A Revised Forensic Process for Aligning the Investigation Process with the Design of Forensic-enabled Cloud Services

Stavros Simou[1] Christos Kalloniatis[1] Stefanos Gritzalis[2] and Vasilis Katos[3]

[1] Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR 81100 Mytilene, Greece
[2] Laboratory of Systems Security, Department of Digital Systems, University of Piraeus, GR 18534, Piraeus, Greece
[2] Department of Computing and Informatics, Bournemouth University, Poole House, Fern Barrow, BH12 5BB, UK
ssimou@aegean.gr

Abstract. The design and implementation of cloud services, without taking under consideration the forensic requirements and the investigation process, makes the acquisition and examination of data, complex and demanding. The evidence gathered from the cloud may not become acceptable and admissible in the court. A literature gap in supporting software engineers so as to elicit and model forensic-related requirements exists. In order to fill the gap, software engineers should develop cloud services in a forensically sound manner. In this paper, a brief description of the cloud forensic-enabled framework is presented (adding some new elements) so as to understand the role of the design of forensic-enabled cloud services in a cloud forensic investigation. A validation of the forensic requirements is also produced by aligning the stages of cloud forensic investigation process with the framework's forensic requirements. In this way, on one hand, a strong relationship is built between these two elements and emphasis is given to the role of the forensic requirements and their necessity in supporting the investigation process. On the other hand, the alignment assists towards the identification of the degree of the forensic readiness of a cloud service against a forensic investigation.

Keywords: Cloud Forensics, Forensic Requirements, Cloud Forensic Investigation Process, Forensic Readiness, Forensic Constraints.

1 Introduction

Since the early days of Cloud Forensics discipline, introduced by Ruan [1], both software engineers and investigators have put a lot of effort to identify the issues of the new discipline and find appropriate solutions. There are many issues associated with legal matters, multi-tenancy, flexibility of deleting instances, data replication, location transparency and dependence on Cloud Service Providers (CSPs) that are unique to cloud forensics and makes the investigation even more complex than in the traditional

environments [1-5]). Investigators' main objective is to conduct an investigation in the cloud in a forensically sound manner and present evidence that can be admissible in a court of law. In order to achieve these goals, investigators should be able to rely both on cloud services that are designed and implemented by software engineers and on the investigation process. Therefore, a strong cooperation between software engineers and investigators is necessary. Software engineers should be able to design and implement forensic-enabled cloud services so as to assist investigators in case of an incident.

Thus, the aim of the specific paper is to examine how the design and implementation of a service can assist investigators in a cloud forensic investigation. Cloud Service Providers are responsible for providing cloud services to consumers. According to a report, 96% of small, medium business and enterprises are using cloud services [6]. A cloud incident may exploit possible vulnerabilities of the cloud services and gain access or harm sensible data. Hence, the cloud service concept plays an important role in a cloud forensic investigation. A great challenge for software engineers is to identify the forensic requirements and design cloud services in a forensically sound manner. To accomplish this, they need to understand the cloud forensic investigation process and how it is conducted.

NAS report (page 181) states that "some agencies still treat the examination of digital evidence as an investigative rather than a forensic activity" [7]. The proposed framework introduced in a way to eliminate the burden of an investigation. It introduces the activities to implement a service so as in case of an incident the outcome of the investigation should be in accordance to the forensic guidelines and principles. All the incidents should be investigated either forensically or not. In this paper the proposed framework achieves the first.

Within this work, an alignment of the design of cloud forensic-enabled services is introduced after an explanation of the forensic requirements, in order first to describe how cloud services can become forensic-enabled and second to understand the role of the design of forensic-enabled cloud services in a cloud forensic investigation. The paper also extends our previous work [8] in the direction of adding a new stage in the process that software engineers may follow for eliciting, modeling, implementing and validating forensic requirements in cloud services. The proposed process is at high level thus, it can be applied in any digital forensic with appropriate adjustments.

The rest of the paper is organized as follows. Section 2 presents the work that has been done so far in relation to cloud forensic investigation and the different processes or models introduced by researchers. Section 3 presents a cloud forensic analysis consisting of the cloud forensic high level requirements that a service need to include in its design and implementation stages as well as the framework for reasoning about cloud forensics so as to make the specific cloud service forensic-enabled. Section 4 aligns the different stages of the cloud investigation process with the forensic constraints in order to validate the forensic requirements. Section 5 presents a validation approach of the work, while section 6 concludes the paper by raising future research on this innovative research field.

2 Cloud Forensic Investigation

One of the most important aspect of implementing a cloud forensic-enabled service is to actually understand how a cloud investigation is conducted. Therefore, a research had to be made in order to design the cloud investigation process. 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 various research efforts concentrate on these directions [8, 9]. In addition, digital forensics methods cannot support an investigation in cloud environments since the particular environments introduce many differences compared to traditional IT environments [1, 10].

2.1 Related Work

In the past years, a number of researchers introduced methodologies and frameworks in relation to the cloud investigation process. In 2012, Martini et al. [11] proposed the Integrated Conceptual Digital Forensic Framework for Cloud Computing, which is based on McKemmish [12] and Kent et al. [13]. The framework emphasizes on the differences in the preservation of forensic data and the collection of cloud computing data for forensic purposes. It includes four stages, identification and preservation, collection, examination and analysis, and reporting and presentation. According to Agarwal et al. [14], the iteration of the framework demonstrates one of the key differences in the identification and analysis of evidence sources.

The same year Ruan et al. [15] presented the Cloud Forensic Maturity Model (CFMM). It 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 introduces four main sections: pre-investigative readiness, core-forensic process, supportive processes and investigative interfaces. 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.

In 2015, Open Cloud Forensics (OCF) model was introduced by Zawoad et al. [16]. It proposes a cloud forensic process, which consists of the preservation stage, which runs throughout the process and the stages of identification, collection, organization, presentation and verification. Examination and analysis is included in the organization stage. During the verification stage, the court authority verifies the cloud-based evidence provided by the investigators. Considering the important role of CSPs, the proposed model can support reliable forensics in a realistic scenario. As stated by the authors, cloud architects can use the model to design clouds that support trustworthy cloud forensics investigations.

There are also some other proposed models concerning cloud forensics such as Adams et al. [17] and Guo et al. [18] but there are limitations mostly in relation to the later stages. Both models do not include any actions or stages after the evidence collection and acquisition. Therefore, the stages of examination, analysis and presentation are out of the scope of the researchers.

2.2 Proposed Cloud Forensic Investigation Process

Simou et al. [9] presented a comparison framework to merge same or similar stages of the previous proposed frameworks and models that produce the same outcome into one stage. The comparison framework consists of the following four sequential stages: identification, preservation-collection, examination-analysis, and presentation and two concurrent stages, the chain of custody and documentation. Authors stated that the preservation stage should also run concurrently with the other two stages or should be included in the chain of custody. Based on the comparison framework and the literature review conducted in [10], Simou et al. [9] proposed a generic process for cloud-forensic investigation including the steps of Incident Confirmation, Incident Identification, Collection-Acquisition, Examination-Analysis, and Presentation. They were stating that understanding the cloud forensic investigation process is of vital importance in order to design and implement cloud forensic-enabled services. The proposed process is illustrated in Figure 1.

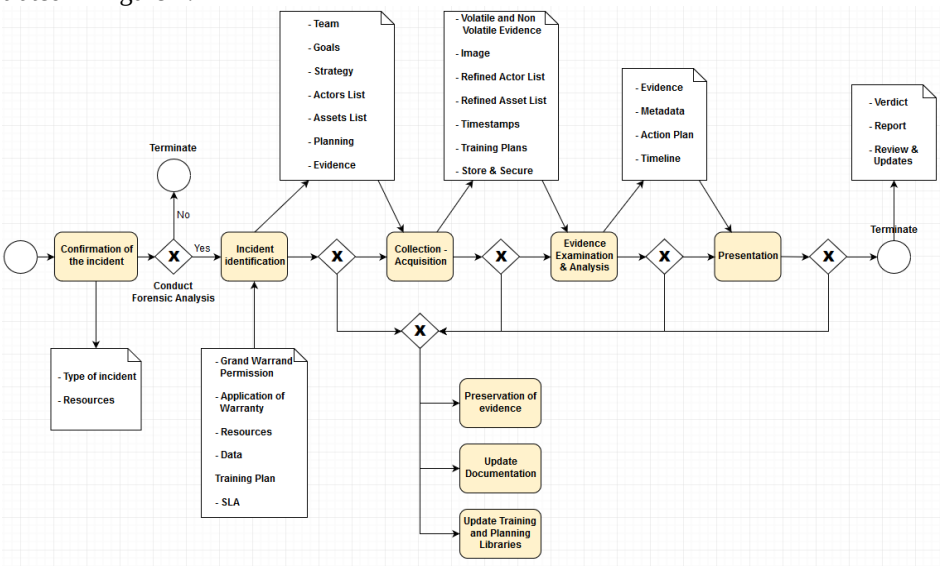

Fig. 1. Process for Cloud Forensic Investigation.

Beside the five sequential steps presented in Figure 1 there are three more steps running throughout the investigation process. They are parallel activities/steps running concurrently with the four steps after the confirmation of the incident. These are: preservation of evidence, documentation, and training and planning.

Even though incident confirmation is not an actual step of the investigation process, it has to be included since it is the stage where the administrator of the Information Technology (IT) department and the stakeholders come together to decide whether the cloud investigation will start or not, depending on the type and the nature of the incident. It also depends on the organization's available resources. During the incident identification stage, all relevant assets (software, hardware and data) that may contain potential evidence should be identified.

In the collection-acquisition stage, the main goal is to obtain the data and the potential evidence in a forensically sound manner. The acquired assets should be securely stored for further analysis. The examination and analysis stage includes the data extraction from the previous stage and the process to analyse the results in order to find any useful evidence. Finally, in the presentation stage 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. The outcome of a trial depends on the weight of the evidence (how concrete they are).

The three concurrent stages are needed in the investigation process since they are the most important and crucial parts of the process. If the evidence are not preserved, anyone from the opposite side can challenge them. The same applies for the documentation since the chain of custody will not be maintained. As far as the training and planning stage concerns, it prepares and ensures that personnel, operations and infrastructures are able to support an investigation.

3 Cloud Forensic Analysis

Since cloud forensics is relative newly developed research area, our main and primary focus was to conduct a thorough analysis of the respective literature in order to identify and present a set of forensic constraints that can be the first step towards the creation of a set of forensic requirements. A reason of this analysis is to examine how the forensic constraints involve in the investigation process.

In [19-20] a thorough literature review was conducted based on the most cited papers presented in respective scientific journals, conferences, books and industrial reports. Based on the specific analysis, the cloud characteristics, and forensic properties, a set of forensic constraints were proposed and presented in [8]. The findings of this analysis constitute an initial but robust set of constraints that designers and software engineers need to consider when designing information systems or individual services in the cloud.

3.1 Cloud Forensic High Level Requirements

Frameworks, models and methodologies in cloud forensics, identify the necessary steps, methods, concepts or activities and produce useful information. This information can be used to specific cases to explain and resolve these cases. Beside the methodologies and models, the forensic requirements need to be clarified to specify capabilities and functions that a cloud service must be able to perform. The identified forensic requirements introduced as forensic constraints since their implementation forces the mandatory use of specific technologies in addition to the existing functionality of the services, to eliminate the existing gap in the cloud environments. Forensic constraints are requirements related to system forensicability (the term forensicability is used as a service that can be forensic-enabled; can be developed in a forensically sound manner) and specify a service's quality attributes. The seven identified forensic constraints are listed as follow.

Internal disciplinary procedure: process through which a CSP or a third party deals with its employees in order to ensure that they follow certain norms of discipline.
Accountability: CSP's obligation to protect and use consumer's data with responsibility for its actions and liability in case of an issue.
Transparency: condition where an entity can have full access to manage and control its own data at any given time and allow feedback from the entities that accommodate it.
Legal matters (Regulatory): procedures and actions that need to be undertaken related to jurisdiction issues, international law, contractual terms, legislative frameworks and constitutional issues.
Access rights (Policies) 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 are parts of this concept.
Isolation is the mechanism to ensure that each consumers' data is sealed and cannot be seen by other tenants.
Traceability is the ability, for the data to be traced or not by the user [21] 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.

3.2 Framework for Reasoning about Cloud Forensics

It is indeed true that designing cloud services capable of assisting investigators to solve an incident is a huge 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 [10]. Thus, to fill the aforementioned gap, a presentation of a requirements engineering framework is introduced in [8], 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 feature diagrams (one for each forensic constraint), a modelling language expressed through a conceptual meta-model and a process based on the concepts identified and presented in the meta-model.

Feature Diagrams. The initial step of our research framework was the design of a set of feature diagrams based on the identified forensic constraints. For every proposed forensic constraint a feature diagram has been introduced for expressing the basic tasks that need to be realized. These diagrams are used to describe the necessary tasks a cloud provider need to consider in order to make a cloud service forensic-enabled. Each feature diagram consists of a set of tasks/nodes that implement a specific forensic constraint. A detailed description of all the feature diagrams and their tasks has been presented in [8]. Also, in section 4, a table (Table 1) is introduced illustrating the different tasks for each forensic constraint. To understand how the feature diagrams of the seven forensic constraints work, one of them, the internal disciplinary procedures feature diagram is illustrated in Figure 2 and explained as follow.

The feature diagram for internal disciplinary procedures constraint presents the tasks that need to be fulfilled to ensure that the constraint is successfully implemented. Cloud providers should implement discipline rules and 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. In the case that one or more of the previous tasks have not been fulfilled, the provider should seek or implement techniques that resolve the issue. The same applies for all the constraints listed in the paper. The rest of the feature diagrams have been illustrated and can be viewed in [8].

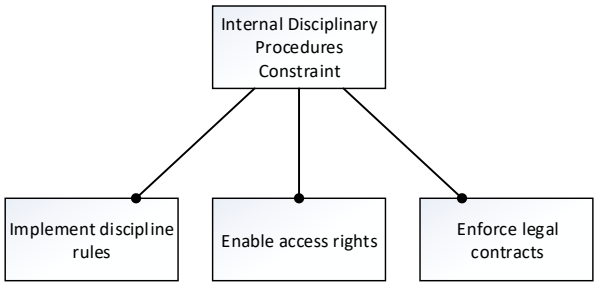

Fig. 2. Internal disciplinary procedures feature diagram

In order for a cloud service to be characterized as forensic-enabled, all the aforementioned seven cloud forensic constraints should be realized at the same time. 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. In the case that a forensic constraint is not satisfied, the investigation does not meet the forensic requirements and cannot be characterized as 100% satisfactory.

Meta-model. The second step of the framework was to propose a common modelling language in order to support the elicitation and modelling of the aforementioned forensic constraints. 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 [8]. Figure 3 presents the meta-model, which consists both the concepts of making a system or a service forensic-enabled and the concepts that form a cloud forensic investigation process. The two groups of concepts are separated with each other with the dotted lines. The one inside the dotted lines is the investigation process group, while the other outside of the lines is the forensic-enabled group. All relationships among critical components are illustrated in Figure 3.

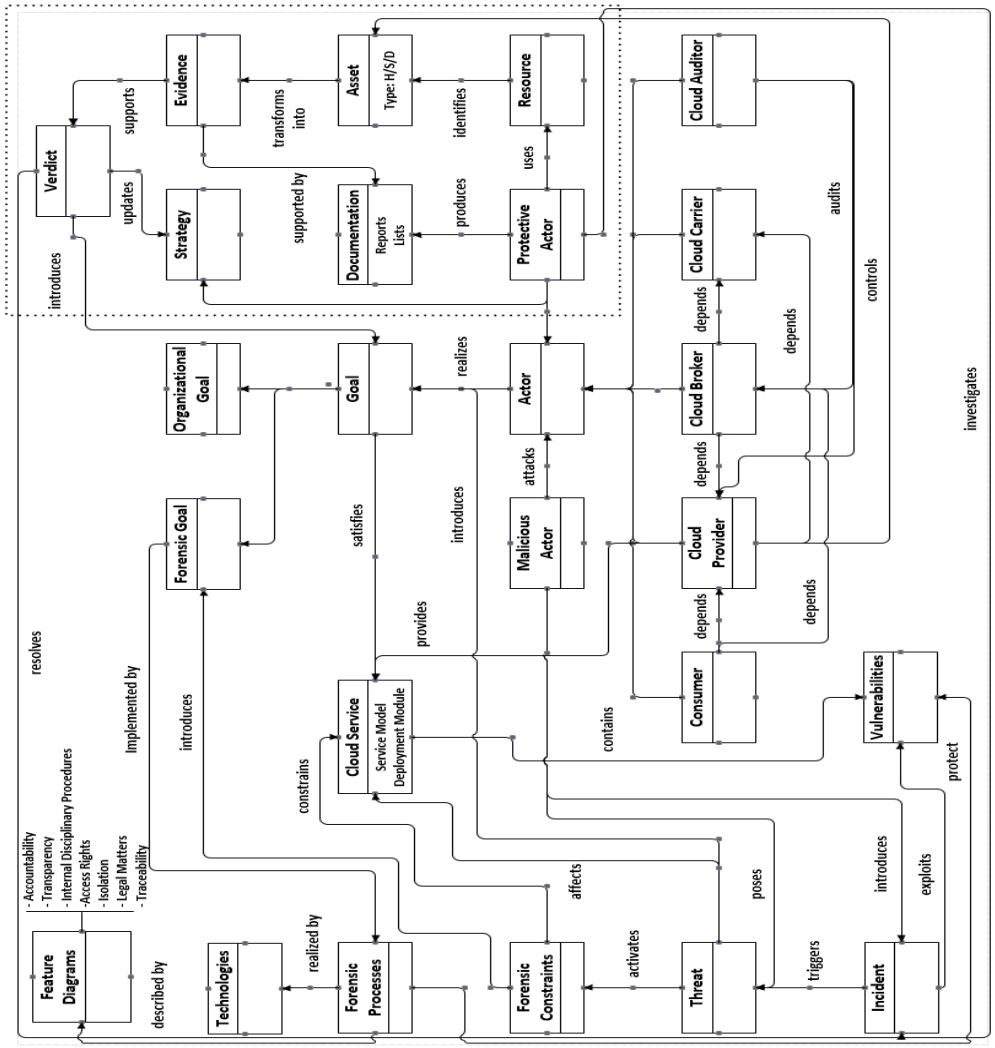

Fig. 3. Meta-model for assisting a cloud forensic process

Framework Process. The last step to the completion of the framework was the development of a process based on the concepts identified and presented in the meta-model. The process provides the necessary steps towards the design of a cloud forensic-enabled service, based on the potential vulnerabilities of the service and the systematic analysis of forensic requirements.

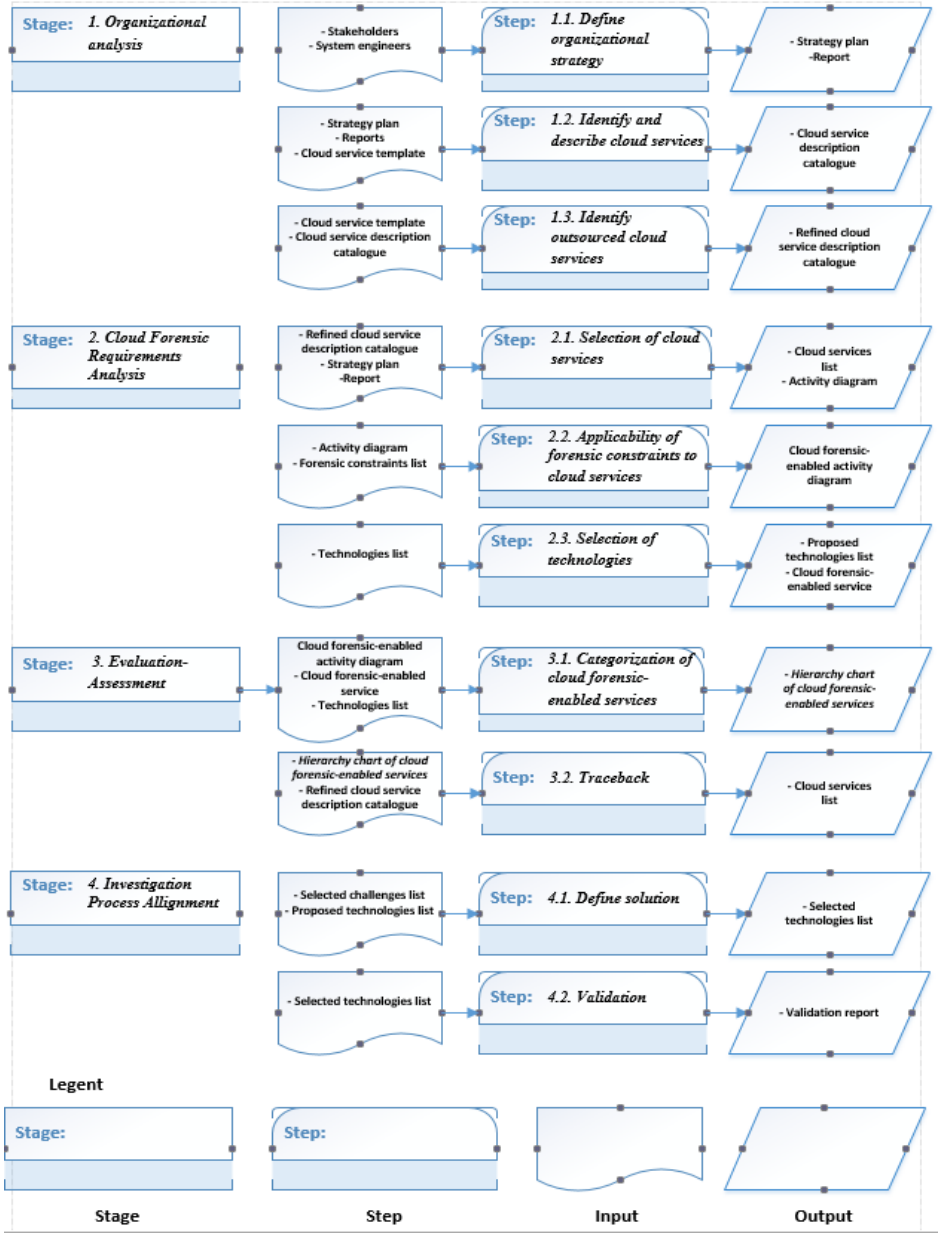

Fig. 4. Forensic requirements engineering process for cloud forensic-enabled services

On one hand, it assists in the identification of the organizational strategy and needs and on the other, it analyses in depth the various organizational cloud services in order to provide the necessary requirements for well-structured cloud forensic-enabled services. The revised process consists of four main stages: Organizational Analysis, Cloud

Forensic Requirements Analysis, Evaluation-Assessment and Forensic Investigation Validation. The first three stages have been introduced and explained in [8], while the fourth one will be presented and detailed described in section 4 of this paper. Figure 4 illustrates the stages and sub-stages of the process.

4 Cloud Forensic Requirements and their support in the Investigation Process

In order to align the design of forensic-enabled cloud services with the investigation process, the seven forensic constraints introduced in [8] have been considered and used. The forensic constraints and their tasks need to fulfil specific stages or inputs and outputs of the investigation process in order to assist the investigators. Within the following paragraphs, an alignment of the design of cloud forensic-enabled services is introduced together with the extension of our previous work [8].

4.1 Forensic Investigation Validation

A new stage is introduced in the forensic requirements engineering process that has to deal with the validation of the selected forensic enabled services against the investigation process. This new stage is placed at the end of the process after the "Evaluation-Assessment". It is called "Investigation Process Alignment" and it consists of two steps: "Define Solutions" and "Validation". In order to assist the investigators when conducting an investigation following the process described in section 3.2.3, an analysis of the seven forensic constraints and the identification of their relation to the proposed forensic investigation stages is presented. This has to be explained and understood, so as to proceed with the description of the two steps of the new stage.

The first forensic constraint, the internal disciplinary procedures contributes to the investigation process in the following ways. Enforcing legal contracts task assists to the incident identification stage with the use of the SLAs. All the contracts should be read in order to prepare the line of defence and the strategy. On the other hand, the team that will be formed to investigate the incident will be in co-operation with the personnel who work in the provider's facilities. Implement discipline rules should be realized at the same stage so as to exclude the providers' personnel, especially those who work in the investigation team and handle the evidence. The access right of the constraint realizes the preservation of evidence stage. Only the personnel that has the proper rights can access specific parts of the infrastructures, eliminating the danger of handling the evidence by unwanted users, aiming to narrow access immediately when an incident occurs. Due to the specific constraint a refined actors list will be produced that it contributes to the collection and acquisition stage.

Both the accountability and transparency constraints contributes to the investigation process in three different stages, beginning with the evidence examination and analysis stage. With the use of special tools, the examination of data takes place. Metadata and evidence are produced concerning the actions of a specific person or different persons. This information will be used in a court, so the provider and the people accessing the

data should be transparent and accountable about the process and their actions. The next two stages are the preservation of evidence and documentation. During the investigation, all data and potential evidence should be preserved in order to maintain the chain of custody. At the same time, personnel actions, assets used and resources provided should be clear documented, so no one can challenge the outcome of the process. In order the investigator's team working on the incident to succeed on this, they should be transparent and accountable for their actions at all times. Besides the above contribution, the accountability constraint also assists to confirmation of the incident by providing attributability. In other words, to reveal the system element or the actor, responsible for a deviation from the expected behavior. On the other hand, the task monitor action is realized in the incident identification stage by monitoring all the actions of the team.

As far as the legal matters constraint is concerned, it assists a wider range of stages in the investigation process. In particular, it realizes the incident identification stage with two of its tasks, the SLAs and jurisdiction. From the SLAs point of view, all contracts and agreements should be read and reviewed to understand all the legal and technical aspects - rights and obligations. This will help to determine the strategy the investigators will take to fulfil the goals. From the jurisdiction point of view, depending on the contracts, application of warranty should be produced to grant permissions to different stages of the investigation. The next stage that the specific constraint is applied to is the preservation of evidence with the maintained trained personnel task. The organization's persons that will assist in the investigation need to be trained in laws and legislations in relation to the Information Technology. By providing the appropriate trained personnel, the constraint fulfils the concurrent stage, training and planning of the investigation process, at the same time. This is because the personnel will be trained to be able to manage any issues that arise and update strategy and plans in accordance. Another point is that the preservation of evidence is exclusively related to legal matters due to the legal frameworks. There are specific rules, policies and regulations on how to preserve the evidence and what processes should be followed. The last stage that the legal matters constraint is applied to is in the presentation. It provides the testimony and the documentation of the evidence. In order for a cloud service to be forensic-enabled, investigators should take under consideration all the legal aspects and present them in a court.

The forensic constraint of access rights is very important in the evidence examination and analysis stage. Depending on the access rights given to the consumers, investigators can put the bits and pieces stored in the log files together. Log files include timestamps with the users' movements, date and time of all authentication and authorization access to the cloud services and accessed files. During the examination of logs, a timeline with the reconstruction of events of the incident can be produced and metadata can be provided. However, access rights constraint also assists to the preservation of evidence stage. It provides the documentation of how the evidence were identified, collected and acquired by investigators, providers and external users, during the investigation process.

The isolation constraint besides the ability of separating the users with one another, reflecting the difficulty of the perpetrator to contaminate the rest of the consumers, also

assists to the cloud forensic investigation process in the following way. During the collection and acquisition stage, it provides confidentiality and privacy to the consumers sharing the same resources by not allowing access to their sensitive data since they are isolated from the rest of the users. In that way, people responsible for collecting potential evidence can move forward without worrying about privacy violation.

Finally, the traceability constraint fits into the investigation process in two different stages. On one hand, at the confirmation of the incident, where the detection of the incident occurs by different sources such as personnel, detection systems, etc. Monitoring users' activities and data logs (two of the tasks of the traceability constraint) can allow systems to capture an incident by detecting any malfunctions or abnormal activities. After the detection, it is up to the organization will to decide whether the incident imposes an immediate threat or not. On the other hand, all four tasks of the traceability constraint can fulfil the examination and analysis stage. Since data is monitored and recorded in log files, investigators can search for these log files during the examination stage and find evidence such as timestamps, metadata or any other information. Log files are also responsible for providing correct timelines and reconstruction of the events, as a result to link users with their data. Besides the two main stages, traceability assists also in the concurrent activities of preservation of evidence and documentation. By storing and securing the log files in restricted areas and taking back-up on a daily basis, investigators can be almost certain that the chain of custody can be preserved and the integrity of the evidence will be maintained at all times. Reports and lists can be also produced from the log files in order to proper document the investigation process.

Now that the seven forensic constraints have been presented in relation to the proposed forensic investigation stages, it is clear their contribution to the investigation process. Thus, the next step is a detailed description of the two steps of the last stage of the proposed process in order to understand its importance.

Define solutions. This step of the process concerns the selection of the solutions. In stage 2 of the framework process, a selection of the technologies for the implementation of forensic constraints took place based on specific criteria. A number of different technologies/solutions have been presented for each task that fulfills the implementation of the constraint. At this point, software engineers should choose the most appropriate solution out of the selected ones that fits into their organization. The selected solution for each forensic constraint will be summarized in the cloud service template [8] introduced in the first stage of the process.

Table 1 presents the seven forensic constraints and their tasks in relation to the cloud investigation process and the stage or stages they apply to. It specifies which task of the constraint fulfils and fits to a specific stage or stages of the process. The first two columns illustrate the forensic constraints and their tasks. The third column illustrates the different stages of the investigation that the constraint/tasks fulfils, while the last one, presents the existing solutions for the specific challenge of the forensic constraint's task. Observing Table 1 someone can notice that all seven forensic constraints contribute to the cloud forensic investigation process. All the stages of the process are aligned

to the seven constraints. This validates that the proposed seven forensic constraints interfere/influence the cloud forensic investigation and they take under consideration the investigation process.

Validation. The last step of the framework process is the validation where software engineers validate the selected solution against the investigation process based on the input of Table 1. The selected solution is tested using a scenario in order to investigate if it is capable to overcome the problems. An incident is initiated and software engineers follow all the investigation process steps in a forensically sound manner to validate the technology/solution chosen and the framework itself.

Table 1. Forensic requirements contribution to cloud investigation process

Constraint	Task	Fulfillment	Indicative Solutions
Internal disciplinary procedures	Implement discipline rules	Incident identification – Collection and acquisition	Define SLA parameters and objectives - Robust SLAs
	Enable access rights	Preservation of evidence – Collection and acquisition	Organizational policies and SLAs
	Enforce legal contracts	Incident identification – Collection and acquisition	Well and clear-written terms - Robust SLAs
Accountability	Ensure agreements	Incident identification – Evidence examination & analysis – Documentation	Define SLA parameters and objectives - Robust SLAs
	Provide assurance	Evidence examination & analysis – Documentation	Accountable cloud - External auditors
	Monitor actions	Preservation of evidence – Evidence examination & analysis – Documentation	Detailed documentation from start to end - Distributed signature detection framework - Unified time system
	Provide attributability	Confirmation of the incident – Evidence examination & analysis – Documentation	Accountable cloud - Define SLA parameters and objectives
Transparency	Ensure visibility	Evidence examination & analysis – Documentation	Accountable cloud - TrustCloud framework
	Provide procedures and policies of treating data	Evidence examination & analysis – Documentation	Define SLA parameters and objectives - Robust SLAs
	Provide notification on policy violation	Evidence examination & analysis – Documentation	Accountable cloud - Robust SLAs
Legal matters	Define SLAs	Incident identification – Presentation	Define SLA parameters and objectives - Robust SLAs
	Ensure jurisdiction	Incident identification – Presentation	Faster compliance with court orders - International laws
	Maintain trained personnel	Preservation of evidence – Update training & planning libraries – Presentation	Team collaboration with wide range of skills - Trained and qualified personnel
Access rights	Ensure registration and validation control	Preservation of evidence – Evidence examination & analysis	Logging mechanism - Secure-Logging-as-a-service - Digital signature
	Enable authentication and authorization control	Preservation of evidence – Evidence examination & analysis	Logging framework - Digital forensic readiness model

	Enable access control	Preservation of evidence – Evidence examination & analysis	Level of access - Organizational policies and SLAs
Isolation	Ensure users do not have access to each other	Collection and acquisition	Proofs Of Retrievability - Identity and access management in future internet architecture
	Prevent contamination of other users	Collection and acquisition	Compartmentalization - Intrusion Detection Systems
	Provide confidentiality	Collection and acquisition	Multi-tenancy model - Digital forensic readiness model - DAC-MACS
Traceability	Monitor user activities	Confirmation of the incident – Evidence examination & analysis	Log-based model - Log management architecture
	Monitor data logs	Confirmation of the incident – Evidence examination & analysis	SecLaas - Log management architecture
	Store and secure logs	Evidence examination & analysis	SecLaas-RW - Log management
	Link users to data	Evidence examination & analysis	Identity management - Identity governance

4.2 Digital Forensic Readiness

The main purpose of the proposed alignment is the identification of the degree of the forensic readiness of a specific cloud service against a forensic investigation. A number of researchers introduced various definitions for cloud forensic readiness [22-24]. In [25] cloud forensic readiness has been defined as “The organization’s preparations to minimize the impact of an incident in a cloud forensic investigation, while identifying and acquiring the maximum amount of digital evidence”.

Cloud forensic readiness is a subset of digital forensics readiness and it designates the need for digital forensic readiness in cloud environments. DFR is important due to the fact that organizations can fortify behind activities and processes that can predict and assist investigators in case of an incident. ISO/IEC 27043: 2015 [26] deals with investigative readiness and the steps that need to be taken prior to an incident occurring. ISO/IEC 27043: 2015 is the only international standard that includes detailed guidelines on the implementation of DFR as a process [27]. The readiness process class is shown outside of the dotted lines since it is a precautionary measure or proactive process that does not have to be involved (an optional process) in the reactive Digital Forensic Investigation (DFI) process [28].

5 Conclusion

Cloud Service Providers bring services to consumers on demand through the internet. In order to provide these services in a forensically sound manner, CSPs should be able to design and implement the services taking under consideration specific forensic requirements. This will assist investigators to acquire and examine evidence in accordance to the forensic investigation rules and procedures and produce admissible evidence

in a court. The research community should bend over the specific field and produce reliable solutions towards this direction. In this paper, an alignment between the forensic requirements that are included in the design of forensic-enabled cloud services and the cloud forensic investigation process took place providing a form of validation to our previous work regarding the design of a framework for designing forensic-enabled cloud services. The results of the validation are encouraging since all the different stages of the investigation process align with the proposed forensic requirements.

References

1. Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud Forensics. In: Peterson G, Shenoi S, editors. Advances in Digital Forensics VII, 7th IFIP WG 11.9 International Conference on Digital Forensics. 1st ed. Berlin, Heidelberg: Springer; 2011. p. 35-46. DOI: 10.1007/978-3-642-24212-0_3
2. Thethi N, Keane A. Digital forensics investigations in the Cloud. In: Proceedings of the IEEE International Advance Computing Conference (IACC'14); 21-22 February 2014; Gurgaon, Harayana, India. New York: IEEE; 2014. p. 1475-1480
3. Orton I, Alva A, Endicott-Popovsky B. Legal Process and Requirements for Cloud Forensic Investigations. In: Ruan K, editor. Cybercrime and Cloud Forensics: Applications for Investigation Processes. Hershey, PA, USA: IGI Global; 2013. p. 186-229. DOI: 10.4018/978-1-4666-2662-1.ch008
4. Freet D, Agrawal R, John S, Walker J, J. Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS. In: Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems (MEDES '15); 25-29 October 2015; Caraguatatuba, Brazil. ACM; 2015. p. 148-155
5. Almulla S, Iaqi Y, Jones A. Cloud forensics: A research perspective. In: 2013 9th International Conference on Innovations in Information Technology (IIT). IEEE; 2013. p. 66-71
6. RightScale. State of the Cloud Report 2018: Data to Navigate your Multi-Cloud Strategy. https://www.rightscale.com/lp/state-of-the-cloud. [Accessed February, 2019]
7. National Research Council. Strengthening forensic science in the United States: a path forward. National Academies Press, 2009.
8. Simou S, Kalloniatis C, Gritzalis S, Katos V. A framework for designing cloud forensic-enabled services (CFeS). Requirements Engineering. 2018; 1-28. DOI : 10.1007/s00766-018-0289-y
9. Simou S, Kalloniatis C, Mouratidis H, Gritzalis S. Towards a Model-Based Framework for Forensic-Enabled Cloud Information Systems. In: Katsikas S, Lambrinoudakis C, Furnell S, editors. 13th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2016). Switzerland: Springer International Publishing; 2016. p. 35-47. DOI: 10.1007/978-3-319-44341-6_3
10. Simou S, Kalloniatis C, Mouratidis H, Gritzalis S. A survey on cloud forensics challenges and solutions. Security and Communication Networks. 2016; 9:6285-6314. DOI: 10.1002/sec.1688
11. Martini B, Choo K-K, R. An integrated conceptual digital forensic framework for cloud computing. Digital Investigation. 2012; 9:71-80. DOI: 10.1016/j.diin.2012.07.001
12. McKemmish R. What is forensic computing?. Canberra, Australia: Australian Institute of Criminology; 1999
13. Kent K, Chevalier S, Grance T. Dang H. Guide to integrating forensic techniques into incident response. NIST Special Publication, SP 800-86. 2006. 121 p.

14. Agarwal R, Kothari S. Review of Digital Forensic Investigation Frameworks. In: Kim K, J, editor. Information Science and Applications. Berlin, Heidelberg: Springer; 2015. p. 561-571. DOI: 10.1007/978-3-662-46578-3_66
15. Ruan K, Carthy J. Cloud Forensic Maturity Model. In: Rogers M, Seigfried-Spellar K, C, editors. Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C. Berlin, Heidelberg: Springer; 2012. p. 22-41. DOI: 10.1007/978-3-642-39891-9_2
16. Zawoad S, Hasan R, Skjellum A. OCF: An Open Cloud Forensics Model for Reliable Digital Forensics. In: Proceedings of the IEEE 8th International Conference on Cloud Computing (CLOUD'15). New York: IEEE; 2015. p. 437-444
17. Adams R. The Emergence of Cloud Storage and the Need for a New Digital Forensic Process Model. In: Ruan K, editor. Cybercrime and Cloud Forensics: Applications for Investigation Processes. Hershey, PA, USA: IGI Global; 2013. p. 79-104. DOI: 10.4018/978-1-4666-2662-1.ch004
18. Guo H, Jin B, Shang T. Forensic investigations in cloud environments. In: Proceedings of the 2012 International Conference on Computer Science and Information Processing (CSIP). 24-26 August 2012; Xi'an, Shaanxi, China. New York: IEEE; 2012. p. 248-251
19. Simou S, Kalloniatis C, Kavakli E, Gritzalis S. Cloud Forensics: Identifying the Major Issues and Challenges. In: Jarke M, Mylopoulos J, Quix C, Rolland C, Manolopoulos Y, Mouratidis H, Horkoff J, editors. 26th International Conference, CAiSE 2014. Cham: Springer International Publishing; 2014. p. 271-284. DOI: 10.1007/978-3-319-07881-6_19
20. Simou S, Kalloniatis C, Kavakli E, Gritzalis S. Cloud Forensics Solutions: A Review. In: Iliadis L, Papazoglou M, Pohl K, editors. CAiSE 2014, International Workshop. Cham: Springer International Publishing; 2014. p. 299-309. DOI: 10.1007/978-3-319-07869-4_28
21. Kalloniatis C, Mouratidis H, Vassilis M, Islam S, Gritzalis S, Kavakli E. Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. Computer Standards & Interfaces. 2014; 36:759-775. DOI: 10.1016/j.csi.2013.12.010
22. Alenezi A, Hussein RK, Walters RJ, Wills GB. A Framework for Cloud Forensic Readiness in Organizations. In: 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud). San Francisco, USA. IEEE; 2017. p. 199-204
23. De Marco L, Kechadi MT, Ferrucci F. Cloud forensic readiness: Foundations. In: P. Gladyshev, A. Marrington & I. Baggili, editors. 5th International Conference on Digital Forensics and Cyber Crime (ICDF2C 2013). Moscow, Russia; Springer International Publishing; 2013. p. 237-244
24. Kebande V, Ntsamo HS, Venter HS. Towards a prototype for achieving digital forensic readiness in the cloud using a distributed NMB solution. In: G. Rodosek & R. Koch editors. 15th European Conference on Cyber Warfare and Security (ECCWS 2016). Munich, Germany; Academic Conferences International Limited; 2016. p. 369-378
25. Simou S, Troumpis I, Kalloniatis C, Kavroudakis D, Gritzalis S. A Decision-Making Approach for Improving Organizations' Cloud Forensic Readiness. In: Katsikas S, Lambrinoudakis C, Furnell S, editors. 15th International Conference on Trust and Privacy in Digital Business (TrustBus 2018). Springer, Cham; 2018. p. 150-164
26. ISO. ISO/IEC 27043:2015: Information Technology - Security techniques - Incident investigation principles and processes; 2015
27. Kigwana I, Venter HS. A digital forensic readiness architecture for online examinations. South African Computer Journal; 2018. 30:1, p. 1-39.
28. Kebande VR, Karie NM, Venter HS. A generic Digital Forensic Readiness model for BYOD using honeypot technology. In: 2016 IST-Africa Week Conference. IEEE; 2016. p. 1-12.