [7]. At the same time, cloud computing is considered a new major change in the way the organizations develop their IT strategies.

By 2017, the public cloud services market is predicted to exceed $244 billion**[**12]. The results of a survey that was conducted with more than 800 organizations decision makers, IBM found that organizations gaining competitive advantage through high cloud adoption are reporting almost double the revenue growth and nearly 2.5 times higher gross profit growth than peer companies that are more cautious about cloud computing [12].

The growth in using cloud computing must be aligned with the growth of digital forensics and the careful consideration of security. Security is a vital requirement for the use of cloud computing. However, digital forensics is seen as a luxury due to the lack of legislations [1].

One of the main questions those days is whether cloud computing will assist digital forensics investigations or it will harden such investigation. The research results indicate that there is no one straightforward answer for the above mentioned questions. There are advantages and disadvantages of using cloud computing on digital forensics. Those advantages and disadvantages will be discussed in the following paragraphs.

A. Benefits of Cloud Computing For Digital Forensics

One of the main benefits is data centralization where having the data in the same place. The IaaS provider can build a dedicated forensics server within the cloud to be ready to be used when needed. This, in consequence, will lead to a quick response to any crime [6]. Another advantage is virtualization. Virtualization is used in clouds to allow multiple users to share the same resources. By using VMware, a disk and memory images can be collected easily via the snapshots. Those snapshots are called forensics image. Through the snapshots, the virtual machines can be cloned by one click [1, 13]. The good side is that the business processes do not have to be shut down for performing a forensics analysis.

Another benefit is the wide scale of services and resources that cloud computing offers to the investigators. By taking advantages of IaaS and the availability of a massive storage space that can be available on the cloud, investigators can store hard drives images. Furthermore, the massive resources support investigators to perform intense jobs such crack passwords, encryption keys or examine many images, all of which can be costly in terms of CPU and memory [6].

B. Challenges of Cloud Computing on Digital Forensics

On the other hand, there are several drawback issues of cloud computing from a digital forensics perspective. First, one of the main drawbacks is data acquisition. Applying digital forensics toward the cloud computing environment will require from the investigators to involve data that is either stored inside or outside the country or both. The investigation process will involve government, politics, law enforcement agencies and also the time where the longer the time taken to seize the data and information from the cloud server, the more opportunities for the suspects to erase and delete the data that is related to the committed crimes [10].

Second, the loss of vital data which can be critical evidence such as registry entries, temporary files and memory. In addition, metadata such as file creation and modification can also be lost if data is downloaded from a cloud [1, 4]. Third, some cloud service providers do not provide any log data from the network components. As a result, that in case of malware infection of an IaaS VM, it will be difficult to get any form of routing information. This situation gets even more complicated in case of PaaS or SaaS [14]. In the forensics investigation, various log files can provide a rich source of information. However, for the fear of performance degradation and log size, keeping logging files is not given a high priority. This problem is very clear in the SaaS model where the cloud user in the SaaS model does not have any control on the infrastructure such as network, servers, operating systems or even the application that is used. Therefore, on those cases the log files will be the main source of details for the investigators. In addition, several SaaS cloud service providers such as Google uses Single Sign-On (SSO) access control to the complete set of their services. Hence, in case of an account attack, the cloud service providers do not provide the cloud user with any useful information about which data has been accessed by the attacker [14, 5].

This issue can be solved by making storing logs files as a required option from the cloud service provider. Most modern operating systems offer extended logging in the form of a C2 audit log files [3]. C2 audit saves data in a file located in the default data directory of the cloud. If the audit log file reaches its maximum size limit of 200 megabytes, the server will create a new file, close the old file, and write all new audit records to the new file. This process will continue until the audit data directory fills up or auditing is turned off [3]. By enabling the C2 audit, the server will record both failed and successful attempts to access statements and objects. This information can help investigators to trace any security policy violations. [4].

V. Conclusion

This paper introduced a general background about cloud computing. As proved for all different resources that cloud computing is considered a significant step in the IT world. Cloud computing will change the IT future. The paper also introduced the process that is used by law enforcement investigators to collect and analyze legal evidence. The paper discussed the strong relationship between cloud computing and digital forensics. The expansion of digital forensics is not less important than the expansion of using cloud computing. The development and the implementation of digital forensics techniques and policies should go in parallel with the expansion of using cloud computing. Until today, the cloud service providers did not implement forensics policies and at the same time forensics investigators did not put clear procedures for dealing with cloud investigation. As a conclusion, the author believes that in the near future, the increase of using cloud computing will encourage and force the cloud service providers to apply clear forensics policies in order to gain customers' trust in cloud computing. Additionally, the investigators will implement systematic procedures on investigating the cloud.

VI. References

[1] A.Juels and B. S. Kaliski. Pors: proofs of retrievability for large files. In CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, pages 584-597. ACM, 2007.

[2] M. Armbrust,A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G.Lee, D. Patterson,A. Rabkin, I.Stoica, M. Zaharia, (2010) A View of Cloud Computing, Communications of the ACM, vol. 53(4), ISSN: 0001-0782.

[3] C2 Audit Mode Server Configuration Option. technet.microsoft.com/en-us/library/ms187634.aspx. Retrieved on 2 March 2016

[4] D. Brezinski, and T. Killalea. Guidelines for Evidence Collection and Archiving, 2002.

[5] D. Chen and H. Zhou, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, pp. 647-651, 2012.

[6] S. Garfinkel. (2007) Commodity grid computing with Amazon's S3 and EC2, login, USENIX, vol. 32(1), pp7-13.

[7] Institute for Communications, Arbitration and

Forensics, (2010) Mobile phone security solutions. http://www.security-technologynews.com/article/mobile-phone-security-solutions.html. Retrieved on March 3, 2016

[8] "Introducing the Open Cloud Manifesto". ElasticVapor. 26 March 2009. Retrieved on March 1 2016.

[9] A. Jones, & C. Valli (2009). Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility. Burlington: Elsevier, Inc.

[10] M. Taylor, J.Haggerty, D. Gresty and R. Hegarty, "Digital Evidence in Cloud Computing Systems," Elsevier- Computer Law and Security Review, vol. 26, pp. 304-308, 2010.

[11] NIST (2010) Definition of cloud computing v15, Computer Security Division, Computer Security Center http://csrc.nist.gov/groups/SNS/cloud-computing

[12] PewResearch Internet Project (2013). SmartPhone Ownership 2013. http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/. Retrieved March 7, 2016.

[13] R. A. Bares. Hiding in a virtual world: using unconventionally installed operating systems. InISI'09: Proceedings of the 2009 IEEE international conference on Intelligence and security informatics pages 276{284, Piscataway, NJ, USA, 2009. IEEE Press

[14] R.Denis, W. Chris, B. Tom (2011). Cloud Computing: Pros and Cons for Computer Forensic Investigations. International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, pp. 26-34

[15] Standard Working Group on Digital Evidence (SWGDE) (1999) Digital evidence standards and principles, http://www.swgde.org/documents.htm.

[16] P. Stephenson (2003) Modeling of post Incident root cause analysis, International Journal of Digital Evidence, vol. 2(2). Retrieved on March 1, 2016