Digital Investigation 13 (2015) 38–57

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Cloud forensics: Technical challenges, solutions and comparative analysis

Ameer Pichan*, Mihai Lazarescu, Sie Teng Soh

Department of Computing, Curtin University, Kent Street, Bentley, Perth, WA 6102, Australia

ARTICLE INFO

Article history:
Received 17 October 2014
Received in revised form 17 March 2015
Accepted 23 March 2015
Available online 14 April 2015

Keywords:
Cloud computing
Cloud forensics
Cloud service provider
Cloud customer
Digital forensics
Digital evidence
Service level agreement
Amazon EC2

ABSTRACT

Cloud computing is arguably one of the most significant advances in information technology (IT) services today. Several cloud service providers (CSPs) have offered services that have produced various transformative changes in computing activities and presented numerous promising technological and economic opportunities. However, many cloud customers remain reluctant to move their IT needs to the cloud, mainly due to their concerns on cloud security and the threat of the unknown. The CSPs indirectly escalate their concerns by not letting customers see what is behind virtual wall of their clouds that, among others, hinders digital investigations. In addition, jurisdiction, data duplication and multi-tenancy in cloud platform add to the challenge of locating, identifying and separating the suspected or compromised targets for digital forensics. Unfortunately, the existing approaches to evidence collection and recovery in a non-cloud (traditional) system are not practical as they rely on unrestricted access to the relevant system and user data; something that is not available in the cloud due its decentralized data processing. In this paper we systematically survey the forensic challenges in cloud computing and analyze their most recent solutions and developments. In particular, unlike the existing surveys on the topic, we describe the issues in cloud computing using the phases of traditional digital forensics as the base. For each phase of the digital forensic process, we have included a list of challenges and analysis of their possible solutions. Our description helps identifying the differences between the problems and solutions for non-cloud and cloud digital forensics. Further, the presentation is expected to help the investigators better understand the problems in cloud environment. More importantly, the paper also includes most recent development in cloud forensics produced by researchers, National Institute of Standards and Technology and Amazon.

Introduction

The advent of cloud computing in recent years has produced major technological advancement in the way Information Technology (IT) services are provisioned and deployed. Cloud computing, which can be used by individuals as well as corporations, continues to grow at remarkable rate due to its many favorable features. Among others, adopting cloud computing users can alleviate big capital investments, replacing them with low cost and more flexible operational expenses, while taking advantage of its speed, agility, flexibility, infinite elasticity and more importantly mobility because services can be accessed anytime from anywhere. The offered features have fuelled a phenomenal growth in cloud services market. Independent studies conducted by organizations, such as the European Network and Information Security Agency (ENISA) and Gartner, predicted a sharp increase in the adoption of cloud

* Corresponding author.
E-mail address: ameer.pichan@postgrad.curtin.edu.au (A. Pichan).

http://dx.doi.org/10.1016/j.diin.2015.03.002
1742-2876/

computing services by corporate organizations, educational institutions and Government agencies (Gartner, 2014; IEEE, 2014). A study by Market Research Media found that the global cloud computing market is expected to grow at a compound annual growth rate of 30% reaching $270 billion by 2020 (Zawaod and Hasan, 2013). The growth is mainly fuelled by the cost savings and pay per use model offered by cloud computing. A similar case study conducted on cloud migration reported an average cost saving of 37% when organizations move their infrastructures to Amazon EC2 cloud, in addition to potentially eliminating 21% of the support calls, showing compelling reasons to adopt cloud computing (Khajeh-Hosseini et al., 2010). A recent study conducted by RightScale group on the adoption of cloud computing, concluded that cloud adoption reaches ubiquity with 87 percent of the surveyed organizations using public cloud. Amazon Web Services (AWS) leading the cloud adoption at 54 percent (RightScale, 2014).

On the other hand, Cloud Security Alliance (CSA) reported a corresponding growth in cloud vulnerability incidents. Specifically, CSA's report shows that cloud vulnerability incidents between 2009 and 2011 have more than doubled, with top three cloud service providers (CSPs), i.e., Amazon, Google and Microsoft, accounted for 56% of all non-transparent cloud vulnerability incidents. The report also cited that the number of vulnerability incidents over the past five years has risen considerably (CSA, 2013b). The increasing security incidents in the cloud are caused, among others, by easy user account registration provided by CSPs, unfettered accessibility, and virtually unlimited computing power. In essence, attackers can open bogus accounts to the cloud, use them to carry out their acts, terminate the accounts and disappear into ether once their malicious acts have been performed. Easy access and almost unlimited power of the cloud allow the attackers, using cloud as a platform, to perform their powerful attacks from anywhere in short periods.

While it is impossible to prevent all attacks totally, they should be traced back to the attackers. Digital forensics is commonly used to track and bring criminals into justice in a non-cloud (traditional) computing environment. However, traditional digital forensics cannot be directly used in cloud systems. In particular, distributed processing and multi-tenancy nature of cloud computing, as well as its highly virtualized and dynamic environment, make digital evidence identification, preservation and collection, needed for forensics, difficult. Note that cloud systems have been hardly designed with digital forensics and evidence integrity in mind, and thus forensics investigators face very challenging technical, legal and logistical issues. Professional organizations, such as CSA and National Institute of Standards and Technology (NIST), and researchers have published papers related to cloud computing in areas such as cloud governance, security and risk assessment (CSA, 2011; Iorga and Badger, 2012; Jansen and Grance, 2011). However, only very little work has been done to develop the theory and practice of cloud forensics (Casey, 2012; Zawaod and Hasan, 2013); some have argued that cloud forensics is still in its infancy (Zawaod and Hasan, 2013).

Recently, several researchers have addressed cloud forensic challenges and issues, and proposed solutions to address the challenges (Damshenas et al., 2012; Daryabar et al., 2013; Grispos et al., 2013; Reilly et al., 2011; Taylor et al., 2011; Zawaod and Hasan, 2013). Since then there has been many advancement in the cloud forensic area. In particular, NIST has formed cloud forensics working group and produced draft publications in July 2014 (NIST, 2014a), and CSPs have started delivering services which supports forensics, e.g., Amazon's security suite of products (AWS Security Centre, 2014) and CloudTrail used for logging in the AWS Cloud (AWS Security Centre, 2013a).

In this paper, we present a comprehensive analysis of cloud forensic challenges and recommended solutions, in the current context as we walk through the forensic phases commonly used in the non-cloud digital forensics. In detail, the contributions of this paper are as follow.

- It presents the forensic process systematically and lists the challenges per different phases of the process, primarily for Infrastructure-as-a-Service cloud model. Its systematic approach would enable forensic practioners and information security professionals to easily comprehend and understand the problem as they go thru the different phases of forensics process.
- It provides a comprehensive analysis of the solutions and evaluates the recommended solutions.
- It identifies the area where the solutions are still immature or not yet fully developed and identifies the opportunities for future work.

The rest of this paper is organized as follows. Section 2 provides the technical background, detailing an overview of cloud computing and its various service and deployment models. The section also presents an overview of digital forensics and cloud forensics and describes the forensic process. Section 3 presents the cloud forensics challenges and solutions and provides a critical analysis of suggested solutions encountered in different phases of the forensic process. Section 4 presents summary of the survey findings and future work. Finally, we conclude this paper in Section 5.

Technical background

Cloud computing: overview

The NIST defines cloud computing 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." (Jansen and Grance, 2011).

In simple terms the cloud computing is a service delivery model, in which IT services are offered as a service to consumers and billed as per usage. The services can be accessed, using a thin client such as web browser, via Internet at any time and from anywhere. The cloud

computing architecture has the following core attributes (IEEE, 2014):

- Elasticity: the ability to scale up or down computing needs as the customer requires.
- Connectivity: the ability to connect and access the services anytime from anywhere.
- Multi-tenancy: the ability to host multiple tenants on the same physical resources, by sharing physical storage, memory, and networks.
- Visibility: the ability for consumers to have full visibility and control of their cloud deployment parameters, usage and cost.
- Measured service: the ability to meter the services and bill as per usage.

The favorable attributes have fuelled the rapid adoption of cloud computing. The major benefit of cloud computing is the economies of scale achieved through versatile and efficient use of resources and specialization. Cloud computing comes in several deployment and service delivery models. The deployment models include:

- Public cloud: Computing infrastructure and services are made available to the public over the Internet. Public cloud is owned and operated by an external provider, selling cloud services.
- Private cloud: Computing environment exclusively owned and operated by the organization or a third party. By virtue, private cloud provides greater control of all computational resources and is intended for single tenant.
- Community cloud: Similar to private cloud, but the computational resources are shared by more than one organizations with similar privacy, security and regulatory rules and requirements.
- Hybrid cloud: A composition of two or more clouds that are bound together by standardized or proprietary technology, which enables interoperability.

According to the nature of service provided by the CSPs, as described in Fig. 1, there are three well-known cloud service models (Jansen and Grance, 2011):

- Software-as-a-Service (SaaS): is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service, accessed using a thin client. This model aims to reduce the total cost of hardware and software development, maintenance, and operations. In this model, the control of the applications and the underlying infrastructure lie with CSPs; consumers have very limited privileges, such as managing application settings and their own data.
- Platform-as-a-Service (PaaS): is a model of software deployment whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, deploying, and managing the underlying hardware and software components of the platform, such as database, operating system and development tools.
- Infrastructure-as-a-Service (IaaS): is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Customers of IaaS avoid purchasing, housing, and managing basic hardware and software infrastructure components; they instead obtain those resources as virtualized objects controllable via a service interface.

Digital forensics: overview

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material or artifacts found in digital device often conducted as a response to computer crime. The first Digital Forensics Research Workshop held in New York in 2001 provided the following working definition of digital forensics (Palmer, 2001): "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*."

NIST provided another definition for digital forensics in their special publication 800-86 (Kent et al., 2006): "*the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data*."

Cloud forensics: overview

Cloud Forensics can be defined as the application of digital forensics in cloud computing platform. It is a cross discipline area. The newly established NIST cloud forensic working group proposed the following definition (NIST, 2014a): "*Cloud Computing forensic science is the application of scientific principles, technological practices and derived and proven methods to process past cloud computing events through identification, collection, preservation, examination and reporting of digital data for the purpose of facilitating the reconstruction of these events*."

The default nature of cloud environment such as multi-tenancy, jurisdiction, data duplication and high degree of virtualization adds multiple layers of complexity in cloud forensics. This is further compounded when the CSPs trade service among themselves, making it difficult to follow the chain of events. Therefore, the forensics process applicable in traditional (non-cloud) environment is no more practical in the case of cloud. Cloud forensics consists of three dimensions: *Technical*, *Organizational and Legal* (Ruan et al., 2011). The technical dimension encompasses the procedures and tools that are needed to perform the forensic process in a cloud-computing environment. This includes

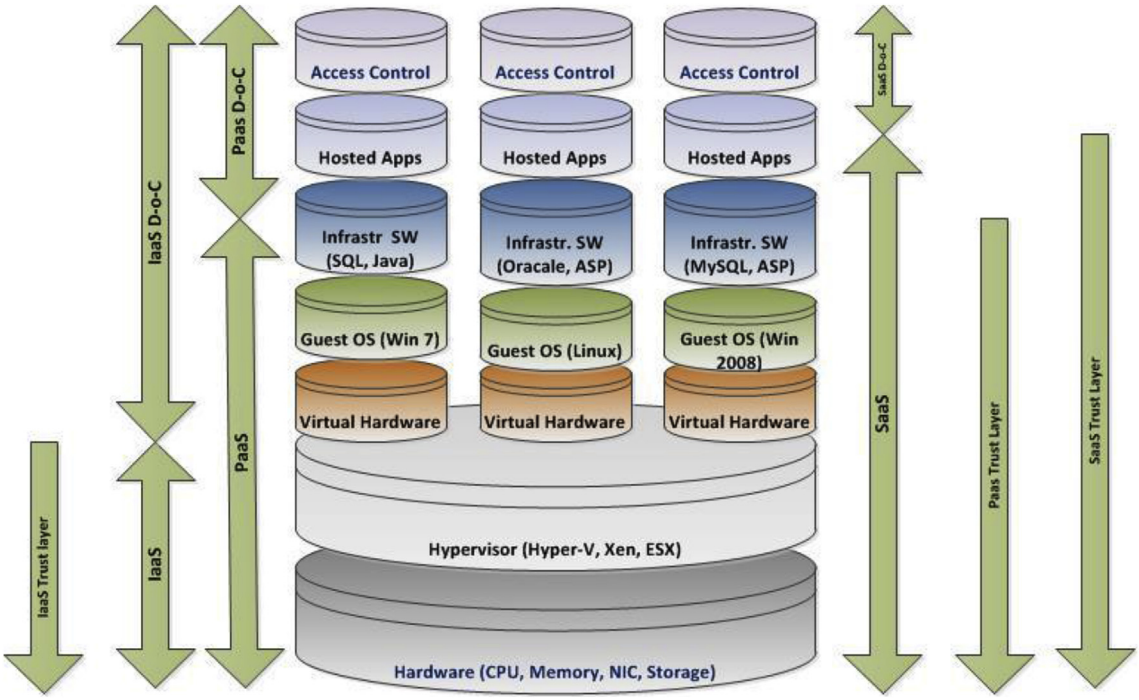

Fig. 1. Cloud model, Degree of Control (D-o-C) and trust layer.

data collection, live forensics, evidence segregation and pro-active measures. On the other hand, the organizational dimension covers the organizational aspects of the forensics. It includes actors like CSPs, customers, legal advisers, incident handlers and objects like binding service level agreements (SLAs), policies and guidelines. Finally, the legal dimension covers the development of regulations and agreements to ensure that forensic activities do not breach laws and regulations in the jurisdictions where the data resides or is collected, simultaneously ensuring the confidentiality of co-tenants who share the same infrastructure.

Forensics process

Forensics process is initiated after the incident happens as a post incident activity. It follows through pre-defined steps. In a cloud computing the process can be grouped to three areas, viz., (i) Client forensics (ii) Cloud forensics and (iii) Network forensics.

Client forensics

Digital crimes are initiated and often carried out from the client side, but the artifacts are left both on the client and server sides. Client side evidence identification and collection is a vital part of the process (Damshenas et al., 2012). The evidence data, such as history logs, temp data, registry, access logs, chat logs, session data and persistent cookies, can be found on the web browser (Guo et al., 2012). It is critical that the data should be collected as early as possible in its sterile state for forensic purposes to use as evidence. There is a potential risk that the data could be erased either purposefully by the actor, or inadvertently by the system due to system configuration; e.g., the web browser history and session logs can be configured to be overwritten or erased after a specified period or when the file size reaches the configured maximum limit.

Proliferation of client side end points, especially to the mobile end points makes the forensic data identification and collection even more challenging (Ruan et al., 2011). For cloud forensics it is critical that those end points are identified and collected timely, keeping evidence integrity in-tact, so that a time line of events can be created.

Cloud (server) forensics

Many digital artifacts that are created and available on the servers form critical part of forensic data and it is essential that this evidence is collected. The artifacts include system logs, application logs, user authentication and access information, database logs etc. The physical inaccessibility and unknown location of the data makes it much harder to conduct the evidence identification, separation and collection in cloud forensics. In a highly decentralized and virtualized cloud environment it is quite common that the data may be located across multiple data centers situated in different geographic locations (Hay et al., 2011). Traditional approach to seizing the system is no more practical either, even if the location is known, as it could bring down whole data center, affecting other customers due to multi-tenancy. A number of researchers have cited this issue and some partially suggested possible solutions (Birk and Wegener, 2011; Guo et al., 2012; Hay et al., 2011; Reilly et al., 2011; Wolthusen, 2009).

Loss of governance is another major issue in cloud forensics. The customers are entrusting the governance to the

providers. This was also flagged by the European Network and Information Security Agency (ENISA)'s cloud computing risk assessment report, which includes the 'loss of governance' as one of the top risks of cloud computing, especially in Infrastructures as a Service (IaaS) (Catteddu and Hogben, 2009). Loss of governance inadvertently that leads to loss of control of information assets by the data owners poses another big bottleneck for evidence collection. The loss of control depends on the cloud model as outlined in Fig. 1. In IaaS users have more control and relatively unfettered access to the system logs and data, whereas in PaaS model their access is limited to the application logs and what pre-defined API provides, and in SaaS model customers have either little or no access to such data. As the customers increasingly rely on the CSPs to provide the functionality and services, they correspondingly give the CSPs more control of their information assets. As the customers relinquishes the control, they lose access to important information and thereby its identification and collection for any subsequent forensic needs (Hay et al., 2011). As the degree of control decreases less forensics data is available for cloud users and therefore there is more dependency on the CSPs to get access to such data. That in turn depends upon the SLAs and what CSPs are willing to provide. This is illustrated in Fig. 1.

In addition, the Virtual Machine (VM) instances are subject to movement within a data center, outside to a different data center in the same jurisdiction or to completely a new data center located in a separate jurisdiction, based upon many factors such as load balancing, business continuity etc. Such moves, carried out by the CSPs, are completely outside the control of the client. This also adds additional challenges to the cloud server side forensics.

Network forensics

Traditional network forensics deals with the analysis of network traffic and logs for tracing events that have occurred in the past. Network forensics is theoretically also possible in cloud environments. The different TCP/IP protocol layers can provide several sets of information on communication between VM instances within cloud, as well as with instances outside the cloud. CSPs ordinarily do not provide the network traces or communication logs generated by the customer instances or applications despite the fact that such logs are critical element of forensic data (Birk and Wegener, 2011). As an example, if someone used an IaaS instance to distribute a malware, the routing information and network log are crucial part of forensic data collection, but they are difficult to obtain. This becomes more challenging for PaaS and SaaS cloud models and the collectability of the information depends heavily on the support investigators receive from the CSPs.

Cloud forensics: process, challenges and solutions

It is not only the digital evidence itself that needs to prevail in any court of law, but also the process followed to conduct the investigation. Researchers and forensic practioners have proposed several digital forensic frameworks. Different researchers have been refining previously published process and framework and proposing new ones, resulting in a variety of digital forensic process models and terminology. A selected number of digital forensic process models are:

1. Digital Investigative Process (DIP) model proposed by the first Digital Forensic Research Conference Workshop (DFRWS) comprising of (i) *identification* (ii) *preservation* (iii) *Collection* (iv) *Examination* (v) *Analysis* (vi) *Presentation phases* (Palmer, 2001).
2. McKemmish model, comprising of a linear process of (i) *identification* (ii) *preservation* (iii) *Analysis* and (iv) *presentation* phases (McKemmish, 1999).
3. NIST Forensic model consisting of (i) *Collection*, (ii) *Examination*, (iii) *Analysis* and *Reporting* phases (Kent et al., 2006).
4. Integrated Digital Forensic Process Model (IDFPM) that consists of (i) *preparation*, (ii) *incident*, (iii) *incident response*, (iv) *physical investigation*, (v) *digital forensic investigation* and (vi) *presentation*. In this model the authors propose a uniform process, a common terminology and standardized digital forensic process model (Kohn et al., 2013).
5. Digital Forensic Analysis Cycle Model that consists of (i) *Commence (scope)*, (ii) *Prepare and Respond*, (iii) *Identify and Collect*, (iv) *Preserve (Forensic Copy)*, (v) *Analyze*, (vi) *Present*, (vi) *Feedback*, and (vii) *Complete or Further Task identified* phases. This is a cyclic and iterative model (Quick and Choo, 2013).
6. Integrated Conceptual Digital Forensic Framework for cloud computing that consists of (i) *Evidence source identification and preservation*, (ii) *Collection*, (iii) *Examination and analysis*, and (iv) *Reporting and Presentation* phases (Martini and Choo, 2012).

In traditional server based environment, where the physical locations of the systems are known, the investigators can have full control over the forensic artifacts. The intrinsic nature and characteristics of the cloud ecosystem produces additional challenges of mapping each traditional forensic framework to cloud environment. For example, IDFPM framework refers the seizure of digital evidence (depending upon circumstances) during incident response, which is not possible in cloud environment. Martini and Choo (2012) proposed an integrated and iterative framework for cloud forensics. In this model during the examination and analysis phase, i.e., step (iii), if more data or evidence is required, the process iterates back to the evidence source identification and preservation phase (Martini and Choo, 2012), i.e., steps (i) and (ii) respectively. In a cloud environment, there is a high probability of evidence being erased or modified at any given time, since the cloud platforms are constantly subject to rapid changes. This highlights the importance of preserving the evidence as soon as it is identified, using proper preservation techniques regardless of the evidence source; such important step has been emphasized by Martini and Choo (2014) in their recent work on distributed file system forensics whereby they also validated their framework.

In this section we consider the DIP model (Palmer, 2001) that could be applied to all digital investigations, and later used by many researchers and practitioners (Grispos et al., 2013; Taylor et al., 2011). The linear process of the model is illustrated in Fig. 2. Martini and Choo (2014) used the DIP model, expanded and applied to distributed file system forensics. We use this model to describe the challenges of each phase of the process and recommended solutions. In the case where a challenge is not unique to a particular phase, we include the challenge in all relevant phases.

Identification

The forensic process begins with the identification of systems, media, mobile devices etc., which is likely to contain potential digital evidence. In reality, Identification is a two-step process: (i) the identification of the incident and (ii) the identification of necessary evidence to prove the incident. Step (i) requires identifying all machines and system files suspected of containing related evidence and step (ii) requires identification of the evidence in the media. Traces of evidence can be found in media such as cloud servers, network devices and mobile devices (Brezinski and Killalea, 2002; McKemmish, 1999). ISO 27037 standard defines the identification process as "*process involving the search for, recognition and documentation of potential digital evidence*" (ISO 27037, 2012). Proper evidence identification requires the knowledge of its present location, type and format. Cloud computing adds new challenges to the *location* identification process, as it is very difficult to identify physical location of data asset at a given time (Martini and Choo, 2012; Taylor et al., 2011).

Multiple jurisdiction and multi-tenancy in a highly decentralized data processing environment are the default settings for the public cloud deployment model. Often CSPs intentionally hide data location to facilitate replication and enhance data availability. The settings pose additional challenges in data identification and subsequent collection because the location of the data is unknown (Birk and Wegener, 2011; Hay et al., 2011; Ruan et al., 2011). System and application logs forms a vital part of forensic investigation and getting to know the location of the logs also poses an equal challenge (Damshenas et al., 2012). Table 1 outlines the challenges in the data identification phase and their recommended solutions, assuming that the client location, from where the incident has been initiated is easy to identify and locate.

In the followings, we discuss the challenges involved in the Identification phase and their possible solutions.

Unknown physical location

The location of virtual instances and digital artifacts, e.g., server system files and logs, is unknown to the customer and therefore it can be difficult to identify the artifacts. This can be due to a number of features intrinsic to cloud computing. For example, (a) the cloud data can be stored out of the jurisdiction from the investigating Law Enforcement Agency, or (b) the consumer's data may be split across a number of storage devices within the cloud environment, with some part of the data remains within the jurisdiction and some other part outside the jurisdiction (Quick et al., 2013). All of this produces challenges in

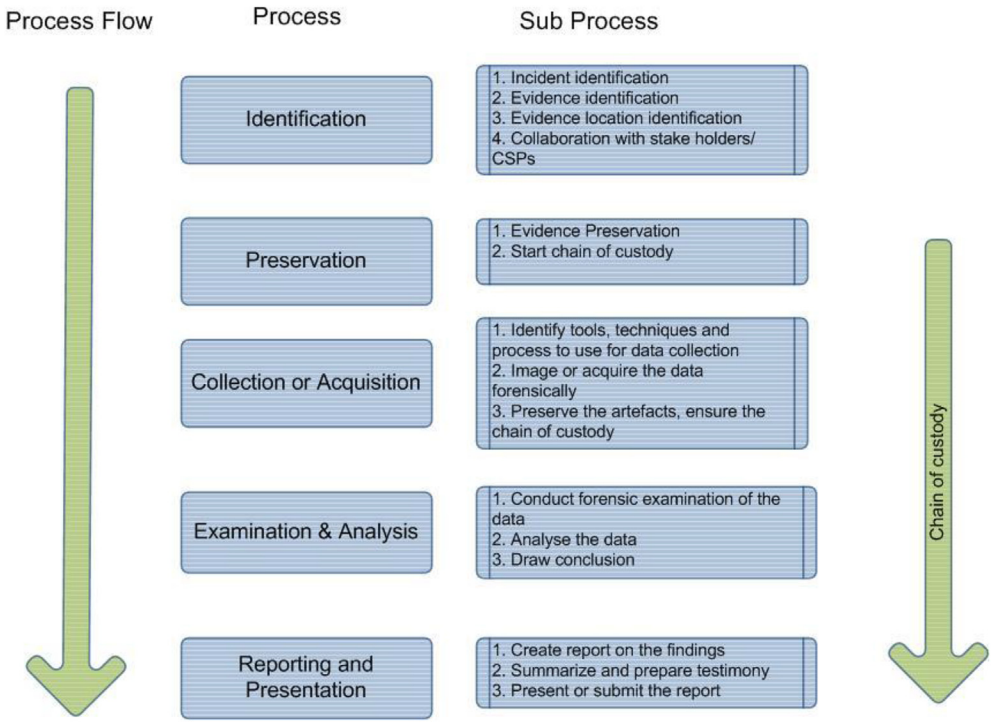

Fig. 2. Digital forensic process.

Table 1
Identification phase: challenges and recommended solutions.

No.	Challenges	Recommended solutions	Comments
1	Unknown physical location	Resource tagging (Hay et al., 2011)	Adversely affects CSPs ability to ensure flexibility, service availability and manageability.
		Robust SLA with CSPs (Alhamad et al., 2010; Birk and Wegener, 2011). SLA in support of cloud forensics ((Ruan et al., 2012)	Most of the SLA guidelines are mainly focused on security requirements and less on forensic requirements.
		System level Logs	System level logs can contain prime information regarding the access, creation and deletion of system level objects
2	Decentralized data	Log frame work (Marty, 2011; Sang, 2013)	Logs including the hypervisor level logs would help the forensic process and time lining of events
3	Data duplication	Resource tagging (Hay et al., 2011)	Can adversely affect the system performance.
4	Jurisdiction	SLA, specifying where the data can be stored or migrated (Alhamad et al., 2010; Jansen and Grance, 2011; Ruan et al., 2012)	Can adversely affect CSPs ability to ensure service availability flexibility and cost benefits to consumers.
		Reverse look up for networked devices conduct a reverse look up of network topology (CSA, 2013a).	This is a very time critical action due to dynamic nature of cloud computing
5	Dependency Chain	None	Lack of solutions in the form of software tools, standard process etc. not available
6	Encryption	Key management system within cloud (CSA, 2013a) and legal authority	Policy guidelines, governance, and process doesn't exist now for key management in cloud
7	Dependence on CSP	SLA specifying the specific forensic services (Alhamad et al., 2010; Kandukuri et al., 2009; Ruan et al., 2012).	Good SLA ensures service availability and compliance (Pichan et al., 2014)

identifying the evidence artifacts. Below we discuss some solutions to the challenge.

- *Resources Tagging*: The cloud resource consumers “tag” their resources to mark the location of their information assets, which can also be used by CSPs to determine whether they can be migrated and if so provide the allowed regional boundary of migration (Hay et al., 2011). It is common for the CSPs to move the VM instances and associated customer files between different physical machines and sometimes across different data centers located in different geographical locations. In such cases resource tagging can be used to inform the CSPs “what can be” and “what cannot be” moved. This addresses the legal issue by dictating the resources that are not allowed to be moved to different jurisdiction. The solution may significantly affect the CSPs' ability to manage their resources efficiently and to provide prime services, e.g., availability and acceptable performance.
- *Robust SLA*: Several CSPs, e.g., Amazon, provide an option to choose a geographic location, from a list of available regions around the globe, to host the VM instance when the instance is first created. Currently Amazon provides public cloud services in the following regions: three regions in US, one in EU (Ireland), three in Asia (Singapore, Tokyo, Beijing), one in Australia (Sydney), and one in South America (Sao Paulo). Amazon doesn't move the user instances or duplicate them across regions by themselves (AWS Security Centre, 2014). This scheme partially solves the jurisdictional or data location issue for Amazon's customers. However, other cloud providers, e.g., Google, Microsoft, do not offer such an option as a common feature.

Incorporating this option into SLA is recommended (Alhamad et al., 2010; Jansen and Grance, 2011) because a customer needs its CSP to identify locations of VM instances, which will be stored only when mandated by the SLA. Alhamad et al. (2010) proposed a conceptual SLA framework for cloud computing. Other researchers have suggested the importance of having a robust SLA with CSPs which can be enforced (Birk and Wegener, 2011; Jansen and Grance, 2011; Kandukuri et al., 2009; Patel et al., 2009; Ruan et al., 2011). Ruan et al. (2012) provided key terms and conditions regarding forensic activities in SLAs between cloud provider and consumer.

- *System Level Logs:* System logs providing detailed access report on data assets, including privileged user access, creation, deletion and modification of system-level objects, etc. For example the logs produced by AWS CloudTrail logs (AWS Security Centre, 2013b) are prime piece of forensic information.

Decentralized data

Decentralized nature of data processing is one of the key attributes of cloud computing. As a result, there is no central location for files, database artifacts, system artifacts and logs, thereby creating great challenges to identify, lock (to ensure integrity) and retrieve them. The CSPs seldom provide the details of how the logs are created and where they are stored. In addition the CSPs use their own proprietary log formats, resulting in non-uniform log structure in cloud computing. Having a uniform and forensically valid *Log Framework* is one way to solve log file access issue. Many researchers have identified the importance of keeping end-to-end and comprehensive transaction logs (Birk and Wegener, 2011; Haeberlen, 2010; Marty, 2011; Sang, 2013). Marty (2011) provided a business oriented logging framework and guidelines suggesting ‘what to log’ and ‘when to log’ and proposed a proactive approach to application logging. However, there is no research so far

regarding a "pre-defined forensically valid log structure and location" that can be easily located, retrieved, and verified for its integrity, using which forensic investigators can produce end-to-end temporal analysis (i.e., timeline of events).

Data duplication

Duplicating data to multiple locations is an inherent feature of cloud computing. The CSPs often provide this feature to ensure business continuity and fault tolerance. From forensic perspective this is a good feature, because it will be very hard to completely destroy all the evidence from cloud (Ruan et al., 2013). However data identification is equally hard because the data is spread out. One can use the resource tagging mechanism (Hay et al., 2011), described in Section 3.1.1, to locate deleted files needed for forensics by following the files' logical chain.

Jurisdiction

Storing customer data outside of the customer's jurisdictional area is quite common in cloud computing; in general, CSPs need not inform the customers the location details of their files. Therefore, depending upon the location, different laws would apply which would significantly impact on the forensic process. For networked devices, although it is theoretically possible to trace back or perform a *reverse look up* to produce overall topology and thereby obtain essential information, the step is quite difficult due to the fast dynamic nature of the cloud systems. The topology information (such as the allocated IP address, storage space etc.) is subjected to rapid changes, and therefore faster response is often required to obtain a meaningful information (CSA, 2013a). The CSPs often keep migrating the VM instances between different physical machines, spreading them across different jurisdictional locations (Hay et al., 2011) and eventually creating legal challenges. The possible solutions to address the jurisdictional issue are:

- *Specific SLA:* Create SLAs that clearly specify where the data can be stored, re-located or duplicated (Biggs and Vidalis, 2009; Ruan et al., 2012).
- *Reverse Look up:* To find the location of networked devices, and conduct a reverse look up of network topology (CSA, 2013a).

Dependency chain

It is very common for the CSPs to trade services among them. For example a CSP providing email service (SaaS) may depend upon a third party CSP offering PaaS to host log files, which in turn depend upon another IaaS provider to store log files. Correlation of activities across the CSPs is a major challenge, creating a chain of dependencies among the CSPs. Moreover, different providers might be hosting their services in different locations. Lack of transparency is another issue associated with multiple levels of outsourcing. Investigators need to trace and follow each link in the chain to trace the link and lock the evidence for collection. However, there is no easy way to perform this process. To date, process, policies and guidelines related to cross provider forensic examination are virtually nonexistent, exacerbated by lack of interoperability framework among cloud providers.

Encryption

Encryption is becoming increasingly relevant for cloud computing. Most CSPs provide encryption as a feature in their security service wrap. CSPs provide the service either by only providing an API for encryption, while customers use their own key management system and keys, or by applying encryption when the data is stored in the cloud and storing the encryption key, which is often linked with user access password (CSA, 2013a). Cloud storage solution providers, such as SpiderOak, encrypt the data at the client location before uploading it to the cloud servers. This method offers 'zero knowledge privacy', meaning that the provider never knows the plain text content of the data being stored; consequently, only the client can unlock the encrypted data using its password. On the SpiderOak servers the files and folders appear as sequentially numbered containers of data (SpiderOak, 2014). Regardless of the method used for encryption, an encrypted data appears as a continuous byte stream, making evidence identification phase and also its subsequent phases challenging problems.

CSA research group suggested the use of proper key management infrastructure and best key management practices (like public key infrastructure) such that the data assets can be decrypted without the need to share keys (CSA, 2011). However, no published guidelines have been found mandating the process nor it is included in the ISO 27037 standards yet.

Dependence on CSP

Due to the intrinsic nature of cloud computing, customers and investigators have to depend upon the CSPs to identify, locate and lock forensic evidence. Incorporating the essential forensic services required from the CSPs in the SLA is the key solution to the issue. The CSPs are becoming more aware of it and some do offer such services.

Dependence on CSP is going to be an issue, until the providers start offering tools to collect forensics artifacts on demand using a provided portal or similar applications. For example, Amazon provides memory dumps and means to ship the memory anywhere for a fee, in addition to its recently released CloudTrail logging application, which allows the logs to be retrieved using AWS portal (AWS Security Centre, 2014).

Preservation

ISO 27037 defines preservation as the "*process to maintain and safeguard the integrity and/or original condition of the potential digital evidence*" (ISO 27037, 2012). Preservation encompasses all activities that protect the integrity of the evidence throughout the process. Appropriate measures should be taken to ensure that the evidence's integrity is maintained throughout the investigation life cycle and proper chain of custody process is initiated. This is critical to provide unquestionable

assurance to the legal authorities that the data found is the accurate representation of the facts (Grispos et al., 2013).

Preservation of digital evidence forms the vital part of the digital investigation process. In cloud computing, it is a very complex step due to the distributed nature of the data (Grispos et al., 2013). Digital evidence is very fragile and easy to change or remove. Therefore, the evidence's integrity should be maintained, ensuring the data is in its original form as it is found (or as close to it) and a strict chain of custody is established starting from this phase until the end of the investigation process. Moreover, the evidence has to be collected and stored securely and accesses to the evidence should be logged (Brezinski and Killalea, 2002; Damshenas et al., 2012) and shown valid.

In reality, evidence preservation is not a one-step process; rather the process continues until the evidence is presented in court. The preservation phase prior to evidence acquisition phase deals with locking or freezing the evidence, making it ready for collection. As the cloud platform is very dynamic, this phase is very critical. Table 2 identifies the challenges in the preservation phase and their possible solutions.

Chain of custody

For conventional forensic process, chain of custody can be defined as "*a roadmap that shows how evidence was collected, analyzed and preserved in order to be presented as evidence in court*" (Grispos et al., 2013). Researchers and legal practitioners have highlighted the importance of maintaining proper chain of custody log. For example, in UK, the Association of Chief Police Officers (ACPO) provides guideline of good practices and principles for computer based electronic evidence, in which Principle 3 states the necessity of keeping audit trail or other record of all processes (ACPO, 2012). Adams (2013) cited that maintaining a chain of custody is essential to satisfy the ACPO principles. Shipley and CFE (2007) stated that "*Basic premises of digital evidence collection include the collection of the data in a manner consistent with the law, verification of the data collected and maintenance of a proper chain of custody of evidence collected*". Although there is no single way to enforce chain of custody in digital forensics, the use of techniques such as time stamping, hashing and e-signatures are central to all methods (Shipley and CFE, 2007).

One way of establishing chain of custody for digital evidence is by using RSA Signature. RSA Signature is a widely used public key crypto system to secure data transmission. Lin et al. (2012) proposed a cloud aided RSA Signature scheme to seal and store the digital evidence in the cloud. The proposed technique would greatly assist in securely collecting and storing evidence, especially from mobile devices that have limited computational and storage power. Digital Signature can also be used to enforce the data integrity, in addition to establishing chain of custody of evidence post seizure. An investigator can perform checksum on the artifacts and digitally sign the checksum using his/her private key.

Evidence segregation

By default cloud computing, is a multi-tenant environment. The multi-tenant characteristics possess difficulties in isolating and preserving evidence without hindering other tenants sharing the same resources. One solution to evidence segregation is by sandboxing each user instance.

Sandboxing is a mechanism by which the running programs are separated into virtual enclaves and each of them uses its own enclave such that no instance knows the existence of its neighbor. Neighbors behave as if they are on separate hosts. Capturing the entire Sandbox instances provides running state of users' virtual machine instances at that point in time, which can be loaded on to a VM instance for analysis.

Though the above mechanism partially addresses the problem, we believe that solutions using the hypervisor level logs, which contains system level info about all tenants such as creation and deletion of virtual machine instances remains challenging, because such logs are not accessible from a normal user account and in addition the logs would potentially contain information about other tenants.

Distributed storage

Due to the distributed and elastic nature of cloud computing, it is often not possible to ascertain where the piece of data is stored, as it could be distributed among many hosts in multiple data centers. Tagging the virtual instances (Hay et al., 2011), described in Section 3.1.1, is a potential solution.

Data volatility

Highly volatile nature of data is a major concern for evidence preservation and collection in a cloud environment. Researchers suggested *Persistent storage* to address the data volatility issue. Having a persistent storage and keeping the storage synchronized frequently between the VM instances and persistent storage have been suggested by researchers to counter the data volatility issues (Birk and Wegener, 2011; Damshenas et al., 2012). However the data

Table 2
Preservation phase: challenges and recommended solutions.

No:	Challenges	Recommended solutions	Comments
1	Chain of custody	RSA Signature (Lin et al., 2012)	Can be used to validate the chain of custody and data integrity.
2	Evidence segregation	Sandboxing	Running programs are separated by virtual enclaves.
3	Distributed storage	VM instance tagging (Hay et al., 2011)	The tagged VM instances can be used to identify the location
4	Data volatility	Persistent storage (Birk and Wegener, 2011; Damshenas et al., 2012)	Providing persistent storage defeats the elastic nature cloud computing.
5	Data Integrity	Checksum algorithms (e.g., MD5, SHA1 SHA256)	

on the running system compromised by an adversary cannot be mitigated, although traces of such ill-action will be available on the persistent storage as an evidence. Note that CSPs usually do not offer a persistent storage as a generic service, which could result in vital data loss when the VM is re-started or shut-down by an adversary. Further, providing persistent storage works against the *on-demand, low cost* and *elastic* nature of the cloud. While synchronizing the volatile data storage to a non-cloud storage is theoretically possible, it is not practical to implement and could defeat the whole purpose of adopting cloud systems. Therefore, it remains very critical to collect forensic data as soon as the incident has been identified; this issue is further explained in Section 3.3.

Data integrity

Data Integrity ensures that the evidence is an accurate representation of the data found in the computer system. Several aspects of the cloud environment affect the data integrity, but maintaining the integrity remains to be a crucial aspect of cloud forensics. The known method to preserve data integrity is using proven hash techniques such as MD5, SHA1 SHA256.

Collection or acquisition

In digital forensics *collection* refers to the "*process of gathering items that contains the potential digital evidence*" and *acquisition* refers to the "*process of creating a copy of the data within a defined set*" (CSA, 2013a). Evidence collection is difficult due to ephemeral nature of the cloud environment and the inaccessibility to the operating system files and artifacts such as temporary Internet files and registry entries. Public and hybrid cloud systems might operate across jurisdictions, making it much more difficult to acquire artifacts. Unless cloud computing applications provide a complete audit trail, it may be difficult to extract the evidence in an admissible manner, or there may be little evidence available to extract (Taylor et al., 2010).

Legal collection refers to the seizure of the physical evidence under the authority of a legal order (i.e., search warrant). Due to the multi-tenancy and the jurisdictional issue associated with cloud environment, collection is not practical and therefore acquisition is the recommended process. Note that collection requires CSP support, whereas acquisition can be done remotely using valid methods and tools, described later. The process of acquisition (making a legal valid copy of all forensic artifacts) should be done using a well-defined, well tested and repeatable process, using trusted tools. Therefore, acquisition is more challenging process than collection. According to ISO 27037, as illustrated in Fig. 3, collection and acquisition are two parallel processes (ISO 27037, 2012).

Table 3 provides a summary of challenges in the Acquisition phase in cloud computing and possible or suggested solutions.

Inaccessibility

Due to the nature of cloud computing, un-restricted access to cloud storage is not possible, something that is guaranteed in traditional client-server environment. Note

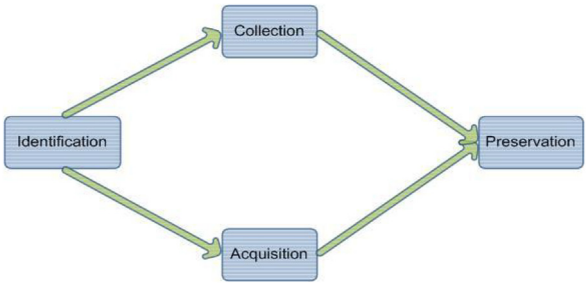

Fig. 3. Evidence Handling process according ISO 27037 (CSA, 2013a).

that the data in the cloud can be duplicated to multiple locations, resulting in decentralized artifacts. Some cloud providers, e.g., Amazon, allow users to choose their geographical location while creating VM instances. Even if the location is known, physical acquisition is not possible due to multi-tenancy.

Researchers have proposed various methods for evidence acquisition from cloud, such as:

- *Remote Data Acquisition*: It refers to acquiring the evidence remotely over a trusted and secure channel. Widely used forensic tools such as Guidance EnCase and Access Data FTK support remote data acquisition (Dykstra and Sherman, 2012). Dykstra and Sherman (2012) reported successful retrieval of volatile and nonvolatile data from Amazon EC2 cloud's active user instance platform using the tools, despite citing many layers of trust required. They validated the data integrity by computing and comparing the hashes of the images before and after downloading data.
- *Management Plane*: Controlling the virtual assets in the cloud using a web interface is often referred as the Management Plane. Using the interface, e.g., Amazon's AWS Management Console, users can conduct data acquisition of forensic artifacts, such as VM image, logs, disk images, user access information etc. is an example. One can use the AWS management console to extract CloudTrail logs without helps from the CSPs (AWS Security Centre, 2013a). However, one more level of 'trust', i.e., trust on the management console application, is required. In spite of the trust issue, researchers have recommended the use of management plane for remote data acquisition, especially for IaaS model (Dykstra and Sherman, 2012; Zawaod and Hasan, 2013). Zafarullah et al. (2011) showed that it is possible to collect necessary logs from cloud infrastructure using open source tools. One can use multi factor authentication for user authentication and acquire the disk image from cloud server using cryptographic tunneling protocol, e.g., virtual private network (VPN), to guarantee the confidentiality and integrity of the data as well as to solve the chain of custody problem, described in Section 3.2.1.
- *Live Forensics*: Forensics on a running system is referred as Live Forensics, in which an investigator performs forensics examination of a system in running state. Such forensics comes with an added advantage as it is able to

Table 3
Collection Phase: Challenges and Recommended solutions.

No:	Challenges	Recommended solutions	Comments
1	Inaccessibility	Remote Data Acquisition (Dykstra and Sherman, 2012)	By data imaging tools such as EnCase, FTK Imager, X-Ways, F-Response, Paladin etc., over a secure network link
		Management Plane (Dykstra and Sherman, 2012; Zawaod and Hasan, 2013)	Preferred option, removes the dependency on CSP
		Live Forensics (Hay and Nance, 2008)	Provides running system info, like process list, open ports etc., which are not available in offline forensics
		Snapshot Analysis (Birk and Wegener, 2011)	Captures the whole system info at the instant of taking the snapshot
2	Dependence on CSP	Management Plane (Dykstra and Sherman, 2012; Zawaod and Hasan, 2013)	Preferred option, but requires an additional level of 'trust' of the management plane
		Stronger SLA (Alhamad et al., 2010; Kandukuri et al., 2009)	Preferred option for customers
3	Ephemeral nature of data	Snapshot Analysis (Birk and Wegener, 2011)	Provides the point in time picture of the whole system.
4	Trust	Hardware Trusted Platform Model (TPM)	Designed to work with single OS, single machine. Fails to scale up to a virtualized cloud environment
		Virtual TPMs (Dongxi et al., 2010)	TPM instances are obtained on demand. Solves scalability issue
		Trusted Virtual Environment Module (Krautheim et al., 2010)	Modular and extensible approach which supports persistent storage of keys
		Trusted Cloud computing Platform (Santos et al., 2009)	Provides a closed box execution environment. Ensures confidentiality and integrity.
		Detective Controls (Ko et al., 2011)	Complements formal preventive approach, and can address the risk that arise from within CSPs
5	Multi-Tenancy	Isolating cloud instance (Delport et al., 2011)	Discussed various methods of isolating cloud instances.
		Sandboxing (Delport et al., 2011; Greamo and Ghosh, 2011)	Most popular method of isolating the instance and widely supported by the vendors.
6	Jurisdiction	SLA	Partially addressed in (Alhamad et al., 2010; Kandukuri et al., 2009)
		International co-operation in the form of agreements and treaties	E.g.: International Mutual Legal Assistance Treaties (MLAT) (INCSR, 2012)
7	Deleted data	Frequent snap shots	Difficult to achieve and manage due to the sheer volume of snap shot images
8	Lack of specialist commercial tools	Cloud data imager (Federici, 2014).	The recommended solutions remains to be commercialized

gather wealth of information, such as process list, kernel modules, open network ports, volatile memory data etc., from the running system, in addition to the information stored in persistent storage. *Virtual Machine Introspection (VMI)* is a live forensic technique where a user can interact with a running system from some other virtual machine, other than that being examined. Hay and Nance (2008) proposed a virtual introspection solution. They demonstrated their solution using Virtual Introspection for Xen (VIX) set of tools as a proof of concept. This has been further enhanced as an introspection library, known as LabVMI (VMITools). However, the live forensic tools are yet to be incorporated and provided as a commercial service by the CSPs.

- *Snapshot Analysis:* Snapshotting is a process of taking a clone of virtual image in running state, including all the system memory, and saving the clone to a persistent storage. Snapshot technology enables customer to freeze a specific state of VM (Birk and Wegener, 2011). Major hypervisor vendors, e.g., Xen, VMWare, ESX, and Hyper-V, support snapshot feature. Though snapshot images are not bit-by-bit copy of their corresponding sources, they provide valuable information regarding the running state of a system. The snapshot images can be restored by loading them to a target VM for analysis. Snapshot feature can capture live VM instance and works across decentralized regions too as long as the instances remain in the same logical infrastructure. Since the cloud environment is subject to rapid changes, a series of snapshot images over a period can provide valuable information regarding changes to the data assets, which can be used to analyze and map on to a time line of events. Therefore, for the cloud to be forensically ready, one should have an inbuilt feature to dump virtual machine snapshots automatically at configurable intervals, since it is impossible to know when the security breach occurs. On the down side, this feature would require more storage space, and can create a performance issues. Nevertheless, system administrators can either purge or overwrite unwanted image dumps.

Dependence on CSP

Many researchers have cited the dependence on CSPs during the forensic investigation process (Dykstra and Sherman, 2011; Zawaod and Hasan, 2013). While it is not common, there is a move by CSPs to provide management tools so that customers can collect the artifacts. To solve the dependency issue, one can use the *Management Plane* and *specific SLAs*, described in Section 3.3.1 and 3.1.4, respectively. Clearly drafted and executed Service Level Agreement between the provider and consumer is one of the key elements to address the CSP dependence challenge. The

SLA should specify specific forensic elements such as monitoring, forensic support services, data ownership (specifically of the data under investigation), responsibility, the right to retain consumer data for investigative purpose even when the consumer decides to change the cloud provider, and regulatory compliance including privacy (Alhamad et al., 2010; Ruan et al., 2012).

Ephemeral nature

The ephemeral nature of cloud data is another major issue facing the data acquisition. For example registry files, temporary files, Internet access history logs etc., are key forensics artifacts; however, data such as this can be difficult to collect from a cloud environment. The report by CSA mentioned the importance of acquiring volatile data in the cloud (CSA, 2013a). The Periodic snapshotting of VM instances, described in Section 3.3.1, is a possible solution.

Trust

In general trust means an act of faith in confidence and reliance on something that's expected to behave or deliver something as promised (Khan and Malluhi, 2010). In the cloud computing context, trust is the belief in the competence and expertise of the CSPs, and the underlying cloud architecture and systems, to reasonably care the valuable information assets of the users. *Trust* and *control* go together, e.g., we trust a system less if it has poor control. Trust also is function of *ownership*, e.g., you trust your own data assets. Note that in a public cloud model the service provider is the custodian of customer's data assets and customers have neither ownership nor control of the environment. When an enterprise adopts cloud and consigns its data (belonging to the enterprise and its clients) to the cloud, it creates an array of complex trust relationships. First, the enterprise must trust the cloud provider. Second, the enterprise should ascertain that their clients have enough reason to trust the same provider. In cloud forensics the lack of transparency and trust, results in untrustworthy evidence data (Birk and Wegener, 2011; Khan and Malluhi, 2010).

Researchers have highlighted the problem associated with Trust in cloud forensics (Birk and Wegener, 2011; Damshenas et al., 2012; Daryabar et al., 2013; Dykstra and Sherman, 2012; Hay and Nance, 2008; Hay et al., 2011; Zawaod and Hasan, 2013). The different layers of trust for IaaS cloud model are: Network, Physical hardware, Host OS, Virtualization, Guest OS, Guest application/data (Dykstra and Sherman, 2012). For the evidence to be valid there is a need to establish trust in the layers of used cloud model. The layers of trust increases cumulatively as more services are subscribed from the CSP, i.e., the layers of trust are the highest for SaaS model and lowest for IaaS model. Fig. 1 describes the trust layers.

Solving the trust issue for cloud forensics remains a big challenge. Trust cannot be solved by using technology means alone; rather the solution should be a combination of process, people and technology. Following an established forensic process, e.g., ACPO guidelines, having appropriately experienced or certified people undertaking forensic collection and evaluation, and using industry recognized forensic software or hardware tools, would together contribute to strengthening the trust in evidence.

Trust can also be treated as a function of security. Consumers will trust the systems that are more secure. Security is a significantly recurring factor in the concept of trust in an IT environment. To place in the context of cloud computing forensics and trust, ultimately we are searching for trustworthy tools, methods and persons to identify, acquire and analyze forensic data, such that the evidence is worthy of trust. In other words, the evidence collected from a more secure system will be more trusted. One of the widely accepted approaches to solve the security issues is using Trusted Platform Model (TPM), which is briefly described as follows.

- *Hardware TPMs*: There are hardware vendors who integrate TPM chip to the motherboard, which is capable of performing platform authentication. TPM contains a private key endorsed with the chip that uniquely identifies the hardware (thereby the physical host) supported by cryptographic functions that cannot be modified. The manufacturer of the chip signs the corresponding public key to validate the correctness of the chip and validity of the key. However TPM chips are usually designed to work with single OS on a single machine and typically would not scale with system virtualization – the default characteristic of cloud computing.
- *Virtual TPM (VTPM)*: Virtual TPM is a novel approach to solve trust issue, where TPMs are located in the cloud as virtual entities. A TPM instance can be obtained from TPM cloud on demand, thereby TPM functionality can be obtained even in platforms that have no TPM chips. This technique scales very much to virtual instances where one can access the same TPM instances from multiple VM instances or locations and the users can use TPM functionality without owning a TPM chip (Dongxi et al., 2010).
- *Trusted Virtual Environment Module (TVEM):* TVEM helps to solve the trust issue by using a trust relationship model, enabling parties to establish trust relationship between information owner and the virtual environment on a platform owned by the CSP. The core component of TVEM is the unique Trusted Environment Key that combines trust from the information owner and the service provider to create a dual root of trust that is distinct for every virtual environment and separate from the hosting platform's trust. The TVEM architecture is modular and extensible that allows flexibility and also provides persistent storage for keys (Krautheim et al., 2010).
- *Trusted Cloud Computing Platform (TCCP)*: TCCP provides a closed box execution environment by extending the concept of trusted platform to IaaS environment. The TCCP guarantees confidentiality and integrity and allows users to attest to the IaaS provider that its service is secure before launching VMs. This is achieved by providing an abstraction of a closed box environment for customer's VM, guaranteeing that none of cloud provider's privileged administrators can inspect or tamper with its content (Santos et al., 2009).

- *Detective Controls*: This is a method of establishing trust in the cloud using detective rather than preventive approaches and thereby increasing accountability. Detective controls are based on policy and process, which complements preventive controls. The benefit of this approach is that it is non-invasive and enforces the need for policy and governance structure for both cloud consumer and provider and thereby establishing accountability and trust (Ko et al., 2011).

Multi-tenancy

One of the prime characteristics of cloud computing is that multiple VMs, hosting multiple tenants instances can share the same physical hardware, and that can spread across different data centers. This model is very much different to single owner system, where it is easy to seize the hardware. The multi-tenancy aspect adds very much to the complexity of forensics data collection in the cloud. Though the VMs operate in their own sandboxes without knowing the existence their neighbors, doing a physical seizure is not at all practical as it can hold other customers' data. CSPs are bound to protect the privacy of customers and abide by the regulations. For example a 2012 report by ENISA emphasized that multi-tenant outsourced services should protect the privacy of co-tenants (Hogben and Dekker, 2012). Further Ruan et al. (2012) highlighted that SLAs must address privacy issue and noted that "*the cloud provider to accurately and comprehensively filter forensic data sources that contain data belonging to multiple tenants and release only the data related to the specific tenant*".

Researchers have recommended to use management plane for forensic data acquisition. Dykstra and Sherman (2012) used forensic tools, such as EnCase and FTK, to successfully return the evidence from Amazon EC2 cloud without violating the privacy of other tenants. Some CSPs, e.g., Amazon, offer a single tenant option while creating an instance for an additional fee. Other suggested solutions are:

- *Isolating cloud instance*: Delport et al. (2011) introduced a new concept of isolating the cloud instance to facilitate forensic investigation, using different methods such as instance relocation, address relocation, server farming etc. The isolated instances can prevent further contamination or tampering of possible evidence.
- *Sandboxing*: Creating sand box image of virtual machine instance is another way of isolating and protecting the evidence (Delport et al., 2011; Greamo and Ghosh, 2011). Sandboxing is an easily executable option and most of the vendors support sandboxing feature. Sandboxed VM images can then be acquired using remote acquisition methods.

Jurisdiction

The CSPs often perform data mirroring to ensure high availability and business continuity. The mirrored databases can be in different jurisdiction than the primary location, causing lack of real time information about the data location as well as introducing high degree of difficulties for data acquisition. Jurisdictional issue associated with data location is one of the major concerns of customers. The cloud consumer should be aware that it could be difficult, to conduct investigation when the data does not reside in jurisdictions with proper regulations (Ruan et al., 2013).

One possible solution to the problem is using specific SLA, described in Section 3.1.4, in which customers could specify where the data could be stored or relocated. The cloud provider should also accurately track the jurisdiction in which a cloud consumer's data resides during a given period (Ruan et al., 2012). If the data assets are spread across logical infrastructures around different locations, then they can be acquired using proven techniques such as Remote Data Acquisition or commercially available tools. Further to that, if the data crosses geo-political borders, stronger international cooperation and agreements also will be required for evidence artifacts collection, establishing chain of custody etc. (Taylor et al., 2011). As an example, international agreements in the form of Mutual Legal Assistance Treaties (MLAT) that exists between US and other countries generally allows the exchange of evidence and information in criminal activities (INCSR, 2012). The Convention on Cyber Crime, held in Budapest on Nov 2001, outlines the legal framework for combating cybercrime; in particular Article 22 to Article 25 discuss Jurisdiction, International cooperation and General principles related to mutual assistance for the purpose of investigations or proceedings concerning offenses related to cybercrime (DOS, 2001).

Prasad (2012) argues the need for stronger and effective international legal framework, citing that the existing international conventions and treaties are not effective for combating cybercrimes, especially when the perpetrator and the victim fall in different jurisdictional area. Leadership of world bodies, such as the United Nations, is essential to facilitate agreements among member states, including the collection and sharing of information by enforcement agencies (Prasad, 2012).

Deleted data

From forensics perspective, deleted data and attributing the deleted data to a specific user are vital sources of evidence. Normally, the deleted data can be collected from the media using data carving methods supported by forensics tools. However, in case of cloud, the volatility and elasticity of cloud environments make it much harder to collect the deleted data. Dykstra and Sherman (2012) showed how to remotely acquire hardware and memory images from Amazon cloud. They also proved the completeness of the data by analyzing the image, as well as the timeline of activity of the actions done (in this case they created and deleted a series of web pages), with no anomalies or anything unusual to suspect the integrity of the data. They could also prove that, it is possible to collect the deleted data (provided that the data volume is not overwritten) by the same tenant, excluding data or residual data from the previous tenant(s) who probably had the same hardware space (Dykstra and Sherman, 2012). Though this satisfies the privacy regulations, it works negatively from forensic

perspective. Those with criminal intention can carry out the tasks using cloud and terminate their account, delete the VM instances and disappear without leaving any trace. CSPs, in an attempt to provide highest respect to privacy, delete the data completely once confirmed by the users. For example, Google's current policy on deleted data states the following:

> "*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, 2014).

This highlights the fact that there is a disconnection between privacy regulations and forensic needs in the cloud. Even if deleted data has been found in the cloud, attributing it to a specific user remains to be a big challenge due to the sheer volume of the data and amount of backup cloud provider would maintain (NIST, 2014b). Taking frequent snapshots of the virtual image is a possible solution, which has been explained in Section 3.3.1, under bullet point *Snapshot Analysis*.

Lack of specialist commercial tools

Full forensic artifacts also include the metadata, full revision history of files and the changes done to the file content, registry contents, deleted partition, network logs, traffic patterns and more importantly the hypervisor level logs which provide critical information such as cloud instance user account creation and deletion times. There is a lack of certified commercial tools that can be used for e-discovery and data acquisition for forensic purposes in cloud environment in its entirety. However, researchers have proved that it is possible to perform remote data acquisition from an active user account (Dykstra and Sherman, 2012).

Researchers have also found that wide range of forensic artifacts remain in the client and server sides as data remnants, e.g., directory listings, pre-fetch files, link files, thumbnails, registry, browser history etc. Further, the link file references still exist even after file erasing tools have been used as reported in the case studies conducted on Microsoft Skydrive and ownCloud instances (Martini and Choo, 2013; Quick and Choo, 2013). All such data remnants and file references forms part of valid forensic artifacts.

Federici (2014) extended the work outlined by Quick and Choo (2013) and presented a Cloud Data Imager. Federici (2014) noted that the motivation for the work is that the traditional approach of bit stream copying of mass storage may not be possible in an investigation concerning crime related information hosted on cloud platform. Applications devoted to remote data acquisition with forensically sound architecture and requirements are not wide spread to date and cloud data imager fills this gap. Cloud data imager is a dedicated forensic software to log the full conversation with the cloud platform at application level and in clear text, which supports remote data collection from cloud storage, conforming to the principle of reliability and integrity of digital evidence by enforcing read only access (Federici, 2014).

However, such kind of holistic and certified tools that provide end-to-end forensic data collection, including hypervisor level information, are not so widespread to date. Therefore, the cloud consumer or investigators have to depend upon the CSPs to provide the evidence.

Examination and analysis

Once the digital artifacts are acquired and preserved the next logical step is the examination and analysis phase. Examination and analysis is one of the crucial elements of forensic computing. According to NIST, *Examination* is defined as "*Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity*" (Kent et al., 2006). NIST states that Analysis "*Involves analyzing the results of the examination to derive useful* information that addresses the questions that were the impetus for performing the collection and examination" (Kent et al., 2006). ISO 27037 defines analysis as "*identification and evaluation of items of evidence from a source of potential digital evidence*" (ISO 27037, 2012).

Typically, in an Analysis phase, the significance of information artefacts evaluated and a narrative produced is supported by the evidence and a timeline of events. A narrative would help to understand the case better and can be easily explained to a jury. However, this is not mandatory and mostly the presence of evidence is enough. Table 4 lists the challenges and recommended solutions in Examination and Analysis phase as applicable to the cloud platform.

Lack of log framework

In general, cloud service providers use their own logging policy and format (AWS Security Centre A, 2013b, 2014, Google, 2014). Lack of proper forensically valid log framework applicable to cloud computing, produces challenges in time lining of events. However, logs are not mandatory for investigative purpose and investigations can be conducted by examining file contents, access time stamps and data remnants. Nevertheless, logs really help an investigator to connect the dots. In Section 3 we discussed various digital forensic frame work. Log framework forms a subset of comprehensive forensic framework. Recommended solutions proposed by researchers are briefly discussed below:

- *Comprehensive Log Management System:* The need for a comprehensive log management system, which contains enough information satisfying the forensic needs has been flagged by many researchers (Dykstra and Sherman, 2012; Marty, 2011; Sang, 2013; Zawoad et al., 2013). Marty (2011) proposed cloud application logging framework, and provided a detailed guidelines regarding when to log, where to log and exactly what to log in order to enable forensic investigation, reporting

Table 4
Examination and Analysis phase: Challenges and Recommended Solutions.

No:	Challenges	Recommended solutions	Comments
1	Lack of Log Frame work	Comprehensive Log Management system (Dykstra and Sherman, 2012; Marty, 2011; Sang, 2013; Zawoad et al., 2013)	A good log helps to timeline the events and understand the case better
		Amazon AWS CloudTrail (AWS Security Centre, 2013a, b)	Provides prime forensic information for Amazon users
2	Evidence time lining	AWS CloudTrail can provide a partial solution (AWS Security Centre, 2013a, b; 2014)	AWS Cloud Trail provides comprehensive access info in UTC format and enables time lining
		Secure Logs with proper time stamps	End-to-end log helps to create a time line of events
		Secure Provenance ((Lu et al., 2010)	Provides the ownership and history of data objects
3	Encrypted data	Cloud key management infrastructure (CSA, 2013a)	Possible future implementation
4	Evidence data Integration	AWS CloudTrail supports aggregation of log files (AWS Security Centre, 2013a, b; 2014)	Requires third party tools for processing and analysis
		Security Information and Event Management (SIEM) (Hewlett-Packard, 2012)	Supported by tools like ArchSight
		Data Tracking (Zhang et al., 2011)	Data tracking in the cloud, using provenance.

and correlation. In the Secure-Logging-as-a-Service (SecLaaS), the authors proposed a scheme to store and provide logs for forensic purposes securely. This scheme will allow the CSPs to store the logs in the cloud while preserving the confidentiality of the cloud users, and maintain the integrity, while at the same time making it available publicly in a secure way (Zawoad et al., 2013).

- *Amazon AWS CloudTrail*: As a part of security operational best practice and to comply with industry and regulatory compliance, Amazon has recently provided AWS CloudTrail audit logging feature. This feature is a web service, which logs the API calls to support AWS services and deliver the log file to a pre-defined Amazon Simple Service Storage (Amazon S3) bucket. Though Amazon has created the cloud audit trail web service by taking into account various logging and compliance requirements from PCI DSS v2.0, ISO 27001:2005 etc., it can also be used for forensics analysis. The log files are written in Java Script Object Notation (JSON) format. The log files can be extracted from the defined S3 bucket using AWS management plane, without requiring any support from the CSP. AWS CloudTrail provides a comprehensive mechanism to restrict the access to the log files itself, such as configuring access using IAM roles or even fortifying the access controls using AWS multi factor authentication services, thereby alleviating the issue related to authenticity or "trust" of logs itself. Moreover, the log files are encrypted using S3 Server Side Encryption (AWS Security Centre, 2013a, b).

The AWS Cloud Trail is a regional service, but allows the aggregation of log files across different regions and multiple accounts to a single S3 bucket. The CloudTrail logs events using UTC format, despite the running system time, and provides a comprehensive information including "who performed the activity, what they did, when and from where", which will be very useful in incident investigations as well as in evidence time lining (AWS Security Centre, 2013a).

Evidence time lining

Time lining provides an association of timestamps with each event or data item of interest in order to reconstruct a sequence of events. Time lining is assisted by the fact that the majority actions performed on the object are time stamped. At this point, it is worth mentioning some of the requirements of digital evidence. Digital evidence must satisfy the same legal requirements as conventional evidence, i.e., it must be (i) Authentic, (ii) Reliable, (iii) Complete, (iv) Believable and (v) Admissible (Reilly et al., 2010, 2011). Further, Reilly et al. (2011) explained how to reconstruct the sequence of events in a hacking attacks between end point device, target, victim and intermediaries in a cloud scenario. Time lining assists to understand evidence and data, putting information into context, which is potentially easier to understand. Further time lining also helps to explain the case better to a jury. Researchers have suggested the following methods to help evidence time lining:

- *Secure Logs with proper time stamps*: Such as AWS CloutTrail logs or Secure Logging as a Service proposed by Zawoad et al. (2013) or similar logs which can be used for end-to-end event time line creation
- *Secure Provenance*: Lu et al. (2010) proposed secure provenance, citing it as the bread and butter of data forensics in cloud computing. Secure provenance records ownership and process history, and provides trusted evidences of data objects; therefore, it plays a key role in cloud forensics. A properly implemented secure provenance helps in evidence time lining, because ownership and process history attributes provide information regarding 'who' owned the data object at a given time, and 'who' updated the objects respectively.

Encrypted data

Encryption is being widely used by cloud customer as a measure of securing the data, or to satisfy legal and

Table 5
Reporting and presentation phase: challenges and recommended solutions.

No:	Challenges	Recommended solutions	Comments
1	Jurisdiction	Cross border law, International relations	Legal Agreements (E.g.: MLAT ((INCSR, 2012)
2	Chain of custody	Well defined principles and guidelines (Biggs and Vidalis, 2009; Grispos et al., 2013; Taylor et al., 2011)	Essential to establish the trust of the evidence
3	Crime scene reconstruction	Framework, process and guidelines, supported by tools and technology	There is a lack of such tools
4	Complexity of Cloud	Time lining of events	Difficult to explain the complexity of cloud to jury
5	Compliance	Established principles, process and procedures (e.g., ACPO guidelines in UK)	–

compliance requirements. However, criminals can also use encryption for illegal purpose. McKemmish (1999) pointed out the wide spread usage of encryption by criminals to hide illegal images. Biggs and Vidalis (2009) mentioned that 70–80% of an investigator's workload in UK law enforcement agency is spent on monitoring cloud computing usage by pedophiles. Therefore, from forensic perspective, the encryption produces a significant barrier for an examiner. Cloud Security Alliance's report suggests that "*key management infrastructure used within the cloud (topology, process, technologies) may create the option to make the key accessible*" for forensic examiners (CSA, 2013a), as a possible future solution. However, such option should be supported by proper regulations and governance structure to avoid possible privacy violations and misuse.

Evidence data integration

In cloud, the evidence data is spread across multitude of devices spread across different locations, including mobile end points, middle tier proxy servers and cloud virtual environment itself. In addition, as Ruan et al. (2011) pointed out, CSPs often trade services among themselves, creating a complex array of intra-cloud dependency chain. The trading produces additional challenges, not only to acquire the evidence from multiple sources, but also in collating and integrating the evidence data as investigators have to follow each link in the dependency chain.

Integrating all these pieces of data and creating the sequence of events are crucial parts of forensics process. Suggested methods are discussed below:

- *AWS CloudTrail* supports aggregation of log files to a single Amazon S3 bucket (AWS Security Centre, 2013a), which is useful only for Amazon customers but requires third party tools for doing business intelligence analysis. In view of forensics, any additional layer of third party tools used adds a layer of 'trust' issue.
- *Security Information and Event Management (SIEM)* tools, such as ArchSight, provide log integration from multiple sources and can be used for evidence time lining (Hewlett-Packard, 2012)
- *Data Tracking*: Zhang et al. (2011) provided a mechanism of data tracking in the cloud using data provenance software tools implemented utilizing data tracking principles would help to integrate user artifacts and draw event time line.

Reporting and presentation

Evidence collected during the collection or acquisition phase and the analytical reports are presented to the court of law during this phase of the forensic process. NIST defined *Reporting* as a process which "*includes describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process*"(Kent et al., 2006). The expertise and the qualification of the presenter and the credibility of the process used to produce the reports can be challenged in the court. Therefore, reporting and presentation are critical to determine the probative value of evidence.

Table 5 lists challenges and their recommended solutions in this phase.

Jurisdiction

In Section 3.3.6, we discussed the jurisdictional issue related to evidence acquisition in cloud. Jurisdiction also is a challenge while presenting the case, because the law of the land is different from place to place. For example, Prasad (2012) cited that, as per Australian law the perpetrator must be in Australia or an Australian citizen overseas for cybercrimes to be accepted by Australian court. If the perpetrator is overseas, but not an Australian citizen, and there is no extradition treaty between the host nation and Australia, then Australian court has no jurisdiction, further strengthening the argument for an international framework (Prasad, 2012). Further, a study conducted on critical criteria for cloud forensic capability found that lack of law, regulations, lack of international cooperation and legislative mechanism in cross nation data access and exchange are by far the most forensic challenges in the cloud (Ruan et al., 2013). Cloud forensics, being a multi-dimensional issue and consisting of technical, organizational and legal domains, requires collaboration between international law enforcement agencies and legal framework to conduct and present crimes conducted using cloud computing (Ruan et al., 2011). Legal framework like MLAT would help in those countries that are signatories to it.

Chain of custody

Proving the chain of custody in cloud forensics is a more complex process as compared to traditional digital forensics when it comes to case presentation. Further, in a survey study, Ruan et al. (2013) found that "*a procedure and a set of*

toolkits to record and maintain the chain of custody in an investigation is very important" to consumers. Following established guidelines, e.g., Association of Chief Police Officers (ACPO) guidelines in UK, is one way to establish chain of custody. These guidelines provide all relevant information to be followed with high standard, for the case to stand in the court and to establish trust in the evidence presented (Biggs and Vidalis, 2009; Grispos et al., 2013; Taylor et al., 2011).

Crime scene reconstruction

Reconstructing crime scene in the cloud remains as a challenge, due to lack of applicable tools and supporting process and guidelines. The algorithms and software tools for reconstruction of cloud storage and evidence are yet to be validated and developed (NIST, 2014b).

Complexity of cloud

Juries in common law system are made of individual from general-public, often with very limited or no understanding of cloud computing technology. Therefore expert witness will be faced with the daunting task of ensuring juries fully understand the principles and technology of cloud computing (Grispos et al., 2013). In simple terms time lining events would help to explain the case better to a jury and easier to understand.

Compliance

For evidence to be legally valid in the court, following an established standard procedure throughout the forensic process is necessary. Several examples of established procedure are (i) ACPO Good Practice Guide for Computer Based Electronic Evidence and (ii) International Organization on Computer Evidence (IOCE). ACPO guide provides the definitions and the four principles of computer based electronic evidence (ACPO, 2012). In general terms the ACPO rules are mirrored by the IOCE in its draft guidelines. But the guidelines are developed prior to the advent of cloud computing (Adams, 2013). Adams (2013) discussed the principles of the guideline provided by the ACPO, their applicability in the cloud environment, and the difficulties in following the principles, despite the authors stressed the importance of following the guidelines to ensure compliance. In the absence of specific process model, higher level frameworks such as ISO, framework would apply. If the organization creates and follows its own standard operating procedures, it may not stand up in the court.

Summary and future work

Digital forensics as a service

We have discussed several digital forensic process models, most of which were developed for traditional forensic purpose. Researchers have tried to extend these models to cloud forensics. Even though the digital forensic process model is not standardized, there exists consensus on the abstract level about the digital forensic model. However, more work remains to be done to produce models that are recognized and accepted by all stakeholders of cloud computing.

Digital forensics in the cloud is an emerging area, and digital forensics-as-a-service is a service based approach for processing and investigating digital material, that has been discussed by many researchers (van Baar et al., 2014; Wen et al., 2013). van Barr et al. (2014) provided an analysis of the digital forensics as a service model (DFaaS) setup in Netherlands. In DFaaS model, the digital investigator focuses on harvesting forensic data continuously and sends the data to a centralized system. Detectives with specific domain expertise and deep knowledge (rather than investigators) are given access to the subset of the harvested data, which they analyze. The detectives functions as analysts, and the investigators functions more as a harvesters of forensic data. Using business intelligence applications, search and filtering techniques, the noise in the data set is much reduced and detectives can easily narrow down the analysis to small sub set of traces, which is of importance to deduce hypothesis and conclusion. The paper concludes that the this model has become a standard in Netherlands with great success (van Baar et al., 2014).

In the work by Wen et al. (2013) on Forensics-as-a-Service (FaaS) used cloud platform to do forensic examination and analysis and proved a forensic workflow management and processing using cloud. The abundant processing and storage power available in cloud is an ideal environment for storing and processing overwhelming magnitude of digital data and to enable interoperability among many forensic data processing softwares. Wen et al. (2013) proved that the cloud based forensic work flow management and processing can save up to 87% of analysis time, in the tested scenarios, in comparison with traditional methods.

Summary of findings

Unknown physical location of forensic artifacts and duplicate copies of the data being spread across different virtual servers, possibly in different countries, in a cloud environment causes significant hurdles not only in the evidence identification phase, but also in preservation and acquisition phases. Further work needs to be undertaken for efficient resource identification without being cost prohibitive. Often Law Enforcement Agencies (LEA) and customers have to depend upon CSPs for full data recovery and that requires stronger SLAs. More work is required to be undertaken addressing cloud forensic SLA guidelines.

The decentralized and ephemeral nature of cloud environment produce not only a technical challenge, but also a legal issue, requiring support from other countries, since it is possible that the victim, the perpetrator and the cloud platform are located in different jurisdictions. Though there exists legal framework for cooperation among some countries, authors identified a lack of international framework and agreements, suggesting urgent attention by lawmakers.

Often CSPs trade service among themselves, creating an array of dependencies and trust issue. Investigators have to follow each link in the chain in order to collect the evidence. Moving forward, there is a strong need for a forensically valid uniform log framework, including the ability to capture hypervisor level logs that are segregated per user

account level (to protect the privacy of co-tenants), and the ability to track the movement of user files in intra-cloud. Such logging mechanism will greatly help the traceability and provide transparency. Guidelines or processes to follow when CSPs trade services among themselves are other avenues for further research work.

Cloud customers are adopting encryption to ensure the confidentiality and integrity of data, or to satisfy the policy or regulatory requirements. However, encryption causes biggest challenge in evidence identification and evidence segregation. Live forensics and frequent capture of snapshot images of the running system enhances the forensic capabilities, but it adds to cost, creates overhead and performance issues. It is equally important to keep the hash values of critical forensic artefacts, like log files securely. More work should be undertaken to create a standard operating procedure and supporting guidelines for the investigators to have access to the decryption key without violating the privacy rules.

Properly implemented secure provenance can play critical part in the future of cloud forensics, as it provides ownership, process history, and comprehensive security features, thereby forming part of trusted evidence (Lu et al., 2010). The data tracking mechanism suggested by Zhan et al. (2011) can be extended to look beyond a single cloud environment to inter-cloud, cloud-to-internet and internet-to-cloud data movement and management scenarios as future work.

We also found that ensuring trust in cloud evidence remains a big challenge in cloud forensics. Also, deleted data is much harder to collect from a cloud partition. In general, forensic requirements and privacy rules often contradict each other and cloud providers, in an attempt to give maximum respect to privacy laws, make the cloud platform more secure, inadvertently making forensic tasks much harder. It is also our observation that the major CSPs have started providing forensic capabilities in their service offerings (e.g., Amazon CloudTrail).

In a recent case study using XtremeFS tool, on distributed file system, which are commonly used in cloud computing environments, Martini and Choo (2014) highlighted the importance of forensically sound process. Such process can provide clear guidance to digital forensic practioners in their investigation, from evidence source identification and preservation, to collection of volatile, non-volatile and network data, to examining and analyzing the data, and finally to reporting and presenting in a court of law (Martini and Choo, 2014).

Conclusion

Cloud computing has changed the way the IT services are being delivered and consumed. There has been a tremendous growth of cloud adoption and that trend is expected to continue. Correspondingly there is growing concern by the consumers about the security and privacy of data assets stored in the cloud. On the other hand there is a growing concerns on the potential to use of cloud as a platform to conduct cybercrimes. With immense computing power and storage offered by cloud, major attacks can be conducted in shorter time periods and at low cost. The criminals can then terminate the account completely and disappear without leaving any traces. This is further exacerbated by the digital forensic difficulties and challenges in cloud environment. In this paper, we have provided systematic analysis of cloud forensics challenges, their possible solutions pertaining to different phases of the forensic process, and detailed analysis of the recommended solutions. We have identified the maturity of solutions and flagged the opportunities for further research and development. We have also provided a brief summary of forensics-as-a-service models.

Acknowledgment

Authors would like to thank the anonymous reviewers and Eoghan Casey, the Editor of Digital Investigation journal for their valuable and constructive comments, which helped improve the paper.

References

ACPO. ACPO good practice guide for digital evidence (Version 5.0). 2012. Available at, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [Accessed 02.12.14]. UK.

Adams R. The emergence of cloud storage and the need for a new digital forensic process model. In: Ruan K, editor. Cybercrime and cloud forensics: applications for investigation processes. IGI Global; 2013. p. 79–104.

Alhamad M, Dillon T, Chang E. Conceptual SLA framework for cloud computing. In: 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST); 2010. p. 606–10.

AWS Security Centre A. AWS cloud trail, user guide. 2013. Available at, https://aws.amazon.com/documentation/cloudtrail/ [Accessed 12.12.14].

AWS Security Centre A. Logging in AWS. 2013. Available at, http://aws.amazon.com/whitepapers/security-at-scale-logging-in-aws/ [Accessed 12.12.14].

AWS Security Centre A. Amazon web services: overview of security process. 2014. Available at, https://aws.amazon.com/security [Accessed 11.12.2014].

Biggs S, Vidalis S. Cloud computing: the impact on digital forensic investigations. In: Proceedings of the 2009 International Conference for Internet Technology and Secured Transactions, (ICITST). London, UK: IEEE; 2009. p. 1–6.

Birk D, Wegener C. Technical issues of forensic investigations in cloud computing environments. In: Proceedings of the 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE). Oakland, CA, USA: IEEE; 2011. p. 1–10.

Brezinski D, Killalea T. Guidelines for evidence collection and archiving. Req For Comments 2002:3227.

Casey E. Cloud computing and digital forensics. Digit Investig 2012;9:69–70.

Catteddu D, Hogben G. Cloud computing risk assessment. European Network and Information Security Agency (ENISA); 2009. Available at, http://wwwenisaeuropaeu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment [Accessed 17.07.14].

CSA. Mapping the forensic standard ISO/IEC 27037 to cloud computing. 2013. Available at, https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf [Accessed 10.08.14].

CSA. Security guidance for critical areas of focus in cloud computing V3.0. Cloud Security Alliance; 2011. Available at, https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/ [Accessed 10.09.14].

CSA. Cloud computing vulnerability incidents: a statistical overview. Cloud Security Alliance; 2013b. Available at, https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/ [Accessed 10.11.14].

Damshenas M, Dehghantanha A, Mahmoud R, bin Shamsuddin S. Forensics investigation challenges in cloud computing environments. In: Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE; 2012. p. 190–4.

Daryabar F, Dehghantanha A, Udzir NI. A survey about impacts of cloud computing on digital forensics. Int J Cyber-Secur Digit Forensics (IJCSDF) 2013;2:77–94.
Delport W, Kohn M, Olivier MS. Isolating a cloud instance for a digital forensic investigation. In: Proceedings of the 2011 Information Security South Africa (ISSA) Conference. Johannesburg, South Africa: ISSA; 2011.
Dongxi L, Lee J, Julian J, Nepal S, Zic J. A cloud architecture of virtual trusted platform modules. In: Proceedings of the 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC). IEEE; 2010. p. 804–11.
DOS. Convention on cyber crime. Department of State, United States of America; 2001. Available at, http://www.state.gov/s/l/treaty/tias/2001/131597.htm [Accessed 08.12.14].
Dykstra J, Sherman AT. Understanding issues in cloud forensics: two hypothetical case studies. J Netw Forensics 2011;3:19–31.
Dykstra J, Sherman AT. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digit Investig 2012;9:S90–8.
Federici C. Cloud data imager: a unified answer to remote acquisition of cloud storage areas. Digit Investig 2014;11:30–42.
Gartner. Forecast: public cloud services, worldwide, 2012–2018, 1Q14 update. 2014. Available at, https://www.gartner.com/doc/2696318?ref=clientFriendlyURL [Accessed 08.09.14].
Google. Google's approach to it security, a google White paper. 2014. Available at, http://www.google.com/enterprise/apps/business/resources/docs/security-whitepaper.html [Accessed 12.12. 2014].
Greamo C, Ghosh A. Sandboxing and virtualization: modern tools for combating malware. Secur Priv IEEE 2011;9:79–82.
Grispos G, Storer T, Glisson WB. Calm before the storm: the challenges of cloud. In: Emerging digital forensics applications for crime detection, prevention, and security; 2013.
Guo H, Jin B, Shang T. Forensic investigations in cloud environments. In: 2012 International Conference on Computer Science and Information Processing (CSIP). IEEE; 2012. p. 248–51.
Haeberlen A. A case for the accountable cloud. SIGOPS Oper Syst Rev 2010;44:52–7.
Hay B, Nance K. Forensics examination of volatile system data using virtual introspection. ACM SIGOPS Oper Syst Rev 2008;42:74–82.
Hay B, Nance K, Bishop M. Storm clouds rising: security challenges for IaaS cloud computing. In: Proceedings of the 2011 44th Hawaii International Conference on System Sciences (HICSS); 2011. p. 1–7.
Hewlett-Packard. Security information and event management. Big data big security (White paper). 2012.
Hogben G, Dekker M. Procure Secure: a guide to monitoring of security service levels in cloud contracts. In: ENISA; April 2012. At, http://www.enisa.europa.eu/activities/Resilienceand-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-incloud-contracts [Accessed: 10.06.14].
IEEE. IEEE cloud computing. In: IEEE cloud computing Premiere issue may 2014. IEEE; 2014. pp. 4–7, 10–9.
INCSR. International narcotics control strategy report (INCSR): treaties and agreements. United States of America: Department of State; 2012. Available at, http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm [Accessed 08.12.2014].
Iorga M, Badger L. NIST: challenging security requirements for US government cloud computing adoption (Draft). 2012. p. 54–6. NIST Special Publication.
ISO 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012.
Jansen W, Grance T. Guidelines on security and privacy in public cloud computing. 2011. p. 1–38. Available at: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf [Accessed 21.12.2014]. NIST special publication.
Kandukuri BR, Paturi VR, Rakshit A. Cloud security issues. In: Proceedings of the 2009 IEEE International Conference on Services Computing, SCC '09 Bangalore, India; 2009. p. 517–20.
Kent K, Chevalier S, Grance T, Dang H. Guide to integrating forensic techniques into incident response. 2006. p. 800–86. NIST Special Publication.
Khajeh-Hosseini A, Greenwood D, Sommerville I. Cloud migration: a case study of migrating an enterprise it system to IaaS. In: Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD). Miami, USA: IEEE; 2010. p. 450–7.
Khan KM, Malluhi Q. Establishing trust in cloud computing. IT Prof 2010;12:20–5.
Ko RK, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, et al. TrustCloud: a framework for accountability and trust in cloud computing. In: Proceedings of 2011 IEEE World Congress on Services (SERVICES). IEEE; 2011. p. 584–8.
Kohn MD, Eloff MM, Eloff JH. Integrated digital forensic process model. Comput Secur 2013;38:103–15.
Krautheim FJ, Phatak DS, Sherman AT. Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. In: Acquisti A, Smith SW, Sadeghi A-R, editors. Trust and trustworthy computing. Berlin Heidelberg: Springer; 2010. p. 211–27.
Lin C-H, Lee C-Y, Wu T-W. A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics. Int J Secur Appl 2012:6.
Lu R, Lin X, Liang X, Shen XS. Secure provenance: the essential of bread and butter of data forensics in cloud computing. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM; 2010. p. 282–92.
Martini B, Choo K-KR. An integrated conceptual digital forensic framework for cloud computing. Digit Investig 2012;9:71–80.
Martini B, Choo K-KR. Cloud storage forensics: ownCloud as a case study. Digit Investig 2013;10:287–99.
Martini B, Choo K-KR. Distributed filesystem forensics: XtreemFS as a case study. Digit Investig 2014;11:295–313.
Marty R. Cloud application logging for forensics. In: Proceedings of the 2011 ACM Symposium on Applied Computing. ACM; 2011. p. 178–84.
McKemmish R. What is forensic computing?: Australian Institute of Criminology. 1999.
NIST. NIST cloud computing collaboration site. 2014.
NIST. In: Group CFSW, editor. NIST Cloud Computing Forensic Science Challenges (Draft NISTIR 8006); 2014.
Palmer G. A road map for digital forensics research, Report from the first Digital Forensics Research Workshop (DFRWS). In: Palmer G, editor. DFRWS Technical Report DTR – T1001-01 FINAL. New York: DFRWS; 2001.
Patel P, Ranabahu AH, Sheth AP. Service level agreement in cloud computing. 2009.
Pichan A, Lazarescu M, Soh ST. Can Nuclear Installations and Research Centres Adopt Cloud Computing Platform? Available at: http://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000075.pdf. Symposium on International Safeguards Linking Strategy, Implementation and People Available at: http://wwwiaeaorg/safeguards/symposium/2014/home/eproceedings/sg2014_eproceedings_onlinepdf. Vienna: IAEA; 2014. p. 1–9.
Prasad K. Cyberterrorism: addressing the challenges for establishing an international legal framework. In: Proceedings of the 3rd Australian Counter Terrorism Conference. Perth, Australia. Perth, Western Australia: SRI Security Research Institute, Edith Cowan University; 2012. p. 9–14.
Quick D, Choo K-KR. Digital droplets: Microsoft SkyDrive forensic data remnants. Future Gener Comput Syst 2013;29:1378–94.
Quick D, Martini B, Choo R. Cloud storage forensics. 1 ed. Massachusetts, USA: Syngress; 2013.
Reilly D, Wren C, Berry T. Cloud computing: forensic challenges for law enforcement. In: Proceeding of the 2010 International Conference for Internet Technology and Secured Transactions (ICITST). London, UK: IEEE; 2010. p. 1–7.
Reilly D, Wren C, Berry T. Cloud computing: pros and cons for computer forensic investigations. Int J Multimed Image Process (IJMIP) 2011;1:26–34.
RightScale. State of the cloud report. RightScale; 2014. Available at, http://assets.rightscale.com/uploads/pdfs/RightScale-2014-State-of-the-Cloud-Report.pdf?mkt_tok=3RkMMJWWfF9wsRonuqvAd%2B%2FhmjTEU5z17%2BokW662gIkz2EFye%2BLIHETpodcMRMFgN6%2BTFAwTG5toziV8R7fBL81u3c8QXRjq [Accessed 20.1.15].
Ruan K, Carthy J, Kechadi T, Baggili I. Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit Investig 2013;10:34–43.
Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics. In: Peterson G, Shenoi S, editors. Advances in digital forensics VII. Berlin Heidelberg: Springer; 2011. p. 35–46.
Ruan K, James J, Carthy J, Kechadi T. Key terms for service level agreements to support cloud forensics. In: Peterson G, Shenoi S, editors. Advances in digital forensics VIII. Berlin Heidelberg: Springer; 2012. p. 201–12.
Sang TA. Log based approach to make digital forensics easier on cloud computing. 2013. p. 91–4.
Santos N, Gummadi KP, Rodrigues R. Towards trusted cloud computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing: San Diego, California; 2009. p. 3.
Shipley TG, CFE C. Collecting legally defensible online evidence. 2007. Available at: http://veresoftware.net/uploads/CollectingLegallyDefensibleOnlineEvidence.pdf [Accessed 17.12.14].
SpiderOak. SpiderOak cloud storage storage solutions. 2014.
Taylor M, Haggerty J, Gresty D, Hegarty R. Digital evidence in cloud computing systems. Comput Law Secur Rev 2010;26:304–8.

Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. Netw Secur 2011:4–10.
van Baar R, van Beek H, van Eijk E. Digital forensics as a service: a game changer. Digit Investig 2014;11:S54–62.
VMITools. LibVMI: An Introspection Tools.
Wen Y, Man X, Le K, Shi W. Forensics-as-a-Service (FaaS): computer forensic workflow management and processing using cloud. In: CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization; 2013. p. 208–14.
Wolthusen SD. Overcast: forensic discovery in cloud environments. In: Fifth International Conference on IT Security Incident Management and IT Forensics. IEEE; 2009.
Zafarullah Z, Anwar F, Anwar Z. Digital forensics for eucalyptus. In: Frontiers of Information Technology (FIT), 2011. IEEE; 2011. p. 110–6.
Zawaod S, Hasan R. Cloud forensics: a meta study of challenges, approaches and open problems. Distrib Parallel Clust Comput 2013. arXiv:1302.6312v1 [cs.DC].
Zawoad S, Dutta AK, Hasan R. SecLaaS: secure logging-as-a-service for cloud forensics. In: Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM; 2013. p. 219–30.
Zhang OQ, Kirchberg M, Ko RK, Lee BS. How to track your data: the case for cloud computing provenance. In: Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom). IEEE; 2011. p. 446–53.