Forensics as a Service Interface in Cloud Computing

Mumtaz Anayit, Dale Lindskog, Pavol Zavarsky, Shaun Aghili

Department of Information Systems Security Management
Concordia University College of Alberta, Edmonton, Canada
mumtazanayit@gmail.com,{dale.lindskog, pavol.zavarsky,
shaun.aghili}@concordia.ab.ca

Abstract. This paper introduces and describes the notion of "Forensics as a Service" (FraaS), an interface integrated into cloud architectures for the purpose of forensic investigations involving cloud environments. The interface is designed to address a class of well-known legal, technical, and privacy concerns related to cloud forensics. An implemented FraaS interface would be available to customers, via their SLAs with their cloud provider, to assist them in their forensic investigations, ensuring secure access to and access control of potential evidence through monitoring and auditing, and maintaining the confidentiality, integrity and availability of the potential forensic evidence

Keywords: Forensics, Forensic issues in cloud computing, forensic as a service, CSP FraaS interface

1 Introduction

Considering the increasing prevalence of cloud computing, there is an urgent need to overcome barriers to sound forensic investigations in cloud environments. When faced with this need for forensic investigation, entities such as cloud regulators, law enforcement, litigators and consultants face a number of well-known legal, technical and privacy challenges. There are challenges around jurisdiction when data is stored in different geographical locations; difficulties separating evidence from other customers' data due to multi-tenancy; there may be a lack of legislative mechanisms to retrieve evidence, given confidentiality and compliance requirements and data retention policies. Other concerns revolve around cloud service provider dependency, chain of dependency preservation, the large bandwidth consumption often associated with forensic investigation, and issues concerning time line analysis of logs, log review, log correlation, and policy monitoring [1].

To address these challenges, we propose Forensics as a Service (FraaS); a service accessed via an interface and designed to facilitate the customer's forensic investigation, acting as a separation and integration layer between the Cloud Service Provider (CSP) and the customer. It would include components to manage SLAs, legal terms and conditions, provide access to forensic tools, logs and APIs, and ensure that access control mechanisms, encryption and authentication, monitoring, logging, etc., are in place.

A CSP would maintain the interface to provide forensic services to the cloud customer. This interface would act as an abstraction layer for other parties associated with the forensic investigation, such as government bodies, other cloud service providers, legal and auditing firms, and software or hardware vendors.

This paper will describe, abstractly, the components of the proposed FraaS interface, including only those specifics necessary to address those well-known issues around cloud forensics outlined above (and described in detail below).

We hope to contribute to improved understanding of these issues in cloud computing forensics, and to begin the process of assisting businesses and legal bodies to overcome these barriers to collecting forensic evidence in cloud environments.

In Section II of this paper, we introduce the reader to related research, focusing on those challenges to forensic investigation in cloud environments. Section III introduces the CSP FraaS interface, and describes its structure and the function of its components. Section IV relates the CSP FraaS interface back to the challenges described in Section II, mapping the elements of the interface to the problems it is designed to address. Finally, we conclude the paper and suggest future work.

2 Challenges To Forensic Investigation In Cloud Computing Environments

In this section, we briefly review cloud computing with a focus on those aspects particularly relevant to digital forensics, and detail the various well known problems that arise when doing forensics in the cloud.

Cloud computing is a model that enables on-demand, convenient and ubiquitous computing, accessible through a shared pool of configurable resources such as services, applications, storage and networks, and that can be provisioned rapidly and released with minimal management effort and/or service provider interaction [2]. These include distributed applications and information infrastructure and services consisting of a shared pool of networks, computers and storage resources [3]. There are three primary cloud service delivery models: Software as a Service (SaaS), where customers rent software for use on a pay-per-use or subscription model; Platform as a Service (PaaS), where customers rent a development environment for application development; and Infrastructure as a Service (IaaS), where customers rent hardware infrastructure on a pay-per-use model or subscription, and the services are scaled depending on demand. Current cloud service providers include Google, Amazon Web Services, Microsoft and Azure Services Platform [4].

Computer forensics is the application of computer analysis and investigation techniques to the task of identifying possible evidence. Traditionally, computer forensics has classified crimes involving computers and associated technologies into three kinds: where the computer is the target of crime; where the computer is a repository of data generated or used during the commission of crime; and where a computer is a tool used in committing crime.

In traditional computer forensics, investigators usually have full or nearly full control over the media storing potential evidence, media such as hard disks, process logs and router logs [1]. Often the investigation process is actually divided into different sub-branches relating to the particular kind of digital devices involved, such as mobile device forensics, network forensics, or computer forensics. A typical investigation at one of these sub-branches normally consists of stages such as imaging, seizure, the analysis of the digital media, and the production of a report from the collected evidence.

This paradigm is not easily applied within a cloud computing environment, and the acquisition and analysis of digital evidence becomes more complex. Computer forensics investigations of cloud computing systems require more time and effort, due to the number of computing devices within the cloud needing forensic examination. Moreover, legally, cloud computing systems make it potentially more difficult for the investigator to analyze and acquire digital evidence with the same standards expected with traditional systems [4].

The nature of cloud computing architecture poses a number of issues and concerns that must be dealt with by forensic investigators. Evidences are stored in various data centers located in various geographical locations making it harder for investigators to retrieve the data particularly if it contains several gigabytes to terabytes. There are also some service providers who don't have their own data center so they rent space from other service providers resulting to a chain of dependency. Before, investigators in computer forensics usually have almost or full control over the evidence. Unfortunately, this is not the same with cloud. In cloud computing, CSP maintains the cloud resources; hence the client depends on CSP to acquire forensic evidence. In addition, Elastic volatile storage of cloud data is also considered as a barrier to cloud forensic compared to other forms of forensic investigation. Multi-tenancy is a feature in cloud which can be an issue in cloud forensic due to impossibility of forensic evidence segregation from other tenant data. CSP dependency issues are inherent in cloud forensic. Third party involvement in cloud is a common scenario. This creates trust, split of control, and level of access issues to forensic evidence.

Due to the nature of cloud computing architecture, evidence can be located in multiple data stores, and in several geographical locations. Evidence can be located in data centers in regions which make it unavailable to the investigator for online retrieval, when there is a large amount of data to retrieve, e.g. several gigabytes to terabytes. As a result, retrieval may require travel, which is time consuming and expensive, and may be even not be possible due to import/export laws or privacy laws.

When a customer needs to perform a forensic investigation, data protection or jurisdiction law in the location where the servers run will apply to the investigation. This can create a situation where the customer and CSP are subject to different laws, in particular when the relevant servers, or when the customer and relevant servers are in different jurisdictions. In a cloud service, providers store data on leased spaces available at large data centers (such as Amazon, Google and Rackspace). Moreover, some services providers do not have data centers in all regions and therefore may store data in spaces rented from other services providers. There can even be chains of such dependency, and as a result of this, a particular client's data may reside in a data store which can be located only by tracing a chain of service provider stores. In such cases a service provider, and therefore its customer, needs to depend on another service providers to locate this storage, and this creates excessive dependency on various service providers. For these reasons, a client may not able to do the forensic investigations in a timely manner, and access to the needed data may even become unreliable if there are a lack of forensic investigation related policies, procedures and agreements between multiple, cross connected service providers. At best, the client must depend heavily on the service provider for their forensic investigation.

In traditional computer forensics, investigators normally have full or almost full control over the evidence (e.g., a hard drive confiscated by police). In a cloud, unfortunately, control over data varies depending on the type of service and the service model. Due to cloud computing architecture, an investigator may not have full control over the disks, as the data may reside in virtual machine snapshots. An investigator therefore needs to depend on the CSP to locate the disks. In addition, and as noted previously, the CSP itself may depend on other CSPs to locate and acquire disk volumes. This lack of control over data volumes is further frustrated by multi-tenancy and privacy issues, which together make cloud forensic investigations potentially difficult [1].

In cloud computing, the CSP maintains the cloud resources, so the cloud client necessarily depends on the CSP to acquire forensic evidence, especially in the case where that evidence is in the form of logs that apply to the cloud environment generally, as opposed to that client specifically, e.g., a cloud host's network, database and operating system logs. But even in those cases where the evidence is clearly associated with the cloud client, there are various problems that arise, which we cover in the following paragraphs.

Cloud computing utilizes so-called 'elastic computing', i.e. on demand resources, and therefore a particular customer's data in the cloud does not always reside in same physical medium, and moreover its particular physical location is volatile, as data stores in virtual machines can move from one physical volume to another.

In cloud computing, multiple VMs may share the same physical infrastructure, i.e., data from multiple customers may be co-located. For example, a block of hard disk may store data from multiple clients. Segregation of data may not be possible even after acquiring the hard disks, because of the complex architecture of cloud data centers. Due to this multi-tenancy, separation of evidence from other customers and therefore preservation of privacy may become challenging.

Related to the above, not only are cloud resources shared among different clients, but similarly, resources can be shared between several cloud service providers. Thus preserving data requires a mechanism to automatically move data belonging to other tenants and allocate resources for them. This creates yet another chain of dependency.

Even when these technical obstacles can be overcome, there are concerns related to forensically sound evidence collection. CSPs may use the cloud resources of other CSPs to ensure highly availability to their clients. In such cases, forensic evidence will be shared amongst CSPs, raising concerns about chain of custody. For evidence to be admissible in court, it should be clear how that evidence was collected, analyzed, and preserved, but the relevant multi-jurisdictional laws, procedures, and proprietary technologies make it a challenge to maintain chain of custody [5].

Finally, a CSP should maintain its client's privacy, but during a forensic investigation, when a CSP obtains the services of outside parties, such as auditing and compliance contractors, law enforcement, forensic investigators, incident handlers, law advisors and software vendors, serious concerns arise around split of control and levels of access [6].

Many problems related to the cloud computing forensics are mentioned in the research including different cloud computing models, multifaceted architectures, access of large data for forensic investigation, unclear boundaries between cloud providers and their sub-contractors which is due to different jurisdictional privacy and legal laws in place. Moreover, there are issues on the dependency of clients on cloud services provider for the forensics investigations. Investigators also faces issues on the complexity of forensic evidence due to multi-tenancy and privacy issues, impossibility to segregate data, elastic storage in cloud computing, management issues, shared responsibilities, dependency of forensics tools on the cloud technologies and other legal issues. Other problems also contribute to complexities such as chains of custody of forensic evidence due to the CSP dependency on different vendors along with the split of control and level of access issue for third parties that make cloud forensic a challenging task for cloud computing.

3 CSP FRAAS INTERFACE DESCRIPTION

In this section we describe the proposed CSP FraaS interface, and provide a high level analysis of how the cloud customer and other parties involved in cloud forensic investigation interact with it. We do not justify its components and features until the following section, where we relate these components and features to the problems associated with forensics in the cloud, as described in the previous section.

The CSP interface acts as an intermediary between the cloud customer and the cloud service provider. The interface provides the cloud customer access to tools, applications, and available services, and also provides service aggregation and integration of multiple CSPs. This layer works as a cloud resource absorption layer. The interface does not reveal the details of the CSP's internal functionality.

The FraaS interface is one amongst other interfaces included in the CSP management plane, and is a composite of two sub-interfaces. These are the customer interface and the publisher interface. Cloud customers connect to the customer interface and cloud service providers connect to the publisher interface. The CSP customer interface and the publisher interface are different views of the CSP FraaS Interface. Access to these views is controlled by encrypted communication channels.

The FraaS interface provides forensic SLA management and monitoring, notifications about forensic events/logging, offers forensic services and communication with other parties such as government bodies, audit and legal firms. The CSP FraaS interface is two dimensional, consisting of interaction between the CSP and cloud customers provided by customer interface, and interaction between the CSP and other external parties. Internal components of the CSP interface provide security and access control, storage, and notification services between these two sub-interfaces. The CSP interface displays forensic services offered by the CSP, a summary of SLA terms and conditions, perhaps promotional offers, prices, etc.

The FraaS publisher interface is the interface that can be viewed by other cloud service providers, government bodies, other cloud standard organizations, and forensic tools developers. Based on the role of the connecting party, access is limited to required functions. This interface is hidden from the cloud customer. The publisher interface includes registration services, help desk management, SLA monitoring and access levels based on user category. The main objective of this interface is to act as a service aggregation layer between the customer and CSP, as well as between the CSP and other external parties. The publisher interface handles back end, third party operations and requests. It includes forensic tool support, external auditing, legal advisories, and compliance requirements.

Service Level Agreements (SLA) is used to maintain the contracts between the CSP and the cloud customer. The cloud customer and CSP should sign the SLA at the time of registering for forensic services. The SLA between the CSP and the customer should cover both functional and non-functional aspects of the agreement. Functional aspects include the activities for forensic investigation, gathering evidence, and data analysis. Non-functional aspects include performance parameters, SLA violations, response time, etc. [7].

The SLA between the CSP and the cloud customer and the SLAs between different CSPs and other parties should be defined in the terms and conditions.

The key points in SLAs between CSP and customer such as, data ownership should be defined by the CSP in case of forensic investigation. The CSP should maintain records of archives, volume snapshots, backups and repositories of data. Access to storage volumes for forensic investigation should be provided by the CSP. Retention period should be defined for data volumes and data on hold. Volume of data that can be provided and preserved should also be defined. SLAs should as well define technical terms, legal terms, organizational terms and auditing terms. SLA violations should be handled according to the agreed actions and corrective mechanisms.

4 How CSP FraaS Interface Address The CSP FraaS Interface Design And Implementation Issues

In this section we cover how the proposed FraaS interface addresses those issues with forensics in the cloud, discussed in Section II.

A CSP FraaS interface overcomes the problem of cloud service provider dependency, replacing direct communication between the customer and the CSP with an interface with components and features guaranteed by SLAs with the different parties involved in the process. The CSP interface is a central point of contact or point of reference between the customer and the service providers. Further, the interface should have information related to forensic tools and applications, forensic service providers; professionals service brokers, government bodies, legal firms, audit firms, cloud standard organizations such as NIST.

The customer decides what data they need to acquire, and based on this would contact the correct CSP. The CSP FraaS interface would have the information available regarding the required data, and would communicate on behalf of the customer. Access to metadata is often required in forensic investigation. Accessing metadata and system logs in the cloud is difficult for a customer who does not have the support of the CSP. Without such support, the customer often needs to identify applicable jurisdiction law based on the CSP's location, in order to determine laws and regulations related to data preservation, litigation, and access [2], whereas a CSP already has this information. This is important if the data is stored in a region other than the customers, since the applicable laws might be different. A possible solution for this issue is to have a clause in the SLA between the CSP and the customer granting the customer access to data through a FraaS interface. The advantage of communication through the FraaS CSP interface is that all the required information will be included. This includes a preservation period, formatting of data, frequency of access, etc., since the interface would provide ready access to the necessary templates and letter formats.

The feasible solution for jurisdictional issues is to define SLAs at the point of signing the service agreement with the CSP, to ensure the specified forms of forensic evidence will be provided when requested. A CSP would have the responsibility to monitor the physical locations of data storage, and keep track of its movement in the cloud. The FraaS interface would include a SLA section to define the terms to keep track of storage movement. When geographically disperse storage is itself a problem, the SLA could specify that its movement be within the regions of close proximity or within the same region.

The SLA between the customer and the CSP should clearly reference those jurisdiction laws that bear on data preservation, and the CSP should maintain this across any chain of dependency between CSPs. There may need to be multiple SLA types between CSPs. For example, a CSP might have a 'counter' SLA with another CSP, related to a given SLA between the CSP and its clients. The terms of this SLA may regulate monitoring the movement of data storage for a particular client or clients. (This is also known as “record keeping”.) Such agreements would reduce that CSP's dependence on other CSPs to locate the stored data.

With such SLAs in place, a CSP will monitor the cloud snapshots and storage. Access to the disks would be governed by the terms agreed in these SLAs. Therefore, the disks which are subject to forensic investigation will be isolated from those of other tenants. A CSP should maintain a record of the VM snapshots; help to overcome issues of multi-tenancy and privacy. Secure channels would be used for communication with external parties without compromising confidentiality, and an interface governed by such SLAs would provide a better level of security throughout the chain of dependency.

Levels of access to and access control of the FraaS interface would be controlled through APIs. Such mechanisms would be built in to the interface, which would include separate contracts for forensic services requested by each client. Through the interface a CSP might assign in-house or outsourced forensic teams for each contract. The interface would provide control of access to different functions, thus ensuring segregation of duties and split of control. There would be procedures for record keeping and monitoring or auditing, the integration of encryption and access control would help to ensure privacy and integrity of forensic operations.

Cloud computing employs elastic computing. Data is stored dynamically based on the availability of cloud resources in different time slots and in different storage blocks, and thus to trace that data storage can be challenging. A record-keeping or tagging system applied to data volumes could be used to identify in which instance the data is stored at a given time. Digital tagging or signatures might be used to identify remaining data, using cookies or any other traces of data storage. Since cloud architectures employ multi-tenancy, data that belongs to different customers can reside in same volume. Digital tags can be used to identify and track the movement of data within the volumes for any client. This feature can integrate with a FraaS interface to trace the forensic evidence.

The following table summarizes this section, outlining how a CSP FraaS interface can address those challenges to cloud forensics discussed in Section II.

Table: Synopsis of Forensic Issues with its corresponding Solutions

Forensic Issues	**Solutions for Interface**	**Description**
Large bandwidth needed for forensic Investigation	Interface backend	Interface contains all the required and all set information for forensic investigation which will reduce the large bandwidth and time constraint issues for investigation.
Chain of Custody	Secure channels, SLA, and policies	Other CSPs will upload the forensic data through the interface which will help reduce the chain of custody
Limited Access to Cloud Resources	Interface backend	Investigator can obtain full access to cloud resources to execute the forensic operation because Interface has provisions to access the needed evidence or resources.
Multi-tenancy issues.	SLA	Through the Interface CSP can do record-keeping of snapshot movements.
Chain of dependency	SLA, Policies	Interface has facility to monitor the volume movements across CSPs. It will be used to streamline forensics operations.

Jurisdictional issues	SLA, CSP /customer policies/procedures	Defining a clause in SLA at the point of signing agreement to track the movement of volumes in cloud. Jurisdictional issues can be minimized by mutual agreement through Interface SLAs between CSP and Cloud Client
Access to System logs	SLA/Policies	Interface will have access to the network, systems and databases logs.
Access level for Third Party	Encrypted secure channels	Interface will have the functionality to maintain the access level for third parties.
Third Party Trust Issues	Policies/terms and conditions/secure channels	When CSPs have direct relationships and communication with third parties through interface, they will maintain trust relationships with the parties involved.
CIA of Evidence	Secure channels, Encryptions	Confidentiality, integrity and availability can be achieved through encrypted access channels, logging and access rules that are integrated with Interface.
Lack of knowledge in forensics	Knowledge base	Interface has a separate section for knowledge base and support to educate clients about forensics procedures and other relevant policies.
Lack of tools	Interface Backend	Interface provides a repository of tools and applications including the process of acquiring new tools.

5 CONCLUSION & FUTURE WORK

In this research paper, we reviewed research concerning the challenges surrounding cloud forensics, and explored previously proposed solutions to these technical, legal and privacy challenges. The main contribution of this paper is to recommend the use of a CSP FraaS interface as a general approach to overcoming these challenges.

For future research, we recommend exploring automation of several functions of the interface, such as SLA definitions, data and signature tagging, and the integration of encryption standards. Since use of a FraaS interface depends on SLAs and legal compliance, future work may include exploring a forensic legal framework for cloud environments or remodeling commonly accepted cloud forensic standards.

REFERENCES

[1] S. Zawoad and R. Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," *arXiv:1302.6312v1 [cs.DC] 26 Feb 2013,* pp. 1-15, 2013.

[2] D. Willson, "Legal Issues of Cloud Forensics," 10 01 2014. [Online]. Available:http://www.titaninfosecuritygroup.com/UserFiles/HTMLEditor/Legal%20Issues%20of%20Cloud%20Forensics.pdf.

[3] H. Takabi, J. B. D. Joshi and G. J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *Security & Privacy, IEEE (Volume: 8, Issue: 6)*, pp. 24 - 31, 2010.

[4] M. Taylor, J. Haggerty, D. Gresty and D. Lamb, "Forensic investigation of cloud computing systems," *Network Security*, pp. 4-10, 2011.

[5] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on*, *pp*. 1-10, 2011.

[6] C. Dumit, E. Sousa, R. Padilha and R. Menzer, "MO447 - Digital Forensics," *Seminar Series – Digital Forensics (MO447/MC919)*, pp. 1-46, 2013.

[7] F. Jrad, J. Tao and A. Streit, "SLA BASED SERVICE BROKERING IN INTERCLOUD ENVIRONMENTS," *CLOSER 2012 - 2nd International Conference on Cloud Computing and Services Science*, pp. 76-81, 2012.