Designing

Cloud Forensic-Enabled System

PhD Thesis

submitted in fulfilment of the requirements for the degree of

Doctor of Cultural Technology and Communication

by

Stavros Simou

To the Faculty of Social Sciences,
Department of Cultural Technology and Communication
University of the Aegean, Mytilene

June 2017

Supervisor : Prof. C. Kalloniatis

Department : Cultural Technology and Communication

Declaration of Authorship

I hereby declare that this thesis titled, “Cloud Forensics” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.
- It is my own account of my research written independently and it has not previously been submitted for a degree at any tertiary education institution.

Mytilene, 16 June 2017

Stavros Simou

Acknowledgements

Completing a doctoral thesis is demanding, toilsome, and a life-changing experience that only with the support of several people could navigation of this experience had led me to its fulfillment.

Therefore, I would like to thank the members of the committee who participated in the assessment of my research, and for their helpful comments: Prof. Gritzalis Stefanos, Prof. Kavakli Evangelia, Prof. Lambrinoudakis Costas, Prof. Katos Vasilios, Prof. Kokolakis Spyros, and Prof. Tsohou Aggeliki. An additional thank to the Dean Prof. Stefanos Gritzalis for his constant support and for believing in me.

Thanks to my IT department and my colleagues who shared with me their expertise and provided me with feedback about the functionality and operation of the systems. Many thanks to my friend and "my brother", Apostolos Spanos, for his psychological support, even though he was thousand kilometers away from me. You are a human inspiration.

Thanks to all the people, especially to Angeliki Kitsiou, who helped me with their advice and their support and made this dream to come true.

Finally, and most importantly, I feel the need to cordially and sincerely thank two special people without their help I would not had been able to complete my dissertation.

First, my supervisor Prof. Christos Kalloniatis; An example for others. It is hard to find a person with his consistency and persistence (insistence). I could not forget our conversations on where we were heading when everything around me was a blur, and the hours he spent giving me valuable feedback. I appreciate all his effort and patience with my "PhD amnesia" and the support in different academic areas like researching, writing, publishing and reviewing. But most of all I feel grateful that I was the first PhD student of the greatest supervisor.

Second, my beloved wife for all her love and encouragement. She has been by my side throughout this dissertation lifting my spirits up whenever I needed it. I could never, never had managed to complete this huge work literally and metaphorically without her support and assistance. Whatever I say about her will be small. Thank you my "stardust".

Stavros Simou
University of the Aegean
June 2017

Abstract

In recent years, cloud computing has gained popularity and it is now used to support various areas of human life. Cloud computing technology and services, despite the advantages they bring to the market, have created number of issues regarding the security and trust of the individuals using them. Incidents occurring in cloud computing environments are hard to be solved since digital forensic methods used to conduct digital investigations are not suitable for cloud computing investigations. This is due to the fact that they do not consider the specific characteristics of the Cloud. 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.

Cloud forensics introduces processes for resolving incidents occurring in cloud computing environments. However, designing cloud services capable to assist a cloud investigation process when an incident occurs is of vital importance and recent research efforts concentrate on these directions. In addition, digital forensics methods cannot support a cloud investigation since cloud environments introduce many differences compared to traditional IT environments. Although cloud forensics assists in the direction of investigating and solving cloud-based cyber-crimes, in many cases the design and implementation of cloud services falls back. Software engineers should focus their attention on the design and implementation of cloud services that can be investigated in a sound forensic manner.

This thesis makes an original contribution to knowledge in the field of cloud forensics by implementing a framework that assists software engineers to design cloud forensic-enabled services. In order to do so, a thorough literature review has been conducted focusing 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 environments. Furthermore, the detailed comparison reveals similarities and drawbacks of the existing methodologies providing some novel future research directions. This thesis moves current research one step further by identifying the major concepts, actors and their relationships that participating in a cloud forensic investigation through the introduction of a meta-model.

The framework, which is implemented in order to support the elicitation of forensic requirements and software engineers consists of an identified number of a set of cloud forensic constraints, a modelling language expressed through a conceptual meta-model and a process based on the concepts identified and presented in the meta-model. The meta-model presented in this thesis not only includes the concepts that make a system forensic-enabled but also the concepts for cloud forensic investigation, raising the importance of the relation between a forensic-enabled system and an investigation process and how the latter is assisted when an incident occurs. In this way an integrated

meta-model is produced to assist designers in a way that, they will be able to design forensic-enabled cloud services. The applicability of the framework is demonstrated through a case study. The main advantage of the proposed model is the correlation of cloud services' characteristics with the cloud investigation while providing software engineers the ability to design and implement cloud forensic-enabled services via the use of process patterns.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction to the Research

1.1. Introduction

Information Technology (IT) has changed the way people think and operate in every aspect of their lives. People heavily depend on the computers, and the use of IT is transforming every day. In recent years, the traditional computer technology has moved into a different, more demanding and promising era dictated by Internet advances. Stand-alone desktops and hard drives have been replaced by mobile phones, tablets and web-browsers. The growing demand of computing power and resources, lead the traditional forms of services to mutate very rapidly. During this period, users have been experiencing a huge offer of applications and services on cloud computing, which is definitely one of the most important services provided in this era.

Cloud computing has dominated our world giving a different perspective and new horizons expanded to companies and organizations due to the numerous advantages they offer, especially flexibility and elasticity to customers through the existence of pay-as-you-use services. Every day, many organizations and companies are migrating their services over the cloud and a great number of companies are considering adopting this technology. However, many drawbacks do exist that make cloud environments vulnerable to various threats depending on the service model used (Kalloniatis et al., 2013, Kalloniatis et al., 2014, Manousakis et al., 2013). 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*" (Dykstra, 2013):19. According to a report sponsored by McAfee, global cyber activity (including crime on cloud) is costing up to $500 billion each year, which is almost as much as the estimated cost of drug trafficking(McAfee, 2014).

Taking into consideration the previous report we could easily come to the 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. 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 raised a new area in the field that is called cloud forensics.

The ability of cloud forensic investigators to carry out an investigation depends completely on the tools and methods used, to acquire the appropriate digital evidence from a device. The current digital forensic methods, tools and frameworks used to conduct a digital investigation cannot meet the requirements and the standards for the new technology on cloud environment (Adams, 2013, Almulla et al., 2014, Kohn et al., 2013, Martini and Choo, 2012, Pichan et al., 2015, Ruan et al., 2011b, Zawoad and Hasan, 2013, Grispos et al., 2012). This happens due to the fact that computer technology is continuously changing and the forensic technology is unable to follow that pace.

Security among others (lack of resources/expertise, compliance, etc.) is one of the most important issues in cloud, according to a survey by RightScale (RightScale, 2016). This creates the need for information system engineers to design forensic-enabled services in order to resolve cloud incidents (cyber-attacks) as fast and efficient as possible raising in parallel the trustworthiness of the services provided. Conducting an effective cloud forensic investigation requires, from an information systems development point of view, the support of the designers in identifying requirements that will assist developers to build a forensic-enabled information system; this is an information system that its architecture supports forensic investigation. The concept of designing a cloud forensic-enabled service is to provide investigators with all the necessary capabilities to solve an incident in a forensically sound manner. In order to do so, designers need to explore those forensic requirements and processes that will identify a cloud service or a system as forensic-enabled.

The literature lacks work to support software engineers in identifying forensic-related requirements for information systems. To address the aforementioned gap this dissertation is concentrating on the requirements engineering framework in order to support the elicitation of forensic requirements. Before implementing the framework a thorough literature analysis has been conducted to identify and critically review the methodologies introduced for digital and cloud forensics investigation as well as the challenges and the solutions presented on the respective field. The necessity of this review is for understanding the investigators' demands during a forensic process and the present efforts already conducted in the cloud in order to implement a cloud forensic-enabled service. The framework consists of a set of cloud forensic constraints, a modelling language expressed through a conceptual meta-model, and a process based on the concepts. The applicability of the framework is tested on a real case study.

1.2. Problem statement

The number of cloud services used by an average organization is increased over the last years rapidly. Cloud providers mainly and software engineers specifically are responsible for the implementation of those services. One of the most important challenges for software engineers is the design and implementation of trustworthy cloud services. Information system designers face an important issue, the design of cloud

forensic-enabled systems/services that could assist investigators solving cloud-based cyber-crimes. Although cloud forensics assists on this direction, limited evidence of cloud-based forensic approaches exist. These approaches do not support information systems developers as they focus on the investigation only and they also do not support modelling potential cases of forensics investigations.

1.3. Motivation for the research

The distributed and virtualized cloud environment attracts an increasing number of users who consider this environment as a field of malicious acting. To protect consumers from being deceived cloud forensics should be applied during a digital investigation in order to identify and acquire the evidence that would be admissible in court. Digital evidence should be maintained and preserved in a forensically sound manner so as no one can potentially question the specific evidence. Although a lot of research has been produced on cloud forensics, a systematic review on the challenges, solutions and methodologies of cloud forensics does not exist. On the other hand, as far as cloud services are concerned they have not been given the proper attention even though they are the most important aspect in the field, since cloud computing is based on the services offered. Software designers and engineers, in many cases do not design and implement the cloud services to be cloud forensic-enabled. This is a major issue in cloud forensic investigation since the investigation cannot be conducted in a forensically sound manner.

1.4. Contribution of the study

This dissertation contributes to the human knowledge by setting the forensic requirements for a cloud service and new guidelines about the way cloud forensics should be conducted. Specifically this research makes the following contributions:

- It brings forward all the work that has been presented until now in cloud forensics in relation to methods, challenges and solutions. Specifically, it critically reviews all the frameworks and methodologies dealing with digital and cloud forensics along with an extended discussion regarding their functionality, drawbacks, and complexity parameters. It also presents all cloud-based challenges, according to the respective literature, and categorizes them for assisting researchers to reason about the necessity of cloud-forensics in specific areas. Finally, existing solutions regarding the aforementioned challenges are also presented so as to identify the respective efforts presented for realizing identified challenges.
- It is the first attempt in the literature to provide a language to support modelling of forensic investigation potential case studies.

- It is the first attempt in the literature to define a model-based process for supporting a forensic investigation of an information system.
- It identifies cloud forensic investigation concepts and uniquely aligns forensics with requirements engineering concepts.
- It identifies and proposes a set of forensic constraints introduced and expressed in a form of activity diagrams that should be considered when designing cloud forensic-enabled services.
- It proposes a novel conceptual meta-model that embodies all the necessary concepts required to design a forensic-enabled cloud service, which at the same time contributes to respective investigation procedures.
- It presents a process that engineers may follow for designing cloud service in forensic-enabled manner.

Publications	
1	Simou S, Kalloniatis C, Kavakli E, Grtzalis S.: Cloud Forensics: Identifying the Major Issues and Challenges. In: M. Jarke, J. Mylopoulos, C. Quix, C. Rolland, Y. Manolopoulos, H. Mouratidis, J. Horkoff (Eds), Advanced Information Systems Engineering, CAiSE 2014 26th International Conference, Lecture Notes in Computer Science 8484, Springer International Publishing, Thessaloniki, Greece, 2014. p. 271-284.
2	Simou S, Kalloniatis C, Kavakli E, Grtzalis S, Cloud Forensics Solutions: A Review. In: L. Iliadis, M. Papazoglou, and K. Pohl (Eds.), Advanced Information Systems Engineering Workshops, CAiSE 2014 International Workshops, Lecture Notes in Business Information Processing 178, Springer International Publishing, Thessaloniki, Greece, 2014. p. 299-309.
3	Simou S, Kalloniatis C, Mouratidis H, Grtzalis S.: Towards the Development of a Cloud Forensics Methodology: A Conceptual Model. In: A. Persson, J. Stirna (Eds), Advanced Information Systems Engineering Workshops, CAiSE 2015 International Workshops, Lecture Notes in Business Information Processing 215, Springer International Publishing, Stockholm, Sweden, 2015. p. 470-481.
4	Simou S, Kalloniatis C, Mouratidis H, Grtzalis S.: A Meta-model for Assisting a Cloud Forensics Process. In: C. Lambrinoudakis, A. Gabillon (Eds), Risks and Security of Internet and Systems. CRiSIS 2015 10th International Conference, Lecture Notes in Computer Science 9572, Springer International Publishing, Mytilene, Greece, 2015. p. 177-187.
5	Simou S, Kalloniatis C, Mouratidis H, Grtzalis S.: Towards a Model-Based Framework for Forensic-Enabled Cloud Information Systems. In: S. Katsikas, C. Lambrinoudakis, S. Furnell (Eds), Trust, Privacy and Security in Digital Business. TrustBus 2016, 13th International Conference, Lecture Notes in Computer Science 9830, Springer International Publishing, Porto, Portugal, 2016. p. 35-47.
6	Simou S, Kalloniatis C, Mouratidis H, Grtzalis S.: A survey on cloud forensics challenges and solutions. Security and Communication Networks. 2016. 9, (18), p. 6285-6314.

7	Simou S, Kalloniatis C, Grtzalis S.: Modelling Cloud Forensic-Enabled Services. In: S. Fischer-Huebner, C. Lambrinoudakis, J. Lopez (Eds), Trust, Privacy and Security in Digital Business. TrustBus 2017, 14th International Conference, Springer International Publishing, Lyon, France, 2017.

1.5. Dissertation outline

Chapter 1 (Introduction to the research) provides a brief summary of the cloud computing environment and highlights the necessity of cloud forensics in a cloud investigation. It also refers to the role of software engineers in designing cloud forensic-enabled systems. It states the problem that needs to be addressed with the motivation for this research and finally the contribution of this thesis.

Chapter 2 (Technical background) provides a technical background on the field of cloud computing. It explains the structure of cloud computing and describes the participation of digital evidence in an on-going investigation. It presents the notions of digital and cloud forensics and the differences between them.

Chapter 3 (Cloud & Digital forensic methodologies) presents a detailed review about the existing digital and cloud forensic methodologies, frameworks and models. A comparison framework is introduced based on a comparison of the presented methodologies and a running example is demonstrated to verify the applicability of the framework.

Chapter 4 (Cloud forensic challenges & solutions) presents the cloud forensic challenges identified from the review conducted in the respective field and introduces a categorization of the challenges based on the cloud forensics process stages of the comparison framework. It also presents the different solutions found in the literature concerning the respective challenges.

Chapter 5 (Cloud forensics investigation meta-model) identifies the major concepts and their relationships that participate in a cloud forensics process through the introduction of a common modeling language presented in terms of a meta-model, which includes all the identified concepts. It introduces a generic process for cloud forensic investigation and concludes with a running example for verifying the applicability of the meta-model.

Chapter 6 (Cloud forensic-enabled framework) presents a framework that assists both designers and investigators with cloud-based cyber-crimes. The framework supports cloud services by implementing a number of steps to make the services cloud forensic-enabled. It consists of a set of cloud forensic constraints, a modelling language expressed through a conceptual meta-model and a process based on the concepts identified and presented in the meta-model.

Chapter 7 (Framework applicability) applies the proposed framework on a real case study, regarding the transformation of cloud services of the University of the Aegean (UoA) in order to make these services cloud forensic-enabled.

Chapter 8 (Conclusion) concludes the dissertation by outlining the key-points of this research and discussing the limitations and future research opportunities.

Chapter 2

Technical Background

2.1. Introduction

This chapter presents the technical details on the field of cloud computing, digital evidence, digital and cloud forensics. It provides the necessary background to understand the nature of cloud computing and the potential evidence stored as information. On the other hand, it explains the terms of digital and cloud forensics and it clarifies their differences and the role they play when chasing evidence in a cyber-crime investigation.

2.2. Cloud computing

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 one of the most important topics in the field of Information Technology in recent years and its popularity is rising very fast. According to Forbes contributor Louis Columbus, two key points from two different studies were 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*" (Columbus, 2014) and "*Worldwide spending on public cloud services will grow at a 19.4% compound annual growth rate (CAGR) from nearly $70B in 2015 to more than $141B in 2019*" (Columbus, 2016). International Data Corporation (IDC) predicts that "*by 2020, organizations' spending on cloud services, the hardware and software to support cloud services, and services for implementing and managing cloud services will exceed $500 billion - over three times what it is today*" (Mahowald et al., 2015):7.

Cloud computing is not owned by companies and the respective Information Technology (IT) systems are not usually managed by them. Instead, Cloud Service Providers 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. National Institute of Standards and Technology (NIST) defines cloud computing as "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*" (Mell and Grance, 2011):6.

The five essential characteristics of the model are on-demand self-service (enables users to provision of computing power, storage, and so on, whenever they want it automatically), broad network access (access resources from any device, such as PC, tablet, mobile phone), resource pooling (resources are pooled to serve multiple consumers), rapid elasticity (provision of scalable services, users can purchase additional computing power as they need) and measured service (services are controlled and monitored by cloud provider). The three service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and the four deployment models are public cloud, private cloud, community cloud, and hybrid cloud. NIST definition is illustrated in visual form in Figure 1.

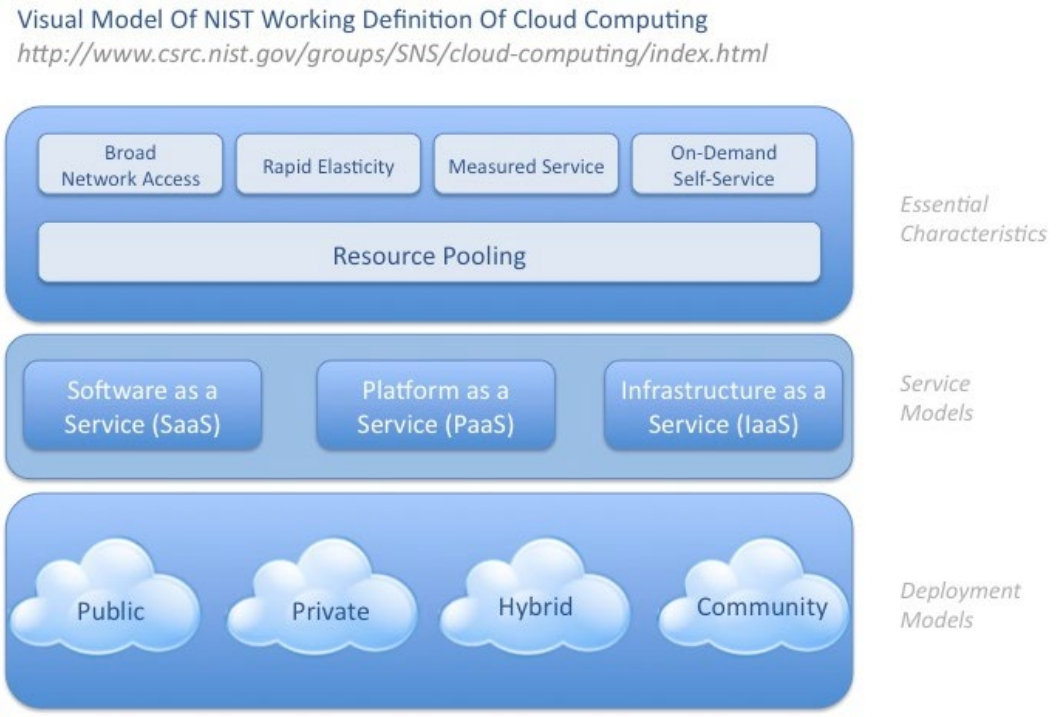


Figure 1 NIST Visual Model of Cloud Computing Definition

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 2 presents an overview of cloud computing with the service and deployment models, while Figure 3 shows a comparison between traditional Information Technology (IT) and cloud computing service models.

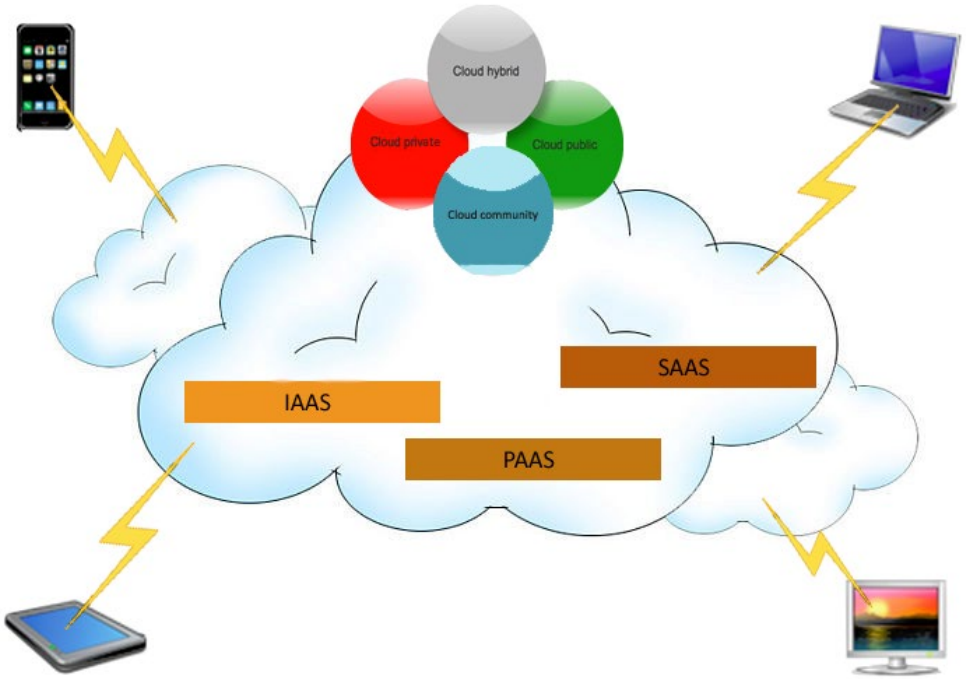
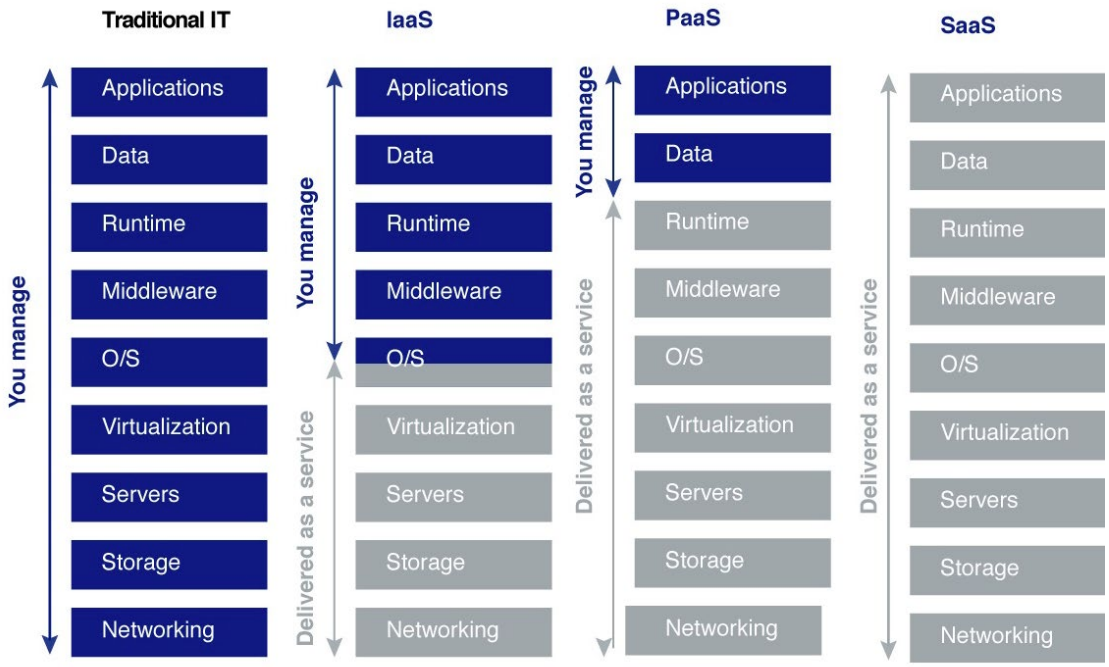


Figure 2 Cloud computing

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, etc.) 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. The cloud provider is also responsible for the maintenance and the updated patches of the installation. Users have very limited privileges. Cloud computing provides many advantages to companies and organizations in comparison to 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.



Source: Microsoft

Figure 3 Comparison between traditional IT and cloud computing

In computing the term *Virtualization* refers to the creation of multiple and separate instances running on a single computer (server) with the use of hypervisor (virtual machine monitor or host) (Goth, 2007). These instances are called Virtual Machines (VMs) and each one of them operates like a fully independent computer using its own hardware (processors, hard disks, memory) and operating system (Bem and Huebner, 2007). Virtualization is being widely used within the cloud computing, once cloud is based on it and, also, on distribution (Lombardi and Di Pietro, 2011, Younge et al., 2011). Cloud computing uses virtualization for load balancing and on the other hand, for increasing its security by providing monitoring (Christodorescu et al., 2009, Lombardi and Di Pietro, 2011).

2.3. Digital evidence

"*Evidence forms the very foundation of any legal system, without which law would be subject to the whims of those with power*" (Speedy-Publishing, 2015). Digital evidence in cloud computing is the information (data) stored on any digital device in the distributed data centers round the world that can be used to prosecute a malicious actor. Investigators are responsible to gather concrete and admissible evidence in the court of law in order to guarantee a verdict in their favor. In cases where evidence could not be identified as relevant evidence (never being collected or processed at all) in a specific timely duration, they might not exist in digital form (erased, deleted, reboot machine, etc.) by the time it will be discovered to have relevance (Cohen, 2010).

The legal system concerning digital evidence is still undeveloped causing some issues in the admissibility process especially for evidence acquired from the cloud (Orton et al., 2013, Dykstra and Sherman, 2011). In the court case of Lorraine v. Markel American Insurance Co. (2007), Judge Grimm provided key guidance to determine whether electronically stored information is admissible as evidence and he recognized that five evidentiary principles must be addressed. These are: relevance, authenticity, hearsay, original or duplicate documentation and probative value against unfair prejudice (Frieden and Murray, 2011). Today, with the technology in motion (cloud data, social media content, internet of things, blogs, etc.) the legal system seems that is not able to follow as quickly. Even though the Cybercrime Convention Committee established the Cloud Evidence Group at its 12th plenary, there are still many gaps that need to be filled in. As the Committee quoted "*This decision was motivated by the recognition that in the light of the proliferation of cybercrime and other offences involving electronic evidence, and in the context of technological change and uncertainty regarding jurisdiction, additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations*" (Cloud_Evidence_Group, 2016):4.

Data stored in cloud should be treated as potential evidence. To identify the evidence in cloud environment is a hard task due to the limitation of seizing (physically) the computer device containing the data and the inability of knowing the exact location of the data. Another issue of acquiring evidence from cloud environment is the continuity of service for the rest of the consumers they share the same service (Taylor et al., 2010). In simple terms, a cloud service or a system cannot stop operating due to the fact that other consumers use it and there will be a huge impact with "*devastating consequences for the clients' business continuity*" (Spyridopoulos and Katos, 2013) and their work. An important factor is that digital evidence should maintain their integrity and chain of custody at all times. In particular, investigators should protect evidence during the acquisition, storage, transportation, examination and analysis from any alterations. A detailed documentation about the handling and use of digital evidence should be kept during the investigative process with all the people who involved in and the actions have been taken (Prayudi and Sn, 2015).

In the United Kingdom, Association of Chief Police Officers (ACPO) issued guidelines (Williams, 2011) for the Law Enforcement Agents (LEA) concerning the authentication and integrity of evidence. The guidelines of digital evidence consist of four principles:

> *"Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.*
>
> *Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*

Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to." (Williams, 2011):6

Based on these principles, LEAs should investigate a crime scene and seek for digital evidence. Even though there is a guidance to follow the principle, in some cases, "*the application of the principles does not preclude a proportionate approach to the examination of digital evidence*" (Williams, 2011):7. The technological evolution and the increase of digital devices means that digital evidence can be found almost in any crime scene. Digital evidence can be found at any digital device includes, but is not limited to:

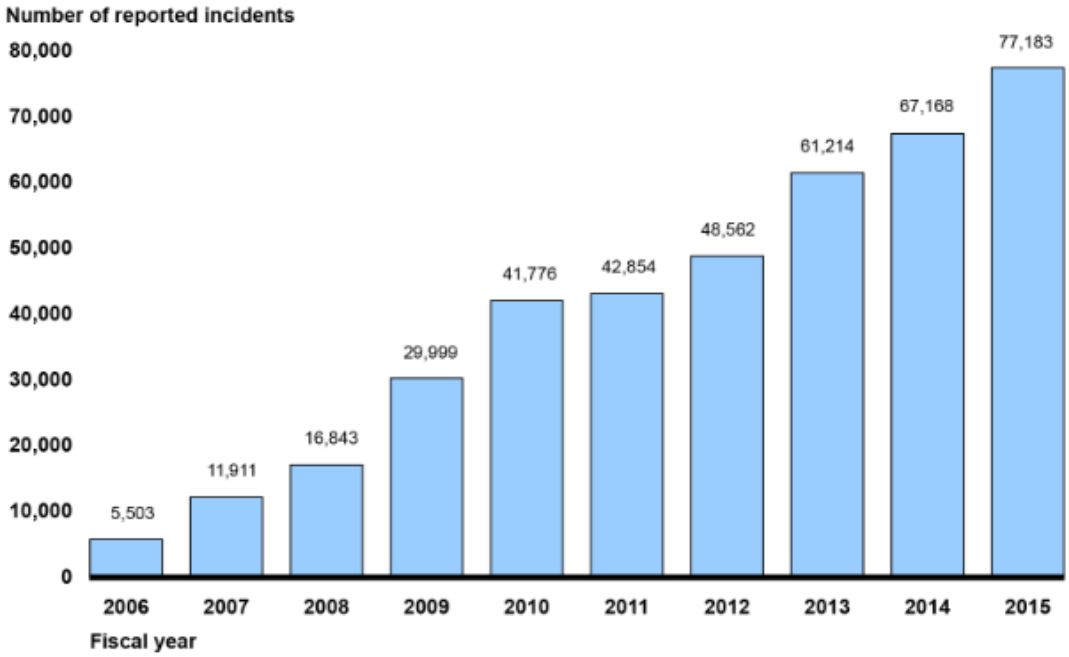
Remote computers, hard discs, USB drives, memory cards, CD/DVD, files and folders, deleted files, times and dates associated with modifications, computer names and IP addresses, usernames and passwords, web server logs, windows event logs, application logs, registry entries and running processes, temporary files and recent documents, network shortcuts and mapped drives, browser history, temporary internet files and cache memory, emails, notes and address books. Assets related to cellular phones could be SIM cards, call logs, contacts, SMS and MMS, calendar, GPS locations and routes.

2.4. Digital & Cloud forensics

Over the past years, the technology of cloud computing has dominated the field of Information Technology (IT) by providing cloud services to consumers. By the end of 2016, an average organization uses 1,427 cloud services, an increase of 23.7% over the same period of the previous year (Skyhigh, 2016). However, cloud computing technology is one more field for criminal exploitation (Martini and Choo, 2014). Perpetrators use cloud computing to gain access to information by exploiting vulnerabilities or they use cloud resources to distribute illegal context. In either case, they are trying to hide their real identity and keep their anonymity behind this "complex" environment.

In the digital world, where modern users live and interact on a daily basis, the number of incidents related to cyber-crime is a major issue among Cloud Service Providers (CSPs), consumers and Law Enforcement Agents (LEA) as it has been growing rapidly over the past few years. According to United States Government Accountability Office (GAO), the number of cyber incidents affecting federal agencies have increased about 1,300 percent the last 10 years (Wilshusen, 2016), as shown in Figure 4. This has an immediate impact to specialists 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 this kind of crimes. Juniper research predicted that the cost of data

breaches will increase to $2.1 trillion globally by 2019, almost four times increasing the estimated cost of breaches in 2015 (Juniper, 2015).



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Figure 4 Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015

The expansion of computer devices and Internet technology forced companies to develop forensic tools and techniques in order to find evidence hidden in the computer and network environments and to assist the investigation process aiming to acquire, preserve, and analyze evidence. The pursuit to identify and reveal evidence to crack-down cyber-crime has been done with the use of digital forensic technology. Digital forensics deals with the digital evidence found in the area where the crime is committed. 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. At the first Digital Forensic Research Workshop (DFRWS) in 2001, digital forensics has been defined as "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*" (Palmer, 2001):22. Since then, more definitions about digital forensics have been proposed but DFRWS definition is the most acceptable by the research community of digital and cloud forensics. Orton, takes a step forward and defines digital forensics as "*the study of evidence from attacks on computer systems in order to learn what has occurred, how to prevent it from recurring, and the extent of the damage*" (Orton et al., 2013):3.

The need to conduct a proper investigation forced researchers and investigators to develop a number of models and processes regarding digital forensics. NIST (Kent et al., 2006) introduced a widely accepted process model that consists of four phases: collection, examination, analysis and reporting. This process is illustrated in Figure 5. Basically, the four-phase process can be presented as follows: First, investigators search the devices and media where the crime has been committed. Next, data is extracted from the media and is transformed into a format that can be processed with the proper tools. Then, in the analysis phase, data is transformed into information and finally, information is transformed into evidence. A detailed discussion about the digital forensic process models and methodologies is presented in Chapter 3.

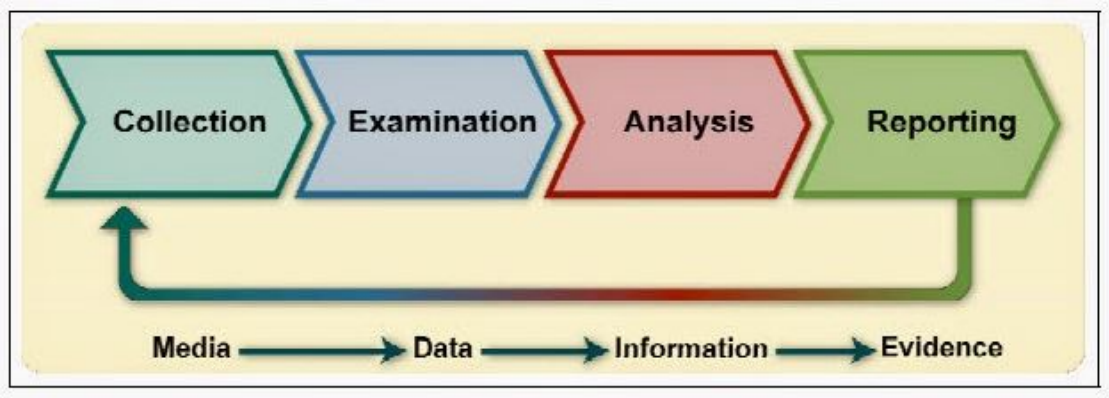


Figure 5 NIST Digital Forensic Process

A digital forensic investigation is performed in two different modes: live and dead or static (Grispos et al., 2011, Rafique and Khan, 2013, Rahman and Khan, 2015, Almulla et al., 2014). Static or dead mode is more traditional during which the devices and media are shut down and analyzed forensically. The devices are moved into a forensic lab where investigators examine them for evidentiary data. On the other hand, live forensics is performed while the device remains powered up (in running mode). This approach is more challenging from the static and includes data snapshots and non-interactive analysis (Rafique and Khan, 2013). Live forensics helps LEA to acquire data stored in persistent memory, that it could be lost when the device is shut down.

The most important element in the digital forensics is to maintain the integrity and the chain of custody of the digital evidence. In other words, the authenticity of the evidence should remain the same as it was first captured until the presentation (Prayudi and Sn, 2015). A break in the chain of custody (alteration to the evidence) simply means that the case is lost in a court of law. A digital forensic investigation should be conducted by a specialized team using different types of personnel such as Information Technology (IT) experts, legal advisors, and Law Enforcement Agents. The team responsible for the investigation should follow the digital forensic standards and procedures and its people should be trained to confront any issue that might arise.

With the evolution of cloud computing digital forensics could not follow the pace of cyber-crimes in cloud environments due to its dynamic nature (Alqahtany et al., 2016).

A new field has been introduced under the name of *cloud forensics*. 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. Ruan et al. (Ruan et al., 2011a) first introduced the multi-dimensional aspect of cloud forensic and presented three dimensions which include the technical, organizational and legal perspectives. The technical dimension concentrates on the procedures and tools that are used in the cloud forensic investigation such as data collection, live forensics, evidence segregation, virtualized environments and proactive measures. The organizational one concentrates on the entities involved in the cloud such as consumer, CSP and third parties and their dependencies. It includes the organizational policies and Service Level Agreements (SLAs). Finally, the legal dimension deals with different jurisdictions, multi-tenancy, regulations and SLAs signed between CSP and consumers.

Due to the absence of a universally accepted definition of cloud forensics Ruan et al. (Ruan et al., 2012):38 proposed a working definition stating that "*Cloud forensics is the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations*".

According to NIST (NIST, 2014):2, 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*".

Crime investigators in cloud environments have to deal with a number of different issues compared to network or computer investigation (digital forensics). The most important is that the evidence can reside everywhere in the world in a virtualization environment (Pătraşcu and Patriciu, 2013). In traditional digital forensics investigators seize the devices and media in order to examine potential evidence (Spyridopoulos and Katos, 2013). However, in cloud forensics with the heterogeneous environment and different jurisdictions to seize equipment containing data makes it impossible. There are also issues associated with legal matters, multi-tenancy, flexibility of deleting instances, data replication, location transparency and dependence on CSPs that are unique to cloud forensics and makes the investigation even more complex (Thethi and Keane, 2014, Orton et al., 2013, Ruan et al., 2011a, Freet et al., 2015).

Identification of evidence in cloud environments is a difficult process due to the different deployment and service models, and the limitation of seizing (physically) the computer device containing the evidence. Even if the investigators had access (physically) to a specific data center, there would have been the probability that the data were split to different data centers, geographically spread, or encrypted (Pătraşcu and

Patriciu, 2013). 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 preserve the non-compromised by third parties evidence, in order for it to be acceptable and presented in the court of law. Third parties are involved in the cloud forensic process due to their collaboration with CSPs. Even though the preservation of evidence can be done in a forensically sound manner there are issues with the provision of pure and original evidence to the court (Almulla et al., 2013, Orton et al., 2013).

In the following chapters a thorough and detailed expatiation of cloud forensics concerning models, challenges and solutions will be presented.

Chapter 3

Cloud & Digital Forensic Methodologies

3.1. Introduction

In this chapter, a detailed review is presented, based on the latest research efforts in cloud and digital forensics after a thorough analysis of the respective literature. The work covers the existing 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 cyber-crime can be resolved.

3.2. Current methodologies

Since 1999, various methods and frameworks have been introduced regarding the way of conducting proper digital forensic investigation including different stages and phases.

3.2.1. Forensic Computing Process

(McKemmish, 1999) 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.

3.2.2. Investigative Process for Digital Forensic Science

The First Digital Forensic Research Workshop (DFRWS) (Palmer, 2001) 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.

3.2.3. Forensic Process

The U.S. Department of Justice introduced in 2001 the Electronic Crime Scene Investigation: A Guide for First Responders (U.S. Department of Justice, 2001). 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.

3.2.4. Abstract Digital Forensic model

The Abstract Digital Forensic model (Reith et al., 2002) 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 to 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 authors themselves identified some disadvantages concerning their own work and (Adams, 2012) outlines three shortcomings in the model, namely:

a) There is a high-level approach to categories that it could be too general to be applied in practice.
b) The model has not been tested nor proven to be efficient and reliable for a digital/cloud forensic framework.
c) With the development of the model it becomes more cumbersome to use (Reith et al., 2002).

3.2.5. Integrated Digital Investigation Process

In 2003, the Integrated Digital Investigation Process (IDIP) (Carrier and Spafford, 2003) 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. (Agarwal and Kothari, 2015) highlighted the absence of the completion of the phases and whether the framework can satisfy an investigation once it cannot be validated. A 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 (Baryamureeba and Tushabe, 2004). There were some more issues with the specific model highlighted by (Shin, 2008) such as the absence of the investigation priority decision, the investigation method about the psychological profile and the classification of the digital crime. Researchers disagree with Shin's position and think that the extra stages add complexity to the forensic process (Adams, 2012).

3.2.6. Enhanced Digital Investigation Process Model

The Enhanced Digital Investigation Process model (Baryamureeba and Tushabe, 2004) 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. (Perumal, 2009) criticized the model stating that it mainly focuses on the digital evidence and it does not take under consideration issues such as chain of custody.

3.2.7. Extended Model of Cybercrime Investigations

The Extended Model of Cybercrime Investigations (EMCI) introduced by (Ciardhuáin, 2004), 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. A shortcoming of the EMCI model is exclusion of important steps such as the return or destruction of the evidence when the investigation closes (Montasari, 2016). According to (Selamat et al., 2008), this framework provides a basis for the development of techniques and tools to support the work of investigators, thus, it is probably considered as the most complete to that time (Montasari, 2016, Selamat et al., 2008).

3.2.8. Hierarchical Objectives Based Framework

The Hierarchical Objectives Based Framework (Beebe and Clark, 2005) 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 Digital Investigation Process (Carrier and Spafford, 2003) and it is also technology independent. A 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. Other weaknesses noted by (Adams, 2012) is the practicality of the model and it focuses towards incident response instead of being more generic. Also, "*the lower-level details are only restricted to an initial Sub-Phase structure for the Data Analysis Process*" (Montasari, 2016):4.

3.2.9. Forensic Process

In 2006, the Forensic Process (Kent et al., 2006) proposed by National Institute of Standards and Technology (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 is examined, extracted from media and transformed into a format that can be processed by forensic tools. Then data is transformed into information through analysis and, finally, the information is transformed into evidence during the reporting phase. Both (Adams, 2012) and (Montasari, 2016) highlighted that important phases related to authorization, planning, interpretation, reconstruction, presentation and closure are missing. They also focused on the absence of a clear structure and important activities that makes model's applicability and practicality to be questioned.

3.2.10. Control Framework for Digital Forensics

In 2006, Von Solms (von Solms et al., 2006) 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.

3.2.11. Digital Forensic Investigation Framework

The Digital Forensic Investigation Framework (DFIF) (Selamat et al., 2008) groups and merges the same activities or processes, which provide the same output into an appropriate phase. The proposed map simplifies the existing complex framework and it can be used as a general DFIF for investigating all incident cases without tampering the evidence and 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. The main problem of the model is the absence of details (Adams, 2012). A brief summary is given with no discussion and without explaining their findings. On the other hand, (Montasari, 2016) states that the applicability of the model to different areas of digital forensics is in question and important phases related to incident response are missing.

3.2.12. Digital Forensic Evidence Processes

In 2010, Digital Forensic Evidence Processes (Cohen, 2010) 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 done in a manner that meets the legal standards of the jurisdiction and the case.

3.2.13. Systematic Digital Forensic Investigation Model

The Systematic Digital Forensic Investigation Model (Agarwal et al., 2011) 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 eleven stages model. The stages are preparation, securing the scene, survey & recognition, documenting the scene, communication shielding, evidence collection, preservation, examination, analysis, presentation and, finally, result & review. Securing the scene stage deals with securing the crime scene from unauthorized access and keeping the evidence from being contaminated. Survey and recognition involves 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 (Agarwal and Kothari, 2015). It has not been applied to all situations such as heterogeneous environments and new technologies. Another shortcoming has to do with the model's consistency in terms of the criteria used for the classification of the model's phases (Adams, 2012). Also, important phases are missing from the model such as incident detection, response, reconstruction, closure, etc. (Montasari, 2016).

3.2.14. Harmonized Digital Forensic Investigation Process Model

The Harmonized Digital Forensic Investigation Process model (Valjarevic and Venter, 2012) 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: 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 time stamping 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.

3.2.15. Forensic Investigations Process

The Forensic Investigations Process (Guo et al., 2012) in cloud environments was based on the Forensic Process with the four stages. Due to the evolution of cloud computing the stages were changed to apply basic forensic principles and processes. The four distinct steps are: a) determine the purpose of the forensics requirement, b) identify the types of cloud services (SaaS, IaaS, PaaS), c) determine the type of background

technology used, and d) examine the various physical and logical locations, which are client side, server side and developer side. The model does not include any actions after the evidence collection.

3.2.16. Cloud Forensics Process

In 2012, Cloud Forensics Process (Chen et al., 2012) 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, collect potential evidence, etc. Again, in this case the model does not include any actions after the evidence collection.

3.2.17. Integrated Conceptual Digital Forensic Framework for Cloud Computing

The Integrated Conceptual Digital Forensic Framework for Cloud Computing (Martini and Choo, 2012) proposed in 2012, is based on (McKemmish, 1999) and (Kent et al., 2006). It emphasizes on the differences in the preservation of forensic data and the collection of cloud computing data for forensic purposes. It consists of four stages, identification and preservation, collection, examination and analysis, reporting and presentation. The iteration of the framework demonstrates one of the key differences in the identification and analysis of evidence sources (Agarwal and Kothari, 2015).

3.2.18. Cloud Forensics Maturity Model

The Cloud Forensic Maturity Model (CFMM) presented by (Ruan and Carthy, 2012b) in 2012, is a reference model for evaluating and improving cloud forensic maturity. The model is composed of a Cloud Forensic Investigative Architecture (CFIA) and a Cloud Forensic Capability Matrix (CFCM). The CFIA consists of four main sections: pre-investigative readiness, core-forensic process, supportive processes and investigative interfaces. The first section includes event management, identity management, encryption management, and interoperability. The four components are used to prepare the investigation. The core-forensic section includes components such as pro-active data collection, re-active data collection, hybrid acquisition, examination and analysis. The supportive process includes evidence management, case management, multiple jurisdiction and multi-tenancy. These components are running concurrently and they are used throughout the investigation. Finally, the investigative interfaces section concerns law enforcement agents and internal forensic team responsible for the cloud forensic investigation. The CFCM is a capability maturity model that consists of six maturity levels. The model is a step forward towards an acceptable solution for cloud forensic investigation.

3.2.19. Advanced Data Acquisition Model

In 2013, (Adams, 2013) introduced the Advanced Data Acquisition Model (ADAM) that can assist digital forensic practitioners when it comes to presenting evidence in court that originated in the cloud. The model comprises of 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. ADAM is a promising model taking into consideration lots of 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.

3.2.20. Integrated Digital Forensic Process Model

The Integrated Digital Forensic Process Model (IDFPM) (Kohn et al., 2013) 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 IDFPM. 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 (Agarwal and Kothari, 2015). The model "has high-order processes" (Montasari, 2016):6 and the level of details is not clear and cannot be applied to all digital forensic environments (Adams, 2012, Montasari, 2016).

3.2.21. Open Cloud Forensics

Finally, in 2015, Zawoad et al. (Zawoad et al., 2015) proposed a cloud forensic process called Open Cloud Forensics (OCF) 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.

Table 1 presents the aforementioned digital and cloud forensic methodologies, frameworks and models that reviewed in this section. The table captures the different number of stages each one of them consist of.

Table 1. Digital and cloud forensic methodologies

McKemmish	***DFRWS***	***D.O.J.***	***Reith et al.***	***Carrier et al.***	***Baryamureeba et al.***	***Ciardhuain***
Identification	Identification	Preparation	Identification	Readiness (includes): Operation and Infrastructure phases	Readiness (includes): Operation and Infrastructure phases	Awareness
Preservation	Preservation	Identification	Preparation	Deployment (includes the following):	Deployment (includes the following):	Authorization
Analysis	Collection	Collection and preservation	Approach strategy	*Detection and notification*	*Detection and notification*	Planning
Presentation	Examination	Packaging, transportation and storage	Preservation	*Confirmation and authorization*	*Physical Crime Scene Phases (includes): Preservation, Survey, Documentation, Search and collection, Presentation*	Notification
	Analysis	Examination and analysis	Collection	Physical crime scene investigation (includes the following):	*Digital Crime Scene Phases (includes): Preservation, Survey, Search and collection, Documentation*	Search and identification
	Presentation	Reporting	Examination	*Preservation*	*Confirmation*	Collection
	Decision	**Concurrent Processes:**	Analysis	*Survey*	*Submission*	Transportation
		Documentation	Presentation	*Documentation*	Traceback (includes the following):	Storage
			Returning evidence	*Search and collection*	*Digital Crime Scene Stages*	Examination
				Reconstruction	*Authorization*	Hypothesis
				Presentation	Dynamite (includes the following):	Presentation
				Digital crime scene investigation (includes the following):	*Physical Crime Scene Stages*	Proof/Defence of hypothesis
				Preservation	*Digital Crime Scene Stages*	Dissemination of information
				Survey	*Reconstruction*	
				Documentation	*Communication*	
				Search and collection	Review Phase	
				Reconstruction		
				Presentation		
				Review Phase		

Table 1. Digital and cloud forensic methodologies (continued)

Beebe et al.	*Kent et al.*	*von Solms*	*Selamat et al.*	*Cohen*	*Agarwal, Gupta*	*Valjarevic, Venter*
Preparation	Collection	Readiness	Preparation	Identification	Preparation	Incident detection
Incident response	Examination	Preservation	Collection and preservation	Collection and preservation	Securing the scene	First response
Collection (preservation, package, transport and store)	Analysis	Acquisition	Examination and analysis	Transportation	Survey and recognition	Planning
Data analysis	Reporting	Analysis	Presentation and reporting	Storage	Documenting the scene	Preparation
Presentation		Presentation	Disseminating the case	Analysis, Interpretation and Attribution	Communication shielding	Incident scene documentation
Incident closure				Reconstruction	Collection	Identification
				Presentation	Preservation	Collection
				Destruction	Examination	Transportation
					Analysis	Storage
					Presentation	Analysis
					Result and review	Presentation
						Conclusion
						Concurrent Processes:
						Authorization
						Documentation
						Information flow
						Preservation
						Interaction

Table 1. Digital and cloud forensic methodologies (continued)

Guo et al.	***Chen et al.***	***Martini et al.***	***Ruan et al.***	***Adams***	***Kohn et al.***	***Zawoad et al.***
Determine the purpose of the forensic	Ascertain the purpose of cloud forensics	Identification and preservation	Pre-investigative readiness (includes the following):	Initial Planning - Preparation, notification and awareness	Preparation	Identification
Determine the type of the cloud service	Ascertain the type of the cloud service	Collection	*Event management, Identity management, Encryption management, Interoperability*	Onsite survey - Identification	Incident	Collection
Determine the type of the technology	Ascertain the type of the technology	Examination and analysis	Core-forensic process (includes the following):	Acquisition of electronic data	Incident response	Organization (Examination - Analysis)
Collection and preservation	Collection and preservation	Reporting and presentation	*Pro-active data collection, Re-active data collection, Hybrid acquisition, Examination, Analysis*	**Concurrent process:**	Digital investigation	Presentation
			Supportive process (includes the following):	Documentation	Physical investigation	Verification
			Evidence management, Case management, Multiple jurisdiction, Multi-tenancy		Presentation	**Concurrent process:**
			Investigative interface (includes the following):		**Concurrent process:**	Preservation
			Law enforcement, Forensic team		Documentation	

3.3. 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 two-fold. First, to merge 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 1 is produced to show the stages and processes of the previously proposed models. The 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, the stages' limitations of the previous models are taken into consideration. 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 (Martini and Choo, 2012) introduced by Martini with two important basic differences. Firstly, identification stage is considered as a unique stage because the first step in an investigation must always identify all the possible evidence. Secondly, preservation and collection stages are proposed 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 6.

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:

i) 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, data) have 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 need to be issued to get 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 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.

ii) 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.

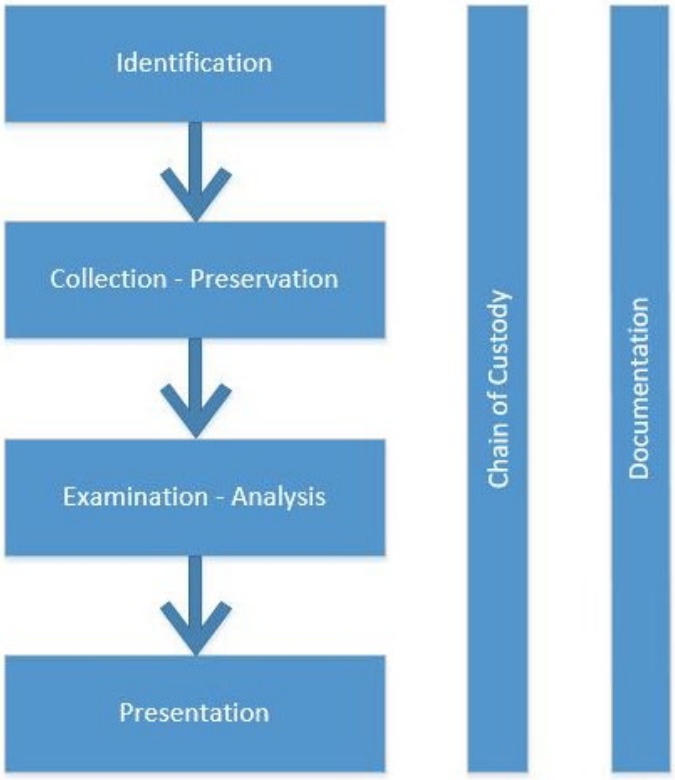


Figure 6 Stages of the Model

iii) 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 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.

iv) 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 due to the fact that 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.

For readability purposes a case study related to the aforementioned comparison framework 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 perpetrator 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 preserve data. A special trained team responsible for the incident is formed consisting of IT and law officers. The identification of the perpetrator's IP address is unsuccessful, due to the third countries proxy servers. Using CSP's assistance, investigators try to find more evidence such as card payment information, subscriber id's, access logs, etc. 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 VM image and respective data, new checks and controls are taking place to ensure its integrity and validity. Using appropriate tools, data is being analyzed for any useful information such as files containing photos, videos and sounds, event logs, IP addresses, timestamps, etc. File system and windows registry is also analyzed. Investigators load the VM snapshot to be able to get 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 perpetrator'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 above-mentioned 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.

3.4. Results discussion

In Table 2 a comparison of the stages of the proposed models found in the literature review with the stages of the comparison framework are presented. From the analysis illustrated in Table 2 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-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.

Table 2. 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.	Readiness - Detection - Notification - Confirmation	Preservation - Survey - Documentation - Search - Collection	Examination - Analysis - Reconstruction	Submission - Communication - Review
Ciardhuain	Awareness - Authorization - Planning -	Collection - Transport - Storage	Examination - Hypothesis	Presentation - Proof/Defence - Dissemination

	Notification - Search - Identification			
Beebe et al.	Preparation - Incident Response	Collection - Preservation - Package - Transport - Store	Analysis	Presentation - Closure
Kent et al.	X	Collection	Examination - Analysis	Reporting
von Solms	Readiness	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 & Recognition	Documentation - Communication Shielding - Evidence - Preservation	Examination - Analysis	Presentation - Result & 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	Reporting - Presentation
Ruan et al.	Pre-investigative readiness - Investigative interface	Pro-active and Re-active data collection - Evidence management	Core-forensic process (Examination - Analysis)	Supportive process (Case management)
Adams	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

In order to examine the complexity of the aforementioned methodologies some complexity indicators have been established 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, three different scales have been introduced; L (low), M (medium) and H (high). If the number of stages and phases is less than 3 the complexity is Low. If the number of stages and phases is 3 or 4 the complexity is Medium, and if the number of stages and phases is more than 4 the complexity is High.

The outcome of the complexity analysis is shown in Table 3. 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 (Pichan et al., 2015).

Table 3. Complexity of methodologies' stages

Methodologies / Models	***Stages (S) and Phases (P)***	***Identification***	***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 et al.	15	6 (H)	5 (H)	3 (M)	1 (L)
Adams	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)

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 Digital Investigation Process model (Baryamureeba and Tushabe, 2004) based on (Carrier and Spafford, 2003), the Integrated Conceptual Digital Forensic Framework for Cloud Computing (Martini and Choo, 2012) based on (McKemmish, 1999) and (Selamat et al., 2008), while the Abstract Digital Forensic model (Reith et al., 2002) and the Systematic Digital Forensic Investigation Model (Agarwal et al., 2011) both inspired by (Palmer, 2001). 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 preservation, iii) examination and analysis, 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 six models (Adams, 2013, Chen et al., 2012, Guo et al., 2012, Martini and Choo, 2012, Zawoad et al., 2015, Ruan and Carthy, 2012b) have been developed for cloud forensic purposes, but only three (Martini and Choo, 2012, Zawoad et al., 2015, Ruan and Carthy, 2012b) of them are complete. (Adams, 2013, Chen et al., 2012, Guo et al., 2012) 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 two models (Valjarevic and Venter, 2012, Ruan and Carthy, 2012b) include 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 (Adams et al., 2013) 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. 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 above. The categorization is based upon models and frameworks introduced and proposed by academics and the industry. To the best of my knowledge the only authors that have developed and introduced a framework or methodology concerning cloud forensics that covers almost every aspect and every phase in a cloud forensic investigation is (Ruan and Carthy, 2012b).

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 due to the fact that 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 since 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 due to 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.

Chapter 4

Cloud Forensic Challenges & Solutions

4.1. Introduction

In this chapter a thorough presentation of cloud forensic challenges identified from the review conducted in the respective area is produced. The presentation moves one step further and accomplishes a categorization of the respective challenges based on the cloud forensics process stages presented. 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. Also, a presentation of the solutions addressing clarified challenges identified from an analytical review conducted in the respective area. In the following chapter identified solutions are presented categorized per challenge.

4.2. Cloud forensic challenges

4.2.1. Identification Stage

Access to evidence in logs. Logs play a vital role in an investigation. Having access to log files in order to identify an incident is the first priority for the investigators. 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 (Zawoad and Hasan, 2013). 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 Virtual Machine (VM), which behaves almost the same as an Actual Machine (Damshenas et al., 2012). 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. (Khan et al., 2016) presented the state of the art of cloud log forensics highlighting the challenges and issues. It includes, but is not limited to log access, log security, decentralized logs, log format, log analysis, etc. According to (Marty, 2011), 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.

Physical inaccessibility. In a cloud environment, data location is a difficult task due to the geographical distribution of the hardware devices. The established digital forensic procedures and tools assume that physical access to the hardware is a fact (Poisel and Tjoa, 2012). 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 (Adams, 2013). There is also, no possibility to seize the hardware containing data (Zawoad and Hasan, 2015), 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 since they belong to private premises, where organizations have full control. The challenge applies to all three-service models.

Volatile data. Data stored in a Virtual Machine instance in an IaaS service model will be lost when the VM is turned off or rebooted (Zawoad and Hasan, 2015). This reflects to the loss of important evidence such as registry entries, processes and temporary Internet files. In case an adversary launches an attack on a VM with no persistent storage synchronization, when the attack is completed, the adversary can shut down the Virtual Machine instance leading to a complete loss of volatile data, if no further countermeasures are installed (Birk and Wegener, 2011). Respective literature (Grispos et al., 2012, Poisel and Tjoa, 2012, Zawoad and Hasan, 2013, Zimmerman and Glavach, 2011) 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.

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 (Birk and Wegener, 2011). 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 (Pichan et al., 2015). 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 due to 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.

Dependence on CSP - Trust. In all respective literature authors point out the CSPs contribution on cloud forensic process. CSPs are responsible for helping and assisting the investigators and the clients with all the information and evidence they can get in their cloud infrastructures. The problem arises when the CSPs are not willing to provide data and information about an incident (Freet et al., 2015). They may be reluctant to give out permission to access their multi-tenant environment(Chen et al., 2015). 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 (Zawoad et al., 2013). 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. Due to the fact of the unknown many users fear to trust the CSP's (Mishra et al., 2012). To prove that data has been preserved during an investigation the integrity method is used. On the other hand, integrity can add difficulties to cloud forensics due to additional trust that is required to be accredited from an investigator to third parties (Aydin and Jacob, 2013). This challenge applies not only to identification stage, but also to preservation and collection stage.

Service Level Agreement (SLA). 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" (Orton et al., 2013). 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 (Ruan et al., 2011b). 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 (Baset, 2012), "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 (Dykstra, 2013). Service Level Agreements concern the stages of identification, preservation and collection.

4.2.2. Preservation – Collection Stage

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) (Damshenas et al., 2012), then the evidence will not be admissible to the court of law. According to (Aydin and Jacob, 2013), integrity can add difficulties to cloud forensics due to additional trust that is required to be placed by 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. Apart from the trust, another factor for losing integrity is the corruption of the stored data due to CSP infrastructure's failure or malicious attacks (Yu et al., 2016). Besides the integrity preservation, it is difficult to maintain the stability of the data because of the transient nature and dedicated description of the data in a Cloud (Chen et al., 2012). According to (Martini and Choo, 2012), 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" (Farina et al., 2015). Due to the multi-tenancy the data can be contaminated by people who have access into the same storage unit with result of losing important evidence. Moreover, the privacy of other tenants needs to be preserved. Due to the fact that a number of tenants share the same sources, a privacy violation can occur during a forensic investigation (Spyridopoulos and Katos, 2013). 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.

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 (Ruan et al., 2011b).

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'" (Orton et al., 2013). Imagine an investigation where the CSP has to submit data to the investigators. The personnel responsible for collecting the data are not trained to preserve evidence according to specific forensic techniques. In this case the chain of custody will not be maintained. For a case to stand in court the investigators have to ensure that the chain of custody should contain information such as, who collected the evidence, how and where the evidence was collected, how the evidence was stored, who accessed the evidence, etc. (Martini and Choo, 2012). Another issue with ensuring a proper chain of evidence according to (Orton et al., 2013) 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.

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 is physically stored on a device hosted by a subcontracted third-party. For SaaS investigators have even less visibility of the hardware (Adams, 2013).

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

Multi-jurisdiction- distribution - collaboration. To acquire evidence from the three models in cloud from different jurisdictions is another issue for the investigators. Due to cloud characteristics system's data are usually spread in places around the globe. Thus, it is very difficult, almost impossible, to conduct evidence acquisition when investigators are dealt with different legal systems, where the related laws or regulations may vary by countries (Chen et al., 2012). A court order issued in the jurisdiction that resides a data center may not be applicable to the jurisdiction that resides another (Farina et al., 2015). "*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*" (Orton et al., 2013). 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. This activity, in many cases, can be time consuming and may lead to loss of useful evidence either deliberately or inadvertently (Spyridopoulos and Katos, 2013). Identifying and gathering information will almost certainly consume more time in the case of cascaded services than a single CSP (Almulla et al., 2013). 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 (Sibiya et al., 2012).

4.2.3. Examination - Analysis Stage

Lack of forensic tools. Data analysis in cloud environments requires appropriate forensic tools. Many of the tools used for a cloud investigation, have been designed and introduced for digital forensic investigations. With the systems distributed all over the world and with no physical access to the computer devices, these kinds of tools cannot fully cover the investigations in IaaS, PaaS and SaaS models (Spyridopoulos and Katos, 2013, Rani and Geethakumari, 2015). 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 (Dykstra, 2013). 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 (Almulla et al., 2013). According to cyber forensics needs analysis survey (Harichandran et al., 2016), 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.

Volume of data. The amount of data, stored in the CSPs' data centers is extremely large and it's increasing on a daily basis. Large amount of data (Petabytes of information) can produce many problems towards the searching of relevant digital evidence (Thorpe et al., 2013). 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 (Quick and Choo, 2014) 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 (Poisel and Tjoa, 2012). 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 (Sang, 2013). 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 (Adams, 2013).

Encryption. Many cloud customers in all three-service models store their data in an encrypted format to protect them from criminal activities. On the other hand, data owners such as organizations or companies, encrypt their data to ensure security and privacy due to the untrusted cloud providers (Yang et al., 2015). 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 (Almulla et al., 2013). 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 (Sibiya et al., 2012).

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 due to the fact that 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" (Trenwith and Venter, 2013). Investigators need to gather all the time stamps from the devices and establish an accurate time line of events (Grispos et al., 2012). Date-time stamps, as digital evidence, are very important in a court of law. Once they can be easily altered, additional verification need to be obtained, otherwise, investigators cannot ascertain whether the event occurred at a certain time (Kao, 2016).

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 (Damshenas et al., 2012). 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. According to (Kebande and Venter, 2015), to perform a digital event reconstruction when the cloud is forensically ready, in relation to the standard of ISO/IEC 27043:2015, is a hard task.

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 (Ruan et al., 2011b).

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 is stored in multiple remote locations in multi-tenant environments, and it is accessed through clients. Users can give fake data to cloud providers in order to avoid revealing their personal data if they think that the provider is an untrusted entity (Anastasopoulou et al., 2013). Hence, to determine that someone is the owner of the data from a large number of cloud users distributed globally is an intricate process (Sibiya et al., 2012). Another prospective is when a user engages a criminal movement through their VM from a veiled IP address and afterwards claims that their credentials have been compromised from another person.

4.2.4. Presentation Stage

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 (Adams, 2013). 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 (Dykstra, 2013). This is an important issue towards the progress of the trial. As (Trenwith and Venter, 2013) state, the reports should be kept as simple as possible and specialized terminology should be avoided at all cost.

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. Due to cloud characteristics where data is 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" (Orton et al., 2013). Without the original evidence, it would be very difficult to persuade the jury, which expects a piece of paper to be presented.

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

4.3. Analysis of cloud forensic challenges

To assign challenges to stages, Integrated Conceptual Digital Forensic Framework (Martini and Choo, 2012) was used with a slight differentiation as presented in chapter 3. 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 4 was designed to assign challenges according to the respective stage and service model they belong to. Some of the challenges' assignments may refer to more than one stage, but for the convenient presentation of the table, each challenge is assigned to one stage.

Table 4. Cloud forensic challenges overview

Cloud Forensic Challenges / Stage	***Applicable to***		
	IaaS	**PaaS**	**SaaS**
Identification			
Access to evidence in logs	partly	√	√
Physical inaccessibility	√	√	√
Volatile data	√	X	X
Client side identification	√	X	√
Dependence on CSP – Trust	√	√	√
Service Level Agreement (SLA)	√	√	√
Preservation – Collection			
Integrity and stability - Multi-tenancy, privacy	√	√	√
Internal Staffing - Chain of custody	√	√	√
Imaging	X	√	√
Bandwidth limitation	√	X	X
Multi-jurisdiction - Distribution - Collaboration	√	√	√
Examination – Analysis			
Lack of forensic tools	√	√	√
Volume of data	√	√	√
Encryption	√	√	√
Time synchronization - Reconstruction	√	√	√
Unification of log formats	√	√	√
Identity	√	√	√
Presentation			
Complexity of testimony	√	√	√
Documentation	√	√	√
Compliance issues	√	√	√

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, hospitals, etc. are not transitioning easily to cloud environments, due to trustworthy data retention issues, together with laws and regulations. There are several laws in different countries, which mandate the trustworthy data retention (Zawoad et al., 2013). 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 (Birk and Wegener, 2011).

NIST (NIST, 2014) has compiled a list of 65 challenges identified in the cloud computing environment. Even though the list of challenges shown in Table 4 consists of only 20 challenges (including compliance issues), most of NIST's challenges are included in the proposed list. This is due to NIST's detailed breakdown in comparison to the proposed list, which is more generic (i.e. NIST identify 4 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. Due to 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 is another sensitive issue to which authors referred thoroughly. Due to 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. (Dykstra and Sherman, 2013) 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. Due to the multi-jurisdiction, 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 are impossibility due to existing sensitivities and threat actors.

The findings are visualized in Figure 7. The challenges are presented with their categories and sub-categories.

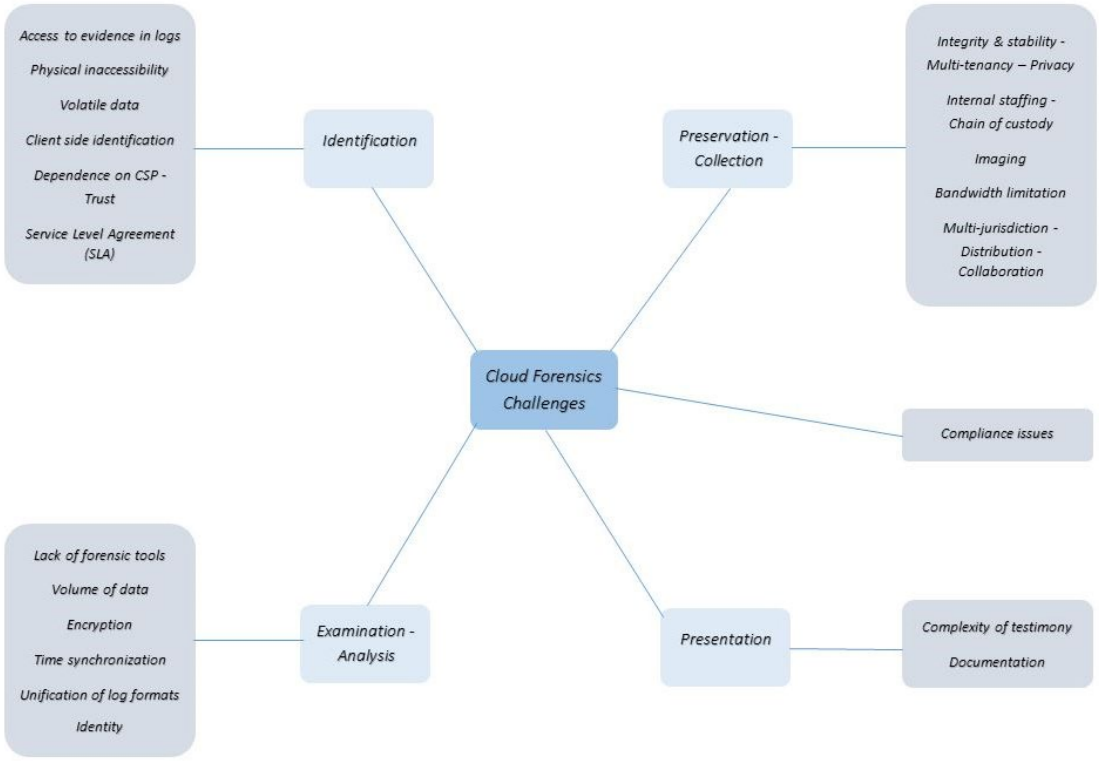


Figure 7 Cloud forensic challenges (categories and sub-categories)

4.4. Cloud forensic solutions

4.4.1. 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 due to the fact, that 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., 2013), who introduced Secure-Logging-as-a-service (SecLaas) mechanism for cloud forensics, which allows CSPs to store virtual machines' logs and provides access to forensic investigators while

preserving the confidentiality of the cloud users. Additionally, an auditor can check the integrity of the logs using the Proof of Past Log (PPL) and the Log Chain (LC).

(Sang, 2013) 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 also be 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 and Venter, 2013) 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 are limitations on prototype.

(Patrascu and Patriciu, 2014) introduced a logging framework – "a hierarchical architectural model - that allows investigators to seamlessly analyze workloads and virtual machines over a cloud infrastructure, while preserving scalability of large scale distributed systems". There is a consideration about the results according the time.

In PaaS, since the customers have full control on their application over a prepared API, system states and specific application logs can be extracted. (Birk and Wegener, 2011) 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 and Sherman, 2012) recommends 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 filesystem and hypervisor, and is used to manipulate the firewall and provision, start and stop virtual machines. Users and investigators can download VM images, log files, disk images and packet captures from the management plane.

Solving the cloud logging problems (Marty, 2011) 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 get 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 and Hasan, 2013) 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., 2012) 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, it depends on the interface, he proposed to implement the feature to check the basic logs and status of the client's usage. The above 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., 2011) 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 & web browser were provided.

4.4.2. Volatile data

To overcome the problem of volatile data, live investigation has been used as an alternative approach to dead acquisition. (Grispos et al., 2012) 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., 2012) proposed the cost to be globalized between CSPs to offer persistent storage device for client's data.

To prevent loss of volatile data, (Birk and Wegener, 2011) suggested frequent data synchronization between the VM and the persistent storage or a non-cloud based storage. According to (Zawoad and Hasan, 2013) 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.

4.4.3. Client side identification

To identify evidence on client's side, (Damshenas et al., 2012) suggested designing and implementing an application to log all potential evidence on the client's machine. However, they did not provide any methodology about the application and the procedure.

4.4.4. 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, 2010) 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., 2011), which consists of five layers of accountability: System, Data, Workflow, Policies and Laws & Regulations layers. To increase accountability detective approaches used rather than preventive.

(Manoj and Bhaskari, 2016) presented a framework for establishing a secure cloud environments with the help of Trusted Third Party (TTP). TTP validates both cloud providers' integrity and cloud consumer identity. In order for a cloud consumer to grant access and use the cloud services, an authentication by TTP is performed and a Short Time Ticket is generated. (Nurmi et al., 2009) 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 and Sherman, 2012). 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.

4.4.5. Service Level Agreement

SLAs can provide useful information to investigators about the rights and obligations between CSPs and users. (Thorpe et al., 2013), states, that users have the right to decide (especially in private cloud) where their data resides as form of jurisdictional control via the SLA. This means that during a cloud forensic investigation LEA can search data that resides 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.

SLAs should include important terms regarding cloud forensic investigations. According to (Ruan et al., 2011b) SLAs should include: 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 et al., 2011b) 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., 2012). (Baset, 2012) 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 Service Level Agreement (Patel et al., 2009) is proposed by (Busalim et al., 2013). It supports the SLA life cycle according to (Keller and Ludwig, 2003) and provides some parameters and objectives, which should be included in the SLA to consider the end user perspective.

(Bouchenak et al., 2013) 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., 2013) introduced the SLA-aware-Service (SLAaaS) 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 (SLO), 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 and Vidalis, 2009) proposed SLA's to be robust in order to be effective in combating cybercrime. For example, illegal activities such as Distributed Denial of Service (DDOS) etc. 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 and Wegener, 2011) suggested a trusted third-party to audit the security measures provided by the CSP. Finally, SLAs' violation is another problem in which (Haeberlen, 2010) proposed the trusted time-stamping. Timing information must be added to a tamper-evident log in order to detect the violations.

4.4.6. Integrity and stability - Privacy and multi-tenancy

To validate the integrity of the evidence (Zawoad and Hasan, 2013) suggested a digital signature on the collected evidence should be generated and then the signature should be checked. (Hegarty et al., 2009) developed and implemented a distributed signature detection framework that enables forensic analysis of storage platforms. Based on the meta-data driven data storage model and provenance integrity, in SaaS, (Shi et al., 2010) 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, 2011) proposed a new cybercrime forensic framework to image the relative records and files absolutely.

(Juels and Kaliski Jr, 2007) 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. (Ateniese et al., 2007) presented a model for Provable Data Possession (PDP) using RSA algorithm with homomorphic verifiable tags. The model verifies that a consumer can access an untrusted server that possesses the consumer's original data without retrieving it. According to (Garg and Bawa, 2016) this solution minimizes the server's workload. The drawback with both POR and PDP solutions is that the provision of evidence concerning the integrity of a remote file is successful "*only at a given time*" (Ateniese et al., 2016). To overcome this problem (Aspnes et al., 2007) proposed the *data entanglement* approach. The idea is to protect a user's data from an untrusted cloud provider by increasing the cost of errors using all-or-nothing integrity (if one's data is lost all user's data is lost). There is also a drawback to this approach according to (Ateniese et al., 2016). A trusted authority was responsible for the creation of the entanglement, thus the trusted authority is the only entity that can retrieve the files. In order to overcome this problem (Ateniese et al., 2016) proposed the entangled encoding scheme, which satisfies both privacy and all-or-nothing integrity.

To preserve the integrity of the data (Birk and Wegener, 2011) proposed the Trusted Platform Module (TPM) 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 (TCCP) provides a closed box execution environment by extending the concept of trusted platform to an entire IaaS backend. The TCCP 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 (Santos et al., 2009). (Damshenas et al., 2012) suggested all the issues concerning clients' privacy data should be included in an SLA contract.

(Zhou et al., 2013), proposed a role-based (RBE) scheme that allows RBAC 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 (Nancy Ambritta et al., 2014), 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 (IAMFI)

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., 2013) proposed data access control for multi-authority cloud storage (DAC-MACS), 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 and Venter, 2013), 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 meta-data file. (Li et al., 2014) 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.

4.4.7. 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., 2011b) 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., 2012) an investigator should possess the abilities of professional forensics skills such programming, networking etc., co-operating, communicating and negotiating with CSPs and understanding laws and regulations.

(Grispos et al., 2012) 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., 2011b) 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.

4.4.8. Imaging

To overcome the issue of acquiring forensic image (Damshenas et al., 2012) 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.

4.4.9. Multi-jurisdiction - Distribution - collaboration

New regulations have to be developed in order to solve the cross border legislation issue. (Biggs and Vidalis, 2009) 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, 2013) 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., 2011b) and (Sibiya et al., 2012) international laws should be developed to secure that forensic activities will not breach any laws or regulations under any jurisdiction.

4.4.10. Forensic Tools

Most of the researchers acknowledge that tools need to be developed to identify, collect and analyze forensic data. (Spyridopoulos and Katos, 2011) specified a number of requirements that an acquisition tool should have in order to meet the criteria of cloud forensic. (Juels and Kaliski Jr, 2007) developed Proofs Of Retrievability (PORs) tool for semi-trusted online archives, which guarantees the privacy and the integrity of files. In IaaS, (Dykstra and Sherman, 2012) 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. (Sang, 2013) proposed a log-based model which aims to reduce the "*complexity of verifying if someone or some device has used the cloud services or not*" (Sang, 2013):94. The drawback of this model concerns its implementation once it was designed to fit in the PaaS and SaaS models.

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 (IEF) and F-Response make use of relevant extensions to recover various cloud and social network related artifacts (Chen et al., 2015). (Dykstra and Sherman, 2013) 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 (FROST). It consists of three new forensic tools and it provides trustworthy forensic acquisition of virtual disks, API logs, and guest firewall logs. The problem with FROST tool is related with the trust in the CSP, once it is deployed by the CSP and on the other hand, it assumes that the user is involved and being part of the investigation (Alqahtany et al., 2016).

Recently, in 2016, (Alqahtany et al., 2016) proposed a new model for acquisition and analysis in cloud called Forensic Acquisition and Analysis System (FAAS). The model ignores the data held by CSP and gives the complete control over the acquisition process to cloud consumer. Images are created in a forensic sound manner and the access is provided to both deleted and over written files. The model applies only in the IaaS

service model. Some issues with the scalability and the size of the forensic image need to be re-examined and solved.

4.4.11. 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 (Grispos et al., 2012). 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 (Quick and Choo, 2014). 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.

4.4.12. Encryption

(Trenwith and Venter, 2013) uses both AES and RSA 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 AES while RSA is used to encrypt the aes-key. (Wan et al., 2012), proposed hierarchical attribute-set-based encryption (HASBE) to achieve scalability, flexibility and fine-grained access control in cloud computing. An extended proxy-assisted approach is introduced by (Yang et al., 2015) to overcome the issue of trusting the cloud server and formulate the threat model for cloud data encryption. The solution based on binding the cloud's server private key to the data decryption operation and a construction of a primitive 'revocable cloud data encryption' was presented.

4.4.13. Time synchronization – Reconstruction

To solve the time zones' problem (Damshenas et al., 2012) 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 et al., 2010). It provides clock synchronization between computer systems. The latest protocol RFC 5905 is considered as the most efficient. Clock Sampling Mutual Network Synchronization is another solution for providing synchronization in the cloud (Freet et al., 2015).

(Kao, 2016), proposed a novel cyber-crime investigation countermeasure using a novel created-accessed-modified (CAM) 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. To overcome the issue with digital event reconstruction, (Kebande and Venter, 2015) proposed the Enhanced Cloud Forensic Readiness (ECFR) process model that enables reconstruction of events and it can support future investigative technologies. The model can assist investigators to the analysis of potential digital evidence.

4.4.14. Complexity of testimony

(Wolthusen, 2009) 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 et al., 2013) 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.

4.4.15. Documentation

The documentation of the investigation according to (Wolthusen, 2009) 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 (Orton et al., 2013).

4.4.16. Compliance issues

According to (Birk and Wegener, 2011) 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 et al., 2013) stated that preservation and proofs of logs could increase the auditability of cloud environments, which is a vital issue to make the cloud compliant with the regulatory acts such as Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), etc.

4.5. Analysis of cloud forensic solutions

After assigning challenges to stages, Table 5 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 5, only for three issues a fair amount of solutions has been given. Access to logs, integrity and privacy and service level agreements 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 are based on the experience of the previous researchers, using similar algorithms or models. Even though, (Zafarullah et al., 2011) managed to collect logs from cloud infrastructure, and (Birk and Wegener, 2011), (Dykstra and Sherman, 2012) managed to mitigate the challenges of log acquisition, none of them succeeded in producing a system of storing the logs in Cloud and making it available publicly in a secure way (Zawoad et al., 2013).

In Table 4, twenty different challenges are cited, whereas in Table 5 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 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 can understand the complexity of the non-standard data sets. Depending on the volume of data, bandwidth limitation is another issue that needs to be addressed, since 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.

Table 5. Cloud forensic solutions

Cloud Forensic Challenges	*Solution*	*IaaS*	*PaaS*	*SaaS*	*Related Work*
Access to evidence in logs	Secure-Logging-as-a-service (SecLaas) mechanism	√	√	√	Zawoad et al.
	Status data extraction and checking	-	√	-	Damshenas et al.
	Log management architecture	-	-	√	Marty
	Logging mechanism	-	√	-	Birk et al.
	Log-based model	-	√	√	Sang
	Digital forensic readiness model	√	√	√	Trenwith et al.
	Management plane	√	-		Dykstra et al.
	Logging framework	√	√	√	Patrascu et al.
	Eucalyptus framework	√	-	-	Zafarullah et al.
Physical inaccessibility	-	-	-	-	-
Volatile data	Cost globalization between CSPs	√	-	-	Damshenas et al.
	Continuous synchronization API	√	-	-	Zawoad et al.
	Data synchronization	√	-	-	Birk et al.
	Live investigation	√	-	-	Grispos et al.
Client side identification	Log application	√	√	√	Damshenas et al.
Dependence on CSP - Trust	Accountable cloud	√	√	√	Haeberlen
	TrustCloud framework	√	√	√	Ko et al.
	Eucalyptus framework	√	-	-	Nurmi et al.
	Trusted Third Party (TTP)	√	√	√	Manoj et al.
	Layers of trust model	√	-	-	Dykstra et al.
Service Level Agreement (SLA)	Well and clear-written terms	√	√	√	Damshenas et al.
		√	√	√	Ruan et al.
		√	√	√	Thorpe et al.
	External auditors	√	√	√	Birk et al.
	Service guarantee, violation detection, credit and standardization	√	√	√	Baset
	Trusted timestamping	√	√	√	Haeberlen
	Define SLA parameters and objectives	√	√	√	Busalim et al.
	QoS and SLA model	√	√	√	Bouchenak et al.
	SLA-aware-Service (SLAaaS)	√	√	√	Serrano et al.
	Robust SLAs	√	√	√	Biggs et al.
Integrity & stability - Privacy & multi-tenancy	SLA contracts	√	√	√	Damshenas et al.
	Digital signature	√	√	√	Zawoad et al.
	Trusted Platform Module	√	√	√	Birk et al.
	Digital forensic readiness model	√	√	√	Trenwith et al.
	Distributed signature detection framework	√	√	√	Hegarty et al.
	Multi-tenancy model	-	-	√	Shi et al.
	Cybercrime forensic framework	√	√	√	Yan et al.
	Proofs Of Retrievability (PORs)	√	√	√	Juels et al.
	Provable Data Possession (PDP)	√	√	√	Ateniese et al.
	Data entanglement approach	√	√	√	Aspnes et al.
	Entangled encoding scheme	√	√	√	Ateniese et al.
	Trusted Cloud Computing Platform (TCCP)	√	-	-	Santos et al.
	Secure role-based access control	√	√	√	Zhou et al.
	Identity and access management in future internet architecture (IAMFI)	√	√	√	Ambritta et al.
	Data access control for multi-authority cloud storage (DAC-MACS)	√	√	√	Yang et al.
	Provenance system	√	√	√	Li et al.
Internal Staffing - Chain of custody	Team collaboration with wide range of skills	√	√	√	Ruan et al.
		√	√	√	Chen et al.
	Trained and qualified personnel	√	√	√	Grispos et al.
	Organizational policies and SLAs	√	√	√	Ruan et al.

Table 5. Cloud forensic solutions (continued)

Cloud Forensic Challenges	***Solution***	***IaaS***	***PaaS***	***SaaS***	***Related Work***
Imaging	Track record generator	√	-	-	Grispos et al.
Bandwidth limitation	-	-	-	-	-
Multi-jurisdiction - collaboration	Faster compliance with court orders	√	√	√	Dykstra
	International laws	√	√	√	Ruan et al.
		√	√	√	Sibiya et al.
	International legislations and global unity	√	√	√	Biggs et al.
Lack of forensic tools	Management plane	√	-	-	Dykstra et al.
	Forensic tools requirements	√	√	√	Spyridopoulos et al.
	Proofs Of Retrievability (PORs)	√	√	√	Juels et al.
	Log-based model	-	√	√	Sang
	Forensic Open-Stack Tools (FROST)	√	-	-	Dykstra et al.
	Forensic Acquisition and Analysis System (FAAS)	√	-	-	Alqahtany et al.
Volume of data	Public cloud storage	√	√	√	Grispos et al.
	Triaging techniques	√	√	√	Grispos et al.
		√	√	√	Quick et al.
Encryption	Digital forensic readiness model	√	√	√	Trenwith et al.
	Extended proxy-assisted approach	√	√	√	Yang et al.
	Hierarchical attribute-set-based encryption	√	√	√	Wan et al.
Time synchronization - Reconstruction	Unified/specific time system	√	√	√	Damshenas et al.
	Network Time Protocol (NTP)	√	√	√	Mills et al.
	Enhanced Cloud Forensic Readiness (ECFR)	√	√	√	Kebande et al.
	Clock Sampling Mutual Network Synchronization	√	√	√	Freet et al.
	Created-Accessed-Modified (CAM) model	√	√	√	Kao
Unification of log formats	-	-	-	-	-
Identity	-	-	-	-	-
Complexity of testimony	Personal knowledge of the case	√	√	√	Orton et al.
	Interactive presentation	√	√	√	Wolthusen
Documentation	Detailed documentation from start to end	√	√	√	Orton et al.
	Targeted/pointed presentation	√	√	√	Wolthusen
Compliance issues	Preservation and proofs of logs	√	√	√	Zawoad et al.
	Survey	√	√	√	Birk et al.
	Transparency	√	√	√	Birk et al.
	Third Party Auditor (TPA)	√	√	√	Birk et al.

Chapter 5

Understanding Cloud Investigation Process

5.1. Introduction

Cloud forensics introduces processes for resolving incidents occurring in cloud computing environments. However, designing cloud services capable to assist a cloud investigation process is of vital importance and the research efforts concentrate on these directions. In addition, digital forensics methods cannot support a cloud investigation since cloud environments introduce many differences compared to traditional IT environments. This chapter moves current research one step further by identifying the major concepts and their relationships that participate in a cloud forensic investigation process. Concepts and their relationships are presented as a map.

One of the main prerequisites for designing the map of concepts was the understanding of how cloud-forensic investigation is conducted. Since most of the research efforts are concentrated on the investigation part this dissertation proposes a generic cloud forensic investigation process in order to clarify all necessary activities required by the investigators for fulfilling their task. The understanding of this process as well as an extensive literature review on respective concepts and challenges for cloud forensics presented by (Simou et al., 2014b, Simou et al., 2014a, Simou et al., 2015) assisted on the design of the proposed map of concepts. The chapter concludes by presenting a running example as well, for addressing the concepts to the process.

5.2. Cloud forensics investigation concepts

In order to design the map of concepts for a cloud forensic investigation all possible aspects and elements must be identified. To identify the main concepts, a literature review has been conducted (Al-Fedaghi and Al-Babtain, 2012, Pooe and Labuschagne, 2012, Ruan and Carthy, 2012a, Selamat et al., 2008, von Solms et al., 2006). Based on this review analysis the most important components are as follows.

5.2.1. Incident

A cloud forensic investigation is initiated when an incident occurs (or being discovered). The staff is informed about the activities of the incident and monitors the system. A team is formed in order to deal with the incident and try to eliminate the risks. The main objective is to identify the incident, secure the evidence and find as much information and details about it. The most important element in the digital forensics is to maintain the integrity and the chain of custody of the digital evidence. Besides identifying evidence, the type of environment and configuration of the system should also be examined and identified and the location of data should be determined.

A good knowledge on the environment means that the investigator can decide what type of method and tools will be used to secure and acquire data. Securing and preserving data should be one of the first priorities practitioners should accomplish. They should require cooperation of the CSP to place a "litigation hold" on the account and prevent any further changes to the data (Martini and Choo, 2012). Authorization is another element that should be highly considered. To receive authorization to investigate an incident it could be a painful process. Law enforcement agents usually require a search warrant or other legal approval describing in details the terms and limits of the investigation (Carrier and Spafford, 2003, Ciardhuáin, 2004). There are different types of authorization provided by several discrete aspects such as internal, law or external (Adams, 2013).

5.2.2. Actor

Three different types of actors are being involved in a cloud forensic investigation:

Malicious actor: Person who wants to exploit a system's vulnerabilities in order to gain control or to harm another user's data. Malicious actor is the one responsible for introducing an incident that initiates the investigation process and for attacking any other actor involved in the cloud.

Protective actor: The people responsible for the investigation and try to solve the incident in a sound forensic manner. They conduct the investigation "*by utilizing and managing the forensic capabilities within the cloud environment adding their own forensic capabilities*" (Ruan and Carthy, 2012b). Protective actors can be the LEA, Organization stakeholders or the victim (consumer). The main task is to form a team that will have the ability to deal with an incident and be able to manage all human resources. The team should consist of both technical staff with great knowledge on new technologies and legal staff with knowledge of legislations and multi-jurisdictional issues. LEA objective according to Association of Chief Police Officers (ACPO) is "*the officers to ensure compliance with legislation and, in particular, to be sure that the procedures adopted in the seizure of any property are performed in accordance with statute and current case law*" *(Wilkinson and Haagman, 2010):6* and also to track-down the people responsible for a criminal activity. Protective actors use resources and develop strategies concerning decisions they have to take, based on the training, planning and preparation activities.

Cloud Service Provider: "*Person, organization or entity responsible for making a service available to Cloud Consumers*" (Liu et al., 2011):11. CSPs assist and help practitioners and consumers with all the information and evidence found in their infrastructures. They should be willing to provide the right access to potential evidence shortly after a request has been placed, without compromising the privacy and security of their tenants. As CSPs have full control of their infrastructures' data they should ensure that their staff are capable and trained to conduct an investigation and they should not tamper any data.

5.2.3. Goal

An incident is introducing goals and protective actors are responsible to realize these goals related to the incident. The most important issue is to resolve the incident and find the malicious actor. The way of realizing the goals depends on the methods and the effectiveness of the team.

5.2.4. Evidence

Depending on the way evidence has been acquired and handled in order to maintain chain of custody it can be admissible or not, in a legal proceeding. The collection of the assets with the use of appropriate resources may lead to the identification of useful evidence. Examining and analyzing the assets with the use of software tools can help investigators to find evidence and build a case in a court of law. Documentation supports the evidence and the strongest type of evidence obtained can support an assertion and pursue a positive verdict. A detailed presentation about evidence is introduced in section 2.3 of Chapter 2.

5.2.5. Resources

People, materials, knowledge that are used during the investigation. All actors use resources (personnel, tools, trainings plans, methods, etc.) either to create the incident or to resolve it. The resources that can be used related to personnel are the technicians (provider, protective or victim), the law officers and everyone else working on the case. Using the resources in a proper way the investigation can move forward since the resources can identify all the assets (especially data) hidden in the cloud environment. When dealing with resources the concentration is focused on whether the resource is available and who is responsible for its delivery(Mouratidis et al., 2016).

5.2.6. Assets

Equipment and information that can be used to find any evidence. CSP is the one who controls all the assets during a forensic investigation. There are three types of assets: hardware, software and data. According to (Kent et al., 2006) the forensic process transforms media into evidence in three steps. First data is extracted from media and transforms it into a new format, then data is transformed into information and finally, information is transformed into evidence. After collecting the assets with the appropriate resources, they might become useful evidence. Analyzing the assets with the use of software tools investigators can find evidence to build a case. The types of assets that can be transformed to evidence have been detailed described in section 2.3 of Chapter 2.

5.2.7. Documentation

The main objective of this is to keep the investigation proper documented in order to increase the probabilities of winning a case in a court of law or in an internal investigation. When the actors start to investigate an incident there is the need to produce proper documentation and detailed reports. Documentation at the early stages of the incident also helps to keep track of all the actions that have been taken and to proceed with different techniques. Any risk analysis or assessment tests performed during the training and preparation should be documented in order to assist the team.

All tools, processes, methods and principles performed should be documented properly in order to maintain the chain of custody. Any changes made to the evidence should also be recorded. According to (Grispos et al., 2012):14 "*a properly maintained chain of custody provides the documentary history for the entire lifetime of evidence discovered during an investigation*". To present the evidence in a court as admissible, all the parties (staff, CSPs, third parties) conducted the investigation should record their actions through logs and notes e.g. who handled the evidence, how it was done, did the integrity of the evidence maintained, how it was stored, etc.

5.2.8. Strategy

Strategy is developed both by protective actors and by consumers. As far as protective actors are concerned, this concept deals with the methods and policies they use to proceed in an investigation. Protective actors have to take decisions about the acquisition of evidence or the presentation. The outcome of the trial depends on their decisions. On the other hand (consumers point of view), strategy plays a vital role in the preparation and planning of the system in order to meet the organizational goals. Training is also part of an organization's strategy in order to support forensic services and be prepared to handle an incident. Planning and organizing the steps an actor will have to take in case of an incident, is very productive when the time comes. An actor can be relief to see that personnel, operations and infrastructures are able to support an investigation in case of an incident (Carrier and Spafford, 2003). A well-organized preparation can improve the quality and availability of digital evidence collected and preserved, while minimizing cost and workload (Beebe and Clark, 2005).

5.2.9. Verdict

This concept is related to the evidence and particularly to its presentation. When the verdict is announced, the incident is either resolved or an appeal follows. Either way, the strategy should be revised and updated to identify areas of improvement and review methodologies and procedures. Even though verdict as a concept does not belong to a cloud forensic investigation (a verdict is a judgment in a court of law, not a protective actors action) I strongly believe that it must be illustrated in the map of concepts. This is due to the fact that the decision of a jury concludes (closes) a forensic investigation. It is the outcome of the investigation whether it is positive or negative.

5.2.10. Cloud forensics investigation map of concepts

Taking under consideration the findings of this section concerning the concepts, the development of the proposed map of concepts is introduced. The goal of the specific map of concepts is to present all necessary concepts that will assist both information systems developers in building better services and investigators to be able to conduct forensics analysis in cloud environments. Figure 9 summarizes the critical components of the map of concepts.

As someone can see from the figure, the forensic investigation process is initiated whenever an incident occurs. Once the incident is brought to investigators' attention, the forensic investigation process is initiated. The whole process must be conducted

using standard procedures and policies in order to ensure that all digital evidence can withstand under scrutiny in the court of law (Casey, 2011):314.

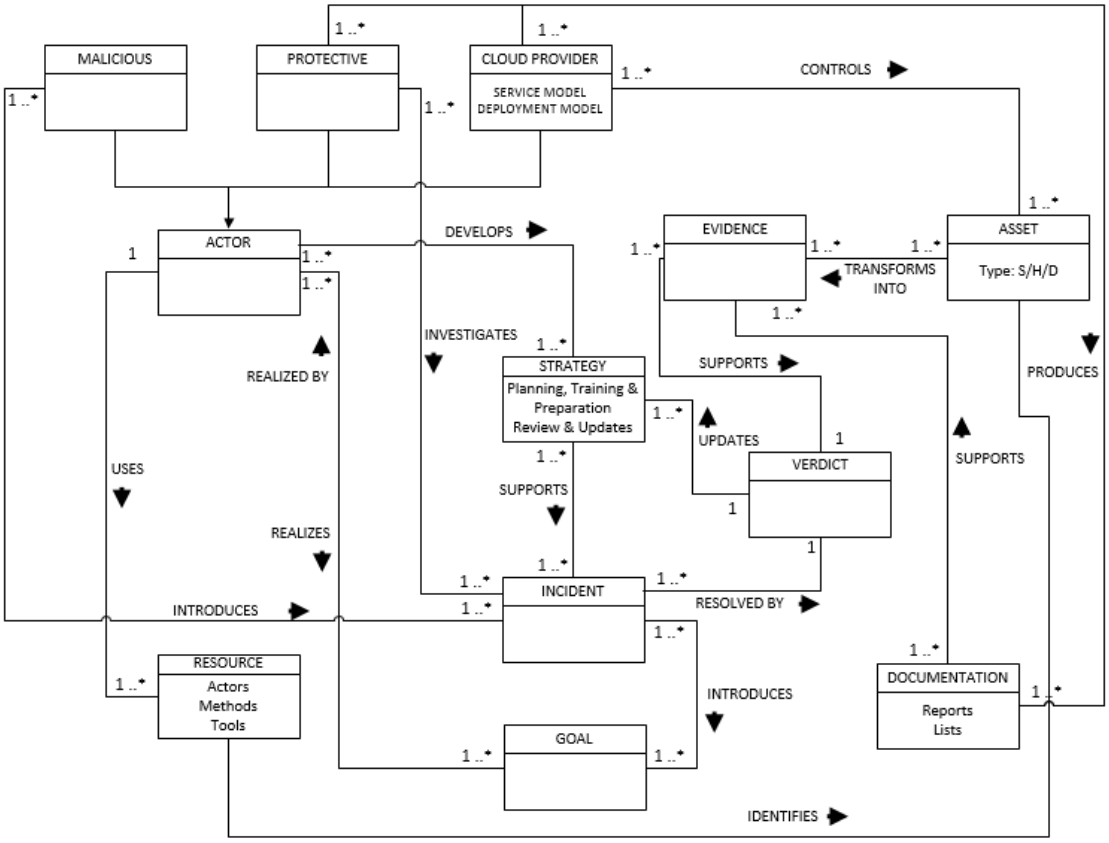


Figure 8 Map of concepts for assisting a Cloud Forensic Investigation Process

Malicious actors are the ones introducing an incident and protective actors are people investigating it and trying to find a solution. On the other hand, whenever there is an attack there is always a target (victim). In cloud forensics, targets are usually individuals, organizations, companies, etc. Malicious actors use Cloud Service Providers' services to launch their attacks hidden behind anonymity. On the other hand, CSPs major concern is to rent as many services to clients. So far four different actors involved in a cloud forensic investigation have been distinguished: malicious actors, protective actors, cloud provider and the victim. The actor victim could be considered as a protective actor. An incident most of the times affects one target (i.e. user or machine) and in parallel introduces goals (to solve the incident, find perpetrators, etc.).

All actors use resources (personnel, tools, trainings plans, methods, etc.). Malicious actors use resources to initiate incidents and protective actors use resources to resolve them. On the other hand, actors develop strategy concerning decisions they have to take, based on the training, planning and preparation activities. Protective actors should be well prepared to confront any incident based on their plans implemented prior to this. Developing an incident response plan ensures that all possible calculated risks are taken under consideration (Beebe and Clark, 2005). Policies and procedures should be clearly

defined and as many likely scenarios should be considered and tested. To support the plans, actors need to have skilled and experienced personnel. The personnel should be trained to the new technologies and follow the latest market trends and methods. Training plays a vital role to all investigations, by minimizing risks and mistakes.

CSPs should be responsible to assist and help practitioners and consumers with all the information and evidence found in their infrastructures. They should be willing to provide the right access to potential evidence shortly after a request has been placed, without compromising the privacy and security of their tenants. In other words, CSP is the one who controls all the assets during a forensic investigation. The three types of assets, hardware, software and data should be preserved at all times. Assets are being acquired using appropriate resources in a forensic sound manner. Specialized technicians with the right resources can transform assets to evidence. By examining and analyzing the assets with the use of software tools investigators can find evidence to build a case in the court of law.

Protective actors and cloud providers should keep detailed documentation about the progress of the investigation. They are responsible for the production of the lists and reports to substantiate that the findings maintained their chain of custody and the investigation have been conducted in accordance with the forensic policies and legislations. Documenting every individual step and every aspect in the investigation process can help protective actors to support their findings (evidence) and build a case in court. Depending on the evidence (how concrete they are), the jury announces the verdict either in favor of or against malicious actor. In other words, a verdict is the concept that resolves the incident and makes protective actors to review and update their strategy.

5.3. Cloud forensics investigation process

After a thorough analysis (Simou et al., 2014b, Simou et al., 2015, Simou et al., 2016b) of the respective literature, a generic process for cloud forensic investigation is proposed, consisting of the following steps: Incident Confirmation, Incident Identification, Collection-Acquisition, Examination-Analysis and presentation. The proposed process is also illustrated in Figure 8. Understanding the cloud forensic investigation process is of vital importance in order to identify the key factors that a modeling language aiming on modeling Cloud-Forensic enabled Services.

5.3.1. Incident Confirmation

The first stage is the confirmation of the incident. An incident may be detected by different sources such as an automated detection system, administrator, external actors, or accidentally. In the confirmation stage the protective actors are made aware that an incident has detected and reported. According to Ciardhuain (Ciardhuáin, 2004) the awareness stage need to be included because the events causing the investigation may influence the type of investigation required. The people responsible for the safety (protective actors) need to be informed about the malicious action and start searching

the incident using all available resources to realize what it concerns. It can be a breach on confidential data, stolen information, a DDOS attack, trafficking illegal content, etc.

Protective actors should be able to understand the nature of the incident and decide if they are willing to proceed with an investigation or not. Their decision involves different factors such as the criticality and severity of the incident, the infection (damage can cause), the cost and the availability on human resources. (Kohn et al., 2013):10, states that "*the detected incident should be confirmed by some other source before action is taken towards an incident response*". Once the incident is confirmed, protective actors need to notify and inform all the stakeholders involved in the investigation. Application of warranty should be prepared and appropriate authorizations need to be obtained in order to grant permissions to different stages of the investigation. On the other hand, if the incident does not impose an immediate threat to organizations, or public security and it can be solved by the inside, then, the investigation is not initiated.

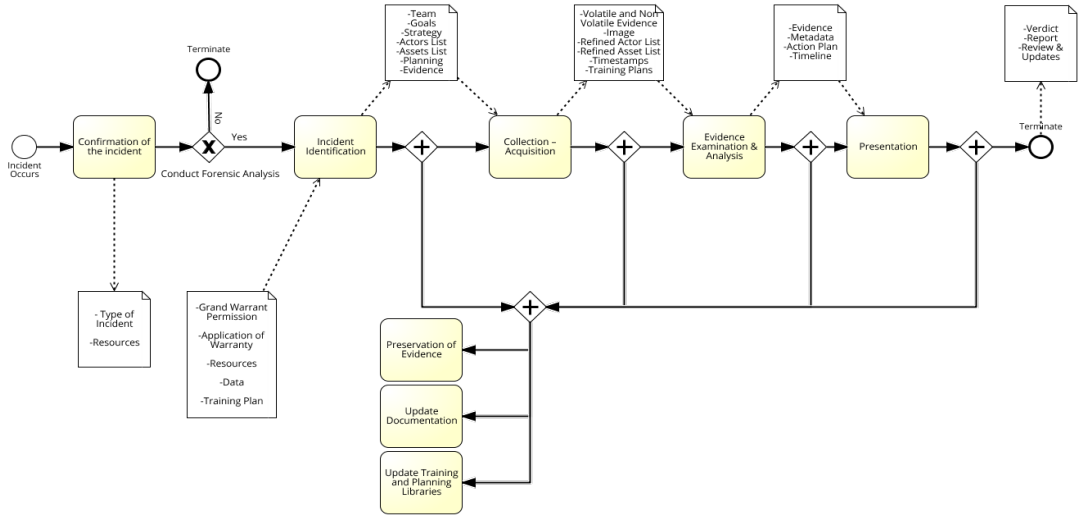


Figure 9 Process for Cloud Forensic Investigation

5.3.2. Incident Identification

The next step is to identify all relevant assets (software, hardware and data) that may contain potential evidence, to build a case. According to (ISO/IEC-27037:2012, 2012):11, identification is the "*process involving the search for recognition and documentation of potential digital evidence*". Protective actors need to determine the type of crime and what type of assets are used. Protective actors also need to identify the assets (potential evidence), the location of the incident, the malicious actor's resources and the cloud provider. An important concern is the trustworthiness of the involved CSP. As (Zawoad et al., 2015) mentioned, most of the existing work on cloud forensics is taking a priori that CSPs are trusted entities and honest in a cloud investigation. "Trust must be managed through detailed Service Level Agreements (SLAs) with clear metrics and monitoring mechanisms and clear delineation of security mechanisms" (Simpson and Chandersekaran, 2014):4.

Once the incident is confirmed, an investigation team should be formed consisting of people with special skills in cloud environments, such as legal advisors, experienced technicians and law officers. Warrant permissions to different stages of the investigation should be granted. All the actions taken should be recorded and documented. A proper documentation can be very helpful in the next stages of the investigation and in parallel it can maintain the chain of custody. Protective actors also need to consult previous cases and all the action plans performed during their training in order to prepare and deploy their strategy. Initial planning is based on respective older documentation and policies. Authorizations should be obtained to carry out the investigation and resources need to be identified. Resources include the personnel (actors) that will form the team to cope with the investigation, the methods and procedures that they will adopt and the tools they will use to identify the potential evidence. An actors list, assets list, system information report, time plan, acquisition plan and action plan (risk assessment plan) will be produced and recorded to maintain the chain of custody. Finally, the Service Level Agreement (SLA) between CSPs and cloud consumer should be reviewed by the actors to understand technical and legal terms.

5.3.3. Collection – Acquisition

After identifying the assets and their location, the collection and acquisition process follows. The goal of this phase is to obtain the potential evidence. Depending on specific factors such as the kind of potential evidence, the criticality of the system or the legal requirements, the actors should decide what type of method must be used to extract them. In an ongoing cloud investigation, the impact for seizing hardware equipment cannot be measured; hence, in most of the cases, acquisition method should be used. (ISO/IEC-27037:2012, 2012):10, defines collection as the "*process of gathering the physical items that contain potential digital evidence*", meanwhile, acquisition is defined as the "*process of creating a copy of data within a defined set*".

The methods of collecting data are either static or live. In the first case, the process is straight-forward; seizing the items and removing them to a forensic lab for further examination. In the second case, the systems are running and the collection is performed on a system in running state. This involves an image or a snapshot acquisition that it can obtain useful information about registry entries, temporary files, memory, running processes, log entries, cache, etc. According to (Alliance, 2013):11, "*the copy created during acquisition can range from the forensic image of a hard drive to a copy of the contents of a server's memory to the logical contents of an individual user's email box*". (Pichan et al., 2015) states that for the cloud a series of snapshot images over a period of time should be taken in order to provide all the information regarding changes.

During the collection-acquisition stage specific resources will be used. This involves well-trained personnel (internal or even external actors), special tools for cloud extraction data and up-to-date methodologies/processes such as protection mechanisms and action plans. Using the appropriate resources, protective actors aim to obtain both volatile and non-volatile potential evidence, in a forensically sound manner. The

acquired assets should be securely stored for further analysis. The acquired evidence should be well documented and checked for their integrity using hash methods and algorithms in order to discover any future alteration.

5.3.4. Examination – Analysis

Once the acquired data has been stored in a safe and se-cure storage a number of identical copies to the original data should be produced for protective actors to work with. This process involves two different sub-processes: evidence examination and evidence analysis. According to NIST (Kent et al., 2006):16, examination is defined as "*the involvement of forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data*" while analysis is defined as "*the process to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination*".

In order to go into a forensic examination, protective actors should obtain a high-level overview of the terrain and form a strategy; otherwise, delays might occur when unforeseen but preventable problems are encountered. "Examination is generally known to be the process where the investigator makes digital evidence visible or extracts the data into a human readable form" (Kohn et al., 2013):113. This phase "*is an important step for data collected from a cloud computing environment as the data is unlikely to be stored and collected in a form which permits immediate forensic analysis*" (Martini and Choo, 2012):77. Technician examiners should be informed by the questions and priorities that protective actors developed during their initial planning (Casey et al., 2013). On the other hand, 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 enormous amount of data collected in the previous stage should be converted into manageable size and form for future analysis (Agarwal et al., 2011). Due to the volume and complexity of data stored on digital devices, examiners should take decisions on what methods and tools they should use in order to focus on the relevant data (Williams, 2011). Examiners should search for timestamps, usernames and passwords, particular keywords using filters, etc. They should use the evidence gathered to reconstruct and create a timeline of events. The findings from the examination will be used as input for the analysis.

During analysis, actors should determine the significance of the data in order to transform them into evidence. Encrypted data should be processed and analyzed and the results will be used to reconstruct the timeline. Metadata from the examination phase will be analyzed and correlated to the potential evidence. Also, "*metadata and other forms of audit data must be properly kept and made available when requested*" (Martini and Choo, 2012):7. The tools used will permit analysts to group related events into meta-events (Kent et al., 2006). This process may perform several iterations to support the investigation depending on the evidence during the analysis phase. It could

iterate back to the collection-acquisition or even identification process. All the resources involved or used during the examination and analysis phase should be properly documented and an actors list should be produced with details such as name, date and time of access to the evidence, actions taken and methodologies used.

5.3.5. Presentation

The last stage is the presentation of the evidence selected during the investigation. (von Solms et al., 2006), states that presentation process involves three steps in order to ensure a successful conclusion to the investigation; these are case preparation, case presentation and evidence preservation. Experts should be prepared to confront the jury who lacks knowledge of cloud computing and try to present the evidence collected in a language that anyone can understand. (Kent et al., 2006):30, uses the word reporting for this process and defines it as "*the process of preparing and presenting the information resulting from the analysis phase*". Taking under consideration the two previous definitions as well as other definitions found in the literature, the definition of presentation could be redefined as:

The process of preparing and presenting the preserved and documented evidence resulting from a cloud investigation.

During presentation, the personnel responsible for presenting the respective report should be well prepared to explain in a logical and understandable way the preserved and documented evidence. The implemented reports along with the supporting materials concerning the chain of custody of the evidence should be submitted to the court of law. At the end of the trial, the evidence and the documentation should be carefully stored and secured to be used either in case of an appeal or for future purpose. In order to preserve evidence and knowledge gained from the case, strategy, methods, procedures, tools and reports used during the investigation should be recorded in a database to be used in similar cases by protective actors.

5.3.6. Concurrent Activities

Some activities are running in parallel with the aforementioned stages. These are the preservation of the evidence, documentation and preparation (training and planning). Preservation of evidence is defined by (ISO/IEC-27037:2012, 2012):11 as the "*process to maintain and safeguard the integrity and/or original condition of the potential digital evidence*". Evidence preservation helps assure admissibility in a court of law (Alliance, 2013). In a cloud environment, the challenge is how to pre-serve the data and then determine whether the existing approaches of measuring data integrity are applicable or not (Almulla et al., 2014). To ensure that the integrity of evidence and the chain of custody are maintained throughout the investigation, this activity should be running in parallel with all the stages of the aforementioned process. The same applies for the documentation activity.

For conventional forensic process, (Vacca, 2005) defines chain of custody as "*a roadmap that shows how evidence was collected, analyzed and preserved in order to be presented as evidence in court*". (Braid, 2001) states that the evidence must meet five criteria in order to be used and support a trial, so it must be: admissible, authentic,

complete, reliable and believable. To preserve the integrity of the evidence, maintain the authenticity and the chain of custody a number of requirements need to be produced, such as reports (handling, methodology, storage, etc.), lists (tools, actors, procedures, etc.) and logs (activity logs). Any change that will produce a different result should be recorded. The main objective of the documentation is to keep the investigation properly documented in order to increase the probabilities of winning a case in a court of law. According to (Prayudi and Sn, 2015) protective actors are facing a serious problem in the chain of custody related to the documentation of the evidence. This is due to tremendous amount of data and the distributed cloud environment that require many different concepts and entities to handle the evidence. "*Documentation can assure the identity, place and time of a snapshot while traditional techniques such as cryptographic hashes and chain of custody processes can provide integrity assurance*" (Alliance, 2013):14.

On the other hand, the main objective of preparation (training and planning) activity is to prepare and ensure that personnel, operations and infrastructures are able to support an investigation in case of an incident (Carrier and Spafford, 2003). A well-organized preparation can improve the quality and availability of digital evidence collected and preserved, while minimizing cost and workload (Beebe and Clark, 2005). Training plans will be used as input in order to organize and prepare the resources of the investigation. SLAs are contracts, usually signed between consumers and CSPs, providing information on how a cloud forensic investigation will be handled (Aydin and Jacob, 2013). Well-written and robust SLAs should be considered in order to provide technical and legal details about the roles and responsibilities between the CSP and the cloud customer, security issues in a multi-jurisdictional and multi-tenant environment in terms of legal regulations, confidentiality of customer data, and privacy policies.

5.4. Running example

For verifying the applicability of the aforementioned cloud forensic investigation process, a running example is presented. Through this example, a basic analysis is conducted for identifying that all concepts presented are indeed the necessary ones required for describing a specific forensic scenario. The words that match the proposed concepts of map of concepts are marked in bold. The case deals with trafficking illegal digital material in cloud environment. The scenario is similar to (Dykstra and Sherman, 2011).

John, a malicious actor, opens an account with Microsoft Azure Cloud Service Provider (CSP). He registers to use IaaS services. He creates a Virtual Machine (VM) and a webserver where he uploads illegal content of photographs, videos, etc. using the storage (hard disks), Azure is providing. All data is encrypted using cryptographic function and anyone can download the material anonymously as long as is a registered user. Once a day the VM is switched off resulting in the loss of data, leaving it to restart

from a clean state. Most of the times John pays the provider with a pay-safe or a pre-paid card, thus his ID remains unknown. Protective actors' primary purpose is to find malicious actor and prosecute him.

Incident Confirmation **- John** (Malicious actor) is responsible for the initiation of the **incident** (trafficking illegal content over the internet). The **Cyber Crime Unit** (Protective actors) detects the illegal activity and brings the case into the **head officer** to **decide** whether they are going to proceed into an investigation or not. The head officer is informed about the **type of incident** and the available **resources** and takes the decision to initiate the investigation.

Incident Identification - John uses the cloud, so protective actors locate the **Cloud Provider** that accommodate malicious actor's **servers** and prepare an **application of warranty**. In parallel a special **trained team** responsible for the incident is formed consisting of **IT** and **law officers**. Once the **warrant permission is granted**, a communication with CSP is established and is being asked to **preserve the data**, through **procedures**, which do not suspect the malicious actor. At the same time, protective actors search for previous **similar cases** to identify any common patterns working in parallel on the investigation **strategy** by setting the **goals** and their **initial plan**. The identification of the malicious actor's **IP address** is unsuccessful, due to the third countries proxy servers. Using CSP's assistance, protective actors try to find more evidence such as **card payment information**, cloud providers' **subscriber id's**, **access logs**, **NetFlow records**, **webserver virtual machine** and **cloud storage data** (Dykstra and Sherman, 2011). According to the data preservations procedures and principles, the **actions** of any **CSP's personnel** involved in the investigation must be **recorded** and **documented**. Also, a research is conducted by protective actors to identify the **source of the evidence** and assets, such as **computers, laptops, mobiles**, etc. Once system information and **potential evidence** have been identified with **forensic tools**, protective actors start to implement the **acquisition plan** and produce an **action plan**, **time plan**, **actors'** and **assets' lists**. Due to the fact that the CSP is operating in a different country and the data are stored in data centers, geographically spanned in various locations, proper procedures need to be followed to cope with the different jurisdictions. **Trained law officers**, specialized on legal issues, are involved.

Collection – Acquisition - Once the remaining issues relating to jurisdiction have been resolved, 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 protective actor, using appropriate software such as the **EnCase** or **FTK**. The tools are part of the resources being used to investigate the incident. This operation is followed according to the **training scenarios** that took place during the preparation/training and takes under consideration the acquisition plan. A proper forensic image contains **volatile evidence**, **metadata**, such as, **hashes** and **timestamps** and it compresses all empty blocks. Then, the technician verifies the image for **integrity** and **authenticity** of data by creating MD5 hash values. These tests reveal any alteration of the evidence, in order to use the evidence in a court of law, through forensically acceptable procedures.

The problem identified in this process is whether the hired technical staff of the cloud provider has the necessary knowledge and training to properly manage forensic evidence collected from the malicious actor's assets and how trustworthy the whole process is mainly against intentional or accidental data alteration. The **chain of custody** could be considered to be violated with negative results. The entire process of creating the image should be documented in detail, presenting the exact **methods** and tools (resources) that have been used, the produced outputs and the results, a **methodology report**, the technical knowledge of the personnel responsible for the creation, the supervisor's position and any other relevant detail that will help in a lawsuit. With the completion of the controls, the provider sends the image and all data collected to protective actors for examination in order to carry on with the investigation.

Examination – Analysis - Once protective actors receive the VM image and respective data, new checks and controls are taking place to ensure the integrity and validity of the assets. Two **identical copies** are produced to work with and the original one is stored in a secure place with limited access to the head of the investigation. Using appropriate resources (**software tools**), data is being analyzed for any useful information such as files containing **photos**, **videos** and **sounds**, **event logs**, IP addresses, timestamps, etc. At this point, protective actors realize that data is encrypted and a search for finding and identifying **decode keys** is starting. With Azure, where the location of applications and data is abstracted, storing a public key in cloud makes it very difficult to find and retrieve it. File system and **windows registry** is also analyzed. Time is valuable and crucial during an investigation and it is directly related to the amount of data to be analyzed. Let us assume that the CSP managed to produce 20MB of event logs, 150MB from NetFlow records, 50GB of VM snapshot and 1TB of data. The protective actors load the **VM snapshot** to be able to get more information regarding the structure of the web site and the encryption methods used. The personnel responsible for analyzing the data follows an action plan designed mainly from previous cases. After a thorough investigation protective actors manage to locate and retrieve the decoding keys and the analysis of 1TB data is starting in order to reveal any evidence. 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 and techniques followed. The reports contain information about the CSP, the persons involved in the investigation, evidence analysis, methods and techniques followed, respective findings and all technical terms used. A **final report** is produced by the head of the investigation and presented to the legal authorities.

Presentation - All the stages followed during the above mentioned investigation have been well documented in accordance with forensic principles and procedures, in order to ensure the integrity and the validity of the evidence and to preserve the chain of custody. Before the presentation all evidence, reports, resources used, have been examined thoroughly and tasks have been assigned to experienced personnel who will present the case. Whatever the outcome (**verdict**) of the trial is, all the investigation is **reviewed** from the start and the necessary **updates** have been recorded. Then the case

is **closed** and the documentation is stored in a database for future use and training purposes.

5.5. Discussion

In order to design cloud forensic-enabled services software engineers need to understand the way a cloud forensic investigation works. The important aspects of the investigation need to be clarified and the dependencies should be introduced. This is due to the fact that designers should be aware about the concepts identified in the cloud forensic investigation since a number of those concepts are directly involved in the design of the services. Concepts such as actors, goal, assets have an active role both in the design of the service and the investigation of an incident. Once a cloud service is designed to be forensic-enabled software engineers need to take under consideration the use of the specific service. Cloud forensic-enabled services should be designed in a manner that the identified information will assist the investigator when an incident occurs.

This map of concepts introduced in this chapter that assists protective actors in a cloud forensic investigation will be part of the design of the cloud forensic-enabled services meta-model so as to understand the relationships of the concepts identified here with the one in the design of the service. The concepts that will be described in the meta-model should be able to collaborate with the information required during an investigation. Even though some concepts that form the groups are related to each other, the way they will be illustrated in the meta-model should be clearly separated to highlight the differences between them in the way they are used in the cloud forensics. On the other hand, the proposed cloud forensic investigation process can assist software engineers in a way that they can be informed about the steps of the investigation and how it can be conducted in order to integrate these information in the design and implementation of the process for cloud forensic-enabled services.

Chapter 6

Cloud Forensic-enabled Framework

6.1. Introduction

Cloud forensics assists investigators on solving cloud-based cyber-crimes. Although investigators use forensic methods and tools to cope with incidents, there are other aspects that put barriers to the whole investigation process. One of these aspects is the way cloud services are designed and implemented. Software engineers are responsible for the design and implementation of them but in many cases, cloud services are not designed nor implemented as cloud forensic-enabled, introducing issues to the outcome of the potential investigation. Software engineers in many cases, appear to forget or fail to pay the proper consideration on cloud forensic needs. This has a huge impact on a cloud forensic investigation due to the fact that the investigation cannot be conducted in a forensically sound manner. In order to deal with this issue and ensure that investigation standards are met, software engineers must comply with forensic standards and develop reliable cloud forensic-enabled services.

To design cloud services capable of assisting investigators to solve an incident is a challenge. A thorough analysis of the respective literature revealed that there is a literature gap in supporting software engineers so as to identify forensic-related requirements for information systems (Simou et al., 2016c). Thus, to fill the aforementioned gap, in this chapter a presentation of a requirements engineering framework is introduced to support software engineers in the elicitation of forensic requirements and the design of forensic-enabled cloud services. The framework supports cloud services by implementing a number of steps to make the services cloud forensic-enabled. It consists of a set of cloud forensic constraints, a modelling language expressed through a conceptual meta-model and a process based on the concepts identified and presented in the meta-model.

The meta-model presented in this chapter not only includes the concepts that make a system forensic-enabled, but also the concepts for cloud forensic investigation identified in (Simou et al., 2016c), raising the importance of the relation between a forensic-enabled system and an investigation process and how the latter is assisted when an incident occurs. In this way, an integrated meta-model is produced to assist designers in a way that, they will be able to design forensicable cloud services (the term forensicable is used to describe a service of being forensic-enabled). The main advantage of the proposed model is the correlation of cloud services' characteristics with the cloud investigation while providing software engineers the ability to design and implement cloud forensic-enabled services via the use of process patterns.

6.2. Forensic constraints

This section presents a list of concepts that should be realized in order for a cloud-service to be characterized as cloud forensic-enabled service. The main question answered here is what are those elements that make a system or a service be characterized as forensic-enabled. To answer this question, a list of concepts is presented following a previews review on the respective field (Simou et al., 2014b). The concepts presented are defined as constraints since their implementation forces the mandatory use of specific technologies in addition to the existing functionality of the services.

Forensic constraints are requirements related to system forensicability (in this dissertation, the term forensicability has been used to denote a system or a service that can be forensic-enabled; can be developed in a sound forensic manner) and specify a system's or service's quality attributes. To identify a set of cloud forensic constraints first a clarification of the concept of cloud service should be given. In fact, a cloud service is any resource made available to consumers over the Internet such as data storage, e-mail, web hosting, etc. CSPs are responsible for providing those services through service models and deployment models. Depending on the design and implementation, a cloud service may contain vulnerabilities that can be exploited by malicious actors (Kalloniatis et al., 2014). These vulnerabilities are sometimes hard to avoid and may harm consumers that use the "infected" cloud service. To investigate the incident in a forensically sound manner and find a solution, the implementation of the specific service should take into consideration various parameters related to forensic requirements. (Zawoad and Hasan, 2015) states "*we need to preserve logs, proof of data possession, provenance information and timestamp securely*" in order to support trustworthy forensics in cloud. On the other hand, evidence should be handed to users, protective actors, or court authorities whenever they asked. Based on these requirements, (Zawoad and Hasan, 2015) introduced a forensics-friendly cloud computing architecture.

For a service to be characterized as cloud forensic-enabled (meeting specific criteria) depends both on the people using the particular service, and from a technical point of view, on the way it has been implemented. From the people's perspective National Institute of Standards and Technology (NIST) highlights that the actors involved in the cloud are: consumers, providers, auditors, brokers and carriers (Liu et al., 2011). Actors interact with one another depending on their roles in the cloud. The technical perspective focuses on the procedures, forensic mechanisms, security and private policies that are used to implement a cloud service in order to make it reliable and trustworthy to the people.

Based on the cloud characteristics and the forensic properties seven cloud forensic constraints have been identified from the respective literature (Newcombe, 2012, Catteddu et al., 2013, NIST, 2013, Cloud_Accountability_Project, 2016, Ruan and Carthy, 2012b, Zawoad and Hasan, 2015, Ruan et al., 2011a). These forensic

constraints have a lot in common with security and privacy concepts identified in various research works (Kalloniatis et al., 2008, Kalloniatis et al., 2014, Shei et al., 2016, Chang and Ramachandran, 2016). Some of the concepts are identical in both worlds, especially when they are examined under a technical point of view. This is due to the fact that the cloud forensic process relies on the privacy and security capabilities to help resolve forensic issues. To clarify the role of the constraints identified in the forensic process, a definition has been given for every single constraint to address its relationship with cloud forensics. Cloud forensic constraints have been also categorized according to the cloud forensic stages that they belong to, the challenges and the solutions that apply to, as well as the actors involved and the respective cloud layers (service models). Stages, challenges and solutions are derived from my previous work in the respective field (Simou et al., 2014b, Simou et al., 2016a, Simou et al., 2014a). The seven forensic constraints are listed in a structured way as follows:

6.2.1 Accountability

Definition: Accountability is the CSP's obligation to protect and use consumer's data with responsibility for its actions and liability in case of an issue.

Stages: Identification, Preservation-Collection, Examination-Analysis, Presentation.

Challenges: Access to evidence in logs, Dependence on CSP-Trust, Service Level Agreement (SLA), Chain of custody, Documentation, Compliance issues.

Solutions: CSPs should ensure that policies and standards are met with great responsibility and any problems arising from their actions are remedied promptly. They should be able to monitor data and logs with appropriate tools in order to satisfy the policies and demonstrate compliance (Cloud_Accountability_Project, 2016). Develop assurance methodologies to resolve problems between providers and consumers. Obtain assurance of the services in cloud by using vulnerability assessment and penetration testing approaches (Newcombe, 2012).

Actors: Consumer, Cloud Service Provider, Cloud Broker, Cloud Auditor.

Layers: SaaS, PaaS, IaaS

6.2.2 Transparency

Definition: Transparency is the condition where an entity can have full access and freedom to manage and control its own data in the cloud at any given time and allow feedback from the entities that accommodate it.

Stages: Identification, Preservation-Collection, Presentation.

Challenges: Access to evidence in logs, Dependence on CSP, Physical inaccessibility, Service Level Agreement, Volatile data, Imaging, Documentation, Compliance issues.

Solutions: CSPs should provide consumers with the freedom to handle and control their own computation and data according to their usage. Cloud providers should implement the obligations (organizational, technical and legal) in order to be transparent about their procedures and functions. Strong SLAs should be built between the parties, and contract agreements should be signed. On the other hand, trusted mechanisms should be implemented to help establish a better relationship between parties and increase mutual trust.

Actors: Consumer, Cloud Service Provider, Cloud Broker.

Layers: SaaS, PaaS, IaaS

6.2.3 Internal disciplinary procedures

Definition: Internal disciplinary procedure is the process through which a cloud provider or broker deals with its employees in order to ensure that its employees follow certain norms of discipline.

Stages: Identification, Preservation-Collection, Examination-Analysis.

Challenges: Internal staffing-Chain of custody, Integrity and stability-Multitenancy and privacy, Service Level Agreement.

Solutions: Frequent personnel surveillance to prevent turning rogue and intentional or accidental compromise consumers' data. Well-trained and accredited personnel to undertake the sensitive parts of the investigation. Access rights both on physical equipment and digital data. Enforce legal contracts in employee behavior policy. Access to critical equipment management is highly restricted.

Actors: Cloud Service Provider, Cloud Broker, Cloud Carrier.

Layers: SaaS, PaaS, IaaS

6.2.4 Access rights (policies)

Definition: Access rights is the permissions that are assigned by an administrator to grand users and applications access to specific operations. Security (data protection) mechanisms for authentication, authorization, access controls, and auditing should be considered in this concept.

Stages: Preservation-Collection, Examination-Analysis.

Challenges: Internal staffing-Chain of custody, Integrity and stability-Multitenancy and privacy, Time synchronization-Reconstruction, Identity.

Solutions: Use security checkpoints. Enforce stringent registration and validation process. Make sure important updates are installed on time in order for the system to be up-to-date. Prohibit user credential sharing among users, applications, and services.

Actors: Consumer, Cloud Service Provider.

Layers: SaaS, PaaS, IaaS

6.2.5 Isolation

Definition: Isolation is the mechanism to ensure that each consumers' data is sealed and cannot be seen by other tenants.

Stages: Preservation-Collection.

Challenges: Integrity and stability-Multitenancy and privacy.

Solutions: Separate data through partitioning. Ensure that memory, storage, and network access are isolated.

Actors: Cloud Service Provider.

Layers: SaaS, PaaS, IaaS

6.2.6 Legal matters (Regulatory)

Definition: Legal matters are the procedures and actions that need to be undertaken related to jurisdiction issues, international law, contractual terms, legislative frameworks and constitutional issues.

Stages: Identification, Preservation-Collection.

Challenges: Access to evidence in logs, Service Level Agreements, Multi-jurisdiction-Distribution-Collaboration.

Solutions: Global unity must be established. New regulations and international laws should be developed to secure forensic activities will not breach any laws or regulations under any jurisdiction. Accessing and handling data by third parties should be ensured and should be structured in a manner consistent with the provider's policies.

Actors: Cloud Service Provider, Cloud Broker.

Layers: SaaS, PaaS, IaaS

6.2.7 Traceability

Definition: Traceability is the ability, for the data to be traced or not by the user (Kalloniatis et al., 2014) and the capability of keeping track of the actions taken at any given point. It also refers to the ability to trace the activities of a consumer in order to lead to him/her.

Stages: Identification, Preservation-Collection, Examination-Analysis.

Challenges: Client side identification, Volatile data, Identity, Time synchronization-Reconstruction.

Solutions: Enterprises should track deployment options from the data center to the business process to make sure the value chain is uncompromised. Traceability through logs from the user's perspective involving the lifecycle of a file (creation to deletion). Track and store all the users' actions through logs. Data and client's traffic should be monitored at all times. Monitor Quality of Service (QoS) for SLAs regularly to determine any vulnerabilities. Users' activities and accounts should be monitored at all times in order to keep records with all transactions and link users to their logs. Their actions should be stored in the CSP's servers and should be kept ready to be processed by trusted personnel.

Actors: Consumer, Cloud Service Provider.

Layers: SaaS, PaaS, IaaS

Trust in the cloud is a very important notion and it could be identified as another forensic constraint besides the seven previously described. Trust is the customer's level of confidence in using the cloud. Due to the fact that trust is fulfilled through the identified forensic constraints it should be dealt in a holistic way and not be dealt independently. Implementing the forensic constraints and using them with cloud services automatically increases the customer's level of confidence. This in turn, making cloud forensic-enabled services, assists towards the implementation of trustworthy services.

These forensic constraints play a vital role in a cloud forensic process and investigation once they can make the investigator's work easier and less demanding. This can be achieved by including the identified forensic constraints in the design and implementation of cloud services. In order for a cloud service to be characterized as forensic-enabled, all the aforementioned seven cloud forensic constraints should be realized. If one of them is missing, the cloud service cannot be considered as forensic-enabled. The implementation of a service consists of numerous actions that need to be

carefully examined to prevent malicious activities. These actions can be implemented using one or more forensic constraints. On the other hand, one forensic constraint can be used to implement more than one action in a cloud service. For example, when we take under consideration the storage cloud service, the authorization access, which is part of the access rights forensic constraint, can be used in different activities.

6.3. Cloud forensic process patterns

For each forensic constraint identified in the previous section, a forensic process pattern is introduced and explained in the form of an activity diagram. Each forensic pattern contains activities and flows that implement a specific forensic constraint. In order to implement these constraints an activity diagram template is introduced, as shown in Figure 10. The template presents the activities that need to be undertaken in order to realize that service. In the case where an activity is not fulfilled, software engineers should seek and implement those techniques that solve the issue and make the service ready for use.

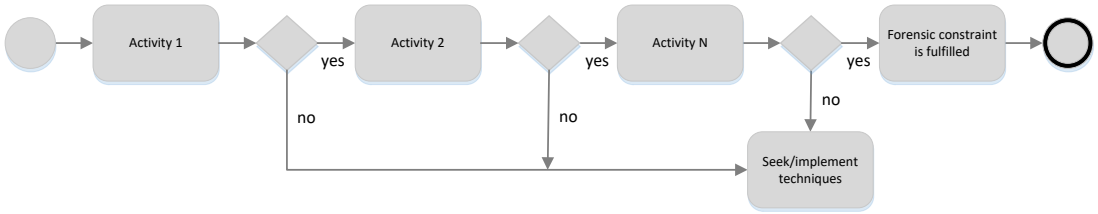


Figure 10. Template of forensic implementing activity diagram

The proposed patterns (following the activity diagram) describe the actions a cloud provider should produce/take in order to make a cloud service forensic-enabled. The forensic constraints focus on the cloud provider side since it is the entity that owns the infrastructures and provides the cloud services to consumers. The activities shown in each diagram refer to the cloud provider's activities, which they should be implemented, while in most cases, the defined order is not mandatory. Thus, the constraints and the patterns presented are executed on the provider's side. On the other hand, whenever a cloud service is implemented by a third party and a contract agreement is signed between the provider and the third party, it is the latter's obligation to comply with the forensic constraints and process patterns and implement techniques so as to make the cloud service forensic-enabled. The same applies for the cloud brokers or any other entity involved. The cloud provider is entitled to reject any third party that refuses to comply with the fulfillment of the forensic constraints and can seek for another party who is willing to do so. For instance, if a provider offers a service to a consumer ensuring there is no problem with jurisdictions, the third party the provider relies on, should also ensure that no issues will arise. Hence, strong SLAs should be built and signed between the parties stating all the necessary details.

The activity diagram for accountability constraint, shown in Figure 11, presents and describes the relevant activities needed to be undertaken to ensure that the constraint is fulfilled. Cloud providers should ensure that strong SLAs will be signed between third parties/consumers and on the other hand, policies and standards are put in practice. Assurance is obtained by providing security certification or validation exercise such as ISO 27001 certification and the results of a SAS70 Type II audit (Catteddu et al., 2013). All the actions undertaken by the provider, third parties and the consumers should be monitored so as to ensure that a prompt solution will be given in case of an incident. Attributability is provided in revealing which system element or actor is responsible in case of a deviation from the expected behavior (Catteddu et al., 2013). In the case that one or more of the previous actions/activities have not been fulfilled, the provider should seek or implement techniques that resolve the issues. The same applies for all the constraints.

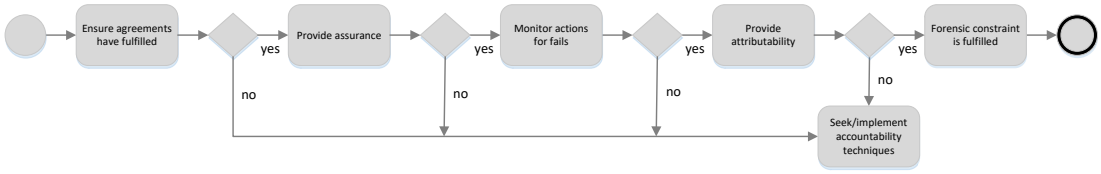


Figure 11. Accountability activity diagram

The transparency activity diagram in Figure 12, highlights three activities that should be implemented. CSPs need to ensure visibility of the applications by providing information about them at any time and inform consumers about the location/s of their data. They also need to notify the consumers about their procedures and policies on how the data is being treated and finally CSPs need to be transparent. Notifications about the policy violations should be used to notify consumers in case of an incident.

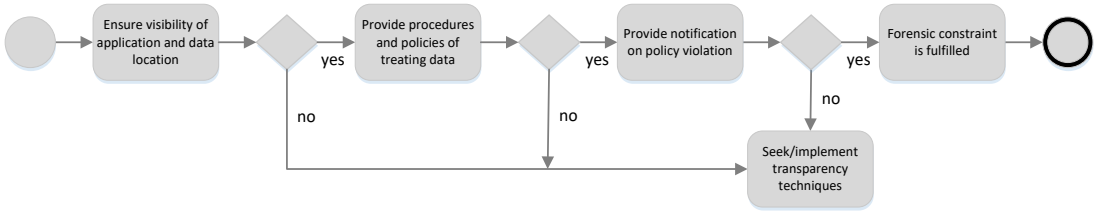


Figure 12. Transparency activity diagram

The steps a CSP needs to undertake to fulfill internal disciplinary procedures constraint are presented in Figure 13. Discipline rules need to be implemented and all the personnel should follow them. In case of any deviations, CSP should be able to discipline the responsible party without harming its interests. Access rights, both physical and digital should be categorized and their allowance should be granted accordingly. Contracts between the CSP and its personnel should be signed, stating all the details about misuse of information and the penalties.

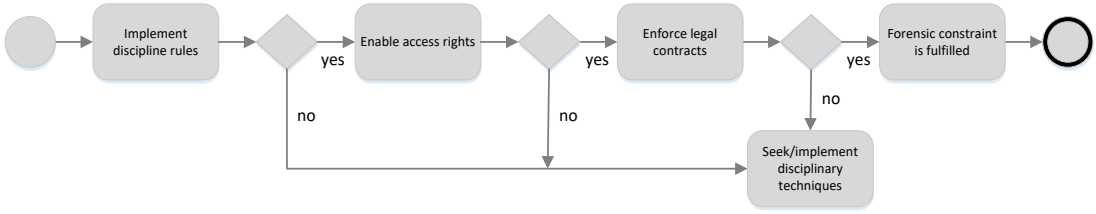


Figure 13. Internal disciplinary procedures activity diagram

The access rights activity diagram in Figure 14 shows the activities a CSP needs to implement to use the constraint. First, registration should provide all the necessary user's details and a control mechanism should validate the registration form to link as much information as possible with the user's true ID. Authentication and authorization control should be used to verify and determine the level of access of the users. Finally, access control should be implemented to enforce resources' required security.

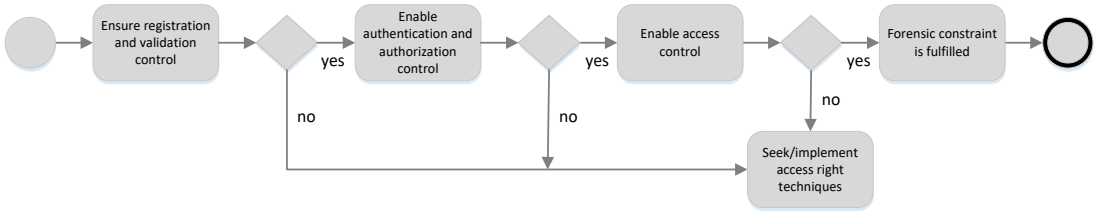


Figure 14. Access rights activity diagram

The isolation activity diagram in Figure 15 ensures that a user does not have the right to access other users' data and that the data is securely stored. User's virtual machines are separated from the rest of the VMs and in case of an incident, contamination of other users is prevented. Privacy and confidentiality should be maintained at all times in such multi-tenant environment.

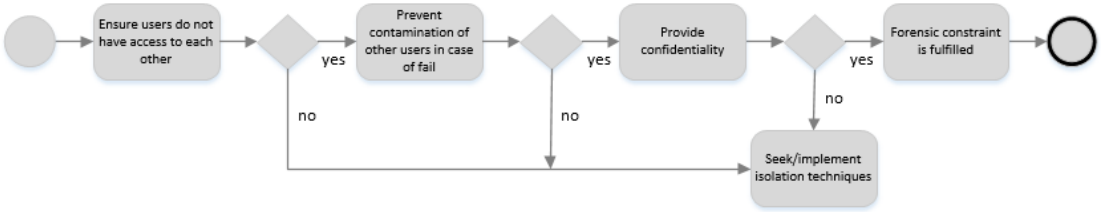


Figure 15. Isolation activity diagram

Legal matters activity diagram in Figure 16 is of vital importance since it is the most difficult to implement with all the different people, countries and laws involved. First, a strong and detailed SLA should be presented to ensure the terms of using cloud infrastructures. Then, ensure that a consumer's data should remain within the geographical boundaries of the country the user belongs to, remain under the same jurisdiction and also ensure that the consumer's data will not be distributed around the world. Finally, CSPs should hire and maintain specialized personnel on domestic/international laws and legislations related to cloud computing and data

handling. The personnel should be trained on a regular basis to be brought up-to-date with new technologies.

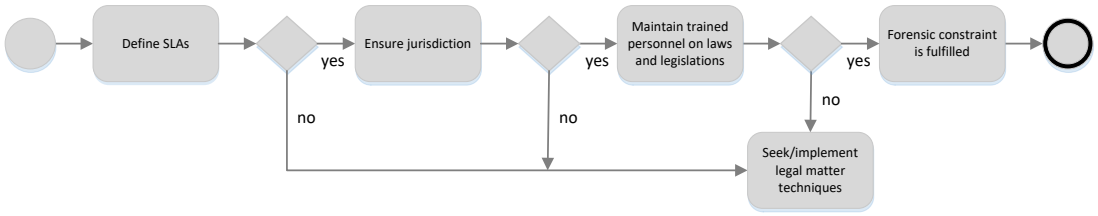


Figure 16. Legal matters activity diagram

Traceability activity diagram in Figure 17 concerns users and their data. Monitoring users' actions is important in order to reveal any faults. On the other hand, monitoring data logs and taking regular backups can reduce time and effort that is required to resolve malicious incidents. All logs should be stored and secured in places with limited access. The CSP should implement procedures to link data logs with a specific user and his/her activities.

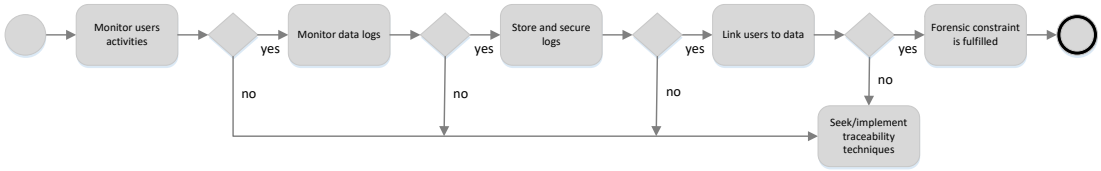


Figure 17. Traceability activity diagram

Each cloud forensic process pattern introduces a set of activities that need to be satisfied in order to implement a forensic constraint. All the activities should be applied to implement the forensic constraint, in any other case the forensic constraint cannot meet the forensic standards. These seven activity diagrams will be used later, in the framework process, to match the activities of the cloud services' activity diagrams with the activities of the process patterns. In this case if a cloud service activity diagram includes the process pattern activities then the service could be defined as forensic-enabled. As mentioned in the previous section, all the aforementioned seven cloud forensic constraints should be applied on a cloud service in order to be forensic-enabled. The forensic constraints process pattern is illustrated in Figure 18 in the form of an activity diagram.

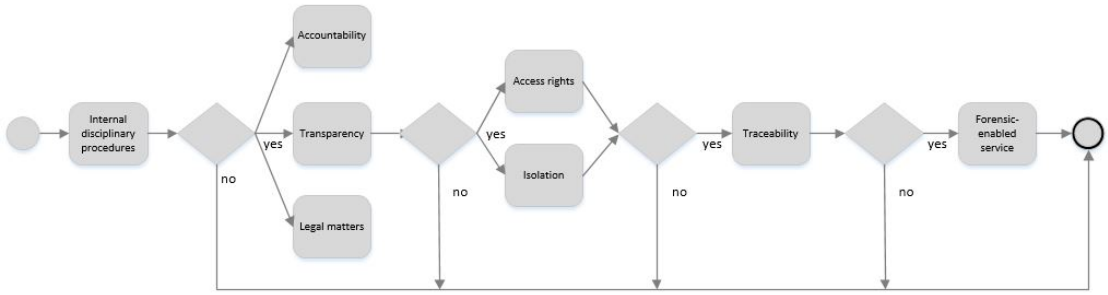


Figure 18. Forensic constraints activity diagram

The seven forensic constraints described in this section can be divided into four sequential categories. The first one is the *preliminary procedures* and includes the internal disciplinary procedures constraint. This constraint should be implemented before all others, since companies need to establish and implement strong disciplinary procedures for internal usage. The second category is the *organizational agreements*, where the three forensic constraints of accountability, transparency and legal matters are included. This category deals with the agreements need to be signed and clarified between the provider and the clients or third parties. The next category is the *implement technical procedures*. This one includes two forensic constraints, the access rights and the isolation. The specific forensic constraints need to be implemented after the contracts are signed between the parties in order to know by which terms they will be implemented. Finally, the fourth category is the *monitoring*, in which the traceability forensic constraint is included. This is the last constraint in sequence that needs to be established since monitoring occurs after the implementation of the whole system or service. The four sequential categories are illustrated in Figure 19 in the form of an activity diagram. The proposed sequence is mandatory to follow and provides an important guidance to software engineers regarding the successful realization of the proposed constraints in the organizational processes.

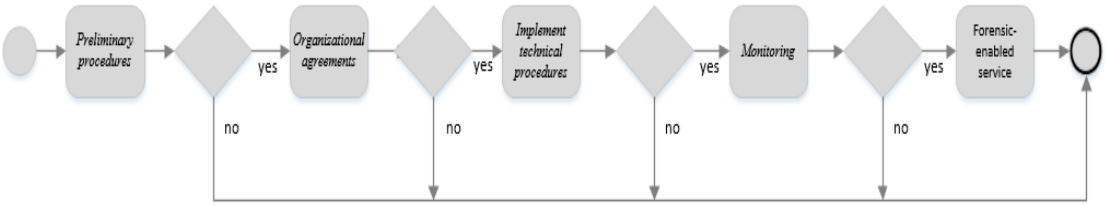


Figure 19. Sequential categories activity diagram

The activities used for each one of the proposed process patterns provide a generic approach for the fulfillment of the constraints. In this case, the constraints can also be applied in various cloud environments providing the proper level of technicality without being narrowed in one specific field.

6.4. Framework modelling language

The use of cloud computing for storing sensitive data raises concerns about the forensic investigation process in case of an incident. Forensic investigation in cloud computing requires a different approach from the traditional forensic process. This approach should take under consideration not only the technical, organizational and legal aspects but also the software engineer's requirements and the investigators' perspective. In order to produce a requirements engineering framework to support the elicitation and modeling of the aforementioned forensic constraints, a common modelling language is introduced. The modelling language is presented in terms of a meta-model, based on the concepts and the forensic constraints identified for designing a cloud forensic-enabled system. The meta-model presented in this dissertation not only includes the concepts that make a system forensic-enabled but also the concepts for a cloud forensic investigation process from my previous work (Simou et al., 2016c). In this way, an integrated meta-model is produced to assist designers in creating cloud forensic-enabled services considering the respective investigation requirements in the case of an incident.

Taking under consideration the forensic constraints identified, we proceed in identifying the concepts from the software engineer's perspective in order to develop a cloud forensic-enabled meta-model. The model illustrated in Figure 20 shows the relationships among critical components through the modelling language. The meta-model is based both on the concepts that make a system forensic-enabled and the concepts that form a cloud forensic investigation process. In the model, the two different groups of concepts are clearly defined and separated from each other since they are used differently in the cloud forensics. On the other hand, some concepts that form the two groups are related to each other, thus the relationships between them must be clarified.

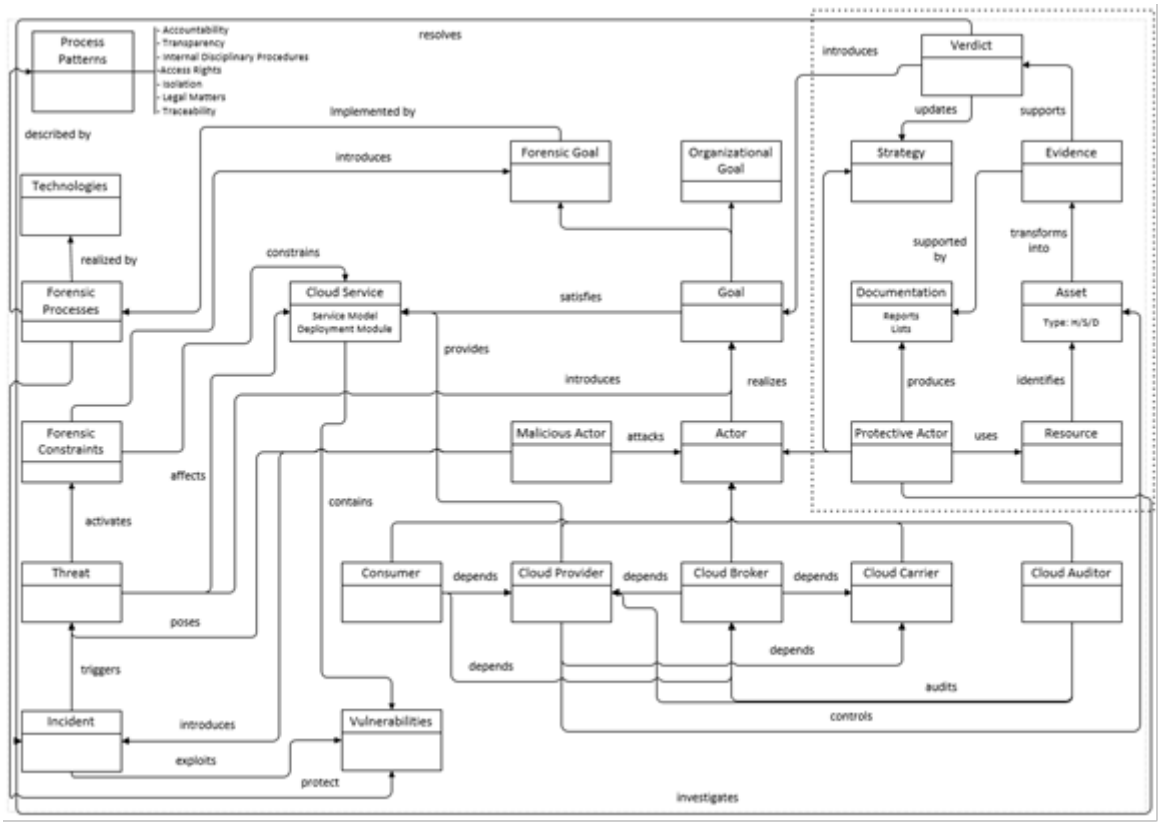


Figure 20**.** Meta-model for assisting a Cloud Forensics Process

The first group (located in the main area of the meta-model) shows the concepts related to a cloud forensic-enabled service. The second group (located on the upper right corner of the meta-model, framed with dots) shows the concepts related to the investigation of an incident. The two groups have a common goal; the design of cloud forensic-enabled services in order for the investigators to solve an incident in a forensically sound manner. Once the process of making a system forensic-enabled is implemented and the cloud forensic investigation process is developed, then, protective actors just need to follow the respective steps.

As it is illustrated in Figure 20, the notion of the metal-model revolves the "*cloud service*" concept. In the next paragraphs, a detailed presentation of the two groups of concepts is introduced describing all the aspects that will assist software engineers in designing a cloud forensic-enabled system/service and investigators to solve an incident in a forensically sound manner.

6.4.1. Concepts related to cloud forensic-enabled system

As mentioned earlier in the previous sections, there are two different groups of concepts concerning the cloud forensic process. The first group assists software engineers in designing and implementing trustworthy cloud services. It describes all those concepts a designer needs to include in his/her design to produce a forensic-enabled service. The list of the concepts is as follows:

Actor: According to NIST (Liu et al., 2011) the actors involved in the cloud are: consumers, providers, auditors, brokers and carriers. The definitions given for the 5 actors are as follows:

Cloud Consumer: "*Person or organization that maintains a business relationship with, and uses service from Cloud Providers*" (Liu et al., 2011). A consumer can be any person that uses the cloud either as a common user or as a malicious user. The malicious actor is the one who introduces an incident and he/she is responsible for attacking any other actor involved in the cloud. He/she uses CSPs' services to launch his/her attacks exploiting vulnerabilities hidden behind anonymity. Consumers have dependencies on both cloud providers and cloud brokers.

Cloud Service Provider: "*Person, organization or entity responsible for making a service available to interested parties*" (Liu et al., 2011). CSPs are responsible for offering multiple services to consumers through their deployment modules and service models. Their major concern is to rent as many services to clients as possible. Their services should be supplied with responsibility and reliability according to service level agreements signed between actors. CSPs depend mostly on cloud carriers.

Cloud Broker: "*An entity that manages the use, performance and delivery of cloud services and negotiates relationships between Cloud Providers and Cloud Consumers*" (Liu et al., 2011). The broker helps the consumer find the suitable cloud providers and negotiate contracts with them. The brokers' main dependencies are on CSPs and cloud carriers.

Cloud Carrier: "*An intermediary that provides connectivity and transport of cloud services between Cloud Providers and Cloud Consumers*" (Liu et al., 2011). Cloud carriers are mostly traditional telecommunication providers responsible for delivering cloud services over their own network and other access devices. The carrier's main objective is to provide CSPs with secure and dedicated connections through service level agreements. In some cases, a cloud carrier can play the role of cloud provider at the same time.

Cloud Auditor: "*A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation*" (Liu et al., 2011). Auditors are responsible for evaluating cloud providers' and brokers' services by performing audits in order to verify if their performance and security mechanisms are acceptable to the consumers.

Goal: The concept of the goal introduced in this model focuses on the realization and achievement of specific objectives, such as the way the system is designed, implemented, and operated. A goal can be either organizational or forensic. "*Organizational goals express the main organization objectives that need to be satisfied by the system into consideration*" (Kavakli et al., 2006). Forensic goals are generated by forensic constraints. In cloud computing, when system engineers develop a service, they need to realize different forensic goals in order to make the service forensic-enabled. These forensic goals are being introduced by specific forensic constraints and are implemented within the use of forensic processes (explained in the next paragraphs). A goal or a number of them can satisfy a cloud service.

Cloud service: A cloud service is any resource made available to users over the Internet. Cloud Service Providers are responsible to provide those services through service models (IaaS, PaaS, and SaaS) and deployment models (public, private, hybrid, and community). Attackers exploit vulnerable services, thus is the most important asset along with the respective resources providing this asset.

Vulnerabilities: A vulnerability is a weakness in design, implementation or operation of a system/service that allows malicious actors to exploit the system/service, and create an incident in order to take control, breach, or violate the system/service. Cloud services may have one or more vulnerabilities that may compromise the integrity or privacy and security of the service. In order to be able to design forensic-enabled services and mitigate the respective vulnerabilities appropriate forensic processes need to be implemented.

Incident: "*A breach of security or a loss of integrity that has impact on the operation of network and information system core services, which public administrations and market operators provide*" (ENISA, 2013). The malicious actor is responsible for introducing an incident in order to exploit vulnerabilities of cloud services. On the other hand, the incident triggers threats for the system. Protective mechanisms should be implemented based on previous incidents to assist software engineers to develop forensic-enabled services.

Threat: A threat is an action that might cause harm to a system/service. Malicious actors pose threats to a system/service and these threats are triggered by their incident. Depending on the type of threat, specific forensic constraints are activated to deal with them. The threat aims to affect cloud services in order to gain control of specific assets.

Forensic constraints: Forensic constraints are non-functional requirements that relate to a system's/service's ability to be forensic-enabled and specify the system's or service's quality attributes. Forensic constraints identified and presented in the previous section allow software engineers to develop forensic-enabled systems/services; systems/services whose architecture supports forensic investigation. The forensic constraints should be applied to cloud services in accordance to the criticality of the service so as to guarantee the forensics. These constraints are being activated by the threats triggered by an incident and their main objective is to introduce and produce forensic goals.

Forensic processes: A forensic process is a mechanism, which handles evidence in a forensically sound manner, on one hand and on the other, determines what the vulnerabilities of the system/service are, so as to protect the system/service and meet the forensic goals introduced by forensic constraints. After identifying the potential vulnerabilities of the system/service, the most appropriate forensic process to attend to the specific vulnerability will be selected to eliminate the threat and make the service forensic-enabled. Forensic processes are realized with the help of technologies and described by forensic process patterns.

Technologies: Technologies are these techniques and solutions used to handle digital evidence (identify, collect, preserve, analyze and present) and achieve protection in cloud systems. Techniques such as registration and validation that allow us to have accurate information about users, or logging and monitoring mechanisms that provide us information at all-time about users' activities. These procedures will be automatically performed to eliminate potential threats.

6.4.2. Concepts related to cloud investigation

The second group of concepts provides Law Enforcement Agents with the ability to understand all those concepts that are involved in a cloud forensic investigation and the importance of their roles. This is of vital importance since the cloud forensic-enabled service should be designed in a manner that the identified information will assist the investigator when an incident occurs. Thus, the concepts describing the proposed meta-model should be able to collaborate with the information required during an investigation. A detailed presentation of the list of the concepts related to the investigation process that is considered in the proposed meta-model is described in section 5.2 of Chapter 5.

The two groups of concepts shown in the meta-model interact with each other in order to produce a meta-model that presents a holistic solution to the cloud forensic investigation problem. This could be achieved by implementing (the software engineers) cloud forensic-enabled services to assist investigators with cyber-crimes. Table 1 presents an instantiation of all the concepts used in the meta-model. This instantiation assigns a value to each one of the concepts. The scenario where the instantiation is based is the following:

An executive member (consumer) of an organization stores sensitive data in the cloud using Microsoft Azure as a CSP. A malicious actor who uses the same provider exploits vulnerability in the system and steals the data from the consumer. LEAs have been called to trace and find the malicious actor in a forensically sound manner.

Table 6**.** Instantiation of concepts

Concepts	Instantiation of concepts
Malicious Actor	A user who wants to steal information
Consumer	Member of the Organization
Cloud Provider	Microsoft Azure
Cloud Broker	Netskope
Cloud Carrier	AT&T
Cloud Auditor	StarAudit
Goal	Provide storage capabilities to organization's members
Cloud Service	Data storage platform in cloud
Vulnerabilities	Failure to provide isolated storage service to consumers
Incident	Sensitive data have been stolen from consumer
Threat	Data Leakage

Forensic Constraint	Traceability
Forensic Processes	Store data in the cloud providing monitoring capabilities
Technologies	Data and operation logs tracing
Protective Actor	Law Enforcement Agents
Resources	Forensic tools, LEA's and CSP's personnel
Assets	Card payment information, CSP's subscriber id, logs, virtual machine and storage data, usernames and passwords
Evidence	IP address, username and password, logs
Documentation	Action plan report, methodology report, resource report, assets report, evidence report
Strategy	LEA acquires evidence through monitoring and snapshots
Verdict	Strong evidence brought a conviction

6.5. Framework process

The next step to the completion of the framework is to develop a process based on the concepts identified and presented in the meta-model. The process should be in accordance with the organization's needs. (Kokolakis et al., 2000) examined the role of business process modelling (BPM) techniques in Information Systems security analysis and design (IS-SAD) and presented a generic framework for IS-SAD. They stated that the BPM technique should support tasks such as:

- *analyze the organization*
- *select the systems to be examined*
- *identify and analyze threats and vulnerabilities*
- *identify and evaluate entities that need protection*
- *design secure processes*
- *assess countermeasures' effectiveness and efficiency*
- *develop a security policy*

The tasks listed in the previous paragraph have been considered and they can be used as a preliminary step in order to implement the process. The process itself provides the necessary steps towards a cloud forensic-enabled system/service based on the potential vulnerabilities of the system/service and the systematic analysis of forensic requirements. On one hand, it assists in the identification of the organizational strategy and needs and on the other, it analyzes in depth the various organizational cloud services in order to provide the necessary requirements for well-structured cloud forensic-enabled services. The process consists of three main stages: *Organizational Analysis, Cloud Forensic Requirements Analysis,* and *Evaluation-Assessment*. Figure 21. Forensic requirements engineering process for cloud forensic-enabled services illustrates the proposed process with its stages, steps, inputs and outputs.

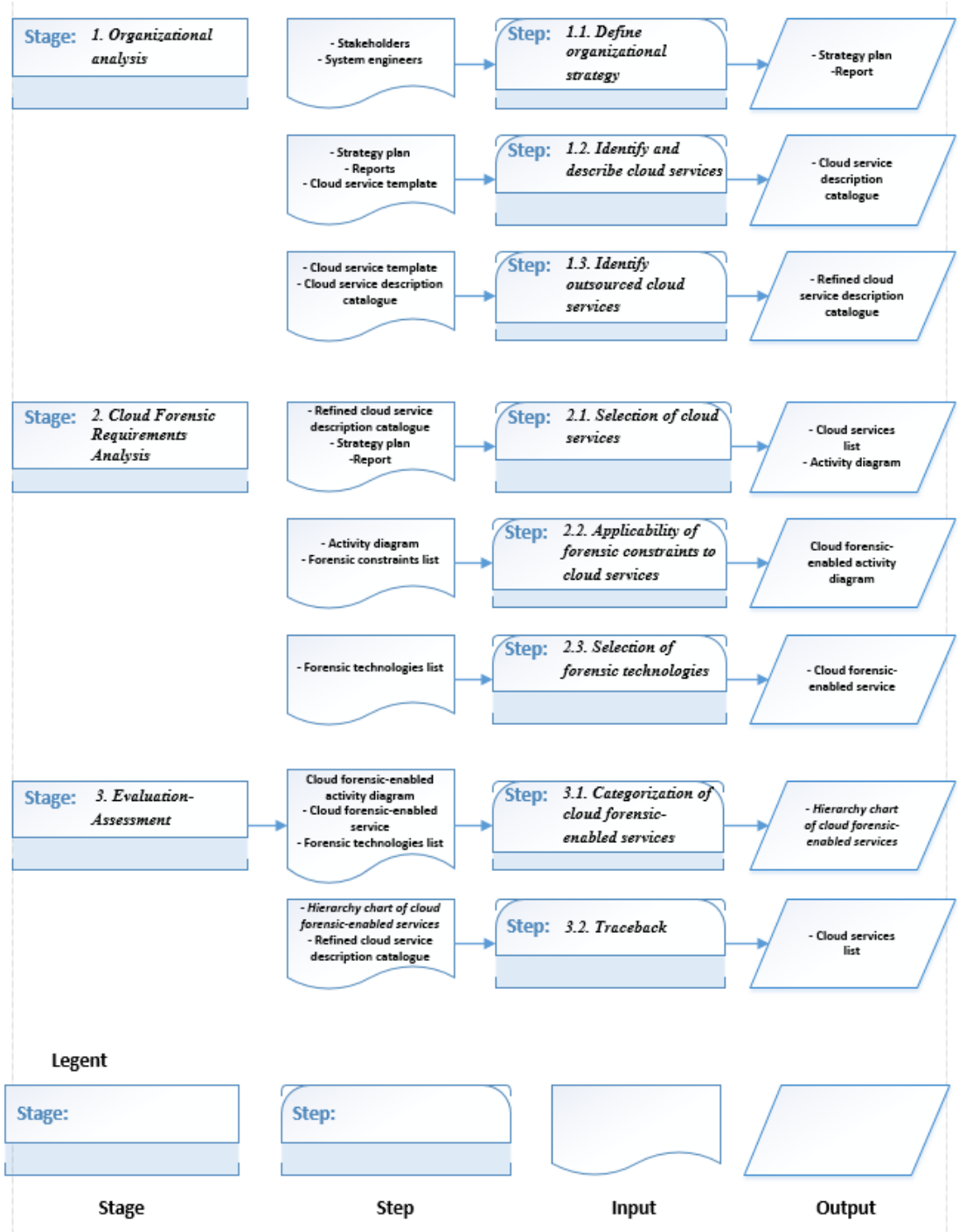


Figure 21. Forensic requirements engineering process for cloud forensic-enabled services

6.5.1. Organizational analysis

The first stage of the proposed process focuses on the presentation of the organization's goals and policies and in parallel produces an illustrated map (full description) of all cloud services the organization provides. This map assists the system analyst who is responsible for the migration of one service/system to the cloud, to identify and explore

the needs, goals and structure of the organization in order to develop and implement the new system/service. This stage consists of three different steps.

6.5.1.1. Define organizational strategy

The first step of the process is to define organizational strategy, the actions a company intends to take in order to achieve its goals. The scope of this action is to be competent and reliable in the market. It is of vital importance to assess and evaluate not only the organizational goals in order to set the organizational needs, but also the consequences in the case those goals are not met. In order to design and implement a system, analysts should be fully aware of the structure of the organization itself. Organizational entities such as actors, goals, assets/infrastructure, resources, strategy and services should be identified and defined. Actors responsible for the system and goal setting should present their requirements and clarify all the aspects that will fulfill their needs. Stakeholders and software engineers need to implement a strategy plan about their cloud services to make them more competitive by producing cloud forensic-enabled services. They have to compare current circumstances with overall objectives to develop services that need improvement later in the process. On the other hand, the system analyst responsible for the migration of the system should be capable of understanding organizational strategy and needs to accomplish and develop a realistic plan. The output of this step is a report describing the organizational strategy on the aforementioned pillars.

6.5.1.2. Identify and describe cloud services

During the next step of the process all cloud services provided to consumers should be presented and analyzed in order to understand the operation of the system. The presentation of cloud services should be thorough and a full analysis of each service should be provided separately. This analysis will contain the name of the service, a description, the deployment and the service model, which is applied to, goal objectives, storage needs, third parties, and all the aspects that an analyst needs to know about the nature of every cloud service. For the analysis of every service, a cloud service template will be used as input with all the necessary fields as shown in Figure 22. This action will assist the analyst to develop a global view of the infrastructures of the organization before the new set of requirements is designed and approved. The output of this step is the development of a description catalogue for each cloud service the organization provides.

Cloud Service Template	
Service Name:	Deployment Model:
Description:	Service Model:
Goal:	
Process:	
Actors involved:	Human Resources:
Hardware Needs:	
Outsourced: ☐	Company Name:
Comments:	

Figure 22. Cloud Service Template

6.5.1.3. Identify outsourced cloud services

The third step of this stage covers the outsourced cloud services that an organization might have. Third parties such as cloud providers, brokers, etc. provide a number of cloud services to organizations to support their needs both on a technological and infrastructural point of view. Some of them are specialized in a specific area, making them more competitive in the market. The pattern followed is the same as in the previous step. Contracts and service level agreements signed between the organization and third parties will be reviewed and used together with the description catalogue from the previous step to record all the necessary information for the outsourced cloud services. The output of this step is the development of a new refined description catalogue for each outsourced cloud service.

6.5.2. Cloud forensic requirements analysis

The next stage in the proposed process is the cloud forensic requirements analysis, which aims, first to identify the cloud services that an organization is willing to make forensic-enabled, and second to apply forensic constraints and technologies in order to

do so. This step is concentrating on the organization's services that need to be forensic-enabled once they are given for public use in the cloud. It is an important stage and relies mostly on a well-structured design of the operation of each cloud service. Once the design of cloud services is developed and forensic constraints and technologies are applied, the organization has a full picture of the forensic requirements of each cloud service. This stage consists of three different stages.

6.5.2.1. Selection of cloud services

This step involves the selection of specific cloud services identified from the previous stage. The organization's stakeholders and software engineers together with the analyst will proceed to the selection of those cloud services that will be implemented in order to become forensic-enabled. This selection should be carried out in relation to the organizational strategy and goals defined earlier in the process. There will be a prioritization of cloud services depending on their importance to organization and a list with those services will be produced. This action can also involve the selection of the entire set of cloud services depending on the organization's budget, resources, etc. After the selection of cloud services, an activity diagram for each service will be generated, illustrating all the activities, actions and dependencies of the service. This diagram will assist the analyst to reason about the degree of forensicability of the service based on the forensic related activities existing in the implementation of the service.

6.5.2.2. Applicability of forensic constraints to cloud services

Within this step, it is important to capture the vulnerabilities and threats of each cloud service the organization wants to implement as forensic-enabled and apply the identified forensic constraints. The activity diagram from the previous step will be used as input and the forensic constraints will be applied on the activities of the diagram in order to investigate the impact they produce. The activities should be thoroughly examined so as to pinpoint which one of them needs to be modified. This is the point where forensic constraints need to be placed to make the activities of the service forensic-enabled. We have to take into account that the organization's software engineers may have already implemented some of the forensic constraints in order to make cloud service reliable and secure for public use. Nevertheless, if some forensic constraints are missing, the cloud service cannot be characterized as cloud forensic-enabled. The output of this step is a refined activity diagram with all forensic constraints identified and illustrated.

6.5.2.3. Selection of forensic technologies

This step aims to identify and apply technologies that support the implementation of the forensic process. A number of technologies have been identified in the literature to support forensic requirements. The selection of the technology, which will be used, depends on a number of factors such as the actors involved, the resources and the

technical complexity. From the actors' perspective, it involves mainly the forensic engineers that will implement the technologies and the stakeholders. As far as the resources are regarded, they depend on the organization's financial capability. From a technical perspective, there are specific steps that need to be followed:

- The Cloud Service Template is used as input to identify two important aspects: the deployment model that the cloud service is applied to and its service model. These two characteristics can help forensic engineers to select only the technologies that concern the specific characteristics excluding the ones that are not applicable.
- The cloud forensic-enabled activity diagram for each cloud service is taken as input to observe the number of the forensic constraints that are not satisfied and they need to implement. The suggested technologies concern only the forensic constraints that are not satisfied.

Figure 23 illustrates the necessary steps that need to be taken in order to identify and select the technologies for the implementation of forensic constraints. When technologies are applied to activity diagrams, a new service is implemented which is cloud forensic-enabled and ready to support a cloud forensic investigation.

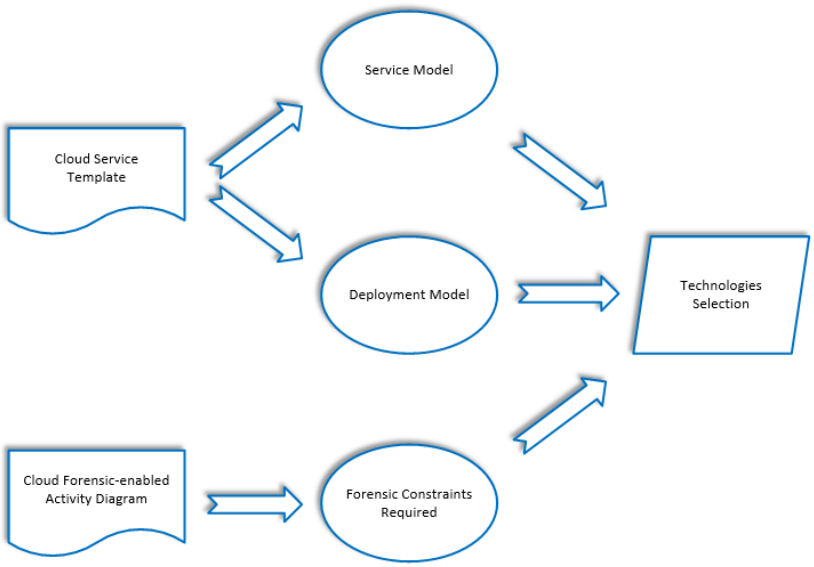


Figure 23. Important steps for the selection of technologies

For suggesting the adequate technologies per forensic constraint taking as input the deployment model, the service model and the missing forensic-related constraints, a list of possible solutions that categorize the existing solutions based on these criteria have been grouped (Simou et al., 2016a). A snapshot of this table is shown in Table 7. The specific categorization is very important and can assist us on automating the suggestion of respective technical solutions based on the aforementioned criteria.

Table 7. Snapshot of a list of possible solutions

Cloud Forensic Challenges	Solution	Private	Public	IaaS	PaaS	SaaS
Access to evidence in logs	Secure-Logging-as-a-service (SecLaas) mechanism	√	√	√	√	√
	Status data extraction and checking	√	√	-	√	-
	Log management architecture	-	√	-	-	√
	Logging mechanism	√	√	-	√	-
	Log-based model	√	√	-	√	√
	Digital forensic readiness model	√	√	√	√	√
	Management plane	-	√	√	-	-
	Logging framework	√	√	√	√	√
	Eucalyptus framework	√	√	√	-	-
Dependence on CSP - Trust	Accountable cloud	√	√	√	√	√
	TrustCloud framework	√	√	√	√	√
	Eucalyptus framework	√	√	√	-	-
	Trusted Third Party (TTP)	-	√	√	√	√
	Layers of trust model	-	√	√	-	-
Service Level Agreement (SLA)	Well and clear-written terms	√	√	√	√	√
	External auditors	√	√	√	√	√
	Service guarantee, violation detection, credit and standardization	-	√	√	√	√
	Trusted timestamping	√	√	√	√	√
	QoS and SLA model	-	√	√	√	√
Integrity & stability - Privacy & multi-tenancy	Digital signature	√	√	√	√	√
	Trusted Platform Module (TPM)	√	√	√	√	√
	Digital forensic readiness model	√	√	√	√	√
	Distributed signature detection framework	√	√	√	√	√
	Multi-tenancy model	√	√	-	-	√
	Proofs Of Retrievability (PORs)	√	√	√	√	√
	Data entanglement approach	√	√	√	√	√
	Entangled encoding scheme	-	√	√	√	√
	Trusted Cloud Computing Platform (TCCP)	√	√	√	-	-
	Secure role-based access control	√	√	√	√	√
	Identity and access management in future internet architecture (IAMFI)	√	√	√	√	√
	Data access control for multi-authority cloud storage (DAC-MACS)	√	√	√	√	√
	Provenance system	√	√	√	√	√

6.5.3. Evaluation - Assessment

The last stage of the process is the evaluation-assessment of cloud forensic-enabled services. During this stage, stakeholders decide which of the cloud services will be implemented according to their strategy and budget. A thorough study of the results produced in the previous stages is taking place and an assessment of the organization strategy is re-evaluated. The stage consists of two steps.

6.5.3.1. Categorization of cloud forensic-enabled services

After the development of the refined activity diagram and the selection of appropriate technologies per selected cloud service, a hierarchy chart of cloud forensic-enabled services is produced in order for the stakeholders and the software analysts to reason

about the services that will finally be implemented in a foresicable way. This list illustrates the number of forensic constraints that are missing from a cloud service and the technologies that can be applied to in order for the service to become forensic-enabled. As mentioned earlier in the process, not all forensic constraints have applicability to a service since some of them may have already been implemented by the organization. A categorization can be produced to present the most costly cloud services; depending on how many constraints need to be implemented. According to this categorization, stakeholders can be aware of the cost of cloud forensic-enabled services and decide in accordance.

6.5.3.2. Evaluation - Trace-back

The last step of the process concerns the assessment of the cloud services. After the hierarchy chart is produced an assessment takes place, where stakeholders evaluate if the chosen cloud services, which they intend to make forensic-enabled, can be implemented. If the evaluation is negative (for example the budget cannot support the implementation of the chosen cloud services), stakeholders may need to re-consider their strategy or may exclude a number of services of the implementation process. On the other hand, if the evaluation is positive (the budget allows the migration of more cloud services), stakeholders can go back to stage 2 and perform the cloud forensic requirements analysis to new services that they are willing to make forensic-enabled. This step is not mandatory and depends on the stakeholders' strategy.

6.5.4. Validation of the process

The research method employed in this thesis is based in the Design Science Research Methodology (DSRM), created by (Peffers et al., 2007). In particular, it follows "*the six activities that make up the DSRM as a nominal sequence*" (Geerts, 2011):144. According to the Peffers et al. model, a problem statement was defined based on the identified gap in current research (activity 1), a literature review was conducted in order to find new ideas and solutions (activity 2), and a prototype was designed and developed to address the gap that existed in designing cloud forensic-enabled services (activity 3). The applicability of the proposed framework was demonstrated through a case study involving a provider (activity 4), and its application on two different cloud services was evaluated (activity 5). Finally, a paper reporting the first stages of the framework was published in the TrustBus 2017 international conference, while further publications of the framework are underway (activity 6).

Based on the Peffers et al. methodology, (Gregor and Hevner, 2013) presented the DSR knowledge contribution framework, where the type of contribution is placed on four distinct quadrants. The four quadrants are the as follow:

- Invention, where new solutions for new problems are invented.
- Improvement, where new solutions for existing problems are developed.
- Exaptation, where existing solutions to new problems are extended.

- Routine design, where existing solutions to existing problems are applied.

The proposed process concerning the CFeS framework belongs in the "Improvement" quadrant since the solutions that have been proposed in the context of digital forensics are evolved. On the other hand, this work moves a step forward by suggesting and providing new solutions in the cloud forensics. In this way, new boundaries are set to assist and define the specific field; hence, the proposed work also belongs in the "Invention" quadrant. The proposed CFeS framework is a new idea and "little understanding of the problem context exists" (Gregor and Hevner, 2013):346. It is an innovative work that defines new research questions and verifies the value of the solutions.

Table 8 illustrates the different DSRM activities, as they were applied in the context of this research along with the main results of each activity. The extra (fourth) column addresses the steps of the proposed process in the DSRM.

Table 8. DSRM applied to CFeS Framework

DSRM activities	***Activity description***	***Results***	***Addressed in the proposed process***
Problem identification and motivation	There is a gap on development a framework that can assist software engineers to design cloud services in a forensic sound manner	Literature review. Understanding the current solutions and their weaknesses	Define organizational strategy. Identify cloud services (local and outsourced)
Define the objectives of a solution	Design cloud services that are able to support cloud forensic investigations	Literature review. Knowledge of emerging technologies, security and privacy requirements	Selection of cloud services (Chapter 6.5.1, pp. 89-91)
Design and development	Design and implementation of the CFeS Framework: Cloud Forensic-enabled Services Framework	Introduce forensic requirements (constraints). CFeS Framework	Development of activity diagrams (Chapter 6.5.2, pp. 91-92)
Demonstration	A case study demonstration using different services	Applying forensic requirements and CFeS to a real-world problem	Applicability of forensic constraints to cloud services (Chapter 7). Selection of forensic technologies in

			accordance to Table 9 (Chapter 7.1.2.3, pp. 104-106)
Evaluation	The CFeS Framework met the project's objectives	Understanding the current solution and its weaknesses	The two services became forensic-enabled by signing contracts between the parties and performing specific actions (Chapter 7.1.3, p.106)
Communication	Published in the TrustBus 2017. To be published in a journal.	Understanding the forensic requirements and the need to design cloud forensic-enabled services	

Chapter 7

Framework Applicability

7.1. The University of the Aegean case study

For examining the applicability of the proposed framework a real case study is used. The framework was applied on the University of the Aegean (UoA) case study. It regards the UoA's transformation of cloud services in order to make these services cloud forensic-enabled. All the steps of the proposed process have been followed to check its applicability.

7.1.1. Stage 1: Organizational analysis

The first stage of the proposed framework is to identify and illustrate the organizational goals and the organization's cloud services. The main activity of the University is to introduce new approaches in higher education in Greece and worldwide and to promote regional development. Due to the fact that the UoA is located on 6 different islands in the Aegean Archipelagos, from its early days it has developed a modern network of IT infrastructures and services. The IT department constantly upgrades both its infrastructures and services and integrates the evolving technology of computer science. The UoA's objective is to bring the new technologies closer to education, research, and administration. A number of cloud services is provided to the academic community, such as e-mail services, web hosting, file storage, nextcloud etc. The UoA is equipped with a new technology data center (IBM) consisting of 22 blades (each one is equipped with 41,58 GHz processors, 256GB RAM) and it is managed by the VMware vSphere ESXi. It also uses IBM's Storwize V7000 for data storage with a capacity of 122TB. The UoA's goal for the following year is to provide the academic community with new and more efficient services by increasing its storage capacity. Both data center and storage are supported by a tape library, which takes backup of the systems on a daily basis. Databases, applications and software are accommodated in the Virtual Machines (VM) of the data center and the equipment is connected to a manageable IBM switch. The people responsible for managing the above equipment are the people who work in the central IT department of the UoA.

7.1.1.1. Define organizational strategy

The main objective of the UoA's administration is to provide high quality research and education to the academic community. In order to achieve this (from a technical point of view) computer equipment needs to be updated on a regular basis and the services provided to the community need to be efficient and at the edge of technology. The infrastructure is constantly updated and the community is brought closer by using reliable services with fast connections. To support the venture, the UoA nodes (islands) are connected with each other through links with transmission speed of at least 1 Gbit

(expandable to 10Gbit). To accomplish its objectives and bring new and reliable services to the academic community the UoA's strategy is to have a powerful IT department and infrastructures as described in the organizational analysis. Experienced personnel on information technology have been hired to manage the network and develop the services. Since the cloud is the technology used by most people nowadays, the UoA seeks and implements cloud services for the academic community. A report is produced describing UoA's IT architecture and the network connections between the nodes (islands). The report also includes the university's strategy related to the new information technologies. The actors involved in the process are the IT staff, the administration, teaching staff, students and some organizations that are using services for web hosting.

7.1.1.2. Identify and describe cloud services

The second step of the first activity is to identify the cloud services provided to the academic community. The cloud services related to the University are as follows:

- Virtual Machines
- E-mail
- Web hosting
- File storage
- Nextcloud storage

For each service identified, a service cloud template is used to illustrate and describe all the aspects of the service. The output of this step is a cloud service description catalogue with all the necessary information. For the sake of the case study two specific services have been chosen to be thoroughly described, virtual machines and nextcloud storage. These two services will also be used to demonstrate the cloud forensic requirements analysis in stage 2. The results are highlighted in Figure 24 and Figure 25.

Cloud Service: 01	
Service Name: **Virtual Machines**	Deployment Model: **Private Cloud**
Description: **Create and deploy virtual machines**	Service Model: **IaaS**
Goal: **Provide hardware resources to academic community to implement their research or academic interests**	
Process: **Virtual Machines**	
Actors involved: **IT department, Academic community**	Human Resources: **3**
Hardware Needs: **At least 4GHz, 4GB RAM, 150GB HD for each VM**	
Outsourced: ☐	Company Name:
Comments:	
In order to use the service, the person requests it should be a member of UoA's academic community. VMs are isolated and the access is made through hypervisor. When a VM is created it resides on a specific VLAN. A generic password is sent to admin where it must be changed when he accesses the VM the first time. There are access rights for users and admins and all access rights are being recorded. There is no obligation for SLA between the IT department and the academic community. Logs and monitor can be applied only for networking and virtualization. The administrative tool used for the data center and the storage is the vSphere. There is the possibility to take VMs snapshots through vSphere and also the administrative tool of the backup which is taking on daily basis. Monitor VMs to measure performance and find issues and detect abnormal activities. VMs can be distributed to other blades automatically if the resources of a specific blade are exhausted. The resources are not being bound from the creation of the VMs. The administrative tool states the limits of each VM. This method can introduce an overload resulting to loss of data.	

Figure 24. Description catalogue for Virtual Machines service

Cloud Service: 02	
Service Name: **Nextcloud storage**	Deployment Model: **Private Cloud**
Description: **Free storage space accessed from anywhere**	Service Model: **SaaS**
Goal: **Provide storage to academic community to store and share their files**	
Process: **Free access to 50GB of storage**	
Actors involved: **IT department, Faculty members, Administrative staff**	Human Resources: **3**
Hardware Needs: **50TB HD**	
Outsourced: ☐	Company Name:
Comments:	
In order to use the service, the person should be a member of UoA's faculty office or administrative office. It can be accessed from anywhere in the world. Access rights only for the people who have a university account through the Active Directory. Both authentication and authorization is applied and in recent future, there will be used two factor authentication. Logs are kept for all the actions of the users and all the data. No SLA is signed between the users and the IT department. Isolation is used for the privacy of the users and their data. Traceability is performed through monitoring. The files uploaded are restricted to specific types (i.e. no videos or executable files can be uploaded) and the files can be in an encrypted format.	

Figure 25. Description catalogue for Nextcloud service

7.1.1.3. Identify outsourced cloud services

The cloud services that the UoA provide to the academic community do not involve third providers' services due to the fact that they are implemented by the institution's own resources and the infrastructures are competent to do so. Thus, this step is not applicable to the whole process.

7.1.2. Stage 2: Cloud forensic requirements analysis

In this stage, the University of the Aegean is willing to implement two services in order to make them forensic-enabled; virtual machines and nextcloud storage. These services are important to the university since critical data and applications are running and stored on them. Forensic constraints and technologies will be applied on these two services to realize the forensic requirements of each service.

7.1.2.1. Selection of cloud services

The first step of the second stage involves the selection of cloud services to be implemented as forensic-enabled. As mentioned earlier and according to the UoA's needs the services that need to be implemented are the virtual machines and the

nextcloud storage. For each service, an activity diagram is implemented as shown in Figure 26 and Figure 27.

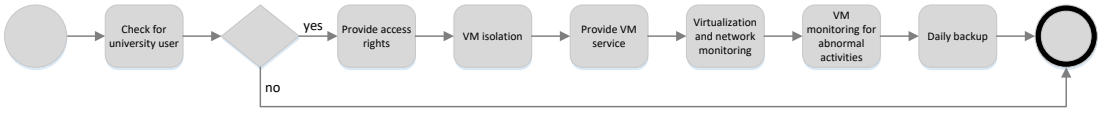


Figure 26. Activity diagram for Virtual Machine service

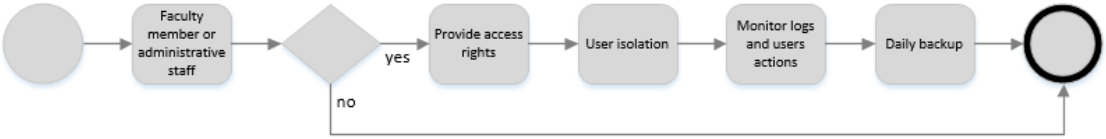


Figure 27. Activity diagram for Nextcloud storage service

7.1.2.2. Applicability of forensic constraints to cloud services

During this step, forensic constraints will be applied to the activity diagrams in order to make these two services cloud forensic-enabled. Taking under consideration the cloud service description catalogue and the activity diagrams, we can come to the conclusion that some forensic constraints are not satisfied. Once there is no SLA or contract signed between the two sides, requirements such as accountability, internal disciplinary procedures and legal matters are not met. The IT department may know the identity of the user who owns the VM but they cannot be certain if the user is willing to hand its logs or even delete its data. On the other hand, VM snapshots are taken only if the IT administrator requests it.

Accountability cannot be met once the IT department is not obliged to sign any contract resulting in providing information as they wish. People working in the IT department are also not obliged to perform any surveillance or behavior policy; hence, there are issues with the internal disciplinary procedures. Legal matters concerning the jurisdiction issues are not applied, since the data center is not geographically distributed and the users are members of the UoA's academic community, but as far as the contract agreements are concerned there is a huge gap to fill. Finally, the access to the computer room where the data center and equipment are operating is not restricted only to the people responsible for the data center, but to all the personnel who is working in the IT. The transparency constraint is fulfilled only in the VM service since the UoA provides all three activities in the specific service. As far as the Nextcloud service concerns the UoA does not provide any notification on policy violation, unless is requested. Traceability is achieved in both cases through the monitoring system, access rights through the users' identification and isolation through the administrative tools and the methods used.

The analysis performed in the previous paragraphs concludes with the implementation of cloud forensic-enabled activity diagrams for each service. These two diagrams are shown in Figure 28 and Figure 29. The black-colored boxes are the forensic constraints that need to be implemented so as the service to be cloud forensic-enabled.

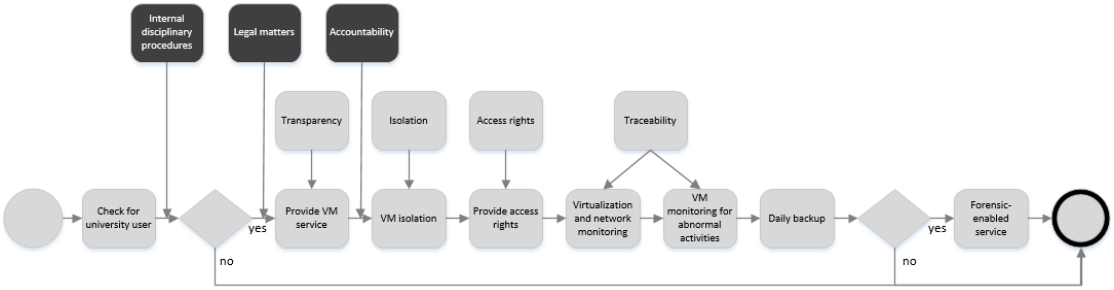


Figure 28. Cloud forensic-enabled activity diagram for Virtual Machines service

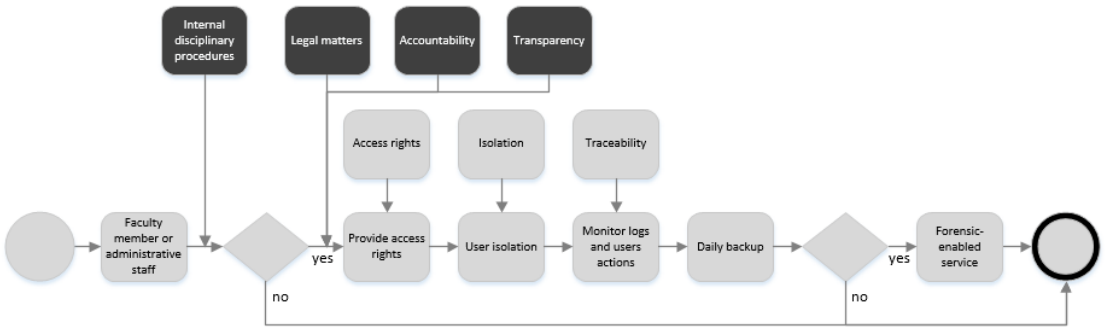


Figure 29. Cloud forensic-enabled activity diagram for Nextcloud service

As we can see from the two figures, the VM service needs three forensic constraints to be implemented so as to make it cloud forensic-enabled while the Nextcloud service needs four. For each forensic constraint that needs to be implemented the corresponding activity diagram is accessed to identify the activities that cannot fulfill the constraint. The detailed activity diagrams for each forensic constraint that is not fulfilled in every service are being illustrated in Figure 30 and Figure 31 respectively.

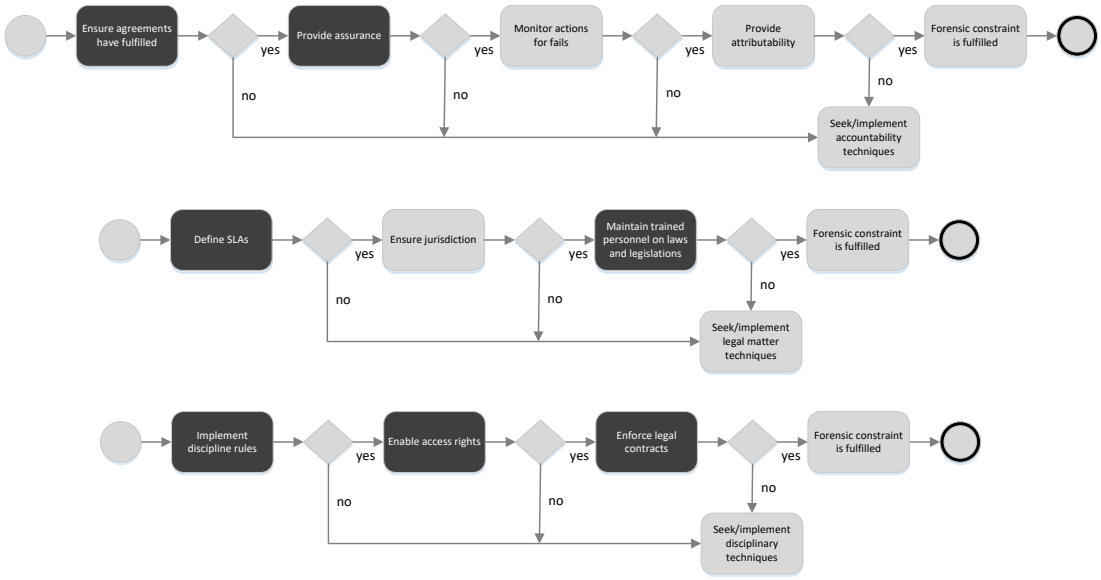


Figure 30. Forensic constraints process patterns for Virtual Machines service

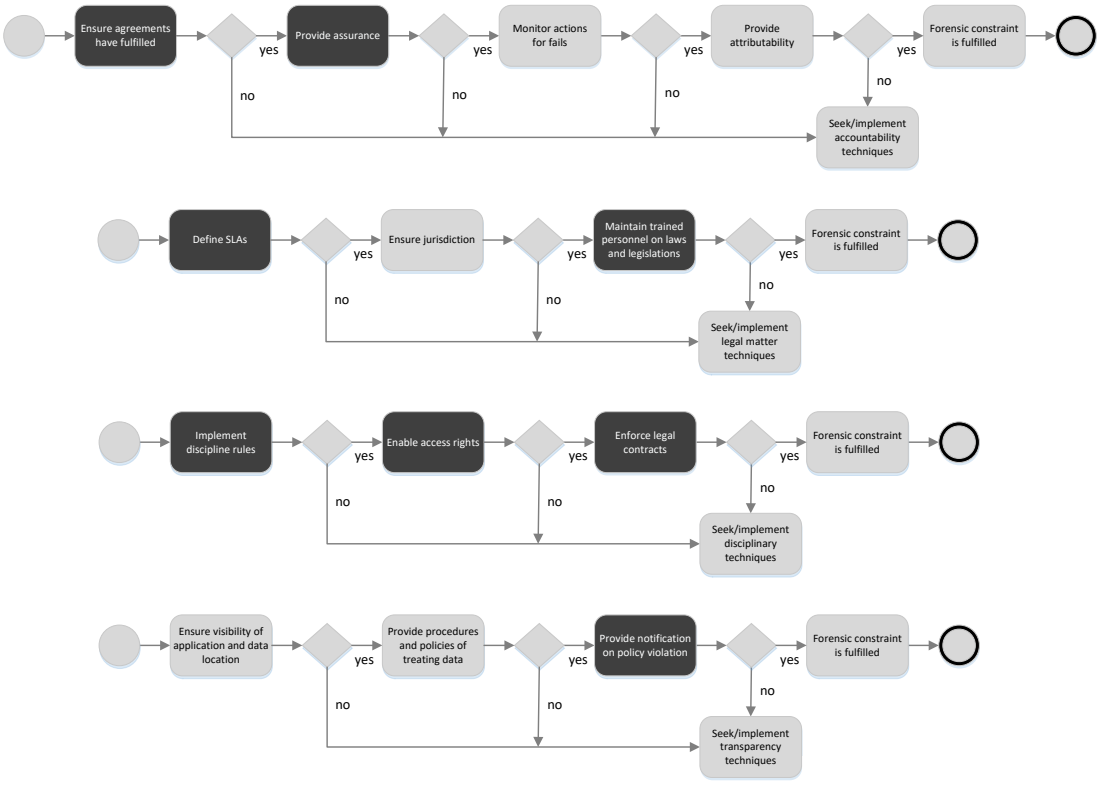


Figure 31. Forensic constraints process patterns for Nextcloud service

7.1.2.3. Selection of technologies

This step involves the technologies identified from the literature that should be applied into forensic constraints. It is obvious from Figure 28 and Figure 29 that the applicability of the technologies concerns only three forensic constraints for the first cloud service and only four for the second cloud services. These constraints have

something in common; they all concentrate on SLAs to solve the issues among other techniques. Service Level Agreements are very important when a cloud provider is hiring its services and infrastructures to consumers and organizations.

In our case for the internal disciplinary procedures constraint, an SLA or a contract should be signed between the UoA and the IT staff responsible for the cloud services clearly stating the rules and the policies they should follow at all times. A mechanism should record and monitor their actions and a report should be sent to the IT administrator when an abnormal activity occurs. On the other hand, the accountability constraint should be solved again with an SLA. The UoA should assure that the consumers using its services are responsible and accountable for their actions and all the above should be written on the SLA. The IT's actions are not monitored nor recorded and this can lead to false assumptions. As far as we know, there is no vulnerability assessment or any penetration testing approach. Transparency constraint is partly fulfilled. Users have the freedom to handle and control their own computation and data according to their usage and they can also be certain that their data is securely backed-up and/or deleted according to their wishes. Again, since there is no SLA signed between them the boundaries are blurred. Finally, legal matters constraint related to jurisdictions issues and international law is not applied in our case study since the data center is not geographically distributed and the users are members of the UoA's academic community. On the other hand, contractual terms, and constitutional issues are not satisfied. Thus, an SLA should also be signed between the two parties.

Table 9. Criteria for selected solutions

Service Name	Deployment Model		Service Model		Forensic Constraints	Suggested Solution
Virtual Machines	Private	√	IaaS	√	Internal disciplinary procedures	Sign robust SLA
						Enforce discipline rules
						Provide physical access rights to specific personnel
			PaaS	□	Legal matters	Sign robust SLA
						Train personnel
	Public	□	SaaS	□	Accountability	Define SLA parameters
						Provide vulnerability assessment

Service Name	Deployment Model		Service Model		Forensic Constraints	Suggested Solution
Nextcloud	Private	√	IaaS	□	Internal disciplinary procedures	Sign robust SLA
						Enforce discipline rules
						Provide physical access rights to specific personnel
			PaaS	□	Legal matters	Sign robust SLA
						Train personnel
	Public	□	SaaS	√	Accountability	Define SLA parameters
						Provide vulnerability assessment
					Transparency	Sign robust SLA

Earlier in the process it was stated that some specific criteria (deployment model, service model and missing forensic-related constraints) need to be taken under

consideration in order to select the technical solutions. Table 8 presents the criteria and suggested solutions for each cloud service in our case study.

7.1.3. Stage 3: Evaluation-Assessment

This is the last stage of the process and the administration of the UoA is called to decide whether the two cloud forensic-enabled services can be implemented or not.

7.1.3.1. Categorization of cloud forensic-enabled services

Based on the previous step "selection of technologies" and its applicability to the activity diagrams, the UoA's administration realized that the cost of implementing both cloud services is within its budget. This arises from the fact that most of the technologies that resolve forensic constraints deal with Service Level Agreements and contracts between the two parties. There is no need to buy new equipment or to upgrade applications and software. Some penetrations tests that need to be performed are also within the UoA's budget.

7.1.3.2. Evaluation - Trace-back

At this point, the UoA's administration decide to hold back the implementation of the rest of the services as cloud forensic-enabled due to the lack of financial resources. Even though its strategy is leaning towards the direction of implementing cloud forensic-enabled services, it is decided to proceed only as soon as the budget allows it.

7.2. Discussion

The University of the Aegean case study brought to light some useful information. It revealed a number of open issues that need to be fixed so as to operate using transparent guidelines and procedures. Open issues related not only to the technical level but also to the administrative level. The persons employed in the UoA's IT department work without signing any contract that states their responsibilities and obligations. This is a major problem for the UoA since anyone from the IT can proceed to actions that may have direct impact to the normal operation. The first action that the UoA need to take is to write procedures and guidelines about the functionality of the systems and the services. Every member of the IT need to be informed about this and a service level agreement need to be signed.

A restriction of the applicability of the framework is that the University does not rely on third parties to outsource its services. All cloud services are accommodated under its own umbrella and its only dependency is with the carrier (Cosmote telecommunication provider). Besides the issue with the dependency, the activity diagrams of the two proposed cloud services, manage to identify the missing forensic constraints. Through the activity diagrams of the missing constraints the technical solutions have been selected to make both cloud services forensicable.

Although the UoA is located in seven different places in Greece, that makes its operation more complicated, it manages through its organizational strategy to be on the top of the technological edge. A number of services have been implemented to bring the university community closer. The applicability of the proposed framework on the UoA's cloud services, manages to successfully identify the organization's goals and forensic needs, and introduces technological activities and solutions based on the forensic requirements. These activities and solutions can guide software engineers to design and implement cloud forensic-enabled services. On the other hand, the applicability of the framework allows organizations to have an overall picture of their cloud services and be more competitive, by recognizing their needs and costs for implementing cloud forensic-enabled services, compared to other organizations.

Chapter 8

Conclusion

8.1. Introduction

This chapter provides the conclusion to the dissertation by outlining the findings of the research and is organized as follows:

The chapter begins with the accomplishments of this work followed by an overall research summary of the study. It briefly explains the main research contribution of the work and concludes with the future directions.

8.2. Accomplishments

This research has focused on the design of cloud forensic-enabled services. Previously researchers had not realized its importance to the forensic investigation, thus no concrete work existed. Specifically this dissertation has managed to introduce a generic framework that can assist software engineers to design and implement cloud forensic-enabled services. A number of concepts concerning both cloud forensic investigation and cloud forensic-enabled services have been defined in order to produce a meta-model that includes all the necessary concepts involved in a cloud forensic incident. In this way the incident can be solved more efficient and in a forensically sound manner.

In this work, besides the identification of the concepts and the development of the meta-model, a generic process has been presented based on both the identified concepts and on a set of forensic constraints (expressed in a form of activity diagrams). The process follows specific steps so as to understand the provider's needs in relation to its cloud services that are made available to consumers. After the identification and the selection of the services that will be implemented the required forensic constraints are applied to the cloud services and make the services forensic-enabled.

8.3. Research summary

The increased use of cloud computing and its different characteristics in relation to the traditional computing, enforced the introduction of a new discipline in the area of computer forensics called cloud forensics. Cloud forensics is a branch of digital forensic science focusing on the evidence found in cloud computing environments. Due to the relative newness of the field of cloud forensics, there is no standardization and accepted procedures/models to assist practitioners. 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. On the other hand, even though cloud computing is based on cloud services, their design and implementation cannot meet the desired level to accomplish a cloud investigation in a forensic sound manner. There is currently no existing framework or model that could assist software engineers to design and implement cloud forensic-enabled services.

The work presented in this dissertation has concentrated on the field of cloud forensic and it specifically identifies the gaps in the field while proposing integrated solutions for solving cloud-based cyber-crimes in an on-going cloud forensic investigation. This research has been conducted to address the problem with the absence of a generic framework or process model for both the cloud forensic investigation and the cloud forensic-enabled services.

- Chapter 1 introduced the research problem which was *the design and implementation of cloud forensic-enabled systems that could assist investigators solving cloud-based cyber-crimes*. The answer to the problem has been given in the following chapters. Apart from the research problem, a motivation for the research was presented alongside with the contribution of this work.
- Chapter 2 provided a technical background for the relative new technology of cloud computing explaining the structure of the technology and the participation of digital evidence in an on-going investigation. A presentation about the disciplines of digital and cloud forensics was produced clarifying their differences and their importance in a digital forensic investigation.
- Chapter 3 presented a review of all the frameworks and methodologies concerning digital and cloud forensics along with an extended discussion regarding their functionality, drawbacks, and complexity parameters. A comparison framework introduced that merges same or similar stages of the proposed frameworks and models into a single stage and take into consideration the stages' limitations of the previous models. A table produced mapping the stages and activities of the models with the comparison framework so as to illustrate and observe the findings. The applicability of the comparison framework was verified through a running example.
- Chapter 4 presented all the cloud-based challenges and issues found in the respective literature, and a categorization of the challenges was conducted in relation to the stages of the comparison framework and the service model they apply to. The categorization is a useful tool for assisting authors to reason about the necessity of cloud-forensics on specific areas. A detailed presentation of the existing solutions regarding the aforementioned challenges was produced in order to identify the respective efforts presented for realizing identified challenges. The solutions given were relative to the service model they apply.
- Chapter 5 identifies the major concepts and their relationships that participate in a cloud forensic investigation. The identified concepts have been presented through the introduction of a common modelling language in terms of a meta-model. This was a necessary step in order to understand the cloud investigation

process and move forward to identify the key factors that assist modelling cloud forensic-enabled services. To verify the applicability of the proposed meta-model, a running example with all the identified concepts has been presented.

- Chapter 6 focuses on the design and implementation of cloud forensic-enabled services. Due to the lack of models and methodologies related to the design of cloud forensic-enabled services a framework was proposed to fill this gap. The framework identified seven forensic constraints that should all be included in the design and implementation of any cloud service. For each forensic constraint, a process pattern is introduced in the form of an activity diagram. A meta-model is also presented based on the concepts and the forensic constraints requirements identified. The meta-model was based both on the concepts that make a system forensic-enabled and on the concepts that form a cloud forensic investigation process. Finally, a process has been developed based on the concepts identified and presented in the meta-model. The process illustrates the stages and the activities that need to be followed to produce cloud forensic-enabled services.
- Chapter 7 evaluates the framework's applicability. The proposed process has been performed in two different case studies concerning cloud services of the University of the Aegean. The results are promising and they can guide, and assist software engineers to design and implement cloud forensic-enabled services.

8.4. Research and contributions

Information system designers have to face an important issue while designing cloud services. They have to design and implement cloud forensic-enabled services that could assist protective actors solve cloud-based cyber-crimes. After a thorough literature review, limited evidence of cloud-based forensic approaches is found. These approaches do not support information systems developers as they focus on the investigation only. A gap in the field of cloud forensics exists since, to the best of my knowledge, there is no framework for handling the design of cloud forensic-enabled services. In this dissertation, the proposed framework aims to fill this gap by supporting the elicitation and modelling of forensic requirements. Specifically, it identifies seven forensic constraints that assist software engineers to implement cloud forensic-enabled services and it introduces a forensic process pattern for each constraint in the form of an activity diagram. Forensic process patterns help software engineers by indicating a number of activities needed to be fulfilled for the service to become forensicable.

The cloud forensic process patterns have been designed to support a generic approach in order to facilitate different environments in the future. This means that the activities and the requirements of the forensic patterns can be used to cloud-based services, or to traditional ones, such as web-services, or even services related to the future technologies. All the aforementioned seven cloud forensic constraints should be applied

on a cloud service in order to be forensic-enabled. Applying the seven activity diagrams on the cloud service activity diagram of the framework process can help software engineers to locate and identify the number of constraints that need to be implemented.

The framework process presented in the dissertation is based on the concepts identified and presented in the meta-model. It aims to identify an organization's strategy and needs, and use the identified forensic process patterns in order to implement cloud forensic-enabled services. It thoroughly analyzes the structure of cloud services an organization provides to consumers and suggests the steps that need to be undertaken and the technologies that need to be used to fulfill the organization's goals. A limitation of the framework is that the case study uses an organization that provides cloud services to consumers in a private cloud deployment model and does not have any dependencies on third parties such as providers, brokers etc. Another limitation is that data is stored in data centers located in a specific geographical area (the islands of the Aegean Sea), thus the issue with different jurisdictions is not applied to the case study. Having created a framework for implementing cloud forensic-enabled services for the needs of protective actors, the next phase is to extend framework tests to other jurisdictions and include organizations with more dependencies on third parties.

This work provides a generic framework that can assist software engineers in a way that they will be able to design and implement cloud forensic-enabled services with immediate impact on a cloud forensic investigation. The framework is implemented in order to fill the gap of non-existing process models and methodologies in the area of cloud services in relation to cloud forensics. This framework is raising the importance of the relation between a forensic-enabled system and an investigation process and how the latter is assisted when an incident occurs.

Another important aspect of this work, which is part of the proposed framework, is the identification of a set of forensic constraints that apply in cloud forensics. The identification of the seven forensic constraints constitutes a first step towards the creation of a set of forensic requirements and a first effort to establish a new category of properties (concepts) in the requirements engineering. The constraints aim to follow a similar pattern with the security and privacy requirements.

8.5. Future directions

In the context of this dissertation, the evaluation and assessment of the applicability of the framework tested on a specific number of cases. The aim is to test the framework on a bigger number of cases with different parameters such as on cloud services that have dependencies on third parties (providers, brokers, etc.) and using different deployment models. Another important aspect is that the data centers of the University are held and operated inside the Greek continent. This automatically has the privilege that only one jurisdiction is engaged in case of an incident.

Taking under consideration the previous statements, future work can be focused on the evaluation of the framework in other jurisdictions and following that in a combination of different jurisdictions involved at the same time. One more field of concentration is the evaluation of the framework by independent organizations or practitioners.

As technology progresses, a new revision of all the seven forensic constraints and their process patterns need to be conducted to search for new aspects. Since there is a gap in the requirements related to cloud forensics, the proposed constraints could be the base of the creation of a set of new forensic requirements.

The goal is to conclude to a standardized framework for the community, the cloud providers and the cloud forensic investigation that can be used by different actors and in different jurisdictions. A formal methodology and tool to provide applicability and compatibility, an international standard.

Another step in the research is the design and implementation of a cloud forensic tool that will be based on the aforementioned framework. The tool will assist practitioners to conduct a cloud forensic investigation in a forensically sound manner. It will also assist software engineers by providing and suggesting technologies to support the implementation of the forensic process based on a number of criteria/parameters.

References

ADAMS, R. 2012. *The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice.* Doctor of Philosophy, Murdoch University.

ADAMS, R. 2013. The Emergence of Cloud Storage and the Need for a New Digital Forensic Process Model. *In:* RUAN, K. (ed.) *Cybercrime and Cloud Forensics: Applications for Investigation Processes.* Hershey, PA, USA: IGI Global.

ADAMS, R. B., HOBBS, V. & MANN, G. 2013. The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice. *Journal of Digital Forensics, Security and Law,* 8**,** 25-48.

AGARWAL, A., GUPTA, M., GUPTA, S. & GUPTA, S. 2011. Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS),* 5**,** 118-131.

AGARWAL, R. & KOTHARI, S. 2015. Review of Digital Forensic Investigation Frameworks. *In:* KIM, K. J. (ed.) *Information Science and Applications.* Springer Berlin Heidelberg.

AL-FEDAGHI, S. & AL-BABTAIN, B. 2012. Modeling the forensics process. *International Journal of Security and Its Applications (IJSIA),* 6**,** 97-108.

ALLIANCE, C. S. 2013. Mapping the forensic standard ISO/IEC 27037 to cloud computing. *In:* GROUP, C. I. M. A. F. W. (ed.).

ALMULLA, S., IRAQI, Y. & JONES, A. Cloud forensics: A research perspective. Innovations in Information Technology (IIT), 2013 9th International Conference on, 17-19 March 2013 2013 Abu Dhabi. IEEE, 66-71.

ALMULLA, S. A., IRAQI, Y. & JONES, A. 2014. A State-of-the-Art Review of Cloud Forensics. *Journal of Digital Forensics, Security and Law,* 9**,** 7-28.

ALQAHTANY, S., CLARKE, N., FURNELL, S. & REICH, C. A Forensic Acquisition and Analysis System for IaaS: Architectural Model and Experiment. 2016 11th International Conference on Availability, Reliability and Security (ARES), Aug. 31 - Sept. 2, 2016 2016 Salzburg, Austria. IEEE, 345-354.

ANASTASOPOULOU, K., TRYFONAS, T. & KOKOLAKIS, S. 2013. Strategic Interaction Analysis of Privacy-Sensitive End-Users of Cloud-Based Mobile Apps. *In:* MARINOS, L. & ASKOXYLAKIS, I. (eds.) *Human Aspects of Information Security, Privacy, and Trust: First International Conference, HAS 2013, Held as Part of HCI International 2013, Proceedings.* Berlin, Heidelberg: Springer Berlin Heidelberg.

ASPNES, J., FEIGENBAUM, J., YAMPOLSKIY, A. & ZHONG, S. 2007. Towards a theory of data entanglement. *Theoretical Computer Science,* 389**,** 26-43.

ATENIESE, G., BURNS, R., CURTMOLA, R., HERRING, J., KISSNER, L., PETERSON, Z. & SONG, D. Provable data possession at untrusted stores. Proceedings of the 14th ACM conference on Computer and communications security, Oct. 29 - Nov. 02, 2007 2007 Alexandria, VA, USA. Acm, 598-609.

ATENIESE, G., DAGDELEN, Ö., DAMGÅRD, I. & VENTURI, D. 2016. Entangled cloud storage. *Future Generation Computer Systems,* 62**,** 104-118.

AYDIN, M. & JACOB, J. A comparison of major issues for the development of forensics in cloud computing. Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, Dec. 9-12, 2013 2013 London, UK. IEEE, 77-82.

BARYAMUREEBA, V. & TUSHABE, F. The enhanced digital investigation process model. Proceedings of the Fourth Digital Forensic Research Workshop, August 2004 2004. Citeseer.

BASET, S. A. 2012. Cloud SLAs: present and future. *ACM SIGOPS Operating Systems Review,* 46**,** 57-66.

BEEBE, N. L. & CLARK, J. G. 2005. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation: The International Journal of Digital Forensics & Incident Response,* 2**,** 147-167.

BEM, D. & HUEBNER, E. 2007. Computer Forensic Analysis in a Virtual Environment. *International Journal of Digital Evidence,* 6**,** 1-13.

BIGGS, S. & VIDALIS, S. Cloud Computing: The impact on digital forensic investigations. Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for, 9-12 Nov. 2009 2009 London. IEEE, 1-6.

BIRK, D. & WEGENER, C. Technical Issues of Forensic Investigations in Cloud Computing Environments. Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, May 26, 2011 2011 Oakland, CA, USA. IEEE, 1-10.

BOUCHENAK, S., CHOCKLER, G., CHOCKLER, H., GHEORGHE, G., SANTOS, N. & SHRAER, A. 2013. Verifying cloud services: present and future. *ACM SIGOPS Operating Systems Review,* 47**,** 6-19.

BRAID, M. 2001. Collecting electronic evidence after a system compromise. *Australian Computer Emergency Response Team (AusCERT)*.

BUSALIM, A. H., HUSSIN, A. R. C. & IBRAHIM, A. Service level agreement framework for e-commerce cloud end-user perspective. Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on, 27-28 Nov. 2013 2013 Kuala Lumpur. IEEE, 576-581.

CARRIER, B. & SPAFFORD, E. H. 2003. Getting physical with the digital investigation process. *International Journal of digital evidence,* 2**,** 1-20.

CASEY, E. 2011. *Digital evidence and computer crime: Forensic science, computers, and the internet. 3rd Edition,* New York, US, Academic Press.

CASEY, E., KATZ, G. & LEWTHWAITE, J. 2013. Honing digital forensic processes. *Digital Investigation,* 10**,** 138-147.

CATTEDDU, D., FELICI, M., HOGBEN, G., HOLCROFT, A., KOSTA, E., LEENES, R., MILLARD, C., NIEZEN, M., NUÑEZ, D. & PAPANIKOLAOU, N. Towards a model of accountability for cloud computing services. Proceedings of the DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC)(May 2013), 2013.

CHANG, C. & RAMACHANDRAN, M. 2016. Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Transactions on Services Computing,* 9**,** 138-151.

CHEN, G., DU, Y., QIN, P. & DU, J. Suggestions to digital forensics in Cloud computing ERA. Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on September 2012 2012. IEEE, 540-544.

CHEN, L., XU, L., YUAN, X. & SHASHIDHAR, N. Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges. Computing, Networking and Communications (ICNC), 2015 International Conference on, 16-19 Feb. 2015 2015 Garden Grove, CA IEEE, 1132-1136.

CHRISTODORESCU, M., SAILER, R., SCHALES, D. L., SGANDURRA, D. & ZAMBONI, D. Cloud security is not (just) virtualization security: a short paper. Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW), November 9-13, 2009 2009 Chicago, Illinois, USA. 1655022: ACM, 97-102.

CIARDHUÁIN, S. Ó. 2004. An extended model of cybercrime investigations. *International Journal of Digital Evidence,* 3**,** 1-22.

CLOUD_ACCOUNTABILITY_PROJECT. 2016. *Accountability in the Cloud - Coceptual Framework* [Online]. Available: http://www.a4cloud.eu/cloud-accountability [Accessed January 25 2017].

CLOUD_EVIDENCE_GROUP 2016. Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Strasbourg, France: Council of Europe Cybercrime Convention Committee (T-CY).

COHEN, F. B. 2010. Fundamentals of digital forensic evidence. *In:* STAVROULAKIS, P. & STAMP, M. (eds.) *Handbook of Information and Communication Security*. Springer Berlin Heidelberg.

COLUMBUS, L. 2014. Roundup of Cloud Computing Forecasts and Market Estimates, 2014. Forbes.

COLUMBUS, L. 2016. Roundup of Cloud Computing Forecasts and Market Estimates, 2016. Forbes.

DAMSHENAS, M., DEHGHANTANHA, A., MAHMOUD, R. & BIN SHAMSUDDIN, S. Forensics investigation challenges in cloud computing environments. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, June 2012 2012 Kuala Lumpur IEEE, 190-194.

DYKSTRA, J. 2013. Seizing Electronic Evidence from Cloud Computing Environments. *In:* RUAN, K. (ed.) *Cybercrime and Cloud Forensics: Applications for Investigation Processes.* Hershey, PA, USA: IGI Global.

DYKSTRA, J. & SHERMAN, A. T. Understanding issues in cloud forensics: two hypothetical case studies. Proceedings of the Conference on Digital Forensics, Security and Law, 25-27 May 2011 Richmond, Virginia, USA. 45-54.

DYKSTRA, J. & SHERMAN, A. T. 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation,* 9, Supplement**,** S90-S98.

DYKSTRA, J. & SHERMAN, A. T. 2013. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation,* 10, Supplement**,** S87-S95.

ENISA 2013. Cloud Computing Incident Reporting: Framework for reporting about major cloud security incidents.

FARINA, J., SCANLON, M., LE-KHAC, N.-A. & KECHADI, M.-T. Overview of the Forensic Investigation of Cloud Services. 2015 10th International Conference on Availability, Reliability and Security, Aug. 24-27, 2015 2015 Toulouse, France. IEEE, 556-565.

FREET, D., AGRAWAL, R., JOHN, S. & WALKER, J. J. Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS. Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems (MEDES '15), October, 2015 2015 Caraguatatuba, Brazil. ACM, 148-155.

FRIEDEN, J. D. & MURRAY, L. M. 2011. The Admissibility of Electronic Evidence Under the Federal Rules of Evidence. *Richmond Journal of Law and Technology,* 17**,** 5-16.

GARG, N. & BAWA, S. 2016. Comparative analysis of cloud data integrity auditing protocols. *Journal of Network and Computer Applications,* 66**,** 17-32.

GEERTS, G. L. 2011. A design science research methodology and its application to accounting information systems research. *International Journal of Accounting Information Systems,* 12**,** 142-151.

GOTH, G. 2007. Virtualization: Old Technology Offers Huge New Potential. *IEEE Distributed Systems Online,* 8**,** 3-3.

GREGOR, S. & HEVNER, A. R. 2013. Positioning and presenting design science research for maximum impact. *MIS Quarterly,* 37**,** 337-356.

GRISPOS, G., GLISSON, W. B. & STORER, T. 2011. Calm Before the Storm: The Emerging Challenges of Cloud Computing in Digital Forensics.

GRISPOS, G., STORER, T. & GLISSON, W. B. 2012. Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. *International Journal of Digital Crime and Forensics (IJDCF),* 4**,** 28-48.

GUO, H., JIN, B. & SHANG, T. Forensic investigations in cloud environments. Computer Science and Information Processing (CSIP), 2012 International Conference on, August 2012 2012 Xi'an, Shaanxi. IEEE, 248-251.

HAEBERLEN, A. 2010. A case for the accountable cloud. *ACM SIGOPS Operating Systems Review,* 44**,** 52-57.

HARICHANDRAN, V. S., BREITINGER, F., BAGGILI, I. & MARRINGTON, A. 2016. A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security,* 57**,** 1-13.

HEGARTY, R., MERABTI, M., SHI, Q. & ASKWITH, B. Forensic analysis of distributed data in a service oriented computing platform. Proceedings of the The Convergence of Telecommunications, Networking & Broadcasting, PG Net, 10th Annual Postgraduate Symposium on 22-23 June 2009 2009 Liverpool.

ISO/IEC-27037:2012 2012. Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence. Geneva, Switzerland: International Organization for Standardization.

JUELS, A. & KALISKI JR, B. S. PORs: Proofs of retrievability for large files. Proceedings of the Computer and communications security, 14th ACM conference on 29 Oct.-2 Nov. 2007 2007 Alexandria, VA, USA. ACM, 584-597.

JUNIPER, R. 2015. Cybercrime will Cost Businesses Over $2 Trillion by 2019. Hampshire, UK: Juniper Research.

KALLONIATIS, C., KAVAKLI, E. & GRITZALIS, S. 2008. Addressing privacy requirements in system design: the PriS method. *Requirements Engineering,* 13**,** 241-255.

KALLONIATIS, C., MANOUSAKIS, V., MOURATIDIS, H. & GRITZALIS, S. 2013. Migrating into the Cloud: Identifying the Major Security and Privacy Concerns. *In:* DOULIGERIS, C., POLEMI, N., KARANTJIAS, A. & LAMERSDORF, W. (eds.) *Collaborative, Trusted and Privacy-Aware e/m-Services: 12th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2013, Athens, Greece. Proceedings.* Berlin, Heidelberg: Springer.

KALLONIATIS, C., MOURATIDIS, H., VASSILIS, M., ISLAM, S., GRITZALIS, S. & KAVAKLI, E. 2014. Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces,* 36**,** 759-775.

KAO, D.-Y. 2016. Cybercrime investigation countermeasure using created-accessed-modified model in cloud computing environments. *The Journal of Supercomputing,* 72**,** 141-160.

KAVAKLI, E., KALLONIATIS, C., LOUCOPOULOS, P. & GRITZALIS, S. 2006. Incorporating privacy requirements into the system design process: the PriS conceptual framework. *Internet research,* 16**,** 140-158.

KEBANDE, V. R. & VENTER, H. S. Adding event reconstruction to a Cloud Forensic Readiness model. 2015 Information Security for South Africa (ISSA), Aug. 12-13, 2015 2015 Johannesburg, South Africa. IEEE, 1-9.

KELLER, A. & LUDWIG, H. 2003. The WSLA framework: Specifying and monitoring service level agreements for web services. *Journal of Network and Systems Management,* 11**,** 57-81.

KENT, K., CHEVALIER, S., GRANCE, T. & DANG, H. 2006. Guide to integrating forensic techniques into incident response. *NIST Special Publication,* SP 800-86**,** 121.

KHAN, S., GANI, A., WAHAB, A. W. A., BAGIWA, M. A., SHIRAZ, M., KHAN, S. U., BUYYA, R. & ZOMAYA, A. Y. 2016. Cloud Log Forensics: Foundations, State of the Art, and Future Directions. *ACM Computing Surveys (CSUR),* 49**,** 7.

KO, R. K. L., JAGADPRAMANA, P., MOWBRAY, M., PEARSON, S., KIRCHBERG, M., LIANG, Q. & LEE, B. S. TrustCloud: A Framework for Accountability and Trust in Cloud Computing. Services (SERVICES), 2011 IEEE World Congress on, 4-9 July 2011 2011 Washington, DC IEEE, 584-588.

KOHN, M. D., ELOFF, M. M. & ELOFF, J. H. 2013. Integrated digital forensic process model. *Computers & Security,* 38**,** 103-115.

KOKOLAKIS, S., DEMOPOULOS, A. J. & KIOUNTOUZIS, E. A. 2000. The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security,* 8**,** 107-116.

LI, J., CHEN, X., HUANG, Q. & WONG, D. S. 2014. Digital provenance: Enabling secure data forensics in cloud computing. *Future Generation Computer Systems,* 37**,** 259-266.

LIU, F., TONG, J., MAO, J., BOHN, R., MESSINA, J., BADGER, L. & LEAF, D. 2011. NIST cloud computing reference architecture. *NIST special publication.* National Institute of Standards and Technology.

LOMBARDI, F. & DI PIETRO, R. 2011. Secure virtualization for cloud computing. *Journal of Network and Computer Applications,* 34**,** 1113-1122.

MAHOWALD, R. P., MATSUMOTO, S., MORRIS, C., TURNER, M. J., GENS, F., HANOVER, J., SENF, D., SAHNI, M., AREND, C., BERGGREN, E., LITTLE, G., VILLARS, R. L., PINA, J., POSEY, M., NEWMARK, E., MCGRATH, B., O'BRIEN, A., BALLOU, M.-C. & KNICKLE, K. 2015. IDC FutureScape: Worldwide Cloud 2016 Predictions - Mastering the Raw Material of Digital Transformation. IDC.

MANOJ, S. K. A. & BHASKARI, D. L. 2016. Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. *Procedia Computer Science,* 85**,** 149-154.

MANOUSAKIS, V., KALLONIATIS, C., KAVAKLI, E. & GRITZALIS, S. 2013. Privacy in the Cloud: Bridging the Gap between Design and Implementation. *In:* FRANCH, X. & SOFFER, P. (eds.) *Advanced Information Systems Engineering Workshops: CAiSE 2013 International Workshops, Valencia, Spain. Proceedings.* Berlin, Heidelberg: Springer.

MARTINI, B. & CHOO, K.-K. R. 2012. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation,* 9**,** 71-80.

MARTINI, B. & CHOO, K.-K. R. 2014. Distributed filesystem forensics: XtreemFS as a case study. *Digital Investigation,* 11**,** 295-313.

MARTY, R. Cloud application logging for forensics. Proceedings of the 2011 ACM Symposium on Applied Computing, 2011 Taichung, Taiwan. ACM, 178-184.

MCAFEE 2014. Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II.

MCKEMMISH, R. A. I. O. C. 1999. *What is forensic computing?,* Canberra, Australia, Australian Institute of Criminology.

MELL, P. & GRANCE, T. 2011. The NIST definition of cloud computing. Gaithersburg, MD, US: National Institute of Standards and Technology.

MILLS, D., MARTIN, J., BURBANK, J. & KASCH, W. 2010. Network time protocol version 4: Protocol and algorithms specification. *IETF RFC5905*.

MISHRA, A. K., MATTA, P., PILLI, E. S. & JOSHI, R. C. Cloud Forensics: State-of-the-Art and Research Challenges. Cloud and Services Computing (ISCOS), 2012 International Symposium on, 17-18 Dec. 2012 2012. IEEE, 164-170.

MONTASARI, R. 2016. Review and Assessment of the Existing Digital Forensic Investigation Process Models. *International Journal of Computer Applications,* 147**,** 41-49.

MOURATIDIS, H., ARGYROPOULOS, N. & SHEI, S. 2016. Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach. *In:* KARAGIANNIS, D., MAYR, H. C. & MYLOPOULOS, J. (eds.) *Domain-Specific Conceptual Modeling: Concepts, Methods and Tools.* Cham: Springer International Publishing.

NANCY AMBRITTA, P., RAILKAR, P. N. & MAHALLE, P. N. 2014. Proposed Identity and Access Management in Future Internet (IAMFI): A Behavioral Modeling Approach. *Journal of ICT Standardization,* 2**,** 1-36.

NEWCOMBE, L. 2012. *Securing Cloud Services: A pragmatic approach to security architecture in the Cloud*, IT Governance Publishing.

NIST 2013. NIST cloud computing security reference architecture. *Working document, NIST.* National Institute of Standards and Technology.

NIST 2014. NIST Cloud Computing Forensic Science Challenges. Gaithersburg, MD, US: National Institute of Standards and Technology.

NURMI, D., WOLSKI, R., GRZEGORCZYK, C., OBERTELLI, G., SOMAN, S., YOUSEFF, L. & ZAGORODNOV, D. The Eucalyptus Open-Source Cloud-Computing System. Cluster Computing and the Grid, 2009. CCGRID '09. 9th IEEE/ACM International Symposium on, 18-21 May 2009 2009 Shanghai. IEEE, 124-131.

ORTON, I., ALVA, A. & ENDICOTT-POPOVSKY, B. 2013. Legal Process and Requirements for Cloud Forensic Investigations. *In:* RUAN, K. (ed.) *Cybercrime and Cloud Forensics: Applications for Investigation Processes.* Hershey, PA, USA: IGI Global.

PALMER, G. A road map for digital forensic research - report from the first Digital Forensics Research Workshop (DFRWS). First Digital Forensic Research Workshop, November 2001 2001 Utica, New York, USA. 1-48.

PATEL, P., RANABAHU, A. H. & SHETH, A. P. Service level agreement in cloud computing. OOPSLA09, Cloud Computing workshop 25-29 October 2009 2009 Orlando, Florida.

PATRASCU, A. & PATRICIU, V.-V. Logging framework for cloud computing forensic environments. Communications (COMM), 2014 10th International Conference on, 29-31 May 2014 2014 Bucharest, Romania. IEEE, 1-4.

PĂTRAŞCU, A. & PATRICIU, V.-V. Beyond digital forensics. A cloud computing perspective over incident response and reporting. 2013 IEEE 8th International Symposium on Applied Computational Intelligence and Informatics (SACI), May 23-25, 2013 2013 Timisoara, Romania. IEEE, 455-460.

PEFFERS, K., TUUNANEN, T., ROTHENBERGER, M. A. & CHATTERJEE, S. 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems,* 24**,** 45-77.

PERUMAL, S. 2009. Digital forensic model based on Malaysian investigation process. *International Journal of Computer Science and Network Security (IJCSNS),* 9**,** 38-44.

PICHAN, A., LAZARESCU, M. & SOH, S. T. 2015. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation,* 13**,** 38-57.

POISEL, R. & TJOA, S. 2012. Discussion on the challenges and opportunities of cloud forensics. *In:* QUIRCHMAYER, G., BASL, J., YOU, I., XU, L. & WEIPPL, E. (eds.) *Multidisciplinary Research and Practice for Information Systems.* Springer Berlin Heidelberg.

POOE, A. & LABUSCHAGNE, L. A conceptual model for digital forensic readiness. 2012 Information Security for South Africa (ISSA), 15-17 Aug. 2012 2012 Johannesburg, Gauteng, South Africa. IEEE, 1-8.

PRAYUDI, Y. & SN, A. 2015. Digital Chain of Custody: State of the Art. *International Journal of Computer Applications,* 114**,** 1-9.

QUICK, D. & CHOO, K.-K. R. 2014. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation,* 11**,** 273-294.

RAFIQUE, M. & KHAN, M. 2013. Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research,* 4**,** 1048-1056.

RAHMAN, S. & KHAN, M. 2015. Review of Live Forensic Analysis Techniques. *International Journal of Hybrid Information Technology,* 8**,** 379-388.

RANI, D. R. & GEETHAKUMARI, G. A meta-analysis of cloud forensic frameworks and tools. 2015 Conference on Power, Control, Communication and Computational

Technologies for Sustainable Growth (PCCCTSG), Dec. 11-12, 2015 2015 Kurnool, Andhra Pradesh, India. IEEE, 294-298.

REITH, M., CARR, C. & GUNSCH, G. 2002. An examination of digital forensic models. *International Journal of Digital Evidence,* 1**,** 1-12.

RIGHTSCALE 2016. State of the Cloud Report, Fifth annual State of the Cloud Survey of the latest cloud computing trends.

RUAN, K. & CARTHY, J. Cloud computing reference architecture and its forensic implications: a preliminary analysis. International Conference on Digital Forensics and Cyber Crime, October 25–26, 2012 2012a Lafayette, Indiana, US. Springer, 1-21.

RUAN, K. & CARTHY, J. 2012b. Cloud Forensic Maturity Model. *In:* ROGERS, M. & SEIGFRIED-SPELLAR, K. C. (eds.) *Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C 2012.* Berlin, Heidelberg: Springer.

RUAN, K., CARTHY, J., KECHADI, T. & CROSBIE, M. 2011a. Cloud Forensics. *In:* PETERSON, G. & SHENOI, S. (eds.) *Advances in Digital Forensics VII, 7th IFIP WG 11.9 International Conference on Digital Forensics.* 1 ed.: Springer Berlin Heidelberg.

RUAN, K., CARTHY, J., KECHADI, T. & CROSBIE, M. 2011b. Cloud forensics: An overview.

RUAN, K., JAMES, J., CARTHY, J. & KECHADI, T. 2012. Key Terms for Service Level Agreements to Support Cloud Forensics. *In:* PETERSON, G. & SHENOI, S. (eds.) *Advances in Digital Forensics VIII.* Berlin, Heidelberg: Springer Berlin Heidelberg.

SANG, T. A Log Based Approach to Make Digital Forensics Easier on Cloud Computing. Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on, 16-18 Jan. 2013 2013 Hong Kong. IEEE, 91-94.

SANTOS, N., GUMMADI, K. P. & RODRIGUES, R. Towards trusted cloud computing. Proceedings of the 2009 conference on Hot topics in cloud computing (HotCloud'09), June 14–19, 2009 2009 San Diego, CA, USA. USENIX Association, 5.

SELAMAT, S. R., YUSOF, R. & SAHIB, S. 2008. Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security,* 8**,** 163-169.

SERRANO, D., BOUCHENAK, S., KOUKI, Y., LEDOUX, T., LEJEUNE, J., SOPENA, J., ARANTES, L. & SENS, P. Towards QoS-Oriented SLA Guarantees for Online Cloud Services. Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on, 13-16 May 2013 2013 Delft. IEEE, 50-57.

SHEI, S., KALLONIATIS, C., MOURATIDIS, H. & DELANEY, A. 2016. Modelling Secure Cloud Computing Systems from a Security Requirements Perspective. *In:* KATSIKAS, S., LAMBRINOUDAKIS, C. & FURNELL, S. (eds.) *Trust, Privacy and Security in Digital Business.* Cham: Springer International Publishing.

SHI, Y., ZHANG, K. & LI, Q. 2010. A new data integrity verification mechanism for SaaS. *In:* WANG, F. L., GONG, Z., LUO, X. & LEI, J. (eds.) *Web Information Systems and Mining.* 1 ed. Sanya, China: Springer Berlin Heidelberg.

SHIN, Y.-D. New Digital Forensics Investigation Procedure Model. *In:* KIM, J., DELEN, D., PARK, J., KO, F. & NA, Y. J., eds. 2008 Fourth International Conference on Networked Computing and Advanced Information Management (NCM '08), September 2-4, 2008 2008 Gyeongju, Korea. IEEE, 528-531.

SIBIYA, G., VENTER, H. S. & FOGWILL, T. Digital forensic framework for a cloud environment. Proceedings of the IST-Africa 2012 Conference 9 May 2012 Tanzania. IIMC.

SIMOU, S., KALLONIATIS, C., GRITZALIS, S. & MOURATIDIS, H. 2016a. A survey on cloud forensics challenges and solutions. *Security and Communication Networks,* 9**,** 6285-6314.

SIMOU, S., KALLONIATIS, C., KAVAKLI, E. & GRITZALIS, S. 2014a. Cloud Forensics Solutions: A Review. *In:* ILIADIS, L., PAPAZOGLOU, M. & POHL, K. (eds.) *Advanced Information*

Systems Engineering Workshops: CAiSE 2014 International Workshops, Thessaloniki, Greece. Proceedings. Cham: Springer International Publishing.

SIMOU, S., KALLONIATIS, C., KAVAKLI, E. & GRITZALIS, S. 2014b. Cloud Forensics: Identifying the Major Issues and Challenges. *In:* JARKE, M., MYLOPOULOS, J., QUIX, C., ROLLAND, C., MANOLOPOULOS, Y., MOURATIDIS, H. & HORKOFF, J. (eds.) *Advanced Information Systems Engineering: 26th International Conference, CAiSE 2014, Thessaloniki, Greece. Proceedings.* Cham: Springer International Publishing.

SIMOU, S., KALLONIATIS, C., MOURATIDIS, H. & GRITZALIS, S. 2015. Towards the Development of a Cloud Forensics Methodology: A Conceptual Model. *In:* PERSSON, A. & STIRNA, J. (eds.) *Advanced Information Systems Engineering Workshops: CAiSE 2015 International Workshops, Stockholm, Sweden. Proceedings.* Cham: Springer International Publishing.

SIMOU, S., KALLONIATIS, C., MOURATIDIS, H. & GRITZALIS, S. 2016b. A Meta-model for Assisting a Cloud Forensics Process. *In:* LAMBRINOUDAKIS, C. & GABILLON, A. (eds.) *Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Mytilene, Greece. Revised Selected Papers.* Cham: Springer International Publishing.

SIMOU, S., KALLONIATIS, C., MOURATIDIS, H. & GRITZALIS, S. 2016c. Towards a Model-Based Framework for Forensic-Enabled Cloud Information Systems. *In:* KATSIKAS, S., LAMBRINOUDAKIS, C. & FURNELL, S. (eds.) *Trust, Privacy and Security in Digital Business: 13th International Conference, TrustBus 2016, Porto, Portugal. Proceedings.* Switzerland: Springer International Publishing.

SIMPSON, W. R. & CHANDERSEKARAN, C. 2014. Cloud forensics issues. DTIC Document.

SKYHIGH 2016. Cloud Adoption & Risk Report Q4 2016. Skyhigh.

SPEEDY-PUBLISHING 2015. Evidence (Speedy Study Guides). Newark: Dot EDU.

SPYRIDOPOULOS, T. & KATOS, V. 2011. Towards a forensically ready cloud storage service. *In:* CLARKE, N. L. & TRYFONAS, T. (eds.) *Digital Forensics & Incident Analysis, WDFIA 2011, Proceedings of the 6th International Workshop on.* Plymouth, UK: University of Plymouth.

SPYRIDOPOULOS, T. & KATOS, V. 2013. Data Recovery Strategies for Cloud Environments. *In:* RUAN, K. (ed.) *Cybercrime and Cloud Forensics: Applications for Investigation Processes.* Hershey, PA, USA: IGI Global.

TAYLOR, M., HAGGERTY, J., GRESTY, D. W. & HEGARTY, R. C. 2010. Digital evidence in cloud computing systems. *Computer Law & Security Review,* 26**,** 304-308.

THETHI, N. & KEANE, A. Digital forensics investigations in the Cloud. Advance Computing Conference (IACC), 2014 IEEE International, 21-22 Feb. 2014 2014 Gurgaon. IEEE, 1475-1480.

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. Services (SERVICES), 2013 IEEE Ninth World Congress on, June 28 2013-July 3 2013 2013 Santa Clara, CA. IEEE, 75-83.

TRENWITH, P. M. & VENTER, H. S. Digital forensic readiness in the cloud. Information Security for South Africa, 2013, 14-16 Aug. 2013 2013 Johannesburg. IEEE, 1-5.

U.S. DEPARTMENT OF JUSTICE, N. 2001. Electronic Crime Scene Investigation: A Guide for First Responders. *NIJ Research Report.* Washington.

VACCA, J. R. 2005. *Computer Forensics: Computer Crime Scene Investigation*, Charles River Media, Inc.

VALJAREVIC, A. & VENTER, H. S. Harmonised digital forensic investigation process model. 2012 Information Security for South Africa (ISSA), 15-17 Aug. 2012 2012 Johannesburg, South Africa. IEEE, 1-10.

VON SOLMS, S., LOUWRENS, C., REEKIE, C. & GROBLER, T. 2006. A Control Framework for Digital Forensics. *In:* OLIVIER, M. S. & SHENOI, S. (eds.) *Advances in Digital Forensics*

II: IFIP international Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, January 29– February 1, 2006. Boston, MA: Springer New York.

WAN, Z., LIU, J. E. & DENG, R. H. 2012. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. *Information Forensics and Security, IEEE Transactions on,* 7**,** 743-754.

WILKINSON, S. & HAAGMAN, D. 2010. Good Practice Guide for Computer-Based Electronic Evidence (ACPO). *Association of Chief Police Officers***,** 72.

WILLIAMS, J. 2011. Good Practice Guide for Digital Evidence version 5.0 (ACPO). *In:* OFFICERS, A. O. C. P. (ed.).

WILSHUSEN, G. C. 2016. Federal Information Security: Actions Needed to Address Challenges. *In:* OFFICE, U. S. G. A. (ed.). Washington, D.C., US: U.S. Government Accountability Office.

WOLTHUSEN, S. D. Overcast: Forensic Discovery in Cloud Environments. IT Security Incident Management and IT Forensics, 2009. IMF '09. Fifth International Conference on, 15-17 Sept. 2009 2009 Stuttgart. IEEE, 3-9.

YAN, C. Cybercrime forensic system in cloud computing. Image Analysis and Signal Processing (IASP), 2011 International Conference on, 21-23 Oct. 2011 2011 Hubei. IEEE, 612-615.

YANG, K., JIA, X., REN, K., ZHANG, B. & XIE, R. 2013. DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. *Information Forensics and Security, IEEE Transactions on,* 8**,** 1790-1801.

YANG, Y., LIU, J. K., LIANG, K., CHOO, K.-K. R. & ZHOU, J. 2015. Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data. *In:* PERNUL, G., Y A RYAN, P. & WEIPPL, E. (eds.) *Computer Security -- ESORICS 2015: 20th European Symposium on Research in Computer Security, Proceedings, Part II.* Cham: Springer International Publishing.

YOUNGE, A. J., HENSCHEL, R., BROWN, J. T., LASZEWSKI, G. V., QIU, J. & FOX, G. C. Analysis of Virtualization Technologies for High Performance Computing Environments. 2011 IEEE 4th International Conference on Cloud Computing (CLOUD), 4-9 July 2011 2011 Washington, DC, USA. 9-16.

YU, Y., XUE, L., AU, M. H., SUSILO, W., NI, J., ZHANG, Y., VASILAKOS, A. V. & SHEN, J. 2016. Cloud data integrity checking with an identity-based auditing mechanism from RSA. *Future Generation Computer Systems,* 62**,** 85-91.

ZAFARULLAH, Z., ANWAR, F. & ANWAR, Z. Digital Forensics for Eucalyptus. Frontiers of Information Technology (FIT), 2011, 19-21 Dec. 2011 2011 Islamabad. IEEE, 110-116.

ZAWOAD, S., DUTTA, A. K. & HASAN, R. SecLaaS: secure logging-as-a-service for cloud forensics. Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, May 2013 2013. ACM, 219-230.

ZAWOAD, S. & HASAN, R. 2013. Cloud forensics: a meta-study of challenges, approaches, and open problems. *Computing Research Repository (CoRR),* abs/1302.6312.

ZAWOAD, S. & HASAN, R. 2015. FECloud: A Trustworthy Forensics-Enabled Cloud Architecture. *In:* PETERSON, G. & SHENOI, S. (eds.) *Advances in Digital Forensics XI.* Springer International Publishing.

ZAWOAD, S., HASAN, R. & SKJELLUM, A. OCF: An Open Cloud Forensics Model for Reliable Digital Forensics. Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on, June 27 2015-July 2 2015 2015 New York City, NY IEEE, 437-444.

ZHOU, L., VARADHARAJAN, V. & HITCHENS, M. 2013. Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. *Information Forensics and Security, IEEE Transactions on,* 8**,** 1947-1960.

ZIMMERMAN, S. & GLAVACH, D. 2011. Cyber forensics in the cloud. *IA Newsletter,* 14**,** 4-7.