

Cloud Computing Reference Architecture and its Forensic Implications: A Preliminary Analysis

Keyun Ruan, Joe Carthy

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

Abstract. In this paper, researchers provide a preliminary analysis on the forensic implications of cloud computing reference architecture, on the segregation of duties of cloud actors in cloud investigations, forensic artifacts on all layers of cloud system stack, cloud actors interaction scenarios in cloud investigations, and forensic implications of all cloud deployment models. The analysis serves as feedback and input for integrating forensic considerations into cloud standardization processes from early stage, and specifies requirements and directions for further standardization efforts.

Keywords: Cloud Forensics, NIST, Cloud Computing, Standardization, Digital Investigation, Digital forensics

1. Introduction

In late 2011, NIST released its final definition of cloud computing after 15 versions of working definitions, and it is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model offers three types of service models, i.e., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and four types of deployment models, i.e., private cloud, community cloud, public cloud and hybrid cloud (Mell and Grance 2011).

As an extension to the NIST cloud computing definition, a NIST Cloud Computing Reference Architecture (Liu et al. 2011) has been released as a generic high-level conceptual model for discussing the requirements that are the basis for discussing the characteristics, uses, and standards for cloud computing (Hogan et al 2011). The NIST Cloud Computing Standards Roadmap (Hogan et al 2011) has also been released after surveying the existing standards landscape for security, portability, and interoperability standards/models/studies/use cases, etc. relevant to cloud computing in order to identify standards gaps and standardization priorities. However, little has been mentioned on the forensic implications and standardization gap in these documents.

Several researchers have identified various challenges posed by cloud adoption to digital investigation (Spyridopoulos and Katos 2011, Birk and Wegener 2011, Biggs and Vidalis 2009, Ruan et al. 2011A). In 2011, hackers rented Amazon servers and launched the second-largest online data breach in U.S. history (Galante et al. 2011). The need for digital investigation in cloud environments is only going to rise as cloud adoption emerges. According to survey results based on 156 forensic experts and practitioners worldwide (Ruan et al. 2011B), more than half of the respondents agree that “establishment of a foundation of standards and policies for forensics that will evolve together with the technology” is an opportunity for cloud forensics, 88.89% of the

respondents agree or strongly agree that “designing forensic architecture for the Cloud” is a valuable research direction for cloud forensics.

Digital forensics has historically been an “after-after-thought” whereas security has been an “after-thought” whenever new technologies emerge. This could be one of the reasons why today cybercrime causes an annual loss of 750 billion Euros in Europe alone, according to new statistics released by Interpol (Cheslow 2012). On the other hand, the field of digital forensics lacks consensus in fundamental aspects of its activities in terms of methodology and procedures (Cohen 2011). There is no single framework that can be used as a general guideline for investigating all incidents cases (Selamat et al 2008), and a comprehensive model of cybercrime investigation is important for standardizing terminology, defining requirements, and supporting the development of new techniques and tools for investigations (Ciardhuáin 2004).

Cloud computing is expected to reach maturity in another decade (CSA 2012, Thomason 2010), as one of most significant paradigm shifts in computing history, it is an unique timing for digital forensics to be pro-actively integrated in cloud architectural design and standard acceleration. As a first step, in this paper researchers analyze the forensic implications based on the high-level conceptual cloud computing reference architecture and specify requirements for the future standardization efforts. The analysis is independent from any specific jurisdiction or specific service offering.

2. Cloud Actors and Segregation of Duties

As shown in Fig 1, Liu et al. (2011) defines five major cloud actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing. In this paper researchers discuss two types of digital investigation, i.e. internal investigation happens within the cloud environment among cloud actors for security and incident response purposes, and external investigations initiated by external parties such as law enforcement for civil or criminal investigation. In this section, segregation of duties of each cloud actor regarding digital investigation is analyzed.

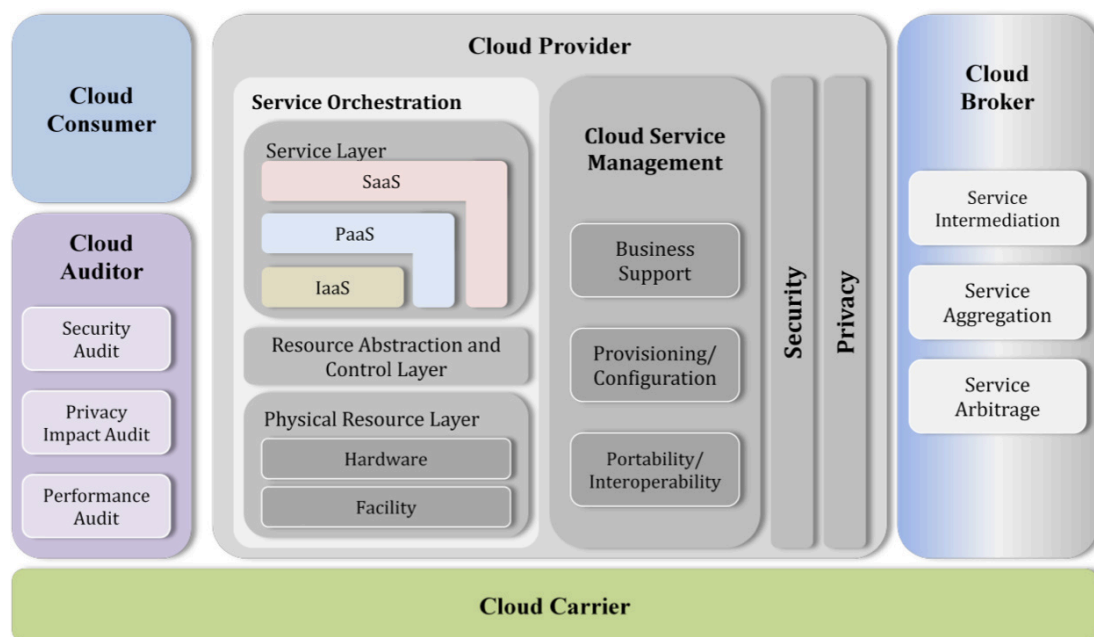


Fig 1. NIST Cloud Conceptual Reference Model (Liu et al. 2011)

2.1 Cloud Provider and Cloud Consumer

According to NIST definition in Liu et al. 2011, the cloud provider is a person, an organization; it is

the entity responsible for making a service available to interested parties through different cloud offerings. A cloud provider acquires and manages the computing infrastructure required for providing the service, runs the cloud software that provides the service, and makes arrangement to deliver the cloud services to the cloud consumers through network access. A cloud provider's activities can be described in five major areas, i.e., service deployment, service orchestration, cloud service management, security, and privacy.

As data is being migrated to cloud providers, so is evidence. Service provider will inevitably be expected to become evidence provider. Increasingly, both consumer and law enforcement will acquire access to evidence and demand forensic support from cloud providers. However, interfaces for such access and requirement of such support are still largely undefined.

As defined in Liu et al. 2011, the cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer is the principle stakeholder for the cloud computing service.

As the principle stakeholder for cloud computing service, the consumer is responsible to demand visibility and control, be aware of its own risks from cloud migration, and make sure that appropriate security controls are implemented. However, guidelines on assessing forensic risks and concerns are still largely missing for consumers.

The segregation of duties between cloud provider and cloud consumers regarding forensic investigations is very complex and needs to be further clarified. With the absence of such clarification, in this section researchers utilize the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) v1.2 which rests on other industry-accepted security standards, regulations and controls frameworks such as HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI, HIPPA, NIST and SAS 70 as a starting point, identify controls that are closely related to forensic process, then group them into a) sole provider responsibility and b) provider and consumer shared responsibility.

The current forensic-related responsibilities expected solely from the provider are as follows:

- 1) Data ownership and stewardship (related control DG-01): all data should be designated with stewardship with assigned responsibilities defined, documented and communicated by the cloud provider. Such designation and documentation can be used for identification of evidence ownership and chain of custody in a forensic investigation.
- 2) Data retention and disposal (related control DG-04 DG-05): cloud provider must ensure backup and redundancy mechanisms are in place for data retention and storage; testing recovery of backups must be implemented at planned intervals by the cloud provider; cloud provider must secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means. Redundant storage is a source for forensic investigation. Event reconstruction and evidence recovery can be made possible through restoring back-ups. However, evidence will not be recoverable if the provider has physically destroyed all storage where evidence might reside.
- 3) Facility Security (related control FS-03 FS-04 FS-05 FS-06): authorization and access control to physical facility security should be ensured and reinforced by the cloud provider. As a result, cloud provider is responsible of providing access logs to physical storage.
- 4) Clock Synchronization (related control SA-12): an external accurate, externally agreed upon, time source should be used by the cloud provider to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timelines. Clock synchronization is critical for analysis of event sequence and event reconstruction in a forensic investigation.
- 5) Audit log and intrusion detection (related control SA-14): audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events shall be retained, complying with applicable policies and regulations. Audit logs shall be reviewed at least daily and file integrity (host) and network intrusion detection (IDS) tools

implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. Physical and logical user access to audit logs shall be restricted to authorized personnel. In cases of an investigation, provider should be responsible of providing such audit logs.

The current forensic-related responsibilities expected to be shared between provider and consumer are as follows:

- 1) Audit (related control CO-01 CO-02 CO-03): audit planning, independent audit, third-party audits should be carried about by both provider and consumer on data duplication, access and data boundary limitations. Forensic related terms need to be defined and included in audit planning, independent audit, and third-party audits from both provider and consumer side.
- 2) Regulatory mapping (related control CO-05): information system elements (data, objects, applications, infrastructure and hardware) may be assigned a legislative domain and jurisdiction to facilitate statutory, regulatory and contractual requirements for compliance mapping. This mapping is of significant value in determining the legislative domain of digital evidence.
- 3) Data classification/labeling/handling (related control DG-02 DG-03): data and objects containing data shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, legal constrains, contractual constrains, and sensitivity that can be useful in a forensic investigation.
- 4) Asset management (related control FS-08): a complete inventory of critical assets shall be maintained with ownership defined and documented. In a forensic investigation, such documentation can be of great value and needs to be provided by both provider and consumer.
- 5) Authentication and Authorization (related control IS-07, IS-08, SA-02, SA-07): granting and revoking normal and privileged access to applications, databases, systems, databases, server, network, and sensitive data should be restricted and approved. Multi-factor authentication is required for all remote user access. In a forensic investigation, authentication and authorization logs and records to critical assets under investigation need to be provided by both provider and consumer.
- 6) Incidence management (related control IS-22 IS-25): policies and procedures should be established to triage security related events and ensure timely and thorough incident management. Mechanism shall be put in place to monitor and quantify the type, volumes and costs of information security incidents. Mechanisms to trigger post-incident investigations need to be included in the incidence management procedures.
- 7) Legal preparation (related control IS-24): in the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction.
- 8) Data integrity and segmentation (related control SA-03 SA-05 SA-09): system interfaces, jurisdictions, or with a third party shared service provider to prevent improper disclose, alteration or destruction. The preservation of evidence integrity and segmentation is also a shared responsibility between provider and consumer.

Despite forensic-related controls are specified in CCM here and there, a separate set of controls explicitly covers the whole forensic process specifying a list of forensic capabilities is needed to further clarify, analyze and enforce the segregation of duties regarding forensic investigations among all cloud actors, especially between provider and consumer at current stage. To develop such a set of controls, researchers suggest the following steps:

- 1) Identification of a list of forensic capabilities include
 - a) Investigative capabilities: a mapping of various existing forensic process models to cloud environment to cover core forensic phases.
 - b) Pre-investigative capabilities: defining a set of capabilities that are needed for pro-active forensic readiness in cloud environment, such as identity management, encryption management, interoperability management capabilities.

c) Supportive capabilities: certain capabilities are needed throughout the whole forensic process but are not core forensic phases, such as evidence management, case management, multi-jurisdiction, multi-tenancy capabilities.

d) Interfacing capabilities: the split of control in cloud environment implies the need for access and exchange forensic data, thus interfacing capabilities need to be defined between cloud actors, especially cloud provider and consumer when it comes to internal investigation. Interfacing capabilities also need to be defined for external investigation when law enforcement is involved.

2) An in-depth analysis of segregation of duties between provider and consumer against the list of forensic capabilities, in which requirement of forensic support from provider side can be better understood and demanded from the consumer through contractual negotiation.

3) Identification of a list of forensic capabilities that can be integrated and provided as a service through standard interfaces, so that providers can start integrating these services at early stage while cloud technology matures.

2.2 Cloud Broker

A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. As shown in Fig 2 below, a cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly, and in this case the actual cloud providers are invisible to the cloud consumer and the cloud consumer interacts directly with the cloud broker. The cloud broker may create a new service by combining multiple services or by enhancing an existing service. In general, a cloud broker can provide services in service intermediation, service aggregation and service arbitrage (Liu et al. 2011)



Fig 2. NIST Usage Scenario for Cloud Broker (Liu et al. 2011)

According to Gartner (Cearley and Smith 2012), cloud brokerage is expected to accelerate over the next three years and will facilitate cloud consumption. Cloud broker can play the following role in a forensic investigation:

- 1) Aggregate forensic capabilities of multiple providers and deliver to consumer while actual providers are hidden from the consumer
- 2) Facilitate investigation by adding an extra layer of forensic support, for example in areas of evidence segregation and interfacing law enforcement

2.3 Cloud Carrier

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication and other access devices. As shown in Fig 3 below, the cloud provider arranges for two unique Service Level Agreements (SLAs), one with a cloud carrier (e.g., SLA2) and one with a cloud consumer (e.g., SLA1). A cloud provider may request dedicated and encrypted connections to ensure the cloud services are consumed at a consistent level according to the contractual obligations with the cloud consumers. In this case, the provider may specify its requirements on capability, flexibility and functionality in SLA2 in order to provide essential

requirements in SLA1. (Liu et al. 2011)

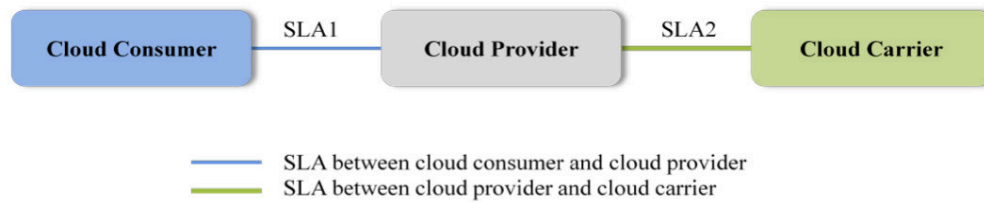


Fig 3. NIST Usage Scenario for Cloud Carrier (Liu et al. 2011)

Carriers are not likely to be directly involved in a forensic investigation, however they can still play a critical role in providing pre-investigative and supportive capabilities, such as evidence transport, chain of custody, and inter-cloud forensic capabilities.

2.4 Cloud Auditor

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc. The audit may involve interactions with both cloud consumer and cloud provider, as shown in Fig 4 below (Liu et al. 2011)

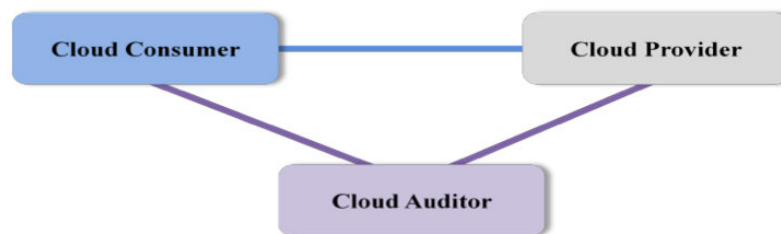


Fig 4. NIST Usage Scenario for Cloud Auditor (Liu et al. 2011)

Forensic capabilities and segregation of duties among cloud actors in delivering these capabilities to facilitate both internal and external cloud investigations need to be reflected into auditable regulatory or contractual language. Currently these terms are missing. A set of key terms for the Service Level Agreement (SLA) between the cloud provider and cloud consumer are identified and recommended by Ruan et al. (2012).

3. Forensic Artifacts in Cloud Environment

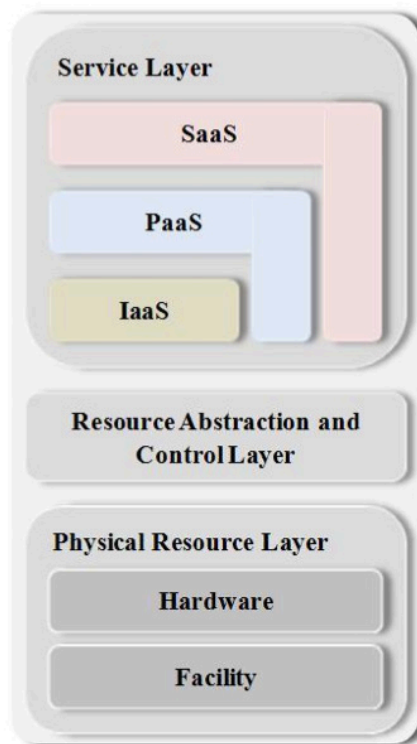


Fig 5. Cloud System Environment (Liu et al. 2011)

A generic stack diagram is defined in NIST Reference Architecture (Liu et al. 2011) to represent the grouping of three types of system components for delivering cloud services, i.e., Physical Resource Layer, Resource Abstraction Layer, and Service Layer, as shown in Fig 5. Similar to traditional computer system stack, a list of forensic artifacts and its order of volatility need to be identified and specified for the cloud system stack.

3.1 Physical Layer

The Physical Resource Layer includes hardware computing resources such as computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces) and storage components (hard disks) and other physical computing infrastructure elements, as well as facility resources such as heating, ventilation, and air conditioning (HVAC), power, communications, and other aspects of the physical plant (Liu et al. 2011).

This layer consists of physical storage and is under control of the cloud provider. It is often geographically distant from the consumer and the law enforcement. Forensic artifacts for the hardware layer include hard disks, network logs, router logs, etc. This layer also includes data center artifacts such as access records, facility logs, activity logs, interior and exterior camera footage, biometrics records, visitor records, organization chart and contact information, etc. Gaining access to actual physical data center and carry out on-site investigation can be too costly or even impossible in most cases. Forensic artifacts on this layer often have to be acquired through remote forensics, or provided by provider.

3.2 Abstraction Layer

The Resource Abstraction and Control Layer contains the system components that Cloud Providers

use to provide and manage access to the physical computing resources through software abstraction. Resource abstraction components typically include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions (Liu et al. 2011).

This layer is under control of the cloud provider and hidden from the consumer. However this layer is extremely critical for addressing multi-tenant issues around evidence segregation, and locating the actual physical computing resources (hard disk storage, etc.) from virtual resources in the Service Layer. Forensic artifacts on this layer include hypervisor event logs, virtual images, etc. Barrett (2012) provides a comprehensive overview of virtual forensics in cloud environments.

3.3 Service Layer

The Service Layer is where Cloud Providers define *interfaces* for Cloud Consumers to access the computing services. Access interface of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components. (Liu et al. 2011)

The Service Layer is where the segregation of duties between the provider and the consumer comes in, and the segregation is where the interface is. Forensic artifacts reside from the service interface above can and need to be collected by the consumer. Forensic artifacts reside from the service interface below (including Resource Abstraction and Control Layer and Physical Resource Layer) can and need to be collected by the provider. As discussed earlier, a set of standardized forensic interfaces need to be defined and integrated into different service layer corresponding to forensic capabilities required from both provider and consumer side.

3.3.1 OS Layer (IaaS)

The IaaS interface layer can also be called OS (Operating System) Layer, as this layer of interface provides interfaces to access operating system and drivers, and is hidden from SaaS consumers and PaaS consumers. An IaaS cloud allows on or multiple guest OS's to run virtualized on a single physical host. Generally, consumers have broad freedom to choose which OS to be hosted among all the OS's that could be supported by the Cloud Provider. The IaaS consumers should assume full responsibility for the guest OS's, while the IaaS provider controls the host OS (Liu et al. 2011).

Forensic artifacts on this layer are similar to forensic artifacts in virtual OSs, which include virtual operating system event logs, configuration logs, audit logs, registry, anti-virus/anti-spyware application logs, intrusion detection system logs, virtual network logs, etc.

3.3.2 Middleware Layer (PaaS)

The PaaS interface layer can also be called Middleware Layer, as this layer of interface provides software building blocks (e.g., libraries, database, and Java virtual machine) for developing application software in the cloud. The middleware is used by PaaS consumers, installed/managed/maintained by IaaS consumers or PaaS providers, and hidden from SaaS consumers (Liu et al. 2011).

Forensic artifacts on this layer are similar to forensic artifacts in traditional (integrated) development environment, which include source code, performance logs, debugging logs, access logs, account information, etc.

3.3.3 Application Layer (SaaS)

The SaaS interface layer can also be called Application Layer, as this layer of interface includes software applications targeted at end users or programs. The applications are used by SaaS consumers,

or installed/managed/maintained by PaaS consumers, IaaS consumers and SaaS providers (Liu et al. 2011).

Forensic artifacts on this layer are similar to forensic artifacts in traditional software applications, which include application logs, authentication and authorization logs, account information, etc. The only difference is the software is hosted remotely from the consumer via the browser (or other thin-client or thick-client) thus thin-client/thick-client forensic data collection will play a major role in forensic data collection on this layer from the consumer side.

3.4 Forensic acquisition in the cloud

Based on the analysis above, researchers conclude that forensic acquisition in the cloud has to resort to a hybrid approach of remote, live, virtual, network, thin-client, thick-client, large-scale forensic acquisition due to the nature of forensic artifacts in cloud environments. A list of pro-active forensic artifacts needs to be identified across the cloud system stack to ensure forensic readiness. The identification of pro-active forensic artifacts must evolve closely with the developments of cloud SIEM solutions. A list of re-active forensic artifacts needs to be identified across cloud system stack with order of volatility for post-incident forensic evidence collection. Some of the e-discovery methodologies can be borrowed in identifying and collecting re-active forensic artifacts, such as creating a “data map” for these artifacts (Gonsowski 2012).

4. Cloud Actors Interactions

There are various ways for cloud actors to interact in cloud investigations. In this section, researchers introduce three main organizational interaction scenarios for cloud investigations based on the analysis of the forensic implications of the three main usage scenarios described in Liu et al. (2011). These interaction scenarios are detailed views of the organizational dimension described in Ruan et al. (2011) and are analyzed under the aspects of 1) Service level agreements 2) Internal and external investigation and 3) Forensic artifacts.

4.1 Scenario 1

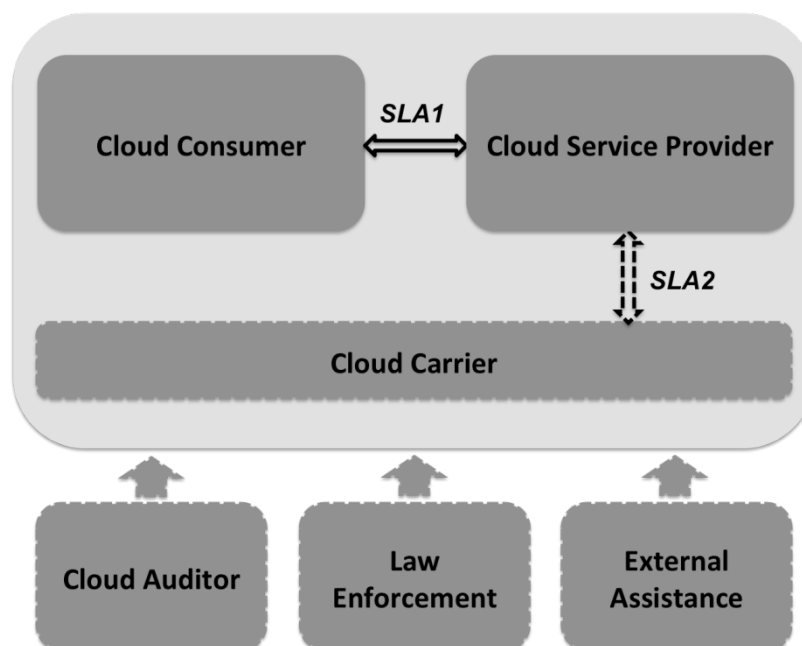


Fig 6. Cloud Actors Interaction Scenario 1

Fig 6 depicts the simplest scenario for cloud actors' interaction. In a service offering, there is a single relation between the cloud consumer and the cloud provider, the cloud provider may or may not provide services through a cloud carrier.

The consumer signs a SLA (SLA1) with the provider. The provider signs a separate SLA (SLA2) with the carrier when the relation between provider and carrier exist. A cloud auditor may be involved to audit SLA(s). Forensic segregation of duties, requirements and implementations need to be defined and audited through the SLA(s).

An internal investigation happens between the provider and consumer shared systems. An external investigation is initiated by law enforcement towards the consumer, provider or system shared by provider and consumer. Provider, or consumer, or may resort to external assistance in enhancing forensic capabilities in facing internal or external investigations.

Forensic artifacts are scattered between provider and consumer systems.

4.2 Scenario 2

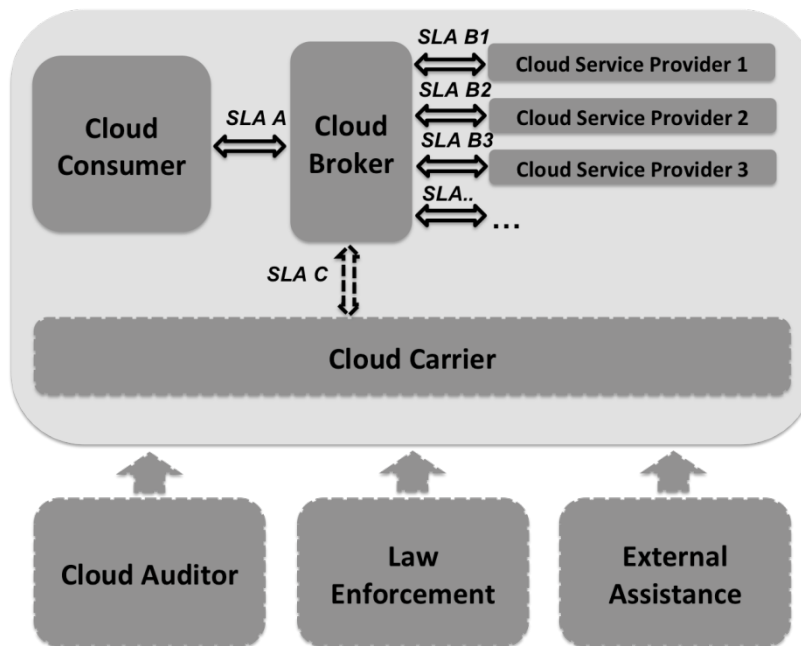


Fig 7. Cloud Actors Interaction Scenario 2

In the scenario shown in Fig 7, the cloud broker is acting as a cloud provider to the cloud consumer. The actual provider(s) are invisible to cloud consumer.

The consumer signs SLA A with broker. The broker signs a range of SLAs (SLA B1, SLA B2, SLA B3, ...) with multiple providers (Cloud Service Provider 1, Cloud Service Provider 2, Cloud Service Provider 3) respectively, and may sign a separate SLA C with a cloud carrier when services are delivered through a carrier. A cloud auditor may be involved to audit SLA(s). Forensic segregation of duties, requirements and implementations need to be defined and audited through the SLA(s).

An internal investigation happens within the shared cloud environment among cloud consumer, broker and provider(s). An external investigation is initiated by law enforcement towards cloud consumer, one or multiple providers, or broker, or cloud resources shared by consumer, broker, and provider(s).

Forensic artifacts are scattered across consumer, provider(s) and broker systems.

Computing resources of one or more of these actors in the shared cloud system and might, and very

likely will involve all of the cloud actors in the investigative process as forensic artifacts are scattered across the shared system.

4.3 Scenario 3

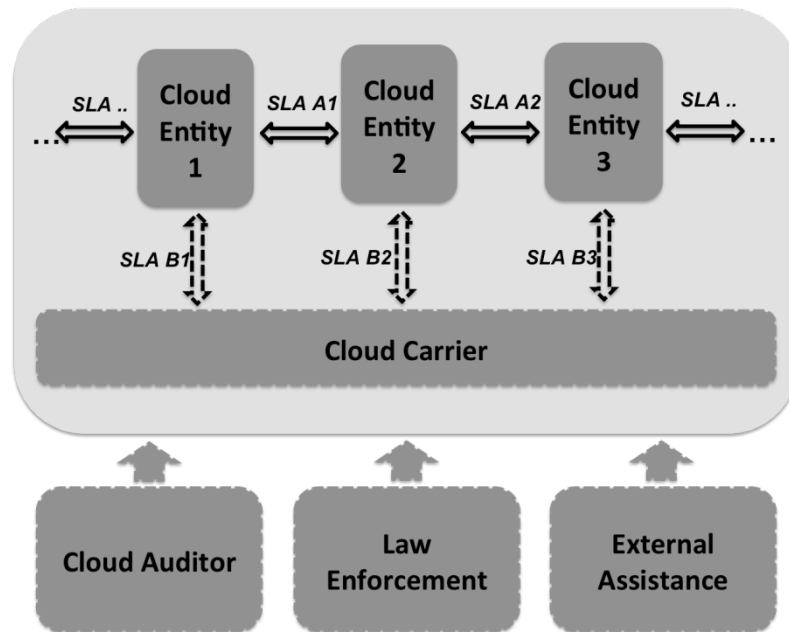


Fig 8. Cloud Actors Interaction Scenario 3

In the third scenario demonstrated in Fig 8, there is a liner chain of dependencies between cloud entities. One cloud consumer uses service(s) from a cloud provider, which uses service(s) from another cloud provider. It is a repetition of scenario 1.

Each pair of service relation between two cloud entities is defined via a SLA (e.g., SLA A1, SLA A2, ..). In cases when services are delivered through a cloud carrier, separate SLAs (e.g. SLA B1, SLA B2, SLA B3) are specified between the cloud entity and the cloud carrier. A cloud auditor might be involved to audit the SLAs among cloud entities, in which case forensic requirements and performances should be audited and evaluated.

An internal investigation happens within the cloud systems shared among the chain of cloud entities. An external investigation happens when law enforcement initiate an investigation to one or more or all entities in the chain of cloud entities which might anyways affect the whole chain of cloud entities later on in the investigative process. Any pair of cloud entities on two sides of a SLA might resort to external assistance in enhancing forensic capabilities in both internal and external investigations, which should be specified in the SLA.

Forensic artifacts are scattered throughout the chain of cloud entities in shared environment. Segregation of duties between each pair of the entities (one acts as provider, another acts as consumer) is similar to scenario 1 described earlier.

5. Cloud Deployment Models and Forensic Implications

There are four types of cloud deployment models according to Liu et al. 2011. In this section, forensic implications in technical, organizational and legal dimensions of these four deployment models are analyzed based on the three-dimensional model proposed in Ruan et al. 2011.

5.1 Public Cloud

A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network, as shown in Fig 9. A public cloud is owned by an organization selling cloud services, and serves a diverse pool of clients (Liu et al. 2011)

Salesforce Chatter, Gmail, Dropbox are popular public SaaS offerings. Force.com and Google App Engine are leading public PaaS offering providers. Amazon Web Service (AWS) and Windows Azure are leading public IaaS offering providers.

5.1.1 Cloud consumers accessing the cloud over a network

In this case, cloud consumers are often small-scale enterprises or personal users who have minimum or none forensic capabilities of their own, or large enterprise or government agencies seeking cheap deployment or storage for non-mission critical services.

Technically, this deployment model often allows easy registration and anonymous usage that could be exploited by malicious users. Personal users need to pay attention to how Personal Identifiable Information (PII) information are used, stored and transferred in the cloud system. Providers need to deliver strong capabilities in evidence segregation in elastic multi-tenant environment and evidence acquisition with the proliferation of client endpoints.

Organizationally, policies and procedures on forensic capabilities and implementations mostly rely on the provider side.

Legally, multiple jurisdictions are a default scenario and there is often standard SLA between provider and consumer with little room for customization and negotiation.

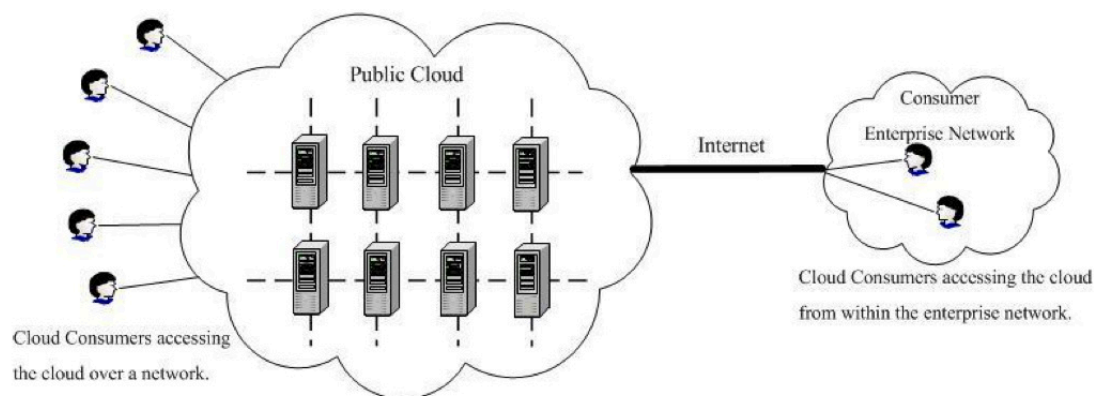


Fig 9. Public Cloud (Liu et al. 2011)

5.1.2 Cloud consumers accessing the cloud from within the enterprise network

In this case, cloud consumers are often enterprises (or government agencies) that deploy non-mission critical services in the public cloud. These consumers typically have certain level of internal security/forensic implementations before migrating to the cloud.

Technically, the default level of security/forensic implementations of the provider can sometimes be higher than consumer's legacy implementations, thus migrating to the cloud can result in an "upgrade" in security/forensic implementations from the consumer side. An extra layer of authorization/authentication and access control can be added through the enterprise network.

Organizationally, consumer may share some of the responsibilities on policy and procedures on forensic implementations.

Legally, consumer can specify the jurisdiction where its data resides via SLA.

5.2 Private Cloud

As shown in Fig 10, a private cloud gives a single cloud consumer's organization the exclusive access to and usage of infrastructure and computational resources. It may be managed either by the cloud consumer organization or a third party, and may be hosted on the organization's premises (i.e. on-site private clouds) or outsourced to a hosting company (i.e. outsourced private clouds) (Liu et al. 2011)

Oracle Grid, IBM Cloudburst are leading private IaaS offerings. Oracle Fusion, IBM Dynamic Infrastructure are leading private PaaS offerings. Sun Comms Suite, IBM LotusLive iNotes, IBM Smart Analytics Cloud, e.g., are private SaaS solutions.

5.2.1 On-site private cloud

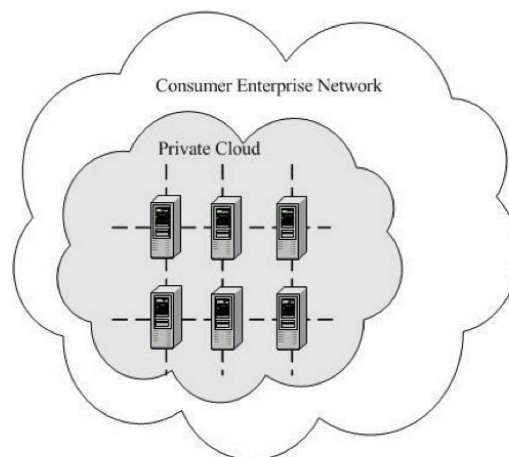


Fig 10. On-site private cloud (Liu et al. 2011)

This deployment model is similar to traditional internal enterprise IT infrastructure. In this case, the cloud consumers are often medium-large enterprise or government agencies that deploy mission critical services in the private cloud. These consumers typically have a high level of internal security/forensic implementation before migrating to the cloud.

Technically, when the level of the consumer's legacy security/forensic implementations is higher than the provider's default offering, cloud migration can result in a "downgrade" on security/forensic implementations on the consumer side in exchange for a reduced cost of IT infrastructure and such risk of "downgrade" needs to be thoroughly assessed before migration.

Organizationally, collaborative efforts need to be made by forensic teams from both provider and consumer side to deliver strong forensic capabilities.

Legally, data resides on-premise thus evidence will be in the same jurisdiction(s) as consumer.

5.2.2 Out-sourced Private Cloud

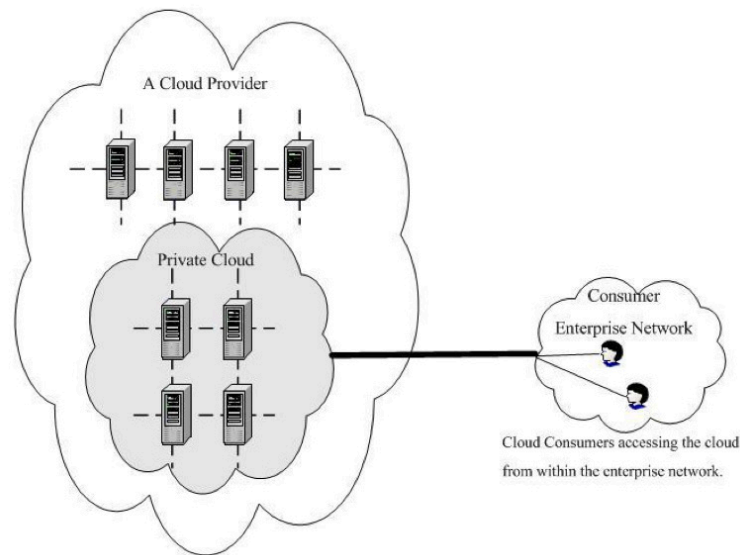


Fig 11. Out-sourced Private Cloud (Liu et al. 2011)

Out-sourced private cloud, as shown in Fig 11, is cheaper compare to on-site private cloud deployment model because maintenance and infrastructure of the private cloud is off-premise. All implications are similar to previous case except that legally, the private cloud can be in different jurisdiction(s) than the consumer.

5.3 Community Cloud

As shown in Fig 12, a community cloud serves a group of cloud consumers who have shared concerns such as mission objectives, security, privacy and compliance policy, rather than serving a single organization as a private cloud does. Similar to private clouds, a community cloud may be managed by the organizations or by a third-party, and may be implemented on customer premise (i.e. on-site community cloud) or outsourced to a hosting company (i.e. outsourced community cloud) (Liu et al. 2011)

IBM's Federal Community Cloud (FCC), for example, is a community cloud solution for federal organizations. NYSE Technologies supports a community cloud called Capital Markets Community Cloud.

5.3.1 On-site community cloud

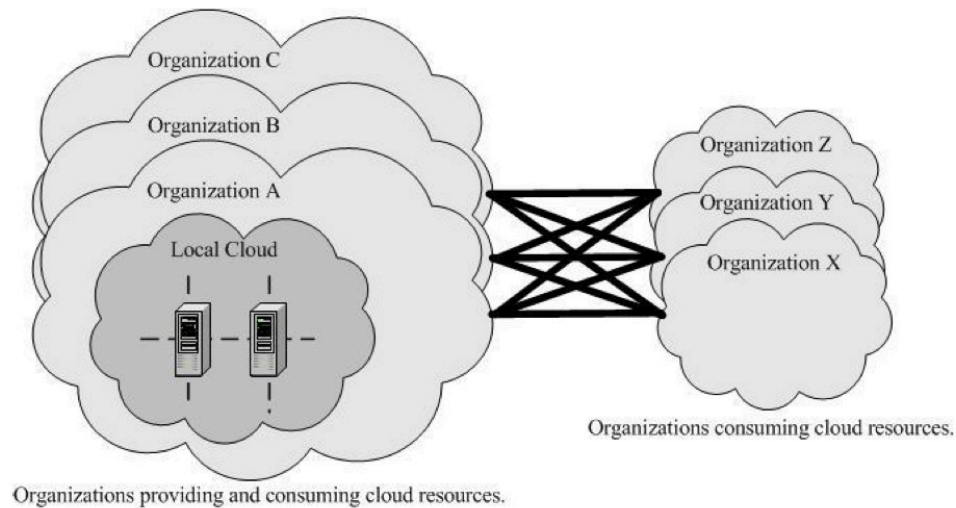


Fig 12. On-site Community Cloud (Liu et al. 2011)

In this case, cloud resources are hosted by one or multiple organizations in the same community that provide and consumer these cloud resources, and these cloud resources can be accessed remotely from other organizations in the same community.

Technically, forensic capabilities are delivered by multiple hosting organizations with a joint effort. Evidence segregation is needed among multiple tenant organization(s) consuming the community cloud.

Organizationally, policies and procedures on forensic implications are shared among hosting organizations and tenant organizations.

Legally, evidence can reside in different jurisdiction(s) when hosting organization(s) and tenant organization(s) are geographically remote. Multi-tenant issues exist among tenant organizations within the community.

5.3.2 Outsourced Community Cloud

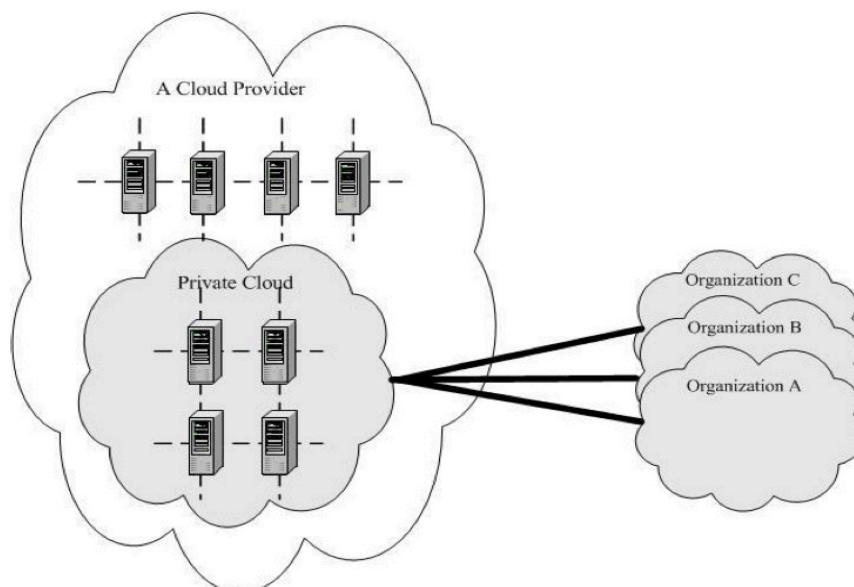


Fig 13. Outsourced Community Cloud (Liu et al. 2011)

In the case of outsourced community cloud as shown in Fig 13, multiple organizations in the same community share a private cloud hosted by a cloud provider and access cloud resources remotely. Outsourced community cloud is cheaper than on-premise community cloud because maintenance and infrastructure of the community cloud is off-premise.

Technically, forensic capabilities are provided by the cloud provider and the tenant organizations in the community. Evidence segregation is needed among multiple consumer organizations consuming the community cloud.

Organizationally, policies and procedures on forensic implications are shared among provider and consumer organizations.

Legally, evidence can reside in different jurisdiction(s) when provider and consumer organizations are geographically remote. Multi-tenant issues exist among consumer organizations within the community.

5.4 Hybrid Cloud

As shown in Fig 14, a hybrid cloud is a composition of two or more clouds (on-site private, on-site community, off-site private, off-site community or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability (Liu et al. 2011)

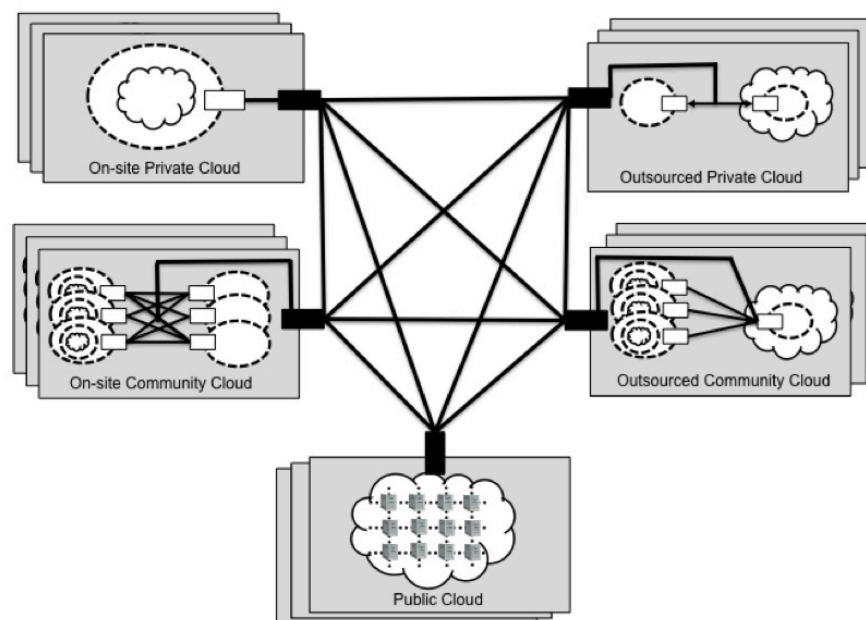


Fig 14. Hybrid Cloud (Liu et al. 2011)

According to Garner, hybrid computing is among top 5 trends of cloud computing and could lead to a unified model over time in which there is a single “cloud” made up of multiple cloud platforms (internal or external) that can be used as needed based on changing business requirements (Cearley and Smith 2012). Both security and forensic implications are extremely complex and are out of scope at current stage.

6. Conclusions and Future Work

Based on the preliminary analysis of the cloud reference architecture researchers conclude the

following directions are important for better integration the missing considerations of forensic capabilities in cloud standardization process.

A standardization gap analysis is needed for forensic capabilities based on a mapping of traditional forensic process models to cloud environments. A forensic reference architecture for the cloud needs to be developed to be used as a baseline for analyzing and discussing forensic issues in cloud environments. A forensic capability model needs to be developed for cloud environments specifying segregation of duties of all cloud actors and mechanisms to access and audit such capabilities. Pro-active and re-active forensic artifacts need to be identified across cloud system stack with order of volatility for collection. A set of forensic interfaces need to be defined and implemented between cloud actors, especially between provider and consumer on the service layer at current stage, in order to collect and aggregate forensic artifacts for both internal and external investigative purposes. Such interfaces can be integrated as a service from the provider. Forensic considerations need to be included in the cloud interoperability discussions as the emergence of cloud brokerage and hybrid cloud deployment model indicates that the complexity of cloud forensics will soon go beyond provider and consumer, becoming a challenge for the entire cloud ecosystem.

Researchers are actively working on some of directions above.

References

- Ciardhuain, S. O. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*, 3(1)
- Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. *International Journal of Computer Science and Network Security*, 8(10).
- Spyridopoulos, T., Katos, V. (2011). Requirements for a Forensically Ready Cloud Storage Service. *International Journal of Digital Crime and Forensics*, 3(3), 19-36
- Birk, D., & Wegener, C. (2011). Technical issues of forensic investigations in cloud computing environments. 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 1–10. doi:10.1109/SADFE.2011.17
- Biggs, S., & Vidalis, S. (2009). Cloud computing: The impact on digital forensic investigations. *International Conference for Internet Technology and Secured Transactions*, 2009. ICITST 2009, 1–6.
- Cohen, F. (2011). Putting the Science in Digital Forensics. *Journal of Digital Forensics, Security and Law*, 6(1), 7-14
- CSA (2012) Cloud Computing Market Maturity Study Results. Cloud Security Alliance, ISACA, Sep 2012
- Galante, J., Kharif, O., Alpeyev, P. (2011) Sony Network Breach Shows Amazon Cloud's Appeal for Hackers, Bloomberg, May 16, 2011 <http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html> retrieved on 22 Jun 2012
- Cearley, D.W., Smith, D.M., (2012) Gartner, Five Cloud Computing Trends That Will Affect Your Cloud Strategy Through 2015, 10 Feb 2012
- Thomason, I. (2010) "Cloud Services a Decade away from Maturity", V3.co.uk, 19 Aug 2010, <http://www.v3.co.uk/v3-uk/news/1999968/cloud-services-decade-away-maturity>
- Hogan, M., Liu, F., Sokol, A., Tong, J. (2011) 'NIST Cloud Computing Standards Roadmap' National Institute of Standards and Technology, Special Publication 500-291
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D. (2011) 'NIST Cloud Computing Reference Architecture' National Institute of Standards and Technology, Special Publication 500-292
- Mell, P., Grance, T. (2011) 'The NIST Definition of Cloud Computing' National Institute of Standards and Technology, Special Publication 800-145
- Ruan, K., Carthy, J., Kechadi, T., Crosbie, M. (2011a) 'CLOUD FORENSICS', *Advances in Digital Forensics VII*, Springer
- Ruan, K., James, J.I., Carthy, J., Kechadi, T., (2012) 'Cloud forensics: key terms for the Service Level Agreement' *Advances in Digital Forensics VIII*, Springer
- Ruan, K., Carthy, J., Kechadi, T. (2011b). Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. 6th annual conference of the ADFS Conference on Digital Forensics, Security and Law, Richmond, Virginia, USA.
- Cheslow, D. (2012) Interpol to crack down on cyber crime, MSNBC.com, http://www.msnbc.msn.com/id/47338831/ns/technology_and_science-tech_and_gadgets/t/interpol-crack-down-cyber-crime/ retrieved on 22 Jun 2012
- Gonsowski, D. (2012) Compliance in the Cloud & the Implication on Electronic Discovery, In K.Ruan (Eds.), *Cyber Crime and Cloud Forensics: Applications of Investigative Processes*: IGI Global, Dec 2012

Barrett, D. (2012) Security Architecture and Forensic Awareness: Forensics in Virtualized Environments, In K.Ruan (Eds.), Cyber Crime and Cloud Forensics: Applications of Investigative *Processes*: IGI Global, Dec 2012