Cloud Forensics: Identifying the Major Issues and Challenges

Stavros Simou[1], Christos Kalloniatis[1], Evangelia Kavakli[1], and Stefanos Gritzalis[2]

[1] Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR 81100 Mytilene, Greece
{SSimou,chkallon}@aegean.gr, kavakli@ct.aegean.gr
[2] Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, GR 83200, Samos, Greece
sgritz@aegean.gr

Abstract. One of the most important areas in the developing field of cloud computing is the way that investigators conduct researches in order to reveal the ways that a digital crime took place over the cloud. This area is known as cloud forensics. While great research on digital forensics has been carried out, the current digital forensic models and frameworks used to conduct a digital investigation don't meet the requirements and standards demanded in cloud forensics due to the nature and characteristics of cloud computing. In parallel, issues and challenges faced in traditional forensics are different to the ones of cloud forensics. This paper addresses the issues of the cloud forensics challenges identified from review conducted in the respective area and moves to a new model assigning the aforementioned challenges to stages.

Keywords: Cloud Computing, Cloud Forensics, Cloud Forensics Process, Cloud Forensics Challenges, Digital Forensics.

1 Introduction

In the last years, the growing demand of computing power and resources, lead the traditional forms of services to mutate very rapidly. During this period users have been experiencing a huge demand on applications and services on cloud computing, which is definitely one of the most important services offered in this era. According to the 3rd Annual Future of Cloud Computing Survey, cloud adoption continued to rise in 2013, with 75 percent of those surveyed reporting the use of some sort of cloud platform – a 67 percent rise from the previous year. Addressing this growth in the worldwide market for cloud computing it is expected to reach $158.8 billion by 2014, an increase of 126.5 percent from 2011 [1]. Recent International Data Corporation (IDC) cloud research shows that spending on public IT cloud services will reach $47.4 billion in 2013 and is expected to be more than $107 billion in 2017. Over the 2013–2017 forecast period, public IT cloud services will have a compound annual growth rate (CAGR) of 23.5%, as companies build out the infrastructure needed to deliver public cloud services. By 2017, IDC expects public IT cloud services to drive 17% of the IT product spending. [2].

M. Jarke et al. (Eds.): CAiSE 2014, LNCS 8484, pp. 271–284, 2014.

Although, organizations are adopting cloud computing technology there is still a great consideration about security and the continuously increasing number of digital crimes occurring in cloud environments. According to a newly-released report sponsored by McAfee, global cyber activity is costing up to $500 billion each year, which is almost as much as the estimated cost of drug trafficking [3]. Investigators have to conduct digital forensic investigation on cloud computers to identify, preserve, collect and analyze all the evidentiary data in order to proper present them in a court of law. This type of forensic has been named as cloud forensics. The ability of cloud forensic investigators to carry out an investigation depends completely on the tools and methods used, to acquire the appropriate digital evidence from a device. The current digital forensic methods, tools and frameworks used to conduct a digital investigation cannot meet the requirements and the standards for the new technology on cloud environment. This happens due to the fact that computer technology is continuously changing and the forensic technology is unable to follow that pace.

Since cloud forensics is a newly developed research area our main and primary focus was to conduct a thorough analysis of the respective literature in order to present an analytic review of the challenges and issues raised so far in the respective field. For conducting this analysis we begun with the most cited papers presented in respective scientific journals, conferences and industrial reports like “Digital Investigation”, “Advances in Digital Forensics”, “International Journal of Digital Evidence”, “Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security”, “Systematic Approaches to Digital Forensic Engineering”, “Digital Forensic Research Workshop”, “Cyber Security, and Cyber Warfare and Digital Forensic” etc.. After conducting this analysis we have broaden our research to less related academic reports and papers from the field of security in information systems.

The findings of this study constitute an initial but robust set of requirements that analysts and developers need to consider when designing information systems or individual services in the cloud. Also this research introduces future research efforts that need to be conducted and tools that need to be implemented for assisting in the process of cyber-crime investigation in cloud-based environments.

2 Technical Background

2.1 Cloud Computing

Companies and organizations are looking for new services and solutions on the Internet, aiming on the reduction of the cost on their infrastructure and support (human resources) and, in parallel, to increase their systems’ scalability. In order to accomplish their objectives, they outsource services and equipment. This solution is a step towards cloud computing. Cloud computing is not owned by companies and the respective IT systems are not usually managed by them. Instead, Cloud Service Providers (CSPs) supply these services after signing contracts with companies. A CSP maintains the computing infrastructure (high availability computer systems in clusters, data centers) required for providing the various services, runs the cloud software and delivers the cloud services to the Cloud Consumers through the Internet.

Cloud computing uses virtualization techniques for providing equipment, software and platform support as remote services. Cloud model is composed of five essential characteristics, i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service, three service models, i.e., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and four deployment models, i.e., private cloud, community cloud, public cloud and hybrid cloud" [4]. Cloud computing provides many advantages to companies and organizations in comparison to traditional private environments.

2.2 Digital and Cloud Forensics

In the digital world were modern users live and interact on a daily basis the number of crimes involving computer devices is growing rapidly. This has an immediate impact to the people who aim to assist law enforcement, using digital evidence to uncover the digital crime. A new battlefield is set and the investigators are trying to cope and bring to justice the people responsible for these kinds of crimes. Digital forensics is the field where the investigators use forensic processes to search for digital evidence in order to use them in a court of law, or to a company's internal investigation. Digital forensics has been defined 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 facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations [5].

Forensic techniques and tools have been created for assisting the investigation process, aiming to acquire, preserve and analyze evidence. Digital forensics deals with the digital evidence found in the area where the crime committed. When we refer to evidence we mean all kind of digital evidence found on any type of digital devices, present or futures. The most important element in the digital forensics is to maintain the integrity and the chain of custody of the digital evidence. Any alteration to the evidence simply means that the case is lost in a court of law.

Identification of evidence in cloud environments is a difficult process due to the different deployment and service models and also the limitation of seizing (physically) the computer device containing the evidence. In the early stages of the new era, investigations on cloud environments were based on methodologies and tools from the digital forensic field. Rapid advances in cloud computing require new methodologies, frameworks and tools for performing digital forensics in cloud environments. Cloud forensic is a subset of digital forensics and it was first introduced by Ruan (2011), to designate the need for digital investigation in cloud environments, based on forensic principles and procedures.

Crime investigators in cloud environments have to deal with a number of different issues compared to network or computer investigation. The most important is that the evidence can reside everywhere in the world in a virtualization environment. The investigators' main concern is to maintain that the evidence has not been compromised by third parties, in order to be presented and being acceptable in the court of law. Third parties are involved in the cloud forensic process due to their collaboration

with CSPs. Service providers sign contracts with other companies possibly in different geographically locations, for help and assistance.

Various cloud forensics techniques are developed and used depending on the cloud deployment and service model the respective crime or incident under investigation have taken place. In service models like PaaS and SaaS for example, consumers do not have the control of the hardware and they depend on the CSP for the logs, whereas in IaaS, consumers have the ability to make an image of the instance and acquire the logs. As for the deployment models, in public cloud consumers do not have the physical access and the privacy compared with the ones in private cloud.

3 The Cloud Forensic Process

3.1 Related Work

Since 2001, various methods and frameworks have been introduced regarding the way of conducting proper digital forensic investigation, including different stages and phases. The First Digital Forensic Research Workshop (DFRWS) [5] defined a generic investigative process that could be applied to the majority of investigations involving digital systems and networks. The model establishes a linear process, which includes identification, preservation, collection, examination, analysis, presentation and decision. In this workshop a discussion was conducted about the use of the term collection and preservation, and the possibility of the first being a subcategory or a separate step with the other.

The Abstract Digital Forensic model [6] was based on DFRWS model and consists of nine stages which are identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence. It adds three more stages and describes what each one of them concern.

In 2003, the Integrated Digital Investigation Process [7] model was introduced based on the crime scene theory for physical investigations. It allows technical requirements for each phase to be developed and for the interaction between physical and digital investigations to be identified. This framework consists of 17 phases organized into five groups: readiness, deployment, physical crime scene investigation, digital crime scene investigation and review.

The Enhanced Digital Investigation Process model [8] separates the investigations at primary and secondary crime scenes while depicting the phases as iterative instead of linear. It is based on the IDIP model and expands the deployment phase into physical and digital crime investigations while introducing the primary crime scene phase. The reconstruction is only made after all investigations have taken place.

The hierarchical, objectives based framework [9] for the digital investigations process in 2005, proposes a multi-layer, hierarchical framework which includes objectives-based phases and sub-phases that are applicable to various layers of abstraction, and to which additional layers of detail can easily be added as needed. The framework includes the stages of preparation, incident response, data collection, data analysis, presentation of findings and incident closure.

In 2006, the Forensic Process [10] proposed consisting of four phases: collection, examination, analysis and reporting. In this model, forensic process transforms media into evidence for law enforcement or for organization's internal usage. First collected data is examined, extracted from media and transforms it into a format that can be processed by forensic tools. Then data is transformed into information through analysis and finally the information is transformed into evidence during the reporting phase.

The Digital Forensic Investigation Framework (DFIF) [11] groups and merges the same activities or processes that provide the same output into an appropriate phase. The proposed map simplifies the existing complex framework and it can be used as a general DFIF for investigating all incident cases without tampering the evidence and protect the chain of custody. The framework consists of five phases which are preparation, collection and preservation, examination and analysis, presentation and reporting and disseminating the case.

In 2010, Digital Forensic Evidence Processes [12] defined nine stages, identification, collection, preservation, transportation, storage, analysis - interpretation and attribution, reconstruction, presentation and destruction. All of these should be done in a manner that meets the legal standards of the jurisdiction and the case.

The Harmonized digital forensic investigation process model [13] introduced in 2012, proposed several actions to be performed constantly and in parallel with the phases of the model, in order to achieve efficiency of investigation and ensure the admissibility of digital evidence. The phases defined in terms of scope, functions and order. These are: incident detection, first response, planning, preparation, incident scene documentation, identification, collection, transportation, storage, analysis, presentation and conclusion.

The Forensic Investigations Process [14] in cloud environments was based on the Forensic Process with the four stages. Due to the evolution of cloud computing the stages were changed to apply basic forensic principles and processes. The four distinct steps are: a) determine the purpose of the forensics requirement, b) identify the types of cloud services (SaaS, IaaS, Paas), c) determine the type of background technology used and d) examine the various physical and logical locations, which are client side, server side and developer side.

In 2012, Cloud Forensics Process [15] focused on the competence and admissibility of the evidence along with the human factor. The process consists of four stages which includes a) ascertain the purpose of the cloud forensic, b) ascertain the type of the cloud service, c) ascertain the type of the technology behind the cloud and d) carry out specific investigation on the base of stage c such as ascertain the role of the user, negotiate with the CSP, collect potential evidence, etc.

Finally, in 2012, the Integrated Conceptual Digital Forensic Framework for Cloud Computing [16] proposed, based on McKemmish and NIST. It emphasizes on the differences in the preservation of forensic data and the collection of cloud computing data for forensic purposes. It consists of four stages, identification and preservation, collection, examination and analysis, reporting and presentation.

In the following section we propose a cloud forensics process as it was derived from the aforementioned findings.

3.2 The Process

In order to identify the cloud forensic process an extensive literature review on the fields of both digital and cloud forensics was conducted. Based on the above frameworks it is obvious that some of the existing models follow similar approaches while others are moving in different areas of investigation, but the outcome in most occasions is almost the same. The model used in this paper is similar to DFWR model with three additions! Firstly we propose the inclusion of collection phase in the preservation stage, secondly we include the analysis stage in the examination stage and finally the decision stage is excluded, due to the fact that it cannot be considered "forensic".

This model is convenient for analyzing and associating challenges in cloud forensics and was derived based on the suggestions and drawbacks located from the investigation of similar approaches presented before. The model is consisted of four steps: i) *Identification* which is the first stage and deals with identifying all possible sources of evidence in a cloud environment in order to prove that the incident took place. It is crucial, because the next processes depend upon the evidence identified here. ii) *Preservation – Collection* which deals with the collection of the evidence, from the locations they reside in clouds, the different types of media and the tools used to do so. Also, investigators need to isolate and preserve the evidence by preventing people from using the digital device or by duplicating digital evidence. Integrity and unauthorized alterations of digital evidence must be ensured. The most important issue in this step is to maintain the chain of custody of the evidence and to ensure the validity and the integrity of them in order to be used in a court of law. Preservation could be a different process in a cloud forensic framework running concurrently with all the other processes, iii) *Examination – Analysis* which involves the extraction of data from the previous stage and the inspection of the huge amount of data identified in order to locate the proper evidence for the incident occurred. The data found will be analyzed by different tools and techniques for revealing any useful information in order to prove if someone is guilty or not. In this stage also, data reconstruction will take place, iv) *Presentation* stage which is the final stage and deals with the presentation of the evidence in a court of law. A well-documented report with the findings must be produced using expert testimony on the analysis of the evidence. Evidence must be presented in a way that the jury will understand all the technical details due to the fact that cloud computing is a very complicated environment for ordinary Internet users to understand.

4 Cloud Forensic Challenges

In this section we present the cloud forensics challenges identified from the review conducted in the respective area. Also we move one step further and accomplish a categorization of the respective challenges based on the cloud forensics process stages presented in section 3. It should be mentioned that most of the challenges presented apply basically on public clouds while fewer have applicability on private cloud architectures as well.

4.1 Identification Stage

Access to Evidence in Logs. Logs play a vital role in an investigation. Having access to log files in order to identify an incident is the first priority for the investigators. In cloud environments where data are stored in unknown locations due to systems' distribution locating logs is a hard and painful process. The detection of logs also depends on the service model. In PaaS and SaaS, checking system status and log files is not feasible because the client access is completely limited to the API or the predesigned interface. It is just partly applicable in IaaS cloud model as it provides the Virtual Machine which behaves almost the same as an Actual Machine [17]. On the other hand many CSPs do not provide services to gather logs and sometimes intentionally hide the details from customers.

Physical Inaccessibility. In a cloud environment, data location is a difficult task due to the geographical distribution of the hardware devices. The established digital forensic procedures and tools assume that physical access to the hardware is a fact [18]. However, in cloud forensics there is no possibility to seize the hardware containing data, because the data are stored in distributed systems usually in different jurisdictions. Thus, this challenge applies to all three service models.

Volatile Data. Data stored in a Virtual Machine instance in an IaaS service model will be lost when the VM is turned off or rebooted. This reflects to the loss of important evidence such as registry entries, processes and temporary internet files. In case an adversary launches an attack on a VM with no persistent storage synchronization, when the attack is completed, the adversary can shut down the Virtual Machine instance leading to a complete loss of volatile data, if no further countermeasures are installed [19]. Respective literature [18, 20, 21, 22] place the specific challenge to preservation and collection stages. Actually this challenge can fit into both stages, because first we have to identify volatile data and then we have to preserve and collect them from any instance.

Distribution - Collaboration. The distribution of computer systems (in all three service models) in the cloud environment makes the investigators to confront problems with different jurisdictions and laws. To access information, they need to wait for a warrant which sometimes can be costly and time consuming. This is why international collaborations between law enforcement and CSPs must be taken into consideration [23]. New guidelines need to be written and adopted by all countries for the aforementioned reasons.

Client Side Identification. Evidence can be found not only in the providers' side but also in the clients' side interface. In most of the scenarios, the user agent (e.g. the web browser) on the client system is the only application that communicates with the service in the cloud. This especially holds for SaaS and IaaS scenarios. Hence, in an exhaustive forensic investigation, the evidence data gathered from the browser environment should not be omitted [19].

Dependence on CSP - Trust. In all respective literature authors point out the CSPs contribution on cloud forensic process. CSPs are responsible for helping and assisting the investigators and the clients with all the information and evidence they can get in their cloud infrastructures. The problem arises when the CSPs are not willing to provide the information reside in their premises. A good reason for not doing so is the fear that these are going to be used against their companies. In all three models, especially in SaaS and PaaS we need to depend on the CSP to identify, preserve and collect all the evidence that could lead us to the incident. Another major issue is the CSPs dependence on third parties. CSPs sign contracts with other CSPs in order to be able to use their services. This means that the investigation has to cover all the parties involved with an immediate impact to the chain of custody. This challenge applies not only to identification stage, but also to preservation and collection stage.

Service Level Agreement (SLA). In many cases important terms regarding forensic investigations are not included in the SLA signed between CSP and customer. This is because there is a lack of customer awareness, a lack of CSP transparencies, trust boundaries and a lack of international regulations. CSPs cannot provide transparency to customers, because they either do not know how to investigate criminal incidents or the methods and techniques they are using are not appropriate in cloud environments [24]. Suppose a customer signed a contract with a CSP regarding the deletion of all data after the contract expires. It is hard for the customer to verify that the CSP has fulfilled the agreement. Service Level Agreements concern the stages of identification, preservation and collection.

4.2 Preservation – Collection Stage

Integrity and Stability. The integrity preservation and the stability of the evidence is essential in cloud investigation for IaaS, PaaS and SaaS. We must preserve data in our effort to acquire evidence in multi-jurisdiction environments, a difficult task to deal with, without violating any law. If the integrity is not preserved (could be compromised by the CSP or the hypervisor [17]), then the evidence will not be admissible to the court of law. Finally, it is difficult to maintain the stability of the data because of the transient nature and dedicated description of the data in a Cloud [15]. According to [16], this challenge applies to analysis stage.

Privacy. The virtualization of the systems in IaaS and multi-jurisdiction affect the privacy of the clients. Investigators must ensure that all regulations and standards are retained in order to collect the evidence without breaching clients' privacy. CSPs also must find a mechanism to ensure clients that their information will not be accessed by any member of the staff even if they have been deleted.

Time Synchronization. In all three service models the time concerning data is also crucial and requires hard work to come with the correct results. This is due to the fact that data are stored in multiple geographical regions with different time zones. Investigators need to gather all the time stamps from the devices and establish an accurate time line of events [20].

Internal Staffing. This issue concerns all three service models and all four stages, from identification to preservation. To conduct an investigation in cloud forensics a number of people must be involved as a team. This team should consist of investigators with technical knowledge, legal advisors and specialized external staff with deep knowledge in new technology and skills [24].

Chain of Custody. The most important thing to present evidence in a court of law is to make sure that the chain of custody of the evidence is maintained throughout the investigation. Any interruption in the chain of custody will be a problem and the evidence will be questionable. Because of the multi-jurisdictional laws and the involvement of the CSPs for maintaining the chain is a huge challenge. Imagine an investigation where the CSP has to submit data to the investigators. The personnel responsible for collecting the data are not trained to preserve evidence according to specific forensic techniques. In this case the chain of custody will not be maintained. For a case to stand in court the investigators have to ensure that the chain of custody should contain information such as, who collected the evidence, how and where the evidence was collected, how the evidence was stored, who accessed the evidence, etc. [16]

Imaging. In IaaS to make an image of the instance to acquire evidence can be accomplished by taking a snap-shot of the VM. In this case client does not need to shut down the VM to clone the instance. The term "Live Investigation" was introduced for the aforementioned method. The method gathers data in rest, in motion and in execution. Using different images of the instance can provide to investigators any change or alteration made. For PaaS and SaaS clients do not have the ability to access the device. This simply means that there is no possibility of making an image, leading to lose potential evidence when a criminal activity takes place.

Bandwidth Limitation. The volume of data is increasing rapidly resulting to an increase of evidence. In the previous paragraph we referred on the VM imaging in IaaS model. In order to collect data, investigators need to download the VM instance's image. The bandwidth must be taken into consideration when they are downloading these large images.

Multi-jurisdiction. To acquire evidence from the three models in cloud from different jurisdictions is another issue for the investigators. Due to cloud characteristics system's data are usually spread in places around the globe. Thus, it is very difficult, almost impossible, to conduct evidence acquisition when investigators are dealt with different legal systems, where the related laws or regulations may vary by countries [15]. Any evidence retrieval must be according to the laws and privacy policies of the specific jurisdiction where forensic investigation took place in order to maintain the chain of custody. Otherwise, the evidence cannot stand in a court of law.

Multi-tenancy. In cloud environments where IaaS and PaaS services are used, customers share the same storage in VMs. This has an immediate effect on the investigation. Evidence retrieval in multi-tenant environments must maintain the confidentiality, preserve the privacy of the tenants and finally ensure that the data to be collected concern specific tenant and no other. Due to the multi-tenancy the data can be contaminated by people who have access into the same storage unit with result of losing important evidence.

4.3 Examination - Analysis Stage

Lack of Forensic Tools. Data analysis in cloud environments requires appropriate forensic tools. Many of the tools used for a cloud investigation, have been designed and introduced for digital forensic investigations. With the systems distributed all over the world and with no physical access to the computer devices, these kinds of tools cannot fully cover the investigations in IaaS, PaaS and SaaS models. New software tools must be developed to assist in the preservation – collection stage acquiring data more efficient and new certified tools must be produced to help the investigators in data examination and analysis.

Volume of Data. The amount of data, stored in the CSPs' data centers is extremely large and it's increasing on a daily basis. This has an immediate impact on the analysis of the information in order to find useful evidence for the investigation. Appropriate capture and display filters have to be developed and set up in order to make the data volume present in Cloud Infrastructures proccessible [21]. It is very difficult to analyze the VMs directly, even if the CSPs cooperate with investigators, because the VMs for SaaS and PaaS may have a huge storage system, and contain many other applications [25].

Encryption. Many cloud customers in all three service models store their data in an encrypted format to protect them from criminal activities. When an investigation is conducted the encrypted data will not be useful once the encryption keys cannot be acquired. The evidence also can be compromised if the owner of the data is the only one who can provide the key, or if the key is destroyed. Furthermore, many CSPs are using encryption methods to store clients' data in the cloud [23].

Reconstruction. During the investigation, crime scene reconstruction might take place. In cloud environments where data are spread across different regions and countries with time differences, to reconstruct the crime scene and place the facts in a logical order might be a difficult work [17]. On the other hand, if a VM instance is forced to shut down, all data and potential evidence will be lost and the reconstruction phase cannot be executed.

Unification of Log Formats. Analyzing data acquired from the service models is a time consuming process, especially if we have to deal with and identify a number of different log formats. Unification of log formats in cloud is a difficult operation when we have to access the huge amount of different resources available. [24].

Identity. In traditional digital forensic associating a user with the data stored in their computer device is comparatively straight forward (assuming that the device belongs to them and found in their house). In cloud investigation is more complicated, because data are stored in multiple remote locations in multi-tenant environments, and are accessed through clients. Hence, to determine that someone is the owner of the data from a large number of cloud users distributed globally is an intricate process [23]. Another prospective is when a user engages a criminal movement through their VM from a veiled IP address and afterwards claims that their credentials have been compromised from another person.

4.4 Presentation Stage

Complexity of Testimony. In a court of law where the jury (often) consists of people with only the basic knowledge in computer systems, the investigators must be ready to deal with this situation. They have to be prepared to give a clear and simple understanding on the terms of cloud computing, cloud forensics and how they work and explain how the evidence acquired preserved and documented during the investigation. This is an important issue towards the progress of the trial.

Documentation. Another challenge is to persuade the jury that the evidence acquired during the investigation has been documented properly and there had been no changes to the evidence in the previous stages. Investigators must ensure that all parties have been involved in the investigation, followed methods and principles in order to maintain the chain of custody of the evidence that has been collected. Documentation of digital evidence concerns all stages.

4.5 Uncategorised

Compliance Issues. Companies and organizations such as banks, brokers, hospitals, etc. are not transitioning easily to cloud environments, due to trustworthy data retention issues, together with laws and regulations. There are several laws in different countries, which mandate the trustworthy data retention [18]. Cloud environments yet, are not being able to comply with the forensic requirements set by laws and regulations, hence the transition of those organizations to cloud is impractical. The same applies to credit card companies, as achieving compliance with standards set in this field cannot be met [19].

5 Discussion

Based on the review analysis it is obvious that cloud forensics is far more demanding than digital forensics and this is why there is a need for the introduction of new frameworks and methodologies on cloud investigation in order to proper preserve evidence and maintain the chain of custody in all stages of the investigation. Since cloud forensic is a new field, methodologies and frameworks were based on the digital forensics. To the best of our knowledge no author developed and introduced a framework or methodology, concerning cloud forensics that covers every aspect and every phase in a cloud forensic investigation. Most of the work conducted on cloud forensics, refers to challenges, issues and threats, suggestions and solutions on the service models. Challenges, though, apply on different phases and processes in an investigation.

The categorization of stages presented above is based upon models and frameworks introduced and proposed by academics and the industry. To assign challenges to phases, DFRW model was used with a slight differentiation as presented in section 3. Cloud forensic as mentioned earlier is a new technology, hence, there are many different opinions on the categorization of the challenges. After thorough study on the literature on cloud forensics table 1 was designed for assigning challenges according to the respective stage and service model they belong to. The table also captures the

Table 1. Cloud Forensics Overview

Cloud Forensic Challenges / Stage	Applicable to			Related Work
	IaaS	PaaS	SaaS	
Identification				
Access to evidence in logs	partly	√	√	[16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27]
Physical inaccessibility	√	√	√	[18], [23], [24], [25], [27]
Volatile data	√	X	X	[17], [18], [19], [20], [21], [22], [24], [25]
Distribution – Collaboration	√	√	√	[23], [24], [26]
Client side identification	√	X	√	[17], [19], [22]
Dependence on CSP – Trust	√	√	√	[18], [19], [20], [22], [24], [25], [26]
Service Level Agreement (SLA)	√	√	√	[19], [24], [26]
Preservation – Collection				
Integrity and stability	√	√	√	[15], [16], [17], [18], [26]
Privacy	X	√	√	[16], [17], [20], [21]
Time synchronization	√	√	√	[18], [20], [24]
Internal Staffing	√	√	√	[24], [26]
Chain of custody	√	√	√	[16], [18], [19], [20], [21], [24], [27]
Imaging	X	√	√	[15], [17], [18], [19], [20]
Bandwidth limitation	√	X	X	[18], [22], [25]
Multi-jurisdiction	√	√	√	[15], [23, [24], [26], [27]
Multi-tenancy	√	√	√	[18], [21], [24], [26]
Examination – Analysis				
Lack of forensic tools	√	√	√	[16], [18], [20], [23], [26], [27]
Volume of data	X	√	√	[15], [17], [21], [25]
Encryption	√	√	√	[16], [20], [23], [24]
Reconstruction	√	√	√	[16], [17], [18]
Unification of log formats	√	√	√	[24]
Identity	√	√	√	[19], [23]
Presentation				
Complexity of testimony	√	√	√	[16], [17], [18], [20], [27]
Documentation	√	√	√	[15], [16]
Uncategorised				
Compliance issues	√	√	√	[18], [19]

√ denotes that a challenge is present and X denotes that a challenge is not present according to the referenced authors.

related work produced by authors on every challenge. Some of the challenges' assignments may refer to more than one stage (see Section 4), but for the convenient presentation of the table each challenge is assigned to one stage.

Preservation of digital evidence along with challenges, such as maintaining chain of custody and documentation, should be applied throughout the digital investigation process. They should run concurrently with all other processes/stages in order to ensure that the evidence will be presented as admissible in a court of law. Procedures must be followed and documented from the moment an incident has occurred until the end of the investigation.

In the field of cloud forensics the most important identifiable challenge is the access to evidence in logs, as all respective authors refer to. To win an investigation, evidence must be presented in a court of law, otherwise no case exists. Once logs are the most valuable and powerful evidence all authors focused on the base on how logs can be identified and accessed in a distributed environment as cloud. The problem relies on the CSPs' dependencies, another sensitive issue to which authors referred thoroughly. Due to the physical inaccessibility, identifying, preserving and collecting evidence depend mostly on CSPs. This is why trusted relations with consumers should be built by allowing the transparency and cooperation in the first stages of an investigation. This could also be ensured with clear written and well-presented SLAs between CSP and consumer.

Forensic tools' challenge is another priority for the authors, as most of them identified that the current tools cannot be efficient and productive for collection and analysis of potential digital evidence. Developers should modify existing tools or produce new ones in order to overcome problems, such as encrypted data, acquiring evidence or the enormous amount of data which sometimes has to be analyzed in a short period of time. Again, by developing appropriate tools the chain of custody could be maintained in a better way and the collection of data would not compromise the evidence making them questionable by the jury.

References

1. http://www.mjskok.com/resource/2013-future-cloud-computing-3rd-annual-survey-results (accessed November 2013)
2. IDC, Worldwide and Regional Public IT Cloud Services 2013 –2017 Forecast, http://www.idc.com/getdoc.jsp?containerId=242464 (accessed November 2013)
3. FOXBusinessReport, Matt Egan. Cyber Crime Costs Global Economy Up to $500B a Year (July 22, 2013), http://www.foxbusiness.com/technology/2013/07/22/report-cyber-crime-costs-global-economy-up-to-1-trillion-year/ (accessed November 2013)
4. Peter, M., Grance, T.: The NIST definition of cloud computing (draft)." NIST special publication 800.145: 7 (2011)
5. Palmer Gary, L.: A Road Map for Digital Forensic Research – report from the First Digital Forensic Research Workshop (DFRWS), Utica, New York, USA, August 2001. Technical Report DTR-T001-01, Digital Forensic Research Workshop, Utica, New York, USA (November 2001)
6. Mark, R., Carr, C., Gunsch, G.: An examination of digital forensic models. International Journal of Digital Evidence 1(3), 1–12 (2002)

7. Brian, C., Spafford, E.H.: Getting physical with the digital investigation process. International Journal of Digital Evidence 2(2), 1–20 (2003)
8. Venansius, B., Tushabe, F.: The enhanced digital investigation process model. In: Proceedings of the Fourth Digital Forensic Research Workshop (2004)
9. Lang, B.N., Clark, J.G.: A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation 2(2), 147–167 (2005)
10. Kent, K., Chevalier, S., Grance, T., Dang, H.: Guide to integrating forensic techniques into incident response, pp. 800–886. NIST Special Publication (2006)
11. Rahayu, S.S., Yusof, R., Sahib, S.: Mapping process of digital forensic investigation framework. International Journal of Computer Science and Network Security 8(10), 163–169 (2008)
12. Cohen, F.B.: Fundamentals of digital forensic evidence. In: Handbook of Information and Communication Security, pp. 789–808. Springer, Heidelberg (2010)
13. Aleksandar, V., Venter, H.S.: Harmonized digital forensic investigation process model. In: Information Security for South Africa (ISSA). IEEE (2012)
14. Hong, G., Jin, B., Shang, T.: Forensic investigations in cloud environments. In: 2012 International Conference on Computer Science and Information Processing (CSIP). IEEE (2012)
15. Chen, G., Du, Y., Qin, P., Du, J.: Suggestions to digital forensics in Cloud computing ERA. In: 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC). IEEE (2012)
16. Ben, M., Choo, K.-K.R.: An integrated conceptual digital forensic framework for cloud computing. Digital Investigation 9(2), 71–80 (2012)
17. Mohsen, D., Dehghantanha, A., Mahmoud, R., Shamsuddin, S.B.: Forensics investigation challenges in cloud computing environments. In: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE (2012)
18. Shams, Z., Hasan, R.: Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. arXiv preprint arXiv:1302.6312 (2013)
19. Dominik, B., Wegener, C.: Technical issues of forensic investigations in cloud computing environments. In: 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE). IEEE (2011)
20. George, G., Storer, T., Glisson, W.B.: Calm Before the Storm: The Challenges of Cloud. In: Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, p. 211 (2013)
21. Poisel, R., Tjoa, S.: Discussion on the challenges and opportunities of cloud forensics. In: Quirchmayr, G., Basl, J., You, I., Xu, L., Weippl, E. (eds.) CD-ARES 2012. LNCS, vol. 7465, pp. 593–608. Springer, Heidelberg (2012)
22. Zimmerman, S., Glavach, D.: Cyber Forensics in the Cloud. IAnewsletter 14.1 (Winter 2011)
23. George, S., Venter, H.S., Fogwill, T.: Digital forensic framework for a cloud environment (2012)
24. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud forensics: An overview. Advances in Digital Forensics 7, 35–49 (2011)
25. Ting, S.: A Log Based Approach to Make Digital Forensics Easier on Cloud Computing. In: 2013 Third International Conference on Intelligent System Design and Engineering Applications (ISDEA). IEEE (2013)
26. Shahrzad, Z., Benford, D.: Cloud Forensics: Concepts, Issues, and Challenges. In: 2012 Third International Conference on Emerging Intelligent Data and Web Technologies (EIDWT). IEEE (2012)
27. Reilly, D., Wren, C., Berry, T.: Cloud computing: Pros and cons for computer forensic investigations. International Journal Multimedia and Image Processing (IJMIP) 1(1), 26–34 (2011)