Cloud Forensic Maturity Model

Keyun Ruan and Joe Carthy

Center for Cybersecurity and Cybercrime Investigation
University College Dublin
{keyun.ruan,joe.carthy}@ucd.ie

Abstract. In this paper we present a shortened version of the Cloud Forensic Maturity Model (CFMM). It composes of two inter-related parts, i.e., the Cloud Forensic Investigative Architecture (CFIA) and the Cloud Forensic Capability Matrix (CFCM). The CFMM is developed in order to create a reference model to evaluate and improve cloud forensic maturity. It is a part an on-going project, and is evaluted by a panel of experts and practitioners as a first step for further cloud forensic standardization efforts.

Keywords: Cloud Forensics, Cloud Computing, Digital Forensics, Cloud Forensic Maturity Model, Cloud Forensic Investigative Architecture, Cloud Forensic Capability Matrix, Cloud Forensic Standardization.

1 Introduction

As the cloud paradigm emerges, the need for carrying out digital investigation in cloud computing environments has become inevitable, no matter it is internal investigation initiated by one of the cloud actors to investigate security incidents and policy violations, or external investigation initiated by law enforcment to investigate crimincal or civil cases. Cloud forensics is at its infancy. It is faced with challenges in technical, organizational, and legal dimensions, as well as promising opportunities as listed in Ruan et al. (2011A). The cloud paradigm shift has initiated a major standardization wave. It is an unique timing to analyze and integrate missing forensic considerations and capabilities into the standardization and maturing process of cloud computing.

Based on the survey “Cloud Forensics and Critical Criteria for Cloud Forensic Capability” carried out for the purpose of this research (Ruan et al. 2011B), we propose the Cloud Forensic Maturity Model (CFMM), a reference model for evaluating, developing and improving cloud forensic maturity. CFMM composes of two inter-related parts, i.e., the Cloud Forensic Investigative Architecture (CFIA), and the Cloud Forensic Capability Matrix (CFCM). CFIA is a conceptural reference architecture for digital investigations in cloud computing environments. CFCM is a matrix to evaluate and improve capabilities that correspond to components in CFIA.

In this paper we introduce a shortened version of CFMM due to the page limit. We dicuss the initial validation and feedback for CFMM carried out by a panel of digital forensic experts and practioners. We then provide three brief use cases of CFMM. Firstly we use it to discuss invesitgative scenarios and generate process models. Secondly we use it to compare current cloud capaiblities of several leading cloud offerings. Lastly we use it to analyze cloud forensic standardization gaps.

M. Rogers and K.C. Seigfried-Spellar (Eds.): ICDF2C 2012, LNICST 114, pp. 22–41, 2013.

This research is still on-going with various in-depth analyses and mappings, however, we believe it is useful to share with the research community our current thinking and progress on developing such a model in order to lay a foundation and provide a structure for various discussions and efforts at the early days of cloud forensic research and development.

2 Cloud Forensic Investigative Architecture (CFIA)

The Cloud Forensic Investigative Architecture (CFIA) is developed to include key components for enabling digital investigations in cloud computing environment. A high level component based representation of the Cloud Forensic Investigative Architecture is shown in Figure 1.

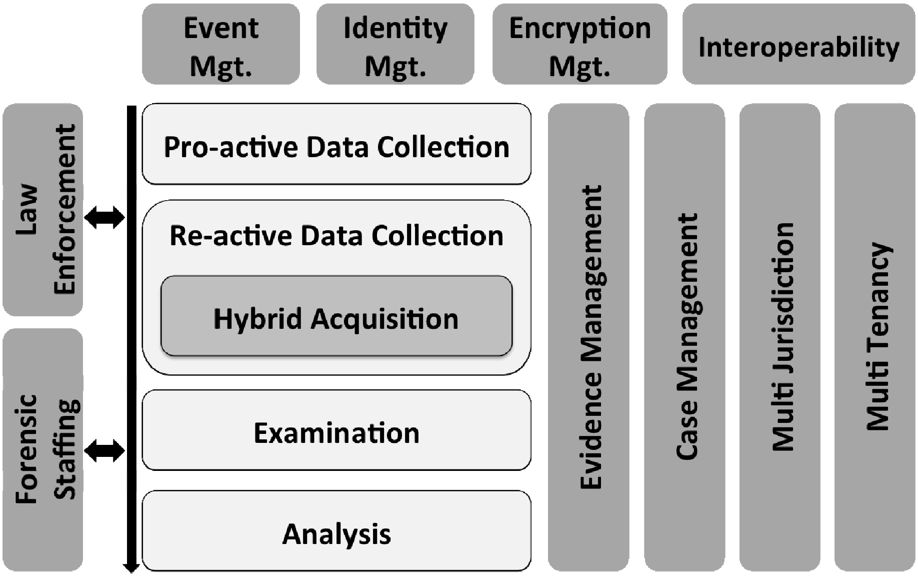

Fig. 1. Cloud Forensic Investigative Architecture

The Cloud Forensic Investigative Architecture is composed of four main sections as follows

- Pre-investigative Readiness
- Core-forensic Process
- Supportive Processes
- Investigative Interfaces

As shown in Fig 1, the black line represents the concept of interface. Everything on the right hand side of the black line is the cloud environment being investigated. The cloud environment consists of its technical infrastructure that is often a shared environment, the organizational interation among all cloud actors (cloud consumer, cloud provider, cloud broker, etc.) and its legal complications such as multi-jurisdiction and multi-tenancy.

On the left hand side of the black line are the “investigators”, either internal forensic team or external law enforcement, who carry out the investigation by utilizing and managing the forensic capabilities within the cloud environment adding their own forensic capabilities.

On the top of the architecture are the pre-investigative readiness components. Pre-investigative readiness components include event management, identity management, encryption management, and interoperability. These components are essential to ensure investigative preparedness and enable investigations.

In the centre of the architecture in the vertical layout are the core forensic process components. Core foensic process components include pro-active data collection, re-active data collection, hybrid acquisition, examination and analysis. Hybrid acquisition is a part of re-active data collection, however, as it includes a wide range of forensic acquisition techniques which will be discussed later in the paper, it is prudent to consider it as a separate core forensic phase.

On the right of the architecture in the horizontal layout are the supportive processes components . Supportive processes components include evidence management, case management, mulitple jurisdiction and multi-tenancy. They are needed throughout the timeline of an investigation.

3 Cloud Forensic Capability Matrix (CFCM)

Borrowing core concepts of the Capability Maturity Model (CMM) for Software developed by Paulk (1993), the Cloud forensic Capability Matrix is a capability maturity model for assessing and improving cloud forensic capability maturity for any given cloud actor (i.e. cloud consumer, cloud provider, cloud broker, cloud carrier, cloud auditor) or law enforcement.

The Cloud Forensic Capability Matrix composes of six maturity levels from low to high as follows:

- Level 1 Minimum
- Level 2 Basic
- Level 3 Ad-hoc
- Level 4 Well-formalized
- Level 5 Mature
- Level 6 Advanced

Cloud forensic capabilities are the basis for the Cloud Forensic Capability Matrix, and are divided into four main categories corresponding to the cloud forensic architecture:

- Pre-investigative capabilities: capabilities in preparation for both internal and external investigations
- Investigative capabilities: capabilities required in the core investigative process
- Supportive capabilities: capabilities required to support and complete the investigation case

- Interfacing capabilities: capabilities dealing with the internal and external interface between the cloud system environment and investigative parties involved in cloud investigations.

Each capability is composed of key capability, sub capability and a set of key criteria in organizational, legal and technical dimensions. Figure 2 shows all key capabilities with sub capabilities as a detailed view of the CFIA.

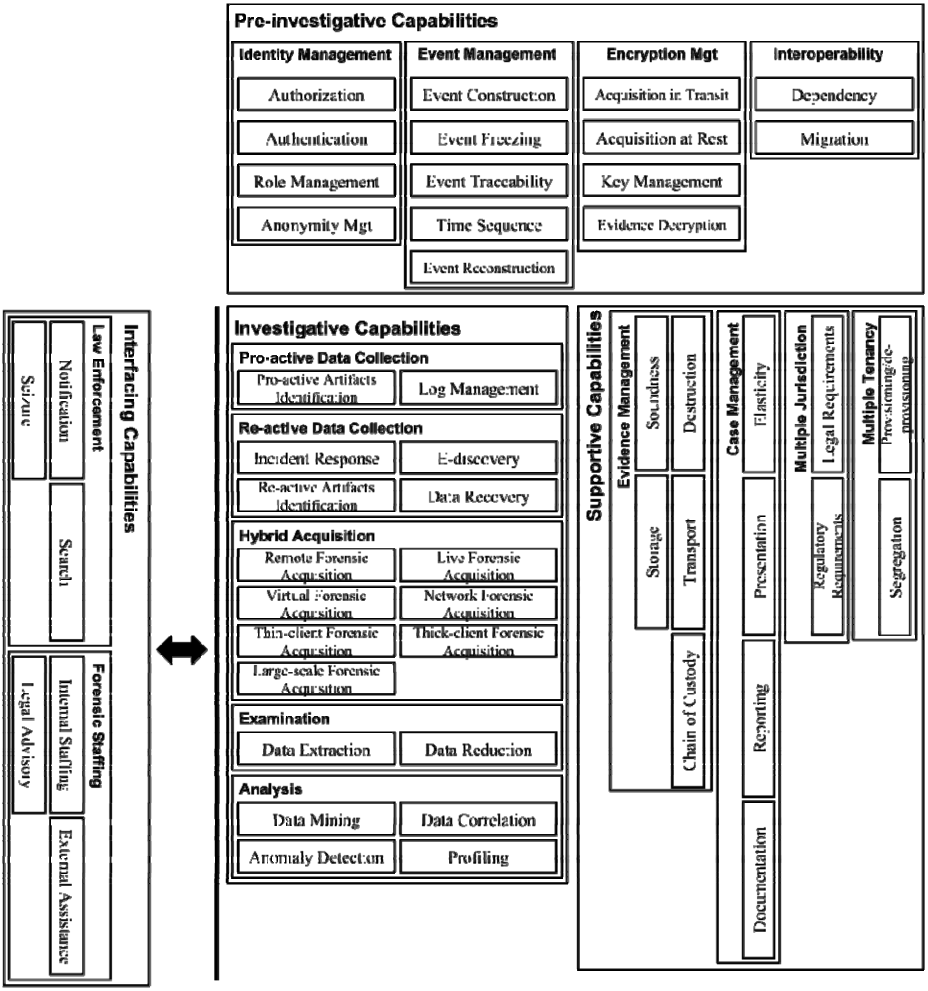

Fig. 2. Cloud Forensic Capabilities

Due to page limit, we provide a section of the CFCM, a top-level pre-investigative capability matrix for cloud consumer, cloud provider, cloud auditor and law enforcement as shown in Table 1 below.

Detailed descriptions and criteria requirements for each actor on each level for each capability are being developed and refined. Use cases are being collected for validation.

Table 1. Pre-investigative Capability Matrix for Cloud Consumer, Cloud provider, Cloud Auditor and Law Enforcement

	Consumer							Provider							Auditor							Law Enforcement						
		1	2	3	4	5	6		1	2	3	4	5	6		1	2	3	4	5	6		1	2	3	4	5	6
Pre-investigative capabilities																												
Identity management																												
Authorization		X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X							
Authentication		X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X							
Role management		X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X							
Anonymity management					X	X	X				X	X	X	X				X	X	X	X						X	X
Event management																												
Event construction						X	X					X	X	X					X	X	X							
Event freezing						X	X						X	X						X	X						X	X
Event traceability						X	X					X	X	X					X	X	X					X	X	X
Time sequence					X	X	X				X	X	X	X				X	X	X	X							
Event reconstruction					X	X	X				X	X	X	X				X	X	X	X				X	X	X	X
Encryption management																												
Acquisition in transit						X	X					X	X	X					X	X	X						X	X
Acquisition at rest					X	X	X				X	X	X	X				X	X	X	X					X	X	X

Table 1. (*Continued.*)

Key management			X	X	X	X	X			X	X	X	X	X		X	X	X	X	X	X							
Evidence decryption					X	X	X				X	X	X	X				X	X	X	X					X	X	X
Interoperability																												
Dependency						X	X						X	X						X	X						X	X
Migration						X	X						X	X						X	X						X	X

4 Cloud Forensic Capabilities

In this section we provide brief descriptions for all cloud forensic key capabilities and sub capabilities. Key criteria for each capability is not included in this paper due to page limit.

4.1 Pre-investigative Capabilities

4.1.1 Identity Management

Identity management capability is the ability of a cloud entity to manage individual user identities, their authentication, authorization, roles and privileges/permissions to access system resources in the cloud environment. It includes four sub capabilities:

- Authorization capability: the ability of a cloud entity to define and enforce access control policy to cloud resouces. An access control policy consists of a list of resoucres and access rights to these resources.
- Authentication capability: the ability of a cloud entity to effectively verify its users' identity when requesting to access cloud resources.
- Role management capability: the ability of a cloud entity to manage user roles.
- Anonymity management capability: the abitily of a cloud entity to manage anonymous users. Anonymity introduces risk and challenges for identity management and increases difficulties for identifying malicious users.

4.1.2 Event Management

Event management capability is the ability of a cloud entity to conceptually construct the unit of an "event" and techniqually implement that concept so that it can be constructed, traced, reconstructed when required, and frozen as a crime scene under investigation when needed. It is a range of high-level advanced pre-investigative capaiblities for cloud environments that must be based on a high level of interoperability among different cloud actors. It includes five sub capabilities:

- Event construction capability: the abitliy of a cloud entity to properly define what is considered to be an "event" in a cloud system, including a set of information needed to describe the "who", "what", "when", "where" and "how" of the event.
- Event freezing capability: the ability of a cloud entity to "freeze" the event at the immediate state in case of criminal offense, intrusion, or investigation.
- Event traceability capability: the ability of a cloud entity to trace the state(s) of an event in the cloud system, or back to its original state.
- Time sequence capability: the ability of a cloud entity to maintain a definite and synchronized time sequence in the (shared) cloud system including maintaining time synchronization across the cloud environment.
- Event reconstruction capability: the ability of a cloud entity to reconstruct the past state of an event with a level of accuracy that the reconstructed information can be admitted as digital evidence.

4.1.3 Encryption Management

Encryption management capability is the ability of a cloud entity to search, acquire and access encrypted forensic data in shared cloud environment without breaching privacy or data protection regulation under jurisdiction(s) of concern. It include four sub capabilities:

- Acquisition in transit capability: the abitliy of a cloud entity to search and acquire potential evidence from encrypted data in transit in live cloud transactions on the servie layer of the cloud system.
- Acquisition at rest capability: the abitliy of a cloud entity to search and acquire potential evidence from encrypted data at rest in physical or virtual cloud storage.
- Key management capability: the abitliy of a cloud entity to ensure encryption keys are accessible to authorized internal investigators (human) or invstigative agents (machine) to decrypt information that might be relevant to the investigation.
- Evidence decryption: the ability of a cloud entity to ensure potential digital evidence in the cloud environment can be appropriately decrypted for the purpose of lawful investigation without breaking laws or regulations under the jurisdicion(s) where the services operate.

4.1.4 Interoperability

Interoperability capability is the abiliyt of a cloud entity to ensure forensic readiness in inter-cloud environments. It includes two sub capabilties:

- Dependency capability: the ability of a cloud entity to ensure forensic readiness when there is a chain of dependency of multiple service providers.
- Migration capability: the ability of a cloud entity to ensure forensic readiness when forensic data or digital evidence is migrated from one cloud to another.

4.2 Investigative Capabilities

4.2.1 Pro-active Data Collection

Pro-active data collection capability is the ability of a cloud entity to maximize its potential to use digital evidence while minimizing the cost of an investigation, i.e., the preparedness and readiness of a cloud entity before an investigation. Pro-active data collection includes two sub capabilities:

- Pro-active artifacts identification: the ability of a cloud entity to identity, document and collect a list of digital artifacts that are essential for a digital investigation or can facilitate a digital investigation that need to be managed pro-actively before an investigation ensuring forensic soundness. These artifacts can be scattered all over the system and the organization, and might include non-digital information that needs to be digitized for future use. These artifacts vary greatly among different cloud actors and in different cloud offerings and are mostly static input for cloud forensic examination and anlaysis.
- Log management capability: the ability of a cloud entity in dealing with, often large volumes of, log messages generated from a cloud system while ensuring forensic soundness. Log messages generated from log management are the main input of static forensic data in forensic collection, and can also be useful for the purpose of regulatory compliance.

4.2.2 Re-active Data Collection

Re-active data collection capability is the ability of a cloud entity to trigger forensic data collection after an incident, either immediately (e.g. an intrusion alert) or after a period of time until the incident is discovered internally in the cloud system or externally notified by the law enforcement. Re-active data collection capabilities include four sub capabilities:

- Incidence response capability: the ability of a cloud entity to receive, review and respond to a (security) incident, from intrusion to criminal act. Analysis can be applied on synthesizing data from various sources to determine trends and patterns in incident activity. This information can be used to help predict future activity or to provide early warning when the activity matches a set of previously determined characteristics. In case of cloud investigation, notice from law enforcement can also be considered as an incident that needs to be responded to.
- Re-active artifacts capability: the ability of a cloud entity to have a well-defined and documented list of forensic artifacts that are essential for a digital investigation or can facilitate a digital investigation that need to be identified, collected and managed re-actively after an investigation. These artifacts can be scattered all over the cloud environment, i.e., in the service layer, abstraction layer, physical layer of the cloud stack, and among all cloud actors. They are often a hybrid combination of static and volatile digital artifacts, and might also include non-digital information that needs to be digitized for forensic examination and analysis. These artifacts vary greatly among different cloud actors and in different cloud offerings. Re-active artifacts capability also includes the ability of a cloud entity to specify the order of volatility of the forensic artifacts in re-active data collection. Generally the order should follow a. Service layer artifacts b. Abstraction layer artifacts c. Physical layer artifacts.
- E-discovery capability: the ability of a cloud entity to search and locate electronically stored information (ESI) about specific topic in the cloud

environment and provide them in a sound fashion. In case of digital investigation, e-discovery is a part of re-active data collection.

- Data recovery capability: the ability of a cloud entity to salvage data from damaged, failed, corrupted, inaccessible, or compromised physical or virtual storage media in the cloud environment when it cannot be accessed normally. Recovery may be required due to physical damage to the storage device, logical damage to the file system that prevents it from being mounted by the host operating system, or intentional damage by the criminal to destroy the digital evidence.

4.2.3 Hybrid Acquistion

Hybrid acquisition capability is the ability of the cloud entity to search and acquire forensic data from different layers and different components in the cloud environment. Cloud computing is a hybrid collection of many existing network, mobile, virtual and grid computing technologies, thus a hybrid combination of forensic acquisition techniques need to be configured in different investigative scenarios. Hybrid forensic acquisition capabilities include seven sub capabilities:

- Remote forensic acquisition capability: the ability of a cloud entity to search and acquire forensic data from geographically remote physical infrastructure via an active network connection. Remote forensic acquisition often consists of installing forensic agent on the remote hardware infrastructure, and grant access to search content and acquire decrypted forensic data to an authorized investigation request.
- Live forensic acquisition capability: the ability of a cloud entity to search and acquire forensic data from a running/live/volatile/dynamic system. Live forensic acquisition is usually carried out as a part of incident response to capture volatile forensic data from a live system before switching off the power to preserve memory, process, and network information that would be lost with traditional forensic approach. Cloud system cannot be easily ‘switched off’, thus making live forensic acquisition capability an essential capability for a cloud investigation to capture volatile forensic data from a cloud system.
- Virtual forensic acquisition capability: the ability of a cloud entity to search and acquire forensic data from virtualized environment, i.e., virtual machines, virtual images, hypervisors, and cloud resource abstraction layer in general.
- Network forensic acquisition capability: the ability of a cloud entity to search and acquire forensic data from a dynamic network. Broad network access is one of the essential characteristics of cloud computing thus making network forensic acquisition and essential capability for cloud investigations.
- Thin client forensic acquisition capability: the ability of a cloud entity to search, recover and acquire forensic data from thin clients, such as web-browser, mobile devices, smart phones, iPads, or any digital device that has both internal memory and communication ability, that are connected to the cloud and heavily dependent on services from the cloud. The rise of cloud computing is enabling a proliferation of “thin” endpoints globally, making thin-client forensic acquisition essential to cloud investigations.

- Thick client forensic acquisition capability: the ability of a cloud entity to search, recover, and acquire forensic data from thick clients, such as workstations, that are connected to the cloud.
- Large-scale forensic acquisition capability: the ability of a cloud entity to search, recover and acquire forensic data from large-scale systems with large data volume. It consists of the techniques to locate and search in large-scale data sets, and to process and transfer large volume of data.

4.2.4 Examination

Examination capability is the ability of a cloud entity to examine forensic data collected from the collection phase to generate input for further forensic analysis. Examination capability includes two sub capabilities:

- Data extraction capability: the ability of a cloud entity to retrieve data out of, often unstructured or poorly structured, raw forensic data sets collected from various sources in a cloud system for further forensic examination and analysis.
- Data reduction capability: the ability of a cloud entity to minimize the amount data that needs to be examined and analyzed in a forensic investigation. It is an automatic or semi-automatic process that can dramatically eliminates redundant data and reduces cost of investigation. Typical techniques of data reduction include data compression, filtering, and data de-duplication.

4.2.5 Analysis

Analysis capability is the ability of a cloud entity to analyze forensic data and generate analysis result as digital evidence. Analysis capability includes four sub categories:

- Data mining capability: the ability of a cloud entity to extract knowledge from large volme data sets in a human-understandable structure automatically or semi-automatically. Data correlation capability is the ability of a cloud entity to analyze whether and how strongly pairs of variables are related using statistical techniques. It is an essential capability to analyze forensic datasets generated from diverse sources.
- Anomaly detection capability: the ability of a cloud entity to detect patterns in a given dataset that do not conform to an established normal behavior in the forensic analysis phase. The patterns detected are called anomalies and are often critical in further analysis of the digital evidence.
- Profiling capability: the ability of a cloud entity to analyze traces from large volume data set in order to draw a profile relevant to the supporting of a digital investigation. It is an analysis process to discover from the correlations between data in forensic datasets that can be used to identify and represent a human or nonhuman subject (individual or group), and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category.

4.3 Supportive Capabilities

4.3.1 Evidence Management

Evidence management capability is the ability of a cloud entity to make sure evidence is kept and handled in a fashion ensuring the integrity of evidence throughout the evidence timeline so that the evidence is admissible to court, i.e., from acquisition, examination, analysis, transport, storage, presentation, to disposal. Evidence management capability includes five sub capabilities:

- Evidence transport capability: the ability of a cloud entity to transport evidence in a forensically sound manner to preserve evidence in its original form without undetectable addition, modification, and deletion of bits.
- Evidence storage capability: the ability of a cloud entity to store digital evidence so that it is well preserved when stored physically or electronically, ensuring the soundness of the evidence and the chain of custody in an investigation.
- Evidence destruction capability: the ability of a cloud entity to destroy evidence and other information associated with a legal matter after its use in the matter ends, often under the order from the courts. In the cloud scenario, the complete destruction of data means the destruction of the actual physical storage (e.g. hard drive) in a way that it is impossible for the data to be recovered.
- Evidence soundness capability: the ability of a cloud entity in ensuring the digital evidence remains in its original form without undetectable addition, deletion or modification of evidence data, throughout the evidence timeline within the cloud entity.
- Chain of custody capability: the ability of a cloud entity to chronologically document the entire digital evidence timeline, showing the seizure, custody, control, transfer, analysis and disposition of the physical or electronic evidence.

4.3.2 Case Management

Case management capability is the ability of a cloud entity to manage the investigative case in an appropriate, sufficient, and well-archived fashion. Case management capability includes three sub capabilities:

- Documentation capability: the ability of a cloud entity to appropriately document the investigative process throughout the case timeline, aspects include investigative techniques applied, chain of custody of evidence, investigators involved in the case, etc.
- Presentation capability: the ability of a cloud entity to appropriately present evidence, analysis, and interpretations in the investigative process in the form of expert reports, depositions, and testimony, aspects ranging from the order of presentation of information to the use of graphics and demonstrations.
- Reporting capability: the ability of a cloud entity to appropriately report the result of the investigative process, whether or not there are enough evidence to validate the hypothesis, based on which the investigate is carried out.

- Elasticity capability: the ability of a cloud entity to be flexible with the scale of the case size. As elasticity is one of the essential characteristics of cloud computing, services are easily scaled up and down based on demand, forensic cases can also range from small scale to large scale in one cloud environment, thus making elasticity a necessary capability for case management.

4.3.3 Multi-jurisdiction

Multi-jurisdiction capability is the ability of a cloud entity to have a clear understanding of different legal, regulatory requirements and forensic process under multiple jurisdictions so that the investigation is carried out in an appropriate, sufficient and legitimate manner. Multi-jurisdiction capability includes three sub capabilities:

Legal requirements: the ability of a cloud entity to have a clear understanding of the legal process(s) required for a digital investigation under the jurisdiction(s) services operate, including the aspects of ciminal/civil processes, warrant, notification, search, seizure, evidence amissibility, etc.

Regulatory requirements: the ability of a cloud entity to have a clear understanding of the regulatory requirements related to digital investigation under the jurisdiction(s) service operate, including the aspects of data retention, evidence decryption, etc.

4.3.4 Multi-tenancy

Multitenancy capability is the ability of a cloud entity (provider, or broker on behalf of providers) to provision and de-provision forensic implementations among multiple tenants sharing same computing resources, as well as the ability to segregate tenants' data throughout the investigation process. Multitenancy capability includes two sub capabilities:

- Segregation capability: the ability of a cloud entity to segregate forensic data among different tenants in a shared cloud environment. In the public and community cloud environment, computing resources are shared on the physical and abstraction control layer of the cloud system stack among multiple tenants, and in both internal and external investigation, there is a need to rapidly and clearly segregate forensic data among different tenants so that tenants who are not related to the investigative case can stay out of the forensic process.
- Provisioning/de-provisioning capability: the ability of a cloud entity to rapidly provision and de-provision computing resources along with the forensic implementations for those computing resources among different tenants when needed.

4.4 Interfacing Capabilities

4.4.1 Law Enforcement

Law enforcement interface capability is the ability of a cloud entity to appropriately interface law enforcement in cases of external investigations while minimizing internal loss due to search and seizure of computing resources in the cloud environment by the law enforcement. Law enforcement capability includes three sub capabilities:

- Notification capability: the ability of a cloud entity to notify all other cloud actors involved in a specific cloud service under investigation of law enforcement in a timely and appropriate manner
- Search capability is the ability of a cloud entity to interface with the law enforcement when facing a search (with warrant).
- Seizure capability: the ability of a cloud entity to properly respond and react to the request from law enforcement to seize its computing resources, or suspend its services to maintain business continuity or minimize financial loss.

4.4.2 Forensic Staffing

Forensic staffing capability is the ability of a cloud entity to organize a functional staffing structure to facilitate both internal and external investigations. Forensic staffing capability includes four sub capabilities:

- Internal forensic team capability: the ability of a cloud entity to form an ad-hoc or well-formalized team of forensic specialists to be in charge of full range of internal forensic capabilities.
- External assistance capability: the ability of a cloud entity to hire external assistance to assist in forensic capabilities, e.g., hybrid forensic acquisition, when they cannot be met internally.
- Legal advisory capability: the ability of a cloud entity to consult both internal and external legal advisory to assist internal or external investigations

5 Initial Validation and Feedback

As part of the initial validation process, a panel of 8 forensic practitioners and experts from law enforcement and academia was invited to assess and evalute the proposed model based on a shortened description of the Cloud Forensic Investigative Architecture and the Cloud Forensic Capability Matrix. The panel was asked the following 3 questions:

(1) Do you think the investigative architecture can work as a high-level reference architecture for investigation in cloud environments?
(2) Are there any major asepcts that are missing in this architecture/model?
(3) In your opinion, is this model possibly a good foundation and first step for cloud forensic standardization? If yes, are there any apsects that can be further improved? If no, why?

All 8 experts answered yes to the first question. In the comments, one expert mentioned that the matrix table is particlarly useful for identifying what role a cloud provider/auditor can play, especially on the pro-active side.

When answering the second question, one expert suggested to include ‘data access/control’ in the case management sub capabilities. The reason is many forensic programs offer a review piece that maybe hosted in the Cloud.

All 8 experts answered yes to the third question. One expert mentioned that the cloud actos and roles need to be more clearly defined, but developing CFCM based on the concept of CMM is a good idea.

6 Sample Usage of CFMM

In this section we demonstrate usage of CFMM through three simple analyses.

6.1 Building Investigative Procedures

We take re-active data collection as an example, take out relavant components of the CFIA, and discuss the following three investigative scenarios and procedures.

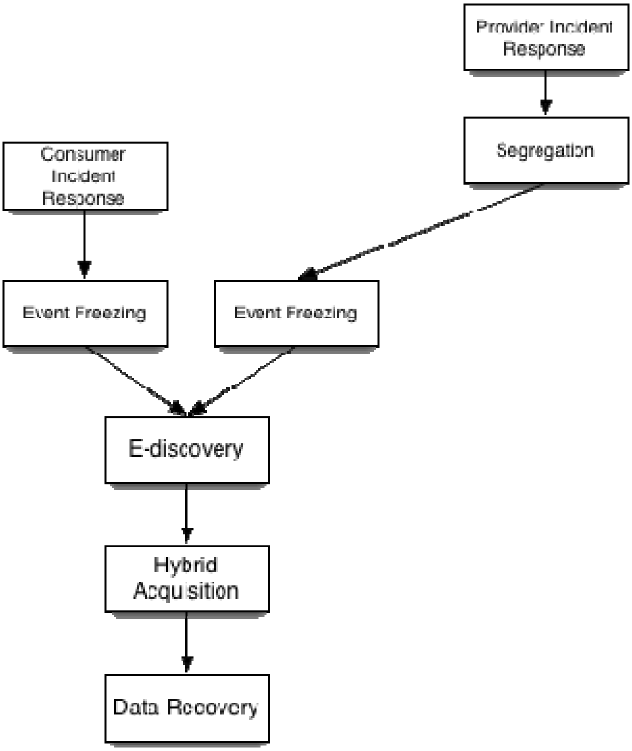

Fig. 3. Re-active Collection Scenario 1

Fig 3 describes the scenario when only one consumer and its provider are involved in an (internal or external) investigation case. In many cases, this scenario is initiated from the consumer side. The consumer first starts the incident response procedure, and then makes an attempt to freeze the “event” on the consumer side (event freezing is a high-level forensic cloud forensic capability, which will be discussed in the next chapter), at the mean time the provider triggers its incident response to the same incident, segregates resources of the consumer in question, makes an attempt to freeze the “event” for that particular consumer after the segregation. In the next step the consumer and the provider should coordinate forensic capabilities to carry out e-discovery, hybrid acquisition and data recovery to collect re-active forensic artifacts according to the order of volatility in the cloud environment they share. Event freezing as a sophisicated capability is not possible until a mature level of cloud forensics capability, in which case the consumer and the provider should coordinate efforts immediately after incident response.

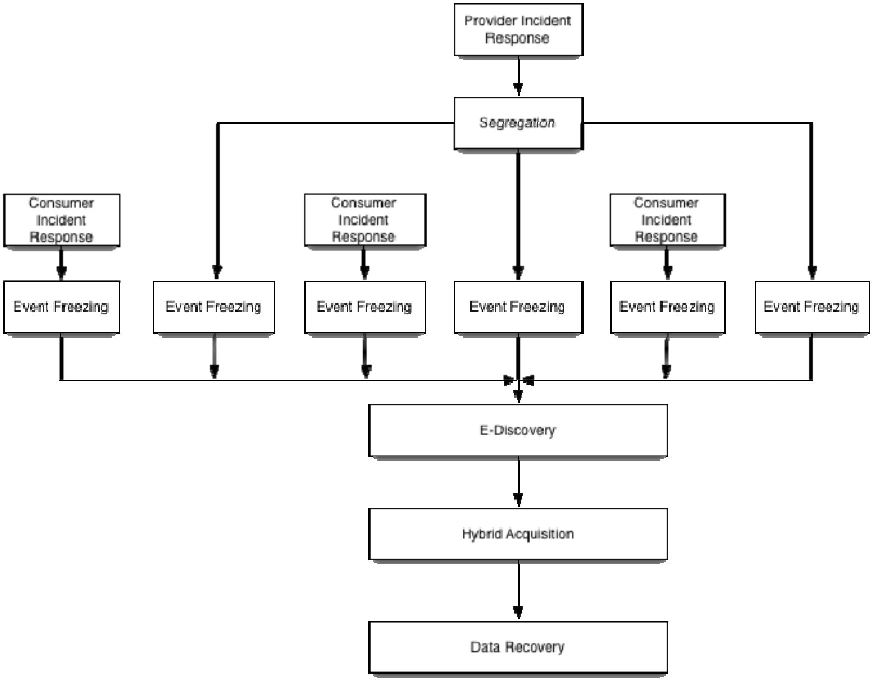

Fig. 4. Re-active Collection Scenario 2

Fig 4 describes the scenario when one provider and more than one of its consumers are involved in an (internal or external) investigation. In many cases, this scenario is initiated from the provider side. The provider first starts its incident response procedure, segregate resources for the consumers in question, and makes an attempt to freeze the “events” for those consumers. At the mean time, various consumers are notified with the same incident, initiate their incident response procedures respectively, and make attempts to freeze their "events" accordingly as the provider. In the next step, the provider and the consumers coordinate their forensic capabilities to carry out e-discovery, hybrid acquisition and data recovery to collect re-active forensic artifacts according to the order of volatility in the cloud environment they all share.

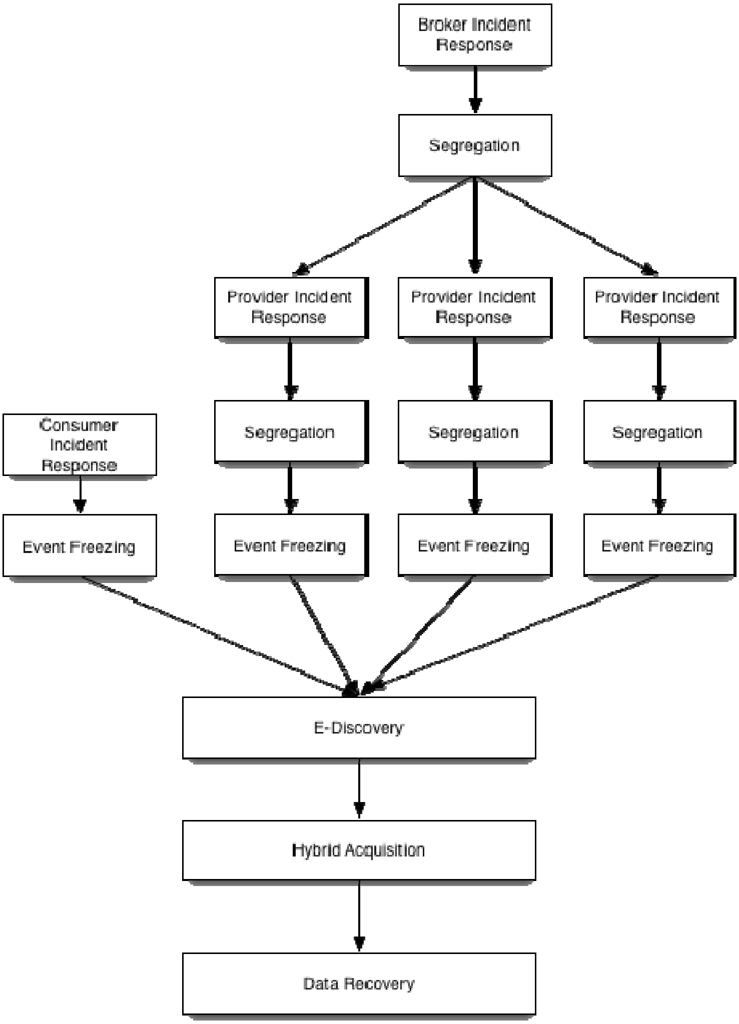

Fig. 5. Re-active Collection Scenario 3

Fig 5 describes the third scenario when one consumer and its broker are involved in an (internal or external) investigation. The broker is coordinating services provided by multiple providers and these providers are often hidden from the consumer. In this case, the broker starts its incident response procedure, segregate resources for the consumer in question, notify the providers for that consumer, the providers starts their incident response procedures respectively, segregates resources for that consumer, and make attempts to freeze the "event" for that consumer. At the mean time, the consumer starts its incident response procedure, makes an attempt to freeze the "event". In the next step, broker coordinates its providers to aggregate forensic capabilities with the consumer's forensic capabilities to carry out e-discovery, hybrid acquisition, and data recovery to collect re-active forensic artifacts according to the order of volatility in the cloud environment they all share.

6.2 Comparing Forensic Capabilities of Cloud Offerings

In this section we take several capabilities specified in the CFCM as examples to compare forensic capability of cloud offerings from four major providers, i.e. Amazon Web Services (Amazon 2011), Google Apps (Google 2011), Force.com (Salesforce.com 2012), and Windows Azure (Kaufman and Venkatapathy 2010), and identity current capabilities that can be utilized or leveraged for investigative purposes. The results are shown in Table 2-6.

Table 2. Encryption in Transit

Provider	Capabilities
Force.com	End-to-end TLS/SSL encryption
Windows Azure	Critical internal comunications are protected using SSL encryption
Amazon CloudFront	HTTPS can be configured for all requests
Amazon	All requests are HMAC-SHA1 signed in Amazon Elastic MapReduce, CloudFront, Auto Scaling, CloudWatch, and Simple Storage Service (Amazon S3)
Google Apps	Google Apps for Business and Google Apps for Education: offer domain administrators the ability to force all users in their domain to use HTTPS

Table 3. Encryption at Rest

Provider	Capabilities
Force.com	Customer passwords stored after applying MD5 hash function; supports the encryption of field data in custom fields.
Windows Azure	.NET Cryptographic Service Providers (CSPs) can be integrated to provide AES algorithms, MD5 and SHA-2 hash functionality, RNGCryptoServiceProvider class, Straightforward key management methods, etc.
Amazon	Amazon S3, EBS, Amazon Simple DB, Amazon Simple Queue Service (Amazon SQS) recommend consumers to encrypt sensitive data before uploading
Google Apps	Data chunks are not stored in clear text so that are not humanly readable

Table 4. Authentication

Provider	Capabilities
Force.com	Two-factor authentication processes; Federated authentication single sign-on; Delegated authentication single sign-on
Windows Azure	Windows Live ID (one of the longest-running Internet authentication services available); Subscription based; SMAPI Authentication
Amazon Web Services	AWS IAM enables a customer to create multiple users and manage the permissions for each of these users within their AWS Account. A user is an identity (within a customer AWS Account) with unique security credentials that can be used to access AWS Services. AWS MFA allows Multi-factor authentication
Google Apps	Service-to-service authentication; x509 host certificates; Two factor authentication mechanisms; Optional two step verification (a built-in two-factor authentication capability);
	Single Sign-On (SSO) with Google Apps for Business, Google Apps for Education, and Google Apps for ISPs

Table 5. Data recovery

Provider	Capabilities
Amazon Web Services	Amazon S3, Amazon Simple DB: removal of the mapping from the public name to the object starts immediately, and is generally processed across the distributed system within several seconds. Once the mapping is removed, there is no remote access to the deleted object. The underlying storage area is then reclaimed for use by the system. Amazon Relational Database Service (Amazon RDS): once an Amazon RDS DB Instance deletion API is run, the DB Instance is market for deletion and once the instance no longer indicates 'deleting' status, it has been removed. At this point the instance is no longer accessible and unless a final snapshot copy was asked for, it cannot be restored and will not be listed by any of the tools or APIs. Amazon S3, Amazong SimpleDB, Amazong Elastic Block Store (EBS): data is redundantly stored in multiple physical locations as part of normal operation of those services at no additional charge. Amazon S3 and Amazon SimpleDB store objects multiple times across multiple Availability Zones on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot. Amazon EBS stores replication within the same Availability Zone. Amazon S3 regularly verifies the integrity of data stored using checksums, and calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. If corruption is detected, it is repaired using redundant data.
Windows Azure	Windows Azure's Storage subsystem makes customer data unavailable once delete operations are called. All storage operations including delete are designed to be instantly consistent. Successful exectuion of a delete operation removes all references to the associated data item and it cannot be accessed via the storage APIs. All copies of the deleted data item are then garbage collected. The physcial bits are overwritten when the assoicated storage block is reused for storing other data, as is typical with standard computer hard drives.
Google Apps	After a Google Apps user or Google Apps administrator deletes a message, account, user, or domain, and confirms deletion of that item (e.g., empties the Trash), the data in question is removed and no longer accessible from that user's Google Apps interface. The data is then deleted from Google's active servers and replication servers. Pointers to the data on Google's active and replication servers are removed. De-referenced data will be overwritten with other customer data over time. Google Apps data is replicated to multiple systems within a data center, and also replicated to a secondary data center.

Table 6. Evidence Destruction

Provider	Capabilities
Amazon Web Services	AWS uses the techniques detailed in DoD 5220.22-M (National Industrial Security Program Operating Manual) or NIST 800-88 (Guidelines for Media Sanitization) to destory data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices.
Google Apps	When retired from Google's systems, disks containing customer information are subject to a data destruction process before leaving Google's premises. First, policy requires the disk to be logically wiped by authorized individuals. using a full write of the drive with all zeroes (0x00) followed by a full read of the drive to ensure that the drive is blank. Then, another authorized individual is required to perform a second inspection to confirm that the disk has been successfully wiped. These erase results are logged by the drive's serial number for tracking. Finally, the erase drive is released to inventory for reuse and redeployment. If the drive cannot be erased due to hardware failure, it must be securely stored until it can be destroyed. Each facility is audited on a weekly basis to monitor compliance with the disk erase policy.

From this comparision analysis we also discovered the following additional capabilities provided by several cloud offerings that worth noticing.

Event reconstruction: Amazon S3 Versioning enables customers to preserve, retrieve, and restore every version of every object stored in Amazon S3 bucket. With Versioning, cusomter can easily recover from both unintended user actions and application failures. By dafault, requests will retrieve the most recently written version. Older versions of an object can be retrieved by specifyng a version in the request.

Multi-jurisdiction: Windows Azure allow all customers choose where their data is stored. Data in Windows Azure is stored in Microsoft datacenters around the world based on the geo-location properties specified by the customer using the Windows Azure Portal.

6.3 Analyzing Standardization Gaps

In this section we list major international cloud standardization working projects that are relevant to forensics capabiities and can be venues to bridge standardization gaps for cloud forensic maturity.

On an architectural and matrix level, the NIST Cloud Computing Security Working Group (NCC-SWG) (NIST 2012) and the Cloud Security Alliance Cloud Control Matrix (CCM) (CCM 2012) are the best fits for forensic related standardization efforts.

On interoperability issues, the Standard for Intercloud Interoperability and Federation (SIIF) being developed by IEEE P2302 InterCloud Working Group (IEEE 2012) is the best fit for defining interoperability capability for cloud forensics.

On interfacing capability provided by cloud management interfaces, the DMTF Cloud Management Working Group (DMTF 2011) is addressing requirements for the management interfaces between the cloud servcie conusmer/developer and the cloud service provider, which can be leveraged for forensic interfaces.

On evidence management, SNIA (Storage Networking Industry Association) Cloud Storage Security working group (SNIA 2011) is developing a standard called Cloud Data Management Interface (CDMI), where basic evidence management requirements can be included and forensic interfaces can be considered.

7 Conclusions and Future Work

In this paper we present a shortened version of the Cloud Forensic Maturity Model and its two inter-related parts, i.e. the Cloud Forensic Investigative Architecture, and the Cloud Forensic Capability Matrix. According to initial evalution and feedback, experts and practitioners agree that this is a good foundation and first step for cloud forensic standardization. We are still actively collecting use cases to validate and refine the model. We are also working on a detailed mapping of the Cloud Forensic Three-Dimensional Model to the CFMM to analyze the interactions and overlap of legal, technical and organizational key criteria to inspire more inter-disciplinary research approaches.

References

Amazon, Amazon Web Services: Overview of Security Processes (2011)

CCM (2012), https://cloudsecurityalliance.org/research/ccm/ (retrieved on July 7, 2012)

DMTF, Cloud Management WG Charter v1.1 – (May 1, 2011), http://members.dmtf.org/apps/org/workgroup/cmwg/ (retrieved on June 26, 2012)

Eucalyptus Systems, Eucalyptus 3.0.1 Administration Guide (2012)

Google Inc., Security Whitepaper: Google Apps Messaging and Collaboration Products (2011)

Kaufman, C., Venkatapathy, R.: Windows Azure Security Overview (2010)

Salesforce.com, Inc., Security Implementation Guide (2012)

Ruan, K., Baggili, I., Carthy, J., Kechadi, T.: Survey on cloud forensics and critical criteria for cloud forensic capability: a preliminary analysis. Journal of Network Forensics (2011B)

Ruan, K., Baggili, I., Cathy, J., Kechadi, T.: Cloud forensics definitions and critical criteria for cloud forensic capability: an analysis of survey results. Digital Investigation (2012) (under review)

Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud Forensics. In: Peterson, G., Shenoi, S. (eds.) Advances in Digital Forensics VII. IFIP AICT, vol. 361, pp. 35–46. Springer, Heidelberg (2011a)

IEEE, ICWG/2302 WG – Intercloud WG (ICWG) Working Group (2012), http://standards.ieee.org/develop/wg/ICWG-2302_WG.html (retrieved on July 6, 2012)

SNIA, Information Technology – Cloud Data Management Interface (CDMI) Version 1.0.1 (September 15, 2011)

NIST, Cloud Security (2012), http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity (retrieved on July 7, 2012)

Paulk, M.: Capability Maturity Model for Software. John Wiley & Sons (1993)