SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:6285–6314
Published online 8 November 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1688

REVIEW ARTICLE

A survey on cloud forensics challenges and solutions

Stavros Simou[1]*, Christos Kalloniatis[1], Stefanos Gritzalis[2] and Haralambos Mouratidis[3]

[1] Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR81100 Mytilene, Greece
[2] Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, GR83200 Samos, Greece
[3] School of Computing, Engineering and Mathematics, University of Brighton, Watts Building, Lewes Road, Brighton, BN2 4GJ, U.K.

ABSTRACT

In recent years, cloud computing has gained popularity, and it is now used to support various areas of human life. Cloud forensics has been introduced to help forensic investigators find potential evidence against cloud criminal activities and maintain the security and integrity of the information stored in the cloud. While great research in the area has been carried out concerning challenges and solutions, the research on methodologies and frameworks is still in its infancy. This article focuses on the methodological aspects of cloud forensics. It critically reviews cloud forensics' existing challenges and solutions, and it explores, based on a detailed review of the area, all the work that has been carried out both in digital and cloud forensic methodologies mainly for supporting the investigation of security incidents in cloud. Furthermore, the detailed comparison reveals similarities and drawbacks of the existing methodologies providing some novel future research directions. Finally, the specific paper can be considered as a starting point for researchers wishing to design cloud-forensicable services over the cloud. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS

cloud forensics; digital forensics methodologies; cloud forensics methodologies; review; cloud forensics challenges; cloud forensics solutions

***Correspondence**

Stavros Simou, Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR81100 Mytilene, Greece.
E-mail: ssimou@aegean.gr

1. INTRODUCTION

Cloud computing is one of the most important topics in the field of Information Technology (IT) in recent years, and its popularity is rising very fast. According to Forbes contributor Louis Columbus, a key point from an IBM study was that "Cloud computing has rapidly accelerated from 30% of Chief Information Officers (CIOs) mentioning it as a crucial technology for customer engagement in 2009 to 64% in 2014" [1]. International Data Corporation (IDC) [2] predicts that by 2020, enterprise spending on cloud services, the hardware and software to support cloud services, and the services for implementing and managing cloud services will exceed $500bn, more than three times what it is today. By 2017, enterprise spending on the cloud will amount to a projected $235.1bn, triple the $78.2bn in 2011, according to Information Handling Services (IHS) Technology [3].

Every day, many organizations and companies are migrating their services over the cloud, and a great number of companies are considering adopting this technology. But companies' primary obstacle to move their systems to the cloud concerns the security and the continuously increasing number of digital crimes occurring in cloud environments. Despite the positive aspects that the rapid development of cloud computing has brought to users, it has also attracted an increasing number of users who consider cloud environment as a field of malicious acting. As it is well known, where the people, the data and the money go, so does crime [4]. According to a report sponsored by McAfee, global cyber activity (including crime on cloud) is costing up to $500bn each year, which is almost as much as the estimated cost of drug trafficking [5]. Based on the Cloud Security Alliance's survey of over 200 IT and security professionals across industries worldwide, 24.6% of companies would be willing to pay a ransom to hackers to prevent a cyber-attack, and 14.0% would pay more than $1mn [6].

Taking into consideration the previous report and survey, we could easily come to conclusion that cyber-crime is a

major issue causing great concerns among cloud service providers (CSPs), users, and law enforcements. Policies, regulations, and secure mechanisms should be developed to protect people from being deceived. Forensics is a step forward to deal with it, and it should be applied during the investigation in order to identify and acquire the evidence that would be admissible in courts. In the case of a traditional digital crime, the investigator follows digital forensic guidelines and methodologies, usually the search and seizure approach. In this case, the process encompasses the seizure, forensic imaging, and analysis of digital media to produce a report. Acquiring digital evidence from cloud environments is more restricted because infrastructures and resources not owned by the cloud users are provided by the CSPs. Users have limited or decreased access to forensic data and no knowledge as to where their data are physically located. CSPs intentional hide the actual physical location of the data, and they avoid to provide those tools and services to help users to acquire evidence in the cloud. Investigators have to conduct digital forensic investigation on cloud computers to identify, preserve, collect, and analyze all the evidentiary so as to acquire accurate results and properly present them in a court of law. This type of forensics has been raised a new area in the field that is called cloud forensics.

The main goal of the article is to present an extensive literature review on the existing methodologies and tools that deal or can potentially assist cloud forensics. It critically reviews cloud forensics' existing challenges and solutions, and it explores, based on a detailed review of the area, all the work that has been carried out both in digital and cloud forensic methodologies. 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.

The paper is organized as follows. In Section 2, a technical background about cloud computing, digital and cloud forensics is presented as well as the related work on current methodologies in digital and cloud forensics. A comparison framework is introduced based on a comparison of the presented methodologies. Finally, the authors' outcomes are discussed. Section 3 presents the cloud forensics' challenges identified from the review conducted in the respective area. A categorization of the respective challenges is accomplished based on the cloud forensics process stages identified in Section 2. Section 4 presents current cloud forensic solutions addressed based on the identified challenges. Finally, Section 5 concludes the paper and raises future research directions.

2. TECHNICAL BACKGROUND—RELATED WORK

2.1. Cloud computing—digital and cloud forensics

Companies' and organizations' main objective is to control costs while increasing profit margins. With the extensive use of Internet and new technologies, they can benefit from adopting advanced services aiming on the reduction of the cost on their infrastructure and maintenance and, in parallel, on the increase of their productivity. In order to accomplish their objectives, they can 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, 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 resources over 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 (resources are pooled to serve multiple consumers), rapid elasticity (capabilities can be elastically provisioned and released, to scale rapidly outward and inward depending on the demand) 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" [7]. A public cloud is one in which the services and infrastructure are provided off-site over a network that is open for public use, while a private cloud is one in which the services and infrastructure are provided for a single organization on a private network. A community cloud is one in which the services and infrastructure are provided between several organizations from a specific community with common concerns, while a hybrid cloud includes a variety of two or more clouds from different service providers. Figure 1 presents an overview of cloud computing with the service and deployment models, while Figure 2 shows a comparison between traditional IT and cloud computing service models.

In IaaS, cloud providers offer to users servers, storage, and hardware to install their operating system and software. The users are responsible for the maintenance. In PaaS, the development platform (environment) is provided to users. Cloud providers deliver the hardware, the operating system, and the software (databases, languages, and so on) to users to develop and run their software packages. Users have control over the deployed applications. Finally, in SaaS, cloud providers install and manage the application software, while users have access to application software. Cloud provider is also responsible for the maintenance and updated patches of the installation. Users have very limited privileges. Cloud computing provides many advantages to companies and organizations in comparison with traditional private environments. Companies can have access to unlimited storage capability and scalability from anywhere in the world. Investments on infrastructure and maintenance will no longer be a major concern.

In the digital world, where modern users live and interact on a daily basis, the number of crimes involving computer

DOI: 10.1002/sec

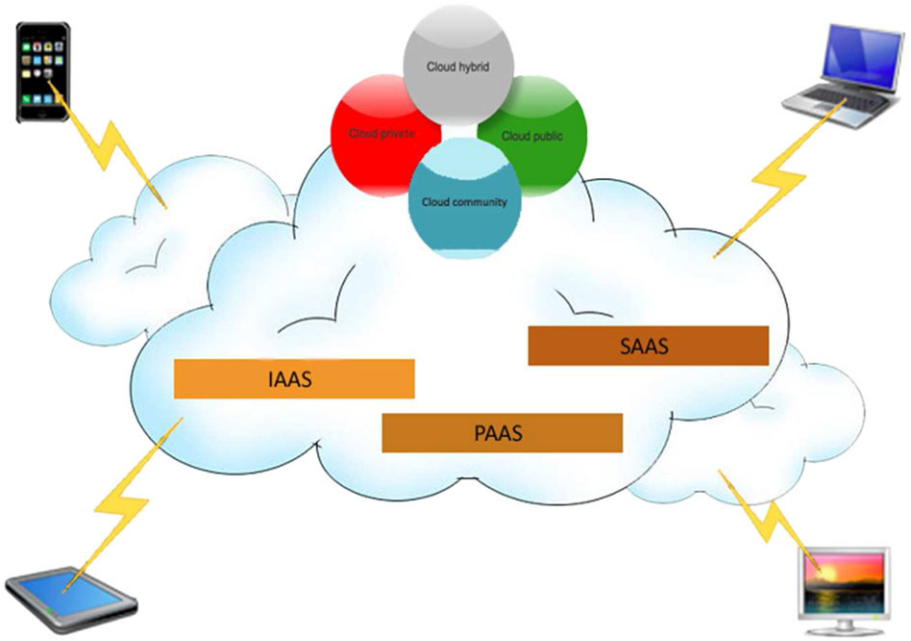

Figure 1. Cloud computing.

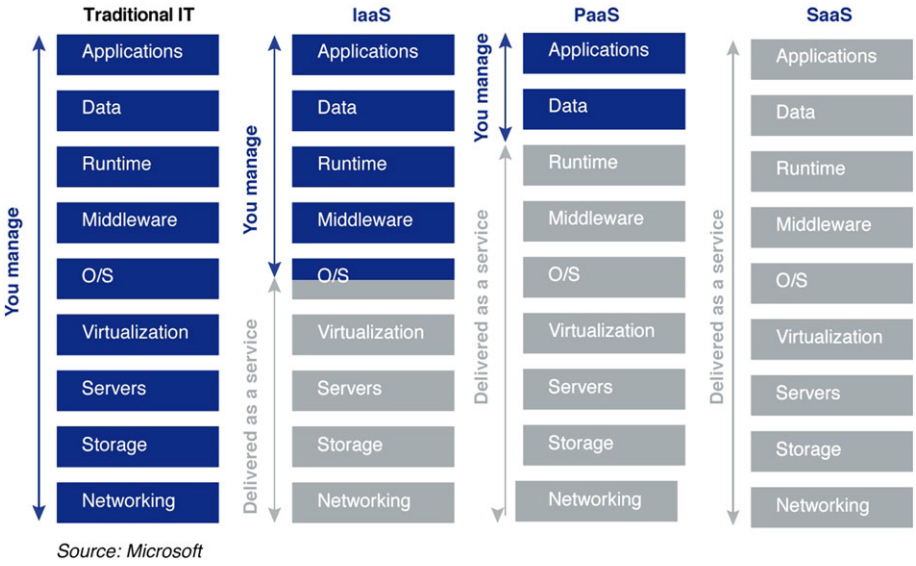

Figure 2. Comparison between traditional IT and cloud computing.

devices is growing rapidly [8], as shown in Figure 3. This has an immediate impact to the people who aim to assist law enforcement using digital evidence to uncover the digital crime. Investigators and law enforcement agents (law) are struggling to find the appropriate evidence 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.

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 is committed. The most important element in the digital forensics is to maintain the integrity and the chain of custody of the digital evidence. A break in the chain of custody (alteration to the evidence) simply means that the case is lost in a court of law.

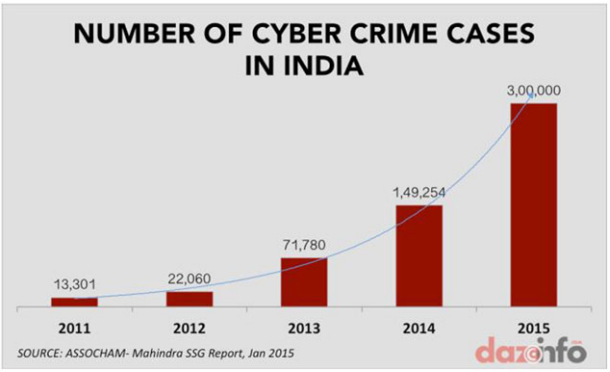

Figure 3. Number of cyber-crime cases in India.

Cloud forensics is a subset of digital forensics, and it designates 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 with network or computer investigation (digital forensics). The most important is that the evidence can reside everywhere in the world in a virtualization environment. There are also issues associated with jurisdiction, multi-tenancy, and dependence on CSPs that are unique to cloud forensics and makes it even more complex. According to National Institute of Standards and Technology (NIST) [9], cloud computing forensic science is defined as "the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence."

Identification of evidence in cloud environments is a difficult process because of 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. The investigators' main concern is to maintain that the evidence has not been compromised by third parties, in order to be presented and acceptable in the court of law. Third parties are involved in the cloud forensic process because of their collaboration with CSPs.

Various cloud forensics techniques have been developed and used depending on the cloud deployment and service model. 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. Private cloud model is closer to traditional local access networks used in the past with the added advantage of virtualization. When the private cloud is hosted on premises (internally), forensic investigation is almost identical with the traditional forensic investigation. On the other hand, if the private cloud is hosted off premises (externally), forensic investigation depends on the CSPs and the signed contracts.

2.2. Current methodologies

In this section, a detailed review is presented, based on the latest research efforts in cloud and digital forensics after thorough analysis of the respective literature. The work covers the methodologies and frameworks proposed by various researchers in digital and cloud forensics. It is worth mentioning that most of the works found are focused mainly on the investigation part and the ways a cybercrime can be resolved.

Since 1999, various methods and frameworks have been introduced regarding the way of conducting proper digital forensic investigation including different stages and phases. McKemmish [10] was one of the first researchers to define the term forensic computing (actual introducing the term digital forensics) and the definition given was "the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable." The forensic computing process consists of four key elements (stages): the identification, preservation, analysis, and presentation of digital evidence. In the identification stage, investigators need to identify all possible sources that may contain potential evidence. In the preservation stage, the chain of custody should be maintained at all times. The analysis stage involves extraction, processing, and interpretation of digital data, while presentation involves the actual presentation by expertise in a court of law.

The first Digital Forensic Research Workshop (DFRWS) [11] 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.

Collection is the activity in which the investigators acquire the evidence, while examination involves the techniques used to find and interpret significant data. Finally, in the decision stage, investigators decide what to do with the case after presenting the evidence in a court of law. 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 from the other. The problem is that the model does not discuss its steps in great detail. For each step, it produces a list of issues with no explanation. Many researchers have used this framework to develop their own work.

The US Department of Justice introduced in 2001 the Electronic Crime Scene Investigation: A Guide for First Responders [12]. It was developed to assist State and local law enforcement and other first responders who might have been responsible for preserving an electronic crime scene and for recognizing, collecting, and safeguarding digital evidence. The model consists of the stages of preparation, identification, documentation, collection and preservation, packaging, transportation and storage, examination and analysis, and finally report. In the documentation stage, all the steps in the investigation should be documented, and the chain of custody should be kept as accurately as possible. Packaging involves the methods used by investigators to pack the evidence. Transportation is to ensure that evidence remains valid for later use, and its integrity is maintained, while storage involves the place in which the evidence will be stored for analysis and further examination. The report stage describes all the actions performed recommending improvements to policies and methods, and the documentation in general. The model attempts to produce a generalized process that will be taking into consideration all the electronic devices. The drawback is that little attention is given to the analysis stage, and it is based on the standard physical crime scene.

The Abstract Digital Forensic model [13] was based on DFRWS model and consists of nine stages, which are identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence. In the preparation stage, investigators need to prepare tools, techniques, search warrants, and monitoring authorizations, while in the approach strategy stage, decisions are taken about the strategy that should be followed. The returning evidence stage ensures physical and digital property is returned to the proper owner. This model adds three more stages compared with the DFRWS model, but preparation and approach strategy could be merged into one single stage. The model allows a standardized process to be defined without specifying the exact technology involved. On the other hand, the model does not deal at all with the chain of custody issue. It assumes that a strong chain of custody will be maintained throughout the investigation. The model has also not been tested nor proven to be efficient and reliable for a digital/cloud forensic framework [13].

In 2003, the Integrated Digital Investigation Process (IDIP) [14] model was introduced based on the crime scene theory for physical investigations. The model lends many of the same phases of the previous models, but it uses the theory that a computer is itself a crime scene. 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 readiness phase is to ensure that operations and infrastructure are able to fully support an investigation. Deployment phase refers to the provision of a mechanism for the incident to be detected and confirmed. Physical crime scene investigation phase deals with the collection and analysis of the physical evidence and the reconstruction of the actions that take place during the incident, while the digital crime scene investigation phase identifies the electronic events that occur on the system. Finally, the review phase involves reviewing the investigation to identify areas of improvement. The drawback of this model is that investigators cannot be sure whether a digital crime was committed or not, unless some preliminary physical and digital investigation has been made.

The Enhanced IDIP model [15] separates the investigations in 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 and introduces the primary crime scene phase. It also presents two additional phases: the trace back and the dynamite one. In the trace back phase, the physical crime scene of operation is tracked down leading to identification of the devices that were used to perform the act. The dynamite phase investigates the primary crime scene aiming to collect and analyze the items that were found to obtain further evidence. The reconstruction is only made after all investigations have taken place.

The Extended Model of Cyber-crime Investigations introduced by Ciardhuain [16] in 2004 identifies the activities of the investigative process and the major information flows in that process, an important aspect of developing supporting tools. The model includes information flow description between different phases and consists of the stages of awareness, authorization, planning, notification, search for and identify evidence, collection, transport, storage, examination, hypothesis, presentation, proof/defense, and dissemination of information. In the awareness activity, awareness is created by events external to the organization, which will carry out the investigation. Authorization activity involves both external and internal entities to obtain the necessary authorization. Planning activity is strongly influenced by information from both inside and outside the investigating organization. Notification activity refers to informing the subject of an investigation or other concerned parties that the investigation is taking place. In the hypothesis activity, the investigators must construct a hypothesis of what has occurred based on the examination of the evidence. In the proof/defense

activity, investigators will have to prove the validity of their hypothesis and defend it against criticism and challenge. Dissemination is the final activity in which some information may be made available only within the investigating organization, while other information may be more widely disseminated. According to Selamat *et al.* [17], this framework provides a basis for the development of techniques and tools to support the work of investigators, and thus, it is probably considered as the most complete to that time.

The hierarchical objectives-based framework [18] for the digital investigations process in 2005 proposes a multi-layer, hierarchical framework, as opposed to the single-tier approach being presented to date. It 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. The incident response phase is to detect, validate, assess, and determine a response strategy for the suspected security incident. The incident closure phase focuses on closure of the investigation. As stated by the authors, the framework offers unique benefits in the areas of practicality and specificity over previously proposed frameworks such as the Integrated IDIP [14]. The drawback is that the model focuses on traditional computer and network forensics, without taking into consideration other digital devices, such as phones and removable data storage.

In 2006, the Forensic Process [19] proposed by NIST consists 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 are examined, extracted from media, and transformed into a format that can be processed by forensic tools. Then data are transformed into information through analysis, and finally, the information is transformed into evidence during the reporting phase.

In 2006, Von Solms [20] introduced a control framework for digital forensics with five high-level control objectives: digital forensic readiness, evidence preservation, forensic acquisition, forensic analysis, and evidence presentation. The control framework is intended to provide a sound theoretical basis for digital forensics, as well as a reference framework for digital forensics governance within organizations.

The digital forensic investigation framework [17] 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 digital forensic investigation framework for investigating all incident cases without tampering the evidence and protects 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 [21] defined nine stages: identification, collection, preservation, transportation, storage, analysis-interpretation and attribution, reconstruction, presentation, and destruction. The analysis–interpretation and attribution stage involves the analysis, examination, and interpretation of the collected evidence, while it creates attribution that can then be used as a basis for further efforts to attribute to the standard of proof required. Reconstruction involves evaluating the context of a scene and the evidence found there in an effort to identify what occurred and in what order it occurred. In the destruction stage, evidence and other information associated with a legal matter will be destroyed or returned after its use. All of these should be carried out in a manner that meets the legal standards of the jurisdiction and the case.

The Systematic Digital Forensic Investigation Model [22] proposed in 2011 helps forensic practitioners and organizations to set up suitable policies and procedures. The proposed model places emphasis on the cyber-crime and cyber-fraud in the form of an 11 stages model. The stages are preparation, securing the scene, survey and recognition, documenting the scene, communication shielding, evidence collection, preservation, examination, analysis, presentation and, finally, result and review. Securing the scene stage deals with securing the crime scene from unauthorized access and keeping the evidence from being contaminated. Survey and recognition involve an initial survey conducted by the investigators for evaluating the scene, identifying potential sources of evidence and formulating an appropriate search plan. In communication shielding, all further possible communication options of the devices should be blocked. A problem with the specific model is that its applicability is limited to computer fraud and cyber-crime only [23]. It has not been applied to all situations such as heterogeneous environments and new technologies.

The Harmonized Digital Forensic Investigation Process model [24], 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. It is an iterative and multi-tiered model, where each phase contains a set of sub-phases. The phases are defined in terms of scope, functions, and order. These are the following: incident detection, first response, planning, preparation, incident scene documentation, identification, collection, transportation, storage, analysis, presentation, and conclusion. In addition to the digital investigation process, there are also six more phases, which should be considered concurrently with the digital investigation processes: authorization, documentation, information flow, preserving chain of custody, preserving digital evidence, and interaction. Information flow phase identifies and describes these information flows so that they can be protected and supported technologically (use of trusted public key infrastructures and timestamping to identify investigators and authenticate evidence). The parallel actions ensure higher

efficiency and digital evidence admissibility. The drawback of the model is that its accuracy and efficiency has not been yet verified.

The Forensic Investigations Process [25] in cloud environments was based on the Forensic Process with the four stages. Because of the evolution of cloud computing, the stages were changed to apply basic forensic principles and processes. The four distinct steps are as follows: (a) determine the purpose of the forensics requirement, (b) identify the types of cloud services (SaaS, IaaS, and 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. The model does not include any actions after the evidence collection.

In 2012, Cloud Forensics Process [26] focused on the competence and admissibility of the evidence while keeping into consideration the human factor. The process consists of the following four stages: (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, and collect potential evidence. Again, in this case, the model does not include any actions after the evidence collection.

The Integrated Conceptual Digital Forensic Framework for Cloud Computing [27], proposed in 2012, is based on [10] and [19]. 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, and reporting and presentation. The iteration of the framework demonstrates one of the key differences in the identification and analysis of evidence sources [23].

In 2013, Adams [28] introduced the Advanced Data Acquisition Model that can assist digital forensic practitioners when it comes to presenting evidence in court that originated in the cloud. The model comprises three stages associated specifically with the acquisition of electronic data, the initial planning stage, the onsite survey, and the acquisition of electronic data. The initial planning stage is where high-level considerations are determined that relate to documentation associated with the investigation. The onsite survey is where all the gaps in knowledge relating to the location, size, and format of the devices holding the electronic data are filled in and main acquisition plan is created. The acquisition of electronic data includes both replication and storage of the acquired data. There is a common factor associated with all the stages, and this is documentation. The model focuses on the process of identifying and acquiring digital data but not on the analysis and presentation of evidence, which it will be in a later work. Advanced Data Acquisition Model is a promising model taking into consideration more factors concerning digital and cloud forensic investigation. It also incorporates procedures and techniques that can be modified and expanded upon to accommodate new technological challenges.

The Integrated Digital Forensic Process Model [29], presented in 2013, is at the same time a merging of existing forensic models, an integration of them and a purification of the terminology used, resulting in an all-encompassing standardized Integrated Digital Forensic Process Model. It consists of the processes of preparation, incident, incident response, physical investigation, digital investigation, presentation, and the concurrent process of documentation. The drawback is that the model is not applicable in all cases as it was made by considering only a small number of the forensic models [23].

Finally, in 2015, Zawoad *et al.* [30] proposed a cloud forensic process called Open Cloud Forensics model. It consists of the preservation stage, which runs in parallel with the stages of identification, collection, organization, presentation, and verification. The organization stage includes examination and analysis. In the verification stage, the court authority will verify the cloud-based evidence provided by an investigator. The proposed model can support reliable forensics in a realistic scenario by considering the important role of CSPs. As stated by the authors, the model can be used by cloud architects to design clouds that support trustworthy cloud forensics investigations.

2.3. Comparison framework

After a thorough study of the digital and cloud forensic models that have been proposed, it was concluded that a comparison framework needs to be created to map the stages of different methodologies. The goal of the comparison framework is twofold: First, to merge the same or similar stages of the proposed frameworks and models into the stages of the comparison framework, and second, to assign the challenges to stages of the comparison framework. For the purposes of the comparison framework, Table I is produced to show the stages and processes of the previously proposed models. Our study has revealed 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. A number of stages and processes are similar, in some cases with identical names and in other cases with different names but with the same meaning. In the next session, cloud forensic challenges will be presented, and each one of them will be assigned to a specific stage.

In order to implement the comparison framework, we take into consideration the stages' limitations of the previous models. Some of them are either very detailed and complicated including a great number of processes to implement or over simplified omitting important aspects. The comparison framework merges the same or similar stages of previous models that produce the same outcome, into one stage. The model is very close to the Integrated Conceptual Digital Forensic Framework introduced by Martini [27] with two important basic differences. First,

Table I. Digital and cloud forensics methodologies.

McKemmish	DFRWS	D.O.J.	Reith *et al.*	Carrier *et al.*	Baryamureeba *et al.*
Identification	Identification	Preparation	Identification	Readiness (includes): Operation and Infrastructure phases	Readiness (includes): Operation and Infrastructure phases
Preservation	Preservation	Identification	Preparation	Deployment (includes the following):	Deployment (includes the following):
Analysis	Collection	Collection and preservation	Approach strategy	*Detection and notification*	*Detection and notification*
Presentation	Examination	Packaging, transportation and storage	Preservation	*Confirmation and authorization*	*Physical Crime Scene Phases* (*includes*): *Preservation*, *Survey*, *Documentation*, *Search and collection*, *Presentation*
	Analysis	Examination and analysis	Collection	Physical crime scene investigation (includes the following):	*Digital Crime Scene Phases (includes): Preservation, Survey, Search and collectionn Documentation*
	Presentation	Reporting	Examination	*Preservation*	*Confirmation*
	Decision	Concurent Processes: Documentation	Analysis	*Survey*	*Submission*
			Presentation	*Documentation*	Traceback (includes the following):
			Returning evidence	*Search and collection*	*Digital Crime Scene Stages*
				Reconstruction	*Authorization*
				Presentation	Dynamite (includes the following):
				Digital crime scene investigation (includes the following):	*Physical Crime Scene Phases*
				Preservation	*Digital Crime Scene Phases*
				Survey	*Reconstruction*
				Documentation	*Communication*
				Search and collection	Review Phase
				Reconstruction	
				Presentation	
				Review Phase	

identification stage is considered as a unique stage because the first step in an investigation must always identify all the possible evidence. Second, we propose preservation and collection to constitute one separate stage as collected data should be simultaneously preserved properly. Therefore, the comparison framework should include preservation in the collection stage. Finally, the reporting and presentation stage is called presentation, which of course includes all the reports that will be used in a court of law and the closure of the case. The stages of the model are illustrated in Figure 4.

This comparison framework 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 framework consists of four steps:

(1) Identification is the first stage, and the main concern is to identify all possible sources that may contain potential evidence in a cloud environment, in order to prove that the incident took place. Investigators need to determine the type of crime and what type of assets (hardware, software, and data) has been used. They also need to identify the location of the incident and the cloud provider. An investigation team is formed consisting of people with special skills in cloud environments, such as legal advisors, experienced technicians, and law officers. In this stage, a search warrant needs to be issued to attain access to CSP's infrastructure. All the actions taken to identify potential evidence to notify people and the methods used during this stage should be properly recorded and documented. Investigators

Table I. Digital and cloud forensics methodologies.

McKemmish	Ciardhuain	Beebe *et al.*	Kent *et al.*	von Solms	Selamat *et al.*	Cohen	Agarwal, Gupta
Identification	Awareness	Preparation	Collection	Readiness	Preparation	Identification	Preparation
Preservation	Authorization	Incident response	Examination	Preservation	Collection and preservation	Collection and preservation	Securing the scene
Analysis	Planning	Collection (preservation, package, transport and store)	Analysis	Acquisition	Examination and analysis	Transportation	Survey and recognition
Presentation	Notification	Data analysis	Reporting	Analysis	Presentation and reporting	Storage	Documenting the scene
	Search and identification	Presentation		Presentation	Disseminating the case	Analysis, Interpretation and Attribution	Communication shielding
	Collection	Incident closure				Reconstruction	Collection
	Transportation					Presentation	Preservation
	Storage					Destruction	Examination
	Examination						Analysis
	Hypothesis						Presentation
	Presentation						Result and review
	Proof/Defence of hypothesis						
	Dissemination of information						

need to prepare the steps they are going to undertake and an action plan of how to move into the investigation should be produced. This stage is crucial, because the next one depends upon the evidence identified here.

(2) Preservation—collection. After identifying the potential evidence, the collection and acquisition of the evidence from the locations they reside in clouds follows. Investigators need to isolate and preserve the evidence by preventing people from using the digital device or by duplicating digital evidence. During the collection-acquisition specific resources will be used. This involves well trained personnel (internal or even external), special tools for cloud extraction data, and up-to-date methodologies/processes such as protection mechanisms and action plans. 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. The acquired evidence should be well documented and checked for their integrity in order to discover any future alteration.

(3) Examination—Analysis involves the extraction of data from the previous stage and the inspection of the huge amount of data identified. Trained personnel and technician experts should examine all the data to find evidence. In order to go into a forensic examination, investigators should obtain a high-level overview of the terrain and form a strategy; otherwise, delays might occur when unforeseen but preventable problems are encountered. Examiners should review previously encountered cases and training plans to find patterns that can help reduce the time of the examination and develop their action plan. The findings from the evidence examination phase will be used as input to the evidence analysis phase. During analysis, actors should determine the significance of the data in order to transform them into evidence. Actors involved in the analysis should be prepared to deal with responsibility and professionalism, once analyzing data can expose other users' sensitive data due to multi-tenancy environment in cloud. In

Table I. Digital and cloud forensics methodologies.

McKemmish	Valjarevic, Venter	Guo *et al.*	Chen *et al.*	Martini *et al.*	Ruan	Kohn *et al.*	Zawoad *et al.*
Identification	Incident detection	Determine the purpose of the forensic	Ascertain the purpose of cloud forensics	Identification and preservation	Initial Planning - Preparation, notification and awareness	Preparation	Identification
Preservation	First response	Determine the type of the cloud service	Ascertain the type of the cloud service	Collection	Onsite survey - Identification	Incident	Collection
Analysis	Planning	Determine the type of the technology	Ascertain the type of the technology	Examination and analysis	Acquisition of electronic data	Incident response	Organization (Examination - Analysis)
Presentation	Preparation	Collection and preservation	Collection and preservation	Reporting and presentation	Concurent process: Documentation	Digital investigation	Presentation
	Incident scene documentation					Physical investigation	Verification
	Identification					Presentation	Concurent process: Preservation
	Collection					Concurent process: Documentation	
	Transportation						
	Storage						
	Analysis						
	Presentation						
	Conclusion						
	Concurrent Processes: Authorization						
	Documentation						
	Information flow						
	Preservation						
	Interaction						

this stage, data reconstruction will also take place. Once again, all the resources involved or used during this phase should be properly documented, and reports should be produced.

(4) Presentation stage is the final stage and deals with the presentation of the evidence in a court of law. A well-documented report with findings must be produced using expert testimony on the analysis of the evidence. Experts with personal knowledge of the procedures that generate the reports should be chosen. They should be prepared to confront the jury who lacks knowledge of cloud computing. Evidence must be presented in a way that the jury will understand all the technical details because cloud computing is a very complicated environment for ordinary Internet users to understand. The implemented reports along with the supporting materials concerning the chain of custody of the evidence should be submitted to the court of law. Information such as type of incident, compromised accounts, who's responsible, what the consequences were, and details of findings will be included in the reports and presented.

2.4. Running example

For verifying the applicability of the aforementioned comparison framework, a case study is presented. Through this, the usage of the stages and the activities of the framework are being identified and described. The case deals with trafficking illicit digital material in cloud environment.

Mary is a malicious user responsible for trafficking illegal content over the Internet. Law enforcement agents detect the illegal activity, and the investigation is initiated. Mary uses the cloud, so investigators locate the Cloud Provider and issue a warrant to access the servers and

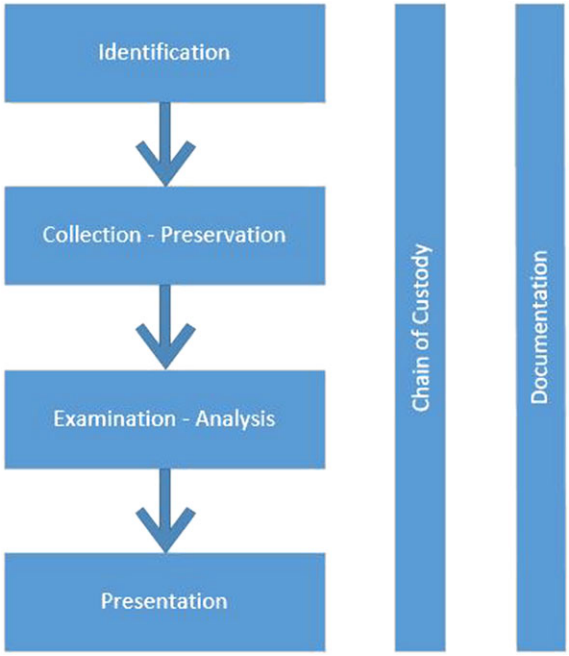

Figure 4. Stages of the model.

preserve data. A special trained team responsible for the incident is formed consisting of IT and law officers. The identification of the malicious actor's IP address is unsuccessful, because of the third countries proxy servers. Using CSP's assistance, investigators try to find more evidence such as card payment information, subscriber id's, and access logs. Also, they are trying to identify the source of the evidence and assets, such as computers, laptops, and mobiles. All personnel involved in the investigation and their actions are recorded and documented according to the data preservations procedures and principles. Once system information and potential evidence have been identified, the CSP assigns an experienced and skilled technician to produce an exact copy of all data of the original media (hard disk) that is under the supervision of the investigators using the appropriate tools. Then, the technician verifies the image for integrity and authenticity of data. These tests reveal any alteration of the evidence through forensically acceptable procedures. The entire process of creating the image should be documented in detail presenting the exact methods and tools that have been used, the technical skills of the personnel responsible for the creation and any other relevant detail. With the completion of the controls, the provider sends the image and all data collected to investigators for examination in order to carry on with the investigation.

Once investigators receive the virtual machine (VM) image and respective data, new checks and controls are taking place to ensure its integrity and validity. Using appropriate tools, data are being analyzed for any useful information such as files containing photos, videos and sounds, event logs, IP addresses, and timestamps. File system and windows registry are also analyzed. Investigators load the VM snapshot to be able to obtain more information regarding the structure of the web site. After a thorough investigation, a precise timeline with evidence related to the investigation is produced. From the examination of the evidence, protective actors manage to trace malicious actor's IP address. Reports are being produced and handled with all the evidence. The reports contain information about the CSP, the persons involved in the investigation, evidence analysis, methods, and all technical terms used. All the stages followed during the aforementioned investigation have been well documented in accordance with forensic principles and procedures, in order to ensure the integrity and validity of the evidence and to preserve the chain of custody. Evidence presentation has been assigned to experienced personnel.

2.5. Methodologies and frameworks discussion

In Table II, a comparison of the stages of the proposed models found in the literature review with the stages of the comparison framework is presented. From the analysis illustrated in Table II, most of the models include the four stages of the comparison framework with few exceptions. Some stages/activities on the proposed models are not mapped entirely with the stages of the comparison framework, but they are merged into a stage. Stages/activities of the proposed models such as preparation, approach strategy, readiness and deployment, awareness, authorization, planning, notification, incident response, and survey have been included in identification stage. In preservation–

Table II. Mapping stages/activities of forensic models with comparison framework.

Comparison framework	Identification	Preservation—collection	Examination—analysis	Presentation
McKemmish	Identification	Preservation	Analysis	Presentation
DFRWS	Identification	Preservation—collection	Examination—analysis	Presentation—decision
D.O.J.	Preparation—identification	Collection—preservation—documentation—packaging—transportation—storage	Examination—analysis	Reporting
Reith *et al.*	Identification—preparation—Approach strategy	Preservation—collection	Examination—analysis	Presentation—returning evidence
Carrier *et al.*	Readiness—deployment	Preservation—survey—documentation—search—collection	Reconstruction	Presentation—review
Baryamureeba *et al.*	Readines—detection—notification—confirmation	Preservation—survey—documentation—search—collection	Examination—analysis—reconstruction	Submission—communication—review
Ciardhuain	Awareness—autorization—planning—notification—search—identification	Collection—transport—storage	Examination—hypothesis	Presentation—proof/defence—dissemiantion
Beebe *et al.*	Preparation—incident response	Collection (preservation—package—transport—store)	Analysis	Presentation—closure
Kent *et al.*	X	Collection	Examination—analysis	Reporting
von Solms	Planning—preparation	Preservation—acquisition	Analysis	Presentation
Selamat *et al.*	Preparation	Collection—preservation	Examination—analysis	Presentation—reporting—dissemination
Cohen	Identification	Collection—preservation—transportation—storage	Analysis—interpretation—attribution—reconstruction	Presentation—destruction
Agarwal, Gupta	Preparation—secure scene—survey and recognition	Documentation—communication shielding—evidence—preservation	Examination—analysis	Presentation—result and review
Valjarevic, Venter	Detection—first response—planning—preparation—Identification	Documentation—collection—transportation—storage	Analysis	Presentation—conclusion
Guo *et al.*	Identification	Preservation—collection	X	X
Chen *et al.*	Identification	Preservation—collection	X	X
Martini *et al.*	Identification	Preservation—collection	Examination—analysis	

(*Continues*)

Table II. (Continued)

Comparison framework	Identification	Preservation—collection	Examination—analysis	Presentation
				Reporting—presentation
Ruan	Planning—preparation—notification—awareness	Preservation—collection—documentation	X	X
Kohn *et al.*	Preparation—incident—approach strategy	DFI (preservation—collection—transport—store…)	DFI (examination—hypothesis—analysis—reconstruction …)	Presentation
Zawoad *et al.*	Identification	Preservation—collection	Organization (Examination—analysis)	Presentation—verification

collection stage, the following stages/activities have been included: acquisition, packaging, transportation, and storage. Examination analysis consists of reconstruction, interpretation, and attribution. Finally, presentation encloses reporting, decision, returning evidence, closure, review, dissemination, and conclusion. Even though documentation is assigned in preservation–collection stage, as an activity runs in parallel with the stages of the comparison framework alongside with the chain of custody.

In order to examine the complexity of the aforementioned methodologies, we have established some complexity indicators based on the number of stages introduced (S) and the number of phases on every stage (P) per methodology. The analysis is conducted based on the comparison framework proposed before. Regarding the complexity indicators, we have introduced three different scales: L (low), M (medium), and H (high). If the number of stages and phases is less than three, the complexity is low. If the number of stages and phases is three or four, the complexity is medium, and if the number of stages and phases is more than four, the complexity is high.

The outcome of the complexity analysis is shown in Table III. The number in each column of the four basic stages is describing the stages and phases of the methodology in this particular stage. The letter describes the complexity of the stages of each methodology.

Based on the review analysis, it is obvious that cloud forensics is far more demanding than digital forensics. This is due to the 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. Most of the methodologies and frameworks, introduced in the past years concerning cloud forensics, are based on digital forensics models. This idea is not wrong as long as there is no mere reproduction of the old models without considering the cloud technology. This is a problem once the two techniques are different. The main difference between cloud forensic methods and previous forensic ones is that the digital forensics methods do not take into consideration the physical inaccessibility and the unknown location the data reside. Another limitation is the dependency by cloud providers and the multi-jurisdiction issues. Even though the techniques seem very similar, the nature and characteristics of cloud environment makes it difficult to map each traditional forensic model to cloud environment [31].

The methodologies/models presented in the previous paragraphs are consisting of different stages. Some of them have been built upon previous ones, such as the Enhanced DIP model [15] based on [14], the Integrated Conceptual Digital Forensic Framework for Cloud Computing [27] based on [10] and [17], while the Abstract Digital Forensic model [13] and the Systematic Digital Forensic Investigation Model [22] both inspired by [11]. The number of stages depends on the complexity and the depth of the details implemented by researchers. A closer look can reveal that almost all the models use four basic stages: (i) identification, (ii) collection and

Table III. Complexity of methodologies' stages.

Methodologies/ models	Stages (S) and phases (P)	Idendification	Preservation—collection	Examination—analysis	Presentation
McKemmish	4	1 (L)	1 (L)	1 (L)	1 (L)
DFRWS	7	1 (L)	2 (L)	2 (L)	2 (L)
D.O.J.	7	2 (L)	3 (M)	1 (L)	1 (L)
Reith *et al.*	9	3 (M)	2 (L)	2 (L)	2 (L)
Carrier *et al.*	17	4 (M)	8 (H)	2 (L)	3 (M)
Baryamureeba *et al.*	14	5 (H)	5 (H)	1 (L)	3 (M)
Ciardhuain	13	5 (H)	3 (M)	2 (L)	3 (M)
Beebe *et al.*	6	2 (L)	1 (L)	1 (L)	2 (L)
Kent *et al.*	4	—	1 (L)	2 (L)	1 (L)
von Solms	5	1 (L)	2 (L)	1 (L)	1 (L)
Selamat *et al.*	5	1 (L)	1 (L)	1 (L)	2 (L)
Cohen	8	1 (L)	3 (M)	2 (L)	2 (L)
Agarwal, Gupta	11	3 (M)	4 (M)	2 (L)	2 (L)
Valjarevic, Venter	12	5 (H)	4 (M)	1 (L)	2 (L)
Guo *et al.*	3	1 (L)	2 (L)	—	—
Chen *et al.*	3	1 (L)	2 (L)	—	—
Martini *et al.*	4	1 (L)	1 (L)	1 (L)	1 (L)
Ruan	4	2 (L)	2 (L)	—	—
Kohn *et al.*	6	3 (M)	1 (L)	1 (L)	1 (L)
Zawoad *et al.*	6	1 (L)	2 (L)	1 (L)	2 (L)

preservation, (iii) examination and analysis, and (iv) presentation and reporting. Preservation in some models is an autonomous stage, while in others is combined with identification or with collection.

Most of the models have been focused on digital forensics. They do not take under consideration the characteristics of cloud environment. Only five models [25–28,30] have been developed for cloud forensic purposes, but only two [27,30] of them are complete. [25,26,28] focus on the first two stages, identification and preservation–collection, and do not include any actions after the evidence collection. A point of consideration is that researchers do not feel comfortable with concurrent processes, other than documentation. Only [24] attempts to propose processes to be performed in parallel with the phases.

Few of the authors have made an attempt to develop new models to conduct digital forensic investigations in the cloud computing environments. Adams [28] introduced a model that covers a great deal of issues on cloud forensics, but it still does not give answers about analysis, examination, and presentation of digital evidence. To the best of our knowledge, no author has 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 stages and processes in an investigation. This is the reason of the categorization of stages presented earlier. The categorization is based upon models and frameworks introduced and proposed by academics and the industry.

Regarding the preservation, this process could be a different activity (separated from collection) in a cloud forensic framework running concurrently with all the other processes. This is because preserving evidence is the most important step in an investigation and must be handled with care in order to be presented in a court of law. Documentation could also be an activity in itself because it is carried out throughout the investigation, from the identification to presentation. These activities together with the chain of custody 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. Another point need to be discussed is the iteration. Some researchers point out that there should be an iteration stage in cloud forensics methodology because of the new evidence that could be revealed during the analysis of data. If that happens, the investigators need to go back to the identification stage and start the procedure again to acquire new evidence for analysis and examination. These issues will be thoroughly studied, and it will be included in a future work.

3. 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 2.3. 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.

3.1. Identification stage

3.1.1. 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. Collecting logs from a cloud environment is a difficult process, given the blur nature of clouds and the multi-tenant cloud models, where a big number of different users share the same processing and network resources [32]. 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 Application Program Interface (API) or the pre-designed interface. It is just partly applicable in IaaS cloud model as it provides the VM, which behaves almost the same as an actual machine [33]. On the other hand, many CSPs do not provide services to gather logs and sometimes intentionally hide the details from customers. Researchers have already identified a number of challenges associated with logging in cloud-based application infrastructure. According to [34], decentralization of logs, volatility of logs, multiple tiers and layers, archival and retention, accessibility of logs, non-existence of logs, absence of critical information in logs, and non-compatible/random log formats are the major challenges associated with cloud-based log analysis and forensics.

3.1.2. Physical inaccessibility

In a cloud environment, data location is a difficult task because of the geographical distribution of the hardware devices. The established digital forensic procedures and tools assume that physical access to the hardware is a fact [35]. However, in cloud forensics, the fact that the data to be acquired may reside on different physical devices, which in turn are being used by multiple cloud consumers and that the configuration of the devices may not be static, makes it almost impossible for the CSP to offer any form of physical acquisition [28]. There is also, no possibility to seize the hardware containing data, because the data are stored in distributed systems usually in different jurisdictions. This challenge does not apply to any kind of geographical distributed corporation, where all the resources are located in the company's premises. In case an incident occurs, all the devices can be accessed immediately because they belong to private premises, where organizations have full control. The challenge applies to all three-service models.

3.1.3. Volatile data

Data stored in a VM 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 VM instance leading to a complete loss of volatile data, if no further countermeasures are installed [36]. Respective literature [35,37–39] places 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.

3.1.4. 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 PaaS scenarios [36]. Once the perpetrator is identified, investigators need to be carefully prepared and move quickly to collect the data as early as possible in its sterile state for forensic purposes to use as evidence [31]. In any other case, the perpetrator could destroy data, and critical evidence could be lost. Client side evidence identification plays a vital role in the investigation, and most of the time is difficult to acquire because of different jurisdictions. In an exhaustive forensic investigation, the evidence data gathered from the browser environment should not be omitted, and their collection should be carefully planned and executed.

3.1.5. Dependence on cloud service provider—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. They may be reluctant to give out permission to access their multi-tenant environment [40]. 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. This is a complicated issue, once the investigators need to rely on the honesty of the CSP's employee, who is not a certified forensic investigator. CSPs can always alter the logs and data as they have the full control over the logs [32]. 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. Finally, transparency is mandatory for raising users' trust. However, in most of the cases, transparency is not provided in current real-world cloud environments. Many cases sensible data are computed on services running in the cloud; thus, transparency plays an important

role. Because of the unknown, many users fear to trust the CSP's [41]. To prove that data have been preserved during an investigation, the integrity method is used. On the other hand, integrity can add difficulties to cloud forensics because of additional trust that is required to be accredited from an investigator to third parties [42]. This challenge applies not only to identification stage but also to preservation and collection stage.

3.1.6. Service level agreement

The terms agreed to within the SLA may provide information on how forensic investigations will be handled. "If the SLA does not include notice of what kind of procedure or forensic data should be provided to the consumer, then the cloud provider has no contractual obligation to provide such information" [43]. 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 [44]. 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. According to Baset [45], "a common aspect of the considered SLAs is that none of the IaaS cloud providers offer any performance guarantees for the compute services. Moreover, no cloud provider automatically credits the customer for SLA violations, and leaves the burden of providing evidence for any such violation on the customer," which may be unacceptable for enterprise. Another problem is that most SLAs for online services do not specify the location where data will be stored. Unless they have reason to believe otherwise, end-users will not know the actual location of their stored data and subsequently the laws governing it [4]. Service level agreements (SLAs) concern the stages of identification, preservation, and collection.

3.2. Preservation—collection stage

3.2.1. Integrity and stability—multi-tenancy and privacy

The integrity preservation and the stability of the evidence are 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 [33]), then the evidence will not be admissible to the court of law. According to [42], integrity can add difficulties to cloud forensics due to additional trust that is required to be accredited from an investigator to third parties in order to verify the data in question. The authority providing verification of integrity need to set in advance a mechanism to be trusted by the courts; otherwise, it will be difficult to justify using them as a source for integrity verification. It is also difficult to maintain the stability of the data because of the transient nature and dedicated description of the data in a Cloud [26]. According to [27], this challenge applies to analysis stage.

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. "Any attempt to physically connect to a data store or virtual host system will run a risk of modifying data that is outside the scope of the investigation insofar as belonging to a system that is not owned or operated by the suspect named in the warrant" [46]. Because of the multi-tenancy, the data can be contaminated by people who have access into the same storage unit with result of losing important evidence. Moreover, the privacy of other tenants needs to be preserved. The virtualization of the systems 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 that clients' information will not be accessed by any member of the staff even if they have been deleted.

3.2.2. 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 [44].

3.2.3. 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, to maintain the chain is a huge challenge. "The first potential failure of the chain is with the cloud provider. There is no control on the forensic investigation with respect to procedure, process, or person; the collection of evidence is conducted 'behind doors' " [43]. 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, and who accessed the evidence [27]. Another issue with ensuring a proper chain of evidence according to [43] is that many CSPs use proprietary file systems for provided services. This introduces questions of validity and presents a gap in familiar digital forensics practices handling hard drives.

3.2.4. Imaging

In IaaS, to make an image of the instance to acquire evidence can be accomplished by taking a snapshot 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 environments, the client will not have any access to the hardware that is provided on the host; thus, the investigators will have to rely on the CSP having the resources and the incentive to be able to acquire client data in a forensically sound matter. It is more complicated if the data are physically stored on a device hosted by a subcontracted third-party. For SaaS, investigators have even less visibility of the hardware [28].

3.2.5. 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.

3.2.6. Multi-jurisdiction distribution—collaboration

To acquire evidence from the three models in cloud from different jurisdictions is another issue for the investigators. Because of 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 [26]. A court order issued in the jurisdiction that resides a data center may not be applicable to the jurisdiction that resides another [46]. "The location of data affects the ability to compel production of such data and may, although unlikely under most states' in USA and countries long arm jurisdiction rules, affect the determination of where a case involving cloud data must be filed/prosecuted" [43]. There is another issue on whose law will be used when the parties and evidence are located in different jurisdictions. The distribution of computer systems in the cloud environment makes the investigators to confront problems with different jurisdictions and laws. To access information, they need to issue a search warrant to the CSP to provide the information required. Identifying and gathering information will almost certainly consume more time in the case of cascaded services than a single CSP [47]. Obtaining data in different countries require reference to treaties between these countries. This is why international collaborations between law enforcement and CSPs must be taken into consideration [48].

3.3. Examination—analysis stage

3.3.1. 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. On the other hand, there are no tools designed specifically for cloud investigations (with few exceptions). Investigators often use existing tools when first investigating cloud crimes, but these commercial tools used for remote forensics have not been tested for correctness or error rate and have not yet been presented in court [4]. To analyze digital evidence is a hard process and requires time. The problem is that the larger the storage capacity, the greater the time required [47]. According to cyber forensics needs analysis survey [49], 40% of the participants indicate that mobile and cloud forensic tools and technology need improvement most. 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.

3.3.2. Volume of data

The amount of data, stored in the CSPs' data centers, is extremely large, and it is increasing on a daily basis. Large amount of data (Petabytes of information) can produce many problems towards the searching of relevant digital evidence [50]. This has an immediate impact on the analysis of the information in order to find useful evidence for the investigation. The problem is also addressed by Quick and Choo [51] stating that research gaps still remain in relation to data reduction techniques, data mining, intelligence analysis, and the use of open and closed source information. Appropriate capture and display filters have to be developed and set up in order to make the data volume present in Cloud Infrastructures able to be processed [35]. 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 [52]. The effect on network performance should be considered in a live acquisition together with the significant impact on the CSP's resources, and the interference with other businesses in case data is being extracted remotely [28].

3.3.3. Encryption

Many cloud customers in all three-service models store their data in an encrypted format to protect them from criminal activities. To investigate encrypted information

is a not an easy task and requires skills from the investigator, both to obtain the encryption keys and forensically analyze the information [47]. 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 [48].

3.3.4. Time synchronization—reconstruction

In all three-service models, the time concerning data is also crucial and requires hard work to come with the correct results. This is because data are stored in multiple geographical regions with different time zones. "The event logs contain a field that logs the timestamp at which an event took place. This value of the logged field however is determined by the date-time of the computer, set by the user. This presents a problem; the times on all the machines may not be synchronized" [53]. Investigators need to gather all the time stamps from the devices and establish an accurate time line of events [38]. Date-time stamps, as digital evidence, are very important in a court of law. Once they can be easily altered, additional verification needs to be obtained; otherwise, investigators cannot ascertain whether the event occurred at a certain time [54].

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 [33]. 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.

3.3.5. 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 [44].

3.3.6. Identity

In traditional digital forensic, associating a user with the data stored in their computer device is comparatively straightforward (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 it is 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 [48]. 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.

3.4. Presentation stage

3.4.1. Complexity of testimony

All the technical information of the acquisition is almost unlikely to be understood by the court where the jury (often) consists of people with only the basic knowledge in computer systems. Thus, the process and the steps followed by the investigators should be explained thoroughly [28]. 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. Cloud computing is one of the most complicated computing environments and may challenge even a juror with great technical background. Thus, all the evidence should be presented carefully, and the expert witness testimony should be understood by the jury [4]. This is an important issue towards the progress of the trial.

Another problem with the presentation of evidence concerns the originality of the evidence: 1002 Federal Rule of Evidence requires the advocate to bring the "original" of writing, recording, or photograph unless the rules provide otherwise. Because of cloud characteristics where data are stored throughout the world, the admissibility of the "original" evidence will almost never be possible. "The inability to 'go back' and obtain the original again is a unique issue that presents challenges for cloud forensic investigations from an authenticity standpoint" [43]. Without the original evidence, it would be very difficult to persuade the jury, which expects a piece of paper to be presented.

3.4.2. 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.

3.5. Challenges analysis

To assign challenges to stages, Integrated Conceptual Digital Forensic Framework [27] was used with a slight differentiation as presented in Section 2. Cloud forensic 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 IV was designed for assigning challenges according to the respective stage and service model they belong to. The table also captures the related work produced by authors on every challenge. Some of the challenges' assignments may refer to more than one

Table IV. Cloud forensic challenges overview.

Cloud forensic challenges/stage	Applicable to IaaS	PaaS	SaaS	Related work
Identification				
Access to evidence in logs	partly	√	√	[27] [32] [33] [34] [37] [36] [38] [35] [39] [41] [44] [48] [52] [55] [56] [57]
Physical inaccessibility	√	√	√	[28] [32] [37] [44] [48] [52] [57]
Volatile data	√	X	X	[31] [33] [37] [36] [38] [35] [39] [48] [41] [44] [52]
Client side identification	√	X	√	[33] [36] [39]
Dependence on CSP—trust	√	√	√	[32] [37] [36] [38] [39] [40] [41] [42] [44] [52] [56]
Service level agreement	√	√	√	[4] [36] [41] [43] [44] [45] [50] [56] [58] [59]
Preservation—collection				
Integrity and stability—multi-tenancy, privacy	√	√	√	[26] [27] [32] [33] [37] [38] [35] [42] [43] [44] [46] [56]
Internal staffing—chain of custody	√	√	√	[4] [27] [32] [37] [36] [38] [35] [42] [43] [44] [56] [57]
Imaging	X	√	√	[26] [28] [33] [37] [36] [38]
Bandwidth limitation	√	X	X	[37] [39] [52]
Multi-jurisdiction—distribution—collaboration	√	√	√	[4] [26] [43] [44] [46] [47] [48] [56] [57]
Examination—analysis				
Lack of forensic tools	√	√	√	[4] [27] [37] [38] [47] [48] [49] [56] [57]
Volume of data	√	√	√	[26] [28] [33] [35] [47] [50] [51] [52]
Encryption	√	√	√	[27] [38] [44] [47] [48]
Time synchronization—reconstruction	√	√	√	[27] [33] [37] [38] [44] [53] [54]
Unification of log formats	√	√	√	[44]
Identity	√	√	√	[36], [48]
Presentation				
Complexity of testimony	√	√	√	[4] [27] [28] [32] [33] [37] [38] [43] [57]
Documentation	√	√	√	[26] [27] [28]
Compliance issues	√	√	√	[32] [37] [36]

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

stage, but for the convenient presentation of the table, each challenge is assigned to one stage.

Among the challenges found in cloud computing environment, there is one that cannot be categorized into a specific stage. This is the compliance issues challenge. Companies and organizations such as banks, brokers, and hospitals are not transitioning easily to cloud environments, because of trustworthy data retention issues, together with laws and regulations. There are several laws in different countries, which mandate the trustworthy data retention [37]. 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 [36].

National Institute of Standards and Technology [9] has compiled a list of 65 challenges identified in the cloud computing environment. Even though our list of challenges consists of 20 (including compliance issues), most of NIST's challenges are included in our list. This is due to NIST's detailed breakdown in comparison with our more generic form (i.e., NIST identify four different challenges for jurisdiction issue).

In the field of cloud forensics, the most important identifiable challenge is the access to evidence in logs, as the majority of the 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. Because of the limited access and control over cloud, to acquire log files is at least challenging. Most of the researchers' solutions are dependable on the CSP's good will to provide the logs.

As mentioned in the previous paragraph, CSP's dependencies and good will are another sensitive issue to which authors referred thoroughly: Because of the physical inaccessibility, identifying, preserving, and collecting evidence depend mostly on CSPs. Most of the researchers have focused on trust and proposed solutions trying to deal with this issue. However, trusted relations with consumers should be built in order to allow the transparency and cooperation in the first stages of an investigation. On the other hand, consumers must choose providers after a thorough search with great consideration and in terms of security assurance. Transparency could also be ensured with clear-written and well-presented

SLAs between CSP and consumer. Regarding SLAs, researchers propose new ideas and methodologies that fit into cloud and future services, leaving behind the traditional forms of contracts.

Finding the appropriate tools 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. Tools are used throughout the investigation. In order to be accepted and used by the investigators and law people, they should be developed according to specific standards, following approved methodologies and being tested in the field of cloud forensics. Dykstra *et al.* [60] developed a tool designed for cloud forensic purposes, one of the few available. 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.

Most of the researchers agree that another major concern is the absence of international standards and policies in cloud computing. Because of the multi-jurisdictional, laws, regulations, and methodologies are hard to be applied in cloud environments; thus, new guidelines and standards need to be written and adopted by all countries. The task for overcoming security and compliance issues within such environments is quite hard to deal with. Governments also need to be more co-operative with the law enforcement agents even if they represent other governments. The ultimate goal for the investigators is to have as less limitations as possible in multi-jurisdictions, given the fact that no limitations is not possible due to existing sensitivities and threat actors.

Our findings are visualized in Figure 5. The challenges are presented with their categories and sub-categories.

4. CLOUD FORENSIC SOLUTIONS

In this section, we present all possible solutions addressing clarified challenges, identified from an analytical review conducted in the respective area. In the following section, identified solutions are presented categorized per challenge.

4.1. Identification stage

4.1.1. Access to evidence in logs

One of the most important issues in cloud forensics is the identification and collection of logs from cloud infrastructures. This is valid because consumers and investigators have almost no control over the CSPs' infrastructures on which the investigation is based upon as discussed before. From the analysis of the cloud forensic literature, it is clear that this challenge is referred from the majority of researchers that deals with the respective field. There are plenty of researchers that tried to come up with approved solutions. One of them is Zawoad *et al.* [32] who introduced secure-logging-as-a-service (SecLaas) mechanism for cloud forensics, which allows CSPs to store VMs' logs and provides access to forensic investigators while preserving the confidentiality of the cloud users.

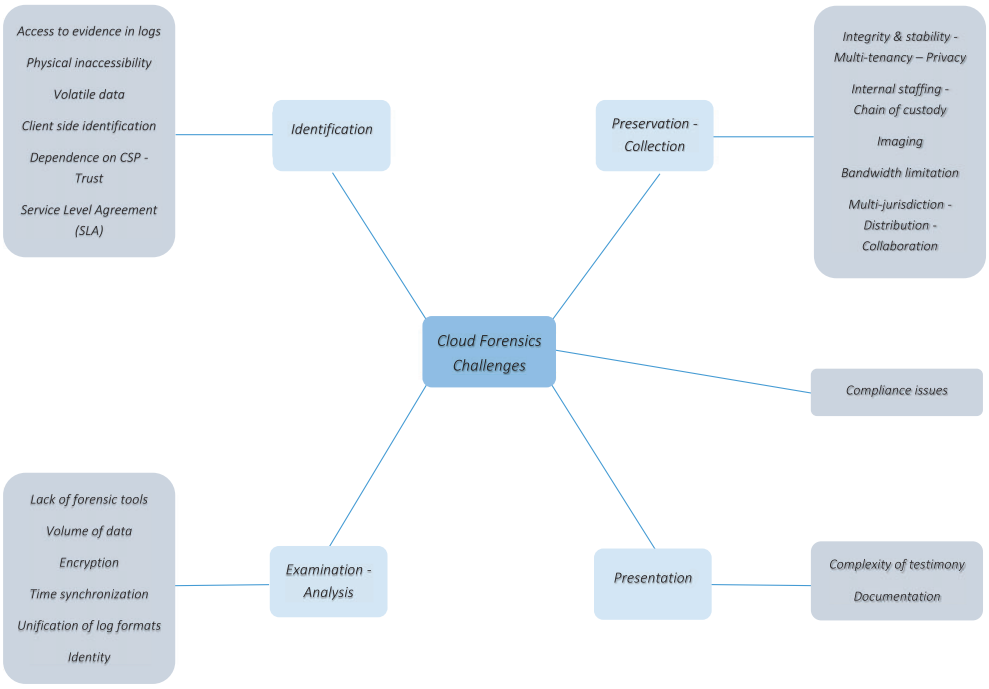

Figure 5. Cloud forensic challenges (categories and sub-categories).

Additionally, an auditor can check the integrity of the logs using the proof of past log and the log chain.

Sang [52] proposed a log-based model, which can help to reduce the complexity of forensic for non-repudiation of behaviors on cloud. He proposes that we should keep another log locally and synchronously, so we can use it to check the activities on SaaS cloud without the CSP's interference. The local log module will use information such as unique id and timestamp on the log record locally. HASH code will be also used to detect modification on the log files. In PaaS, the CSPs should supply a log module on PaaS to the third-party in order to create a customized log module, for both of the consumer side and the cloud side.

Trenwith [53] proposed "the design of a model that considers centralized logging of all activities of all the participants within the cloud in preparation of an investigation." It collects log evidence and transports them to a remote and central log server where they are archived. This approach shortens the acquisition of evidence when an investigation is required. The model was developed for windows platforms only, and also, it does not address the security issues, such as access control on the central server, which is limitations on prototype.

Patrascu *et al.* [61] introduced a logging framework —"a hierarchical architectural model - that allows investigators to seamlessly analyze workloads and VMs over a cloud infrastructure, while preserving scalability of large scale distributed systems." There is a consideration about the results according the time.

In PaaS, because the customers have full control on their application over a prepared API, system states and specific application logs can be extracted. Birk *et al.* [36] proposed a logging mechanism, which automatically signs and encrypts the log information before its transfer to a central logging server under the control of the customer. This mechanism will prevent potential eavesdroppers from being able to view and alter log data information on the way to the logging server.

Dykstra *et al.* [62] recommend the cloud management plane, an out-of-band channel that interfaces with the cloud infrastructure for using in IaaS model. This system interfaces with the provider's underlying file system and hypervisor and is used to manipulate the firewall and provision, start and stop VMs. Users and investigators can download VM images, log files, disk images, and packet captures from the management plane.

Solving the cloud logging problems Marty [34] proposed a log management architecture that involves three steps: enable logging on all infrastructure components to collect logs from, setup and configure log transport, and finally tune log sources to make sure we obtain the right type of logs and the right details collected. He states that every log entry should log what happened, when it happened, who triggered the event and why it happened. According to this, the minimum fields need to be present in every log record are timestamp, application, user, session ID, severity, reason, and categorization. He also recommends an application on how log entries should be structured. At the end, an application logging infrastructure at SaaS company was implemented using application components such as Django, JavaScript, Apache, MySQL, Operating system, and Java Backend. Zawoad *et al.* [37] mentioned that although the advantages to this approach are several, the specific work does not provide any solution about logging network usage, file metadata, process usage, and other evidence, which are important for forensic investigation in IaaS and PaaS.

Damshenas *et al.* [33] suggested a solution in PaaS, to prepare an API to extract relevant status data of the system, limited by the data related to the client only. In SaaS, depends on the interface, he proposed to implement the feature to check the basic logs and status of the client's usage. The aforementioned features should provide read-only access only and demands for specific log and system status manager running as a cloud service.

According to Zafarullah *et al.* [63] logging standards should be developed, which ensure generation and retention of logs and a log management system that collects and correlates logs. A cloud computing environment was setup using Eucalyptus. Using Snort, Syslog, and Log Analyzer (e.g., Sawmill) Eucalyptus behavior was monitored, and all internal and external interaction of Eucalyptus was logged. Observing the log entries that were generated by the Eucalyptus, not only the attacker's IP address was recorded but also details on number of http requests along with timestamps, http requests/responses and fingerprinted attacker's OS and web browser were provided.

4.1.2. Volatile data

To overcome the problem of volatile data, live investigation has been used as an alternative approach to dead acquisition. Grispos *et al.* [38] mentioned that the specific approach enables investigators to gather data that might otherwise be lost if a computer is powered down. On the other side, it may increase the amount of information an investigator is able to extract. To address this challenge, Damshenas *et al.* [33] proposed the cost to be globalized between CSPs to offer persistent storage device for client's data.

To prevent loss of volatile data, Birk *et al.* [36] suggested frequent data synchronization between the VM and the persistent storage or a non-cloud-based storage. According to Zawoad *et al.* [37], this solution does not provide any guideline about the procedure, and he proposed two possible ways of continuous synchronization. CSPs can provide a continuous synchronization API to customers, and CSPs can integrate the synchronization mechanism with every VM and preserve the data within their infrastructure.

4.1.3. Client side identification

To identify evidence on client's side, Damshenas *et al.* [33] suggested designing and implementing an application to log all potential evidence on the client' machine.

However, they did not provide any methodology about the application and the procedure.

4.1.4. Dependence on CSP—trust

In cloud environments, customers have to depend completely on the CSPs, which affect the trust relationship between them. The lack of transparency and trust between CSP's and customers is an issue that Haeberlen [64] was dealt with considering the accountable cloud. He suggested a basic primitive called AUDIT that an accountable cloud could provide. The idea is that the cloud records its actions in a tamper-evident log, customers can audit the log and check for faults, and finally they can use log to construct evidence that a fault has (or not) occurred. When an auditor detects a fault, it can obtain evidence of the fault that can be verified independently by a third party. A TrustCloud framework proposed by Ko *et al.* [65] consists of five layers of accountability: system, data, workflow, policies, and laws and regulations layers. To increase accountability detective approaches used rather than preventive.

Nurmi *et al.* [66] presented Eucalyptus, an open-source software framework for cloud computing that implements IaaS, which is the answer to the trust relationship between CSPs and customers. A model showing the layers of trust has been introduced by Dykstra *et al*. [62]. In IaaS, six layers have been established, and more layers would have added in the other two cloud models. Each layer requires a different amount of confidence. The further down the stack, the less cumulative trust is required.

4.1.5. Service level agreement

Service level agreements can provide useful information to investigators about the rights and obligations between CSPs and users. Thorpe [50] states that users have the right to decide (especially in private cloud) where their data reside as form of jurisdictional control via the SLA. This means that during a cloud forensic investigation LEA can search data that reside on premise, therefore evidence will be in the same jurisdiction as the users. For this purpose, a number of SLA-based solutions have been identified, which besides the coverage of the aforementioned statement contribute to the down measures valuation of service performance.

Service level agreements should include important terms regarding cloud forensic investigations. According to Ruan *et al.* [44], SLAs should include the following: service provided, techniques supported, access granted by the CSP to the customer, trust boundaries, roles and responsibilities between the CSP and the cloud customer, security issues in a multi-jurisdictional environment in terms of legal regulations, confidentiality of customer data, and privacy policies and security issues in a multi-tenant environment in terms of legal regulations, confidentiality of customer data and privacy policies. In the following paragraphs, a number of SLA-based solutions presented. They follow the logic that Ruan [44] describes about the role of SLAs in a cloud forensic process, and they can be an added value to the forensic process.

A well-written SLA between CSP and customer should include the client's privacy policies Damshenas *et al*. [33]. Baset [45] provided guidance on how SLA should be defined for future cloud services. An SLA should be providing components such as service guarantee time period, service guarantee time period and granularity, service violation detection and credit, outcome-based SLAs, and finally standardization of SLAs. An SLA framework for ecommerce cloud based on the Web SLA [55] is proposed by Busalim *et al*. [58]. It supports the SLA life cycle according to [67] and provides some parameters and objectives, which should be included in the SLA to consider the end user perspective.

Bouchenak *et al.* [68] defined a new cloud model where quality of service (QoS) and SLA are first-class citizens. The model should be orthogonal to other cloud models and may apply to any of them. It should involve both CSP and user. A control-theoretic approach should be followed to design fully autonomic cloud service in order to provide better than best-effort cloud QoS. Cloud services also should be designed to be controllable by construction, and benchmarking tools are necessary to have measurable results. Serrano *et al.* in [59] introduced the SLA-aware-service cloud model that defines a non-functional interface, which exposes the SLA associated with a cloud functional service. CSLA, the Cloud Service Level Agreement, language has been introduced to describe QoS-oriented SLA associated with cloud services, and a control-theoretic approach has been presented to provide performance, dependability, and cost guarantees for online services. Both authors use the term service level objective, a means of measuring the performance of the service provider and are outlined as a way of avoiding disputes between the two parties based on misunderstanding

Biggs *et al.* [69] proposed SLA's to be robust in order to be effective in combating cyber-crime. For example, illegal activities such as distributed denial of service should test cloud vendors' systems and procedures and return useful feedback to assist forensic procedures. To overcome the SLA's issue with different and multiple relationships, Birk *et al.* [36] suggested a trusted third-party to audit the security measures provided by the CSP. Finally, SLAs' violation is another problem in which Haeberlen [64] proposed the trusted time-stamping. Timing information must be added to a tamper-evident log in order to detect the violations.

4.1.6. Integrity and stability—privacy and multi-tenancy

To validate the integrity of the evidence, Zawoad *et al.* [37] suggested a digital signature on the collected evidence should be generated and then the signature should be checked. Hegarty *et al.* [70] developed and implemented a distributed signature detection framework that enables forensic analysis of storage platforms. Based on the metadata-driven data storage model and provenance integrity, in SaaS, Shi *et al.* [71] presented a multi-tenancy model where the data storage security issue should be

mapped as a series of integrity issues of data chunks. To ensure the primitiveness and integrity of the evidence, Yan [72] proposed a new cyber-crime forensic framework to image the relative records and files absolutely.

Juels *et al.* [73] explored proofs of retrievability (PORs) in which a prover (i.e., back-up service) can produce a concise proof that a verifier (client) can retrieve a file in its entirety. PORs method and cryptographic techniques can help users to ensure the privacy and integrity of files they retrieve. To preserve the integrity of the data, Birk *et al.* [36] proposed the Trusted Platform Module to assure the integrity of a platform. This standard allows a secure storage and detects changes to previous configurations. A traditional trusted platform can secure the computation on a single host. The trusted cloud computing platform provides a closed box execution environment by extending the concept of trusted platform to an entire IaaS backend. The trusted cloud computing platform guarantees the confidentiality and the integrity of a user's VM and allows a user to determine up front whether or not the IaaS enforces these properties [74]. Damshenas *et al.* [33] suggested all the issues concerning clients' privacy data should be included in an SLA contract.

Zhou *et al.* [75] proposed a role-based (RBE) scheme that allows role-based access control policies to be enforced for the encrypted data stored in public clouds. Based on RBE scheme, a secure cloud data storage architecture was developed using both public and private cloud. Specifically, public cloud was used for allowing users to store data in encrypted form securely, and private cloud was used for maintaining the sensitive information related to the organization's structure. After the experimental evaluation, the results are promising, given efficient performance characteristics such as efficient encryption and decryption on the client side as well as superior characteristics of the proposed RBE. According to Ambritta *et al.* [76], the proposed scheme is based on centralized approach wherein a user has to register to the organizations authority to obtain keys to access and decrypt the required data and there are some scalability issues. They proposed the Identity and Access Management in Future Internet architecture, which provides a mechanism of privacy of the attribute information while liberates the owner from the overhead of managing the user registration and key management activities.

Yang *et al.* [77] proposed data access control for multi-authority cloud storage, to secure privacy with efficient decryption (using a token-based decryption method) and revocation (that achieves both forward and backward security). To ensure authentication of log data and proof of integrity, Trenwith *et al.* [53] used the SHA-256 cryptographic hash algorithm. The original hash of the log used as an encryption key to encrypt a salt value and the resulting cipher-text then saved to the metadata file. Li *et al.* [78] proposed a provenance system with fine-grained access control based on an ABS scheme. The proposed system provides confidentiality, unforgeability, anonymous authentication, fine-grained access control, and provenance tracking. Furthermore, the computation and communication overhead for the data owner is low. However, the cloud server is considered as an honest cloud server with huge computation capacity, while users are regarded as devices with low-computation capability.

4.1.7. Internal staffing—chain of custody

It is hard to find the right people to work as a team in order to be involved in a cloud investigation. Ruan *et al.* [44] proposed a solution that involves internal staffing, CSP-customer collaboration and external assistance with specific roles. Individuals of the team must be trained on, law regulations, new methodologies, specialized tools, and techniques. According to Chen *et al.* [26], an investigator should possess the abilities of professional forensics skills such programming, networking, co-operating, communicating and negotiating with CSPs and understanding laws and regulations.

Grispos *et al.* [38] suggested trained and qualified personnel in forensic investigations should be hired by CSPs. When an investigation arises, the personnel should begin the chain of custody process, which will be passed onto the investigation party. They also suggested that a partial solution to different jurisdictions is having trained and qualified personnel to perform forensic investigations when needed. According to Ruan *et al.* [44], organizational policies and legally binded SLAs need to be written, in which, communications and collaborations regarding forensic activities through the chain of CSPs and customers' dependencies should be clearly stated. The need for well-trained personnel is necessary to fulfill chain of custody.

4.1.8. Imaging

To overcome the issue of acquiring forensic image, Damshenas *et al.* [33] proposed to generate a track record of all clients' activities. After that, to generate a forensic image of specific clients, all it requires is to check the track record of the client and then copy bit-by-bit stream of all the area the client has accessed to. The captured VM image is always on the CSP's data centers, and it cannot be taken from the client's side, once it is capable of being reached only with great difficulty.

4.1.9. Multi-jurisdiction—distribution—collaboration

New regulations have to be developed in order to solve the cross border legislation issue. Biggs *et al.* [69] proposed an international legislation that will police the Internet and cloud computing specifically. Global unity must be established so the investigations on cloud environment to be fast and successful. Dykstra [4] suggested the search warrant for cloud-based data should not specify a physical address to be searched. Instead, the warrant should specify the desired data and the warrant served to the data custodian. According to Ruan *et al.* [44] and Sibiya *et al.* [48], international laws should be developed to secure that forensic activities will not breach any laws or regulations under any jurisdiction.

Table V. Cloud forensics solutions.

Cloud forensic challenges	Solution	IaaS	PaaS	SaaS	Related work
Access to evidence in logs	Secure-logging-as-a-service mechanism	√	√	√	[32]
	Status data extraction and checking		√		[33]
	Log management architecture			√	[34]
	Logging mechanism		√		[36]
	Log-based model		√	√	[52]
	Digital forensic readiness model	√	√	√	[53]
	Management plane	√			[62]
	Logging framework	√	√	√	[61]
	Eucalyptus framework	√			[63]
Physical inaccessibility	—	—	—	—	—
Volatile data	Cost globalization between CSPs	√			[33]
	Continous synchronization API	√			[37]
	Data synchronization	√			[36]
	Live investigation	√			[38]
Client side identification	Log application	√	√	√	[33]
Dependence on CSP—trust	Accountable cloud	√	√	√	[64]
	TrustCloud framework	√	√	√	[65]
	Eucalyptus framework	√			[66]
	Layers of trust model	√			[62]
Service level agreement (SLA)	Well and clear-written terms	√	√	√	[33]
		√	√	√	[44]
		√	√	√	[50]
	External auditors	√	√	√	[36]
	Service guarantee, violation detection, credit and standardization	√	√	√	[45]
	Trusted timestamping	√	√	√	[64]
	Define SLA parameters and objectives	√	√	√	[58]
	QoS and SLA model	√	√	√	[68]
	SLA-aware-service	√	√	√	[59]
	Robust SLAs	√	√	√	[69]
Integrity and stability—privacy and multi-tenancy	SLA contracts	√	√	√	[33]
	Digital signature	√	√	√	[37]
	Trusted Platform Module	√	√	√	[36]
	Digital forensic readiness model	√	√	√	[53]
	Distributed signature detection framework	√	√	√	[70]
	Multi-tenancy model			√	[71]
	Cyber-crime forensic framework	√	√	√	[72]
	Proofs of retrievability	√	√	√	[73]
	Trusted cloud computing platform	√			[74]
	Secure role-based access control	√	√	√	[75]
	Identity and access management in future internet architecture	√	√	√	[76]
	Data access control for multi-authority cloud storage	√	√	√	[77]
	Provenance system	√	√	√	[78]
Internal staffing—chain of custody	Team collaboration with wide range of skills	√	√	√	[44]
		√	√	√	[26]
	Trained and qualified personnel	√	√	√	[38]
	Organizational policies and SLAs	√	√	√	[44]
Imaging	Track record generator	√			[38]
Bandwidth limitation	—	—	—	—	—
Multi-jurisdiction—collaboration	Faster compliance with court orders	√	√	√	[4]
	International laws	√	√	√	[44]
		√	√	√	[48]

(*Continues*)

Table V. (Continued)

Cloud forensic challenges	Solution	IaaS	PaaS	SaaS	Related work
	International legislations and global unity	√	√	√	[69]
Lack of forensic tools	Management plane	√			[62]
	Proofs of retrievability	√	√	√	[73]
	Forensic Open-Stack Tools	√			[60]
Volume of data	Public cloud storage	√	√	√	[38]
	Triaging techniques	√	√	√	[38]
		√	√	√	[51]
Encryption	Digital forensic readiness model	√	√	√	[53]
	Hierarchical attribute-set-based encryption	√	√	√	[79]
Time synchronization—reconstruction	Unified/specific time system	√	√	√	[33]
	Network Time Protocol	√	√	√	[80]
	Created-Accessed-Modified model	√	√	√	[54]
Unification of log formats	—	—	—	—	—
Identity	—	—	—	—	—
Complexity of testimony	Personal knowledge of the case	√	√	√	[43]
	Interactive presentation	√	√	√	[81]
Documentation	Detailed documentation from start to end	√	√	√	[43]
	Targeted/pointed presentation	√	√	√	[81]
Compliance issues	Preservation and proofs of logs	√	√	√	[32]
	Survey	√	√	√	[36]
	Transparency	√	√	√	[36]
	Third Party Auditor	√	√	√	[36]

4.1.10. Forensic tools

Most of the researchers acknowledge that tools need to be developed to identify, collect, and analyze forensic data. Juels *et al.* [73] developed PORs tool for semi-trusted online archives, which guarantee the privacy and the integrity of files. In IaaS, Dykstra *et al.* [62] recommended the appropriate forensic tool for acquiring cloud-based data is the management plane. This is a web-based point and click interface to manage and monitor the infrastructure. They concluded that it offers the most attractive balance of speed and control with trust option.

En-Case and Accessdata FTK tools were also used to acquire evidence, and the results were successful, but authors do not recommend them because too much trust is required. On the other hand, tools such as Internet Evidence Finder, and F-Response make use of relevant extensions to recover various cloud and social network related artifacts [40]. Dykstra *et al.* [60] designed and implemented a management plane forensic toolkit in a private instantiation of the OpenStack cloud platform (IaaS), which is called Forensic Open-Stack Tools—It consists of three new forensic tools, and it provides trustworthy forensic acquisition of virtual disks, API logs, and guest firewall logs.

4.1.11. Volume of data

A solution to the challenge is to use the public clouds to store the evidence, but this method arises new issues from a legal and technical perspective [38]. The other solution is the adoption of triaging techniques, but first, an assessment on the influence of the various triage processes on real-world devices and data should be conducted [51]. They also state that data mining provides a potential solution to understanding the increasing volume of data as long as it is used as an intelligence and knowledge tool. New methods should be developed to allow only partial recovery of data, and they should be according to accepted forensic principles.

4.1.12. Encryption

Trenwith *et al.* [53] use both Advanced Encryption Standard and Rivest–Shamir–Adleman algorithms to solve the problem with the encrypted data, once this scheme guarantees confidentiality and authenticity over unsecured connections. Large data files are encrypted with using Advanced Encryption Standard, while Rivest–Shamir–Adleman algorithm is used to encrypt the aes-key. Wan *et al.* [79] proposed hierarchical attribute-set-based encryption to achieve scalability, flexibility, and fine-grained access control in cloud computing.

4.1.13. Time synchronization—reconstruction

To solve the time zones' problem, Damshenas *et al.* [33] suggested a specific time system (i.e., GMT) to be used on all entities of the cloud, as it brings the benefit of having a logical time pattern. In IaaS, the VM time is under the client's control meaning that all date and times used in logs and other records should be converted to the specific time system. Another solution to overcome the problem is the Network Time Protocol, designed by Mills [80]. It

provides clock synchronization between computer systems. The latest protocol RFC 5905 is considered as the most efficient. Kao [54] proposed a novel cyber-crime investigation countermeasure using a novel created-accessed-modified model for the control and continuous improvement of digital evidence processes in a cloud environment. This countermeasure is an important contribution to the field of cloud storage forensics. It improves the accuracy of date-time stamps in a cloud storage device.

4.1.14. Complexity of testimony

Wolthusen in [81] suggested of using interactive presentation and virtualization environments, which allow the exploration of data sets in such a way that a focus on relevant data is possible without engendering the risk of leading questions and investigations. Orton in [43] proposed that persons with personal knowledge of the procedures in cloud forensics should present the evidence and to be able to show and explain the process used to extract data. The person should be able to describe the testing results and most important to describe the logic behind the process.

4.1.15. Documentation

The documentation of the investigation according to Wolthusen [81] must be presented in a way pointing: possible gaps in the data sets, uncertainties about the semantics and interpretation of data and the limitations of the collection mechanisms alongside the actual data. Detailed documentation should include all the persons involved in the investigation, the exact steps taken for ensuring that the evidence has not been tampered (e.g., how the evidence was transported and stored securely) and that verification occurred through hashes [43].

4.1.16. Compliance issues

According to Birk *et al.* [36], recommended customers should check their compliance requirements and CSPs services to find out which CSP matches customers' needs. On the other hand, CSP should offer as much transparency as possible. Finally, a Third Party Auditor could be used acting as a trustee between the customer and the CSP.

Zawoad [32] stated that preservation and proofs of logs could increase the auditability of cloud environments, which are a vital issue to make the cloud compliant with the regulatory acts such as Payment Card Industry Data Security Standards, Health Insurance Portability and Accountability Act, and Sarbanes–Oxley Act.

4.2. Solution's summary

After assigning challenges to stages, Table V has been produced from the findings regarding the available solutions for every identified cloud forensics challenge. All the solutions presented have been assigned according to the service model they belong to. If the solution concerns the Platform as a service model, a check sign confirms it; otherwise, the minus sign is illustrated.

Most authors dealing with cloud forensics solutions have focused their research study on specific issues. As seen in Table V, only for three issues, a fair amount of solutions has been given. Access to logs, integrity and privacy and SLAs are those issues, having almost the same number of solutions with all the others added up. It might be worthwhile for future research to focus on the above. Many of the solutions to access to logs, privacy, and encryption issues based on the experience of the previous researchers using similar algorithms or models. Even though [63] managed to collect logs from cloud infrastructure, and [36,62] managed to mitigate the challenges of log acquisition, none of them managed to produce a system of storing the logs in Cloud and making it available publicly in a secure way [32].

In Table IV, 20 different challenges are cited, whereas in Table V, the challenges with the corresponding solutions proposed by the authors are only 16. This is due to the absence of a solution for a respective challenge. Physical inaccessibility, bandwidth limitation, unification of log formats, and identity are those challenges that solutions could not be found in the literature review. Even though, forensic investigation in cloud environments has moved forward the past years, there are still open issues to explore. Dependence on CSP is still required in various issues, such as access to log files and trust relationship. Most of the problems rely on the CSPs' point of view. Absence of international standards and regulations cannot establish the global unity, which can help to cross the boundaries in multi-jurisdiction and collaboration challenge.

Unification of log formats is another issue, which needs to be solved. All the evidence needs to be presented in a court of law in such a way that the jury could understand the complexity of the non-standard data sets. Depending on the volume of data, bandwidth limitation is another issue that needs to be solved, when the time is a crucial factor to an ongoing investigation. The identity of the user who has been engaged in a criminal act is also an unanswered case.

5. CONCLUSION

Besides its obvious advantages, the complexity of cloud computing provides a shelter to malicious users for proceeding on a number of criminal activities. Methodologies, challenges, and solutions have been identified and proposed by researchers in order to make cloud environments more secure to users. Within this work, an updated and most recent review in cloud forensics has been presented based on the latest research efforts in cloud forensics. First, all the frameworks and methodologies dealing with digital and cloud forensics have been presented along with an extended discussion regarding their functionality, drawbacks, and complexity parameters. Next, all respective cloud-based challenges, according to the respective literature, have been identified and categorized assisting authors to reason about the necessity of cloud forensics on specific

areas in accordance with the efforts conducted so far. Finally, existing solutions regarding the aforementioned challenges were also presented in order to identify the respective efforts presented for realizing identified challenges. Our main goal was to bring forward all the work that has been carried out till now in cloud forensics and discuss the methods and solutions introduced by the researchers.

Designing and developing trustworthy software and services is of vital importance for modern Internet users who are extremely aware about the protection of their security and privacy when using online services. Thus, the design and implementation of cloud services that can assist investigators conducting cyber-crime investigations in a more efficient way raises users' trustworthiness and system's security as well. For implementing cloud-forensicable software and services, first, we need to understand which are the main requirements that need to be fulfilled in such systems. This review moves towards this direction by identifying the respective efforts from the investigation side in order to understand what investigators demand during a forensic process and which are the present efforts already conducted in the cloud.

REFERENCES

1. Forbes "Roundup of cloud computing forecasts and market estimates, 2014", http://www.forbes.com/sites/louiscolumbus/2014/03/14/roundup-of-cloud-computing-forecasts-and-market-estimates-2014/ [Accessed March 2016].
2. IDC "IDC predicts the emergence of "the DX Economy" in a critical period of widespread digital transformation and massive scale up of 3rd platform technologies in every industry", FRAMINGHAM, Mass., November 4, 2015, https://www.idc.com/getdoc.jsp?containerId=prUS40552015 [Accessed March 2016].
3. IHS "Cloud-related spending by businesses to triple from 2011 to 2017", El Segundo, Calif. February 14 2014, http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017 [Accessed March 2016].
4. Dykstra J. Seizing electronic evidence from cloud computing environments. In *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, Ruan K (ed). Hershey: IGI Global, 2013; 156–185.
5. McAfee, Center for strategic and international studies, economic impact of cybercrime II, "net losses: estimating the global cost of cybercrime", June 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [Accessed July 2016]
6. Cloud Security Alliance, Skyhigh. The cloud balancing act for IT: between promise and peril CSA. January 13, 2016, http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP%20CSA%20Survey%20Cloud%20Balancing%20Act%200116.pdf.
7. Mell P, Grance T. The NIST definition of cloud computing, NIST special publication. Gaithersburg. 2011.
8. The Associated Chambers of Commerce & Industry of India, ASSOCHAM-Mahindra SSG, "Cyber crimes in India is likely to cross 300,000 by 2015: study", January 4, 2015, http://www.assocham.org/newsdetail.php?id=4821. [Accessed July 2016]
9. N. C. C. F. S. W. Group. NIST cloud computing forensic science challenges. Draft NISTIR 8006, 2014.
10. McKemmish R. What is forensic computing? Australian Institute of Criminology. Canberra. 1999; 118.
11. G. Palmer. A road map for digital forensic research—report from the first Digital Forensics Research Workshop (DFRWS), In: The First Digital Forensic Research Workshop. Utica, New York, 2001; 1–48.
12. National Institute of Justice (U.S.) & Technical Working Group on Crime Scene Investigation. Electronic crime scene investigation: a guide for first responders. Washington. 2001.
13. Reith M, Carr C, Gunsch C. An examination of digital forensic models. *International Journal of Digital Evidence* 2002; **1**(3):1–12.
14. Carrier B, Spafford EH. Getting physical with the digital investigation process. *International Journal of Digital Evidence* 2003; **2**(2):1–20.
15. Baryamureeba V, Tushabe F. The enhanced digital investigation process model. In the Proceedings of the Fourth Digital Forensic Research Workshop. 2004.
16. Ciardhuáin SÓ. An extended model of cybercrime investigations. *International Journal of Digital Evidence* 2004; **3**(1):1–22.
17. Selamat SR, Yusof R, Sahib S. Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security* 2008; **8**(10):163–169.
18. Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation: The International Journal of Digital Forensics & Incident Response* 2005; **2**(2):147–167.
19. Kent K, Chevalier S, Grance T, Dang H. Guide to integrating forensic techniques into incident response. NIST Special Publication. 2006.
20. von Solms S, Louwrens C, Reekie C, Grobler T. A control framework for digital forensics. In *Advances in Digital Forensics II*, Vol. **222**, Olivier M, Shenoi S (eds). Springer: New York, 2006; 343–355.
21. Cohen FB. Fundamentals of digital forensic evidence. In *Handbook of Information and Communication Security*. Berlin Heidelberg: Springer, 2010; 789–808.

22. Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)* 2011; **5**(1):118–131.
23. Agarwal R, Kothari S. Review of digital forensic investigation frameworks. In *Information Science and Applications, Lecture Notes in Electrical Engineering*, Vol. **339**. Springer Berlin: Heidelberg, 2015; 561–71.
24. Valjarevic A, Venter HS. Harmonised digital forensic investigation process model. In *Information Security for South Africa (ISSA)*. IEEE: Johannesburg, Gauteng, 2012; 1–10.
25. Guo H, Jin B, Shang T. Forensic investigations in Cloud environments. In Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE Xi'an, Shaanxi: 2012; 248–251.
26. Chen G. Du Y, Qin P, Du J. Suggestions to digital forensics in cloud computing ERA. In *Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on*. IEEE, 2012; 540–544.
27. Martini B, Choo KKR. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation* 2012; **9**(2):71–80.
28. Adams R. The emergence of cloud storage and the need for a new digital forensic process model. In *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, Ruan K (ed). Hershey: IGI Global, 2013; 79–104.
29. Kohn MD, Eloff Mariki M, Eloff Jan HP. Integrated digital forensic process model. *Computers & Security* 2013; **38**:103–115.
30. Zawoad S, Hasan R, Skjellum A. OCF: an open cloud forensics model for reliable digital forensics. In 8th International Conference on Cloud Computing (CLOUD), IEEE, New York City, 2015; 437–444.
31. Pichan A, Lazarescu M, Soh ST. Cloud forensics: technical challenges, solutions and comparative analysis. *Digital Investigation* 2015; **13**:38–57.
32. Zawoad S, Dutta AK, Hasan R. SecLaaS: secure logging-as-a-service for cloud forensics. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, 2013; 219–230.
33. Damshenas M, Dehghantanha A, Mahmoud R, Shamsuddin bin S. Forensics investigation challenges in cloud computing environments. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012\ International Conference on. IEEE, **2012**; 190–194.
34. Marty R. Cloud application logging for forensics. In Proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011; 178–184.
35. Poisel R, Tjoa S. Discussion on the challenges and opportunities of cloud forensics. In *Multidisciplinary Research and Practice for Information Systems*, Quirchmayer G, Basl J, You I, Xu L, Weippl E (eds). Berlin Heidelberg: Springer, 2012; 593–608.
36. Birk D, Wegener C. Technical issues of forensic investigations in cloud computing environments. In Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on. IEEE, 2011; 1–10.
37. Zawoad S, Hasan R. Cloud forensics: a meta-study of challenges, approaches, and open problems. arXiv preprint arXiv:1302.6312, 2013.
38. Grispos G, Storer T, Glisson WB. Calm before the storm: the challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics (IJDCF)*, IGI Global: Hershey 2012; **4**(2):28–48.
39. Zimmerman S, Glavach D. Cyber forensics in the cloud. *IA Newsletter* 2011; **14**(1):4–7.
40. Chen L, Xu L, Yuan X, Shashidhar N. Digital forensics in social networks and the cloud: process, approaches, methods, tools, and challenges. In Computing, Networking and Communications (ICNC), International Conference on. IEEE, 2015; 1132–1136.
41. Mishra AK, Matta P, Pilli ES, Joshi RC. Cloud forensics: state-of-the-art and research challenges. In Cloud and Services Computing (ISCOS), 2012 International Symposium on. IEEE, 2012; 164–170.
42. Aydin M, Jacob J. A comparison of major issues for the development of forensics in cloud computing. In Information Science and Technology (ICIST), 2013 8th International Conference for. IEEE, 2013; 77–82.
43. Orton I, Alva A, Endicott-Popovsky B. Legal process and requirements for cloud forensic investigations. In *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, Ruan K (ed). Hershey: IGI Global, 2013; 186–229.
44. Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics: an overview. In *Advances in Digital Forensics VII, 7th IFIP WG 11.9 International Conference on Digital Forensics*, Vol. **361**, Peterson G, Shenoi S (eds). Springer: Berlin Heidelberg, 2011; 35–46.
45. Baset SA. Cloud SLAs: present and future. *ACM SIGOPS Operating Systems Review*. ACM 2012; **46**(2):57–66.
46. Farina J, Scanlon M, Le-Khac NA, Kechadi M. Overview of the forensic investigation of cloud services. In Availability, Reliability and Security (ARES), 2015 10th International Conference on. IEEE, 2015; 556–565.

47. Almulla S, Iraqi Y, Jones A. Cloud forensics: a research perspective. In Innovations in Information Technology (IIT), 2013 9th International Conference on. IEEE, 2013; 66–71.
48. Sibiya G, Venter HS, Fogwill T. Digital forensic framework for a cloud environment. In Proceedings of IST-Africa 2012 Conference. IIMC: Tanzania, 2012.
49. Harichandran VS, Breitinger F, Baggili I, Marrington A. A cyber forensics needs analysis survey: revisiting the domain's needs a decade later. *Computers & Security* 2016; **57**:1–13.
50. Thorpe S, Grandison T, Campbell A, Williams J, Burrell K, Ray I. Towards a forensic-based service oriented architecture framework for auditing of cloud logs. In Services (SERVICES), 2013 IEEE Ninth World Congress on. IEEE, 2013; 75–83.
51. Quick D, Choo KKR. Impacts of increasing volume of digital forensic data: a survey and future research challenges. *Digital Investigation* 2014; **11**(4): 273–294.
52. Sang T. A log-based approach to make digital forensics easier on cloud computing. In *Proceedings of the Intelligent System Design and Engineering Applications* (*ISDEA*), *2013 3rd International Conference on*. IEEE, 2013; 91–94.
53. Trenwith PM, Venter HS. Digital forensic readiness in the cloud. In Information Security for South Africa. IEEE, 2013; 1–5.
54. Kao DY. Cybercrime investigation countermeasure using created-accessed-modified model in cloud computing environments. *The Journal of Supercomputing* 2015:1–20.
55. Patel P, Ranabahu AH, Sheth AP. Service level agreement in cloud computing. In Cloud Computing Workshop at OOPSLA09. Orlando, Florida, 2009.
56. Zargari S, Benford D. Cloud forensics: concepts, issues, and challenges. In Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on. IEEE, **2012**; 236–243.
57. Reilly D, Wren C, Berry T. Cloud computing: pros and cons for computer forensic investigations. *International Journal Multimedia and Image Processing (IJMIP)* 2011; **1**(1):26–34.
58. Busalim AH, Hussin ARC, Ibrahim A. Service level agreement framework for e-commerce cloud end-user perspective. In Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on. IEEE, 2013; 576–581.
59. Serrano D, Bouchenak S, Kouki Y, *et al.* Towards QoS-oriented SLA guarantees for online cloud services. In Cluster, Cloud and Grid Computing (CCGrid), 2013 \13th IEEE/ACM International Symposium on. IEEE, 2013; 50–57.
60. Dykstra J, Sherman AT. Design and implementation of FROST: digital forensic tools for the OpenStack cloud computing platform. The *Proceedings of the 13th Annual DFRWS Conference*, *Digital Investigation.* Elsevier, 2013; 10 Supplement: S87–S95
61. Patrascu A, Patriciu VV. Logging framework for cloud computing forensic environments. In Communications (COMM), 2014 10th International Conference on. IEEE, **2014**; 1–4.
62. Dykstra J, Sherman AT. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. The *Proceedings of the 12th Annual DFRWS Conference*. *Digital Investigation*. Elsevier, 2012; 9 Supplement: S90–S98.
63. Zafarullah Z, Anwar F, Anwar Z. Digital forensics for eucalyptus. In Frontiers of Information Technology (FIT). IEEE, 2011; 110–116.
64. Haeberlen A. A case for the accountable cloud. *ACM SIGOPS Operating Systems Review*. ACM 2010; **44**(2):52–57.
65. Ko RKL, Jagadpramana P, Mowbray M, *et al.* TrustCloud: a framework for accountability and trust in cloud computing. In Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011; 584–588.
66. Nurmi D, Wolski R, Grzegorczyk C, *et al.* The eucalyptus open-source cloud-computing system. In Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on. IEEE, 2009; 124–131.
67. Keller A, Ludwig H. The WSLA framework: specifying and monitoring service level agreements for web services. *Journal of Network and Systems Management*, Plenum Press 2003; **11**(1):57–81.
68. Bouchenak S, Chockler G, Chockler H, Gheorghe G, Santos N, Shraer A. Verifying cloud services: present and future. *ACM SIGOPS Operating Systems Review*. ACM 2013; **47**(2):6–19.
69. Biggs S, Vidalis S. Cloud computing: the impact on digital forensic investigations. In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. IEEE, 2009; 1–6.
70. Hegarty R, Merabti M, Shi Q, Askwith B. Forensic analysis of distributed data in a service oriented computing platform. In Proceedings of the Convergence of Telecommunications, Networking & Broadcasting, PG Net, 10th Annual Postgraduate Symposium on Liverpool. 2009.
71. Shi Y, Zhang K, Li Q. A new data integrity verification mechanism for SaaS, In: FL Wang, Z Gong, X Luo, J Lei (eds). *Web Information Systems and Mining. WISM 2010 International Conference*. Springer: Berlin Heidelberg, 2010; 236–243.

72. Yan C. Cybercrime forensic system in cloud computing. In Image Analysis and Signal Processing (IASP), 2011 International Conference on. IEEE, 2011; 612–615.
73. Juels A, Kaliski Jr BS. PORs: proofs of retrievability for large files. In Proceedings of the Computer and communications security, 14th ACM conference on. ACM: Alexandria, VA, USA, 2007; 584-597.
74. Santos N, Gummadi KP, Rodrigues R. Towards trusted cloud computing, in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing (HotCloud'09). 2009.
75. Zhou L, Varadharajan V, Hitchens M. Achieving secure role-based access control on encrypted data in cloud storage. *Information Forensics and Security IEEE Transactions on IEEE* 2013; **8**(12):1947–1960.
76. Nancy Ambritta P, Railkar PN, Mahalle PN. Proposed identity and access management in future internet (IAMFI): a behavioral modeling approach. *Journal of ICT Standardization*. River Publishers, 2014; **2**(1):1–36.
77. Yang K, Jia X, Ren K, Zhang B, Xie R. Effective data access control for multiauthority cloud storage systems. *Information Forensics and Security, IEEE Transactions on IEEE* 2013; **8**(11):1790–1801.
78. Li J, Chen X, Huang Q, Wong DS. Digital provenance: enabling secure data forensics in cloud computing. *Future Generation Computer Systems* 2014; **37**:259–266.
79. Wan Z, Liu JE, Deng RH. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *Information Forensics and Security, IEEE Transactions on IEEE* 2012; **7**(2):743–754.
80. Mills D, Martin J, Burbank J, Kasch W. Network time protocol version 4: Protocol and algorithms specification. IETF RFC5905. 2010.
81. Wolthusen SD. Overcast: forensic discovery in cloud environments. In IT Security Incident Management and IT Forensics, IMF'09, Fifth International Conference on. IEEE, 2009; 3–9.