2016-03

A forensic acquisition and analysis system for IaaS

Alqahtany, S

10.1007/s10586-015-0509-x
Cluster Computing
Springer Science and Business Media LLC

A Forensic Acquisition and Analysis System for IaaS

Saad Alqahtany · Nathan Clarke · Steven Furnell·

Christoph Reich

Abstract Cloud computing is a promising next-generation computing paradigm that offers significant economic benefits to both commercial and public entities. Furthermore, cloud computing provides accessibility, simplicity, and portability for its customers. Due to the unique combination of characteristics that cloud computing introduces (including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), digital investigations face various technical, legal, and organizational challenges to keep up with current developments in the field of cloud computing. There are a wide variety of issues that need to be resolved in order to perform a proper digital investigation in the cloud environment. This paper examines the challenges in cloud forensics that are identified in the current research literature, alongside exploring the existing proposals and technical solutions addressed in the respective research. The open problems that need further effort are highlighted. As a result of the analysis of literature, it is found that it would be difficult, if not impossible, to perform an investigation and discovery in the cloud environment without relying on cloud service providers (CSPs). Therefore, dependence on the cloud service providers (CSPs) is ranked as the greatest challenge when investigators need to acquire evidence in a timely yet forensic manner from cloud systems. Thus, a fully independent model requires no intervention or cooperation from the cloud provider is proposed. This model provides a different approach to a Forensic Acquisition and Analysis System (FAAS) in an Infrastructure as a Service (IaaS) model. FAAS seeks to provide a richer and more complete set of admissible evidence than what current CSPs provide, with no requirement for CSP involvement or modification to the CSP's underlying architecture.

Keywords: Cloud computing · Digital forensics · Cloud forensic challenges · Cloud forensic solutions · Forensic acquisition · Forensic analysis

S. Alqahtany, N. Clarke, and S. Furnell
Saad.alqahtany@plymouth.ac.uk
Centre for Security, Communications and Network Research
Plymouth University, Plymouth, UK
Christoph Reich
Information and Media Centre
Hochschule Furtwangen University
Furtwangen, Germany

1 Introduction

In the past few years, cloud computing has become an attractive solution for many Internet users and organizations [1]. Cloud computing offers significant economic benefits to users by providing a highly scalable infrastructure, pay-as-you-go service at low cost, and on-demand computing. Nonetheless, the same technology also poses a number of threats, including criminal exploitation, which can leave little evidence behind and enable the carrying out of malicious activities with ease. For example, cybercriminals are utilizing existing cloud services as their infrastructure to target their victims. In 2013, a Chinese gang exploited cloud file-hosting services and utilized Dropbox to distribute its malware in preparation for an initial stage of Distributed Denial of Service (DDoS) attacks [2].

Indeed, the issues of security and privacy are listed as the top concern for cloud adoption [3],[4]. Thus, several enterprises look at cloud computing cautiously [5]. Critical public sectors including finance and healthcare are slowly coming round to the idea of entrusting its apps and data to the cloud. However, several approaches are integrated with cloud computing aiming at assessing the general security requirements for cloud adoption. Despite this, academics and industry are still at lookout point to find the applicable approaches to govern cloud computing adoption[3]. While security has frequently been an afterthought in new technologies such as the cloud, digital forensics has historically been an "after-after-thought" [6]. Due to the distributed nature and configuration of the cloud-computing infrastructure, investigators face several challenges when performing a digital investigation in the cloud environment. These challenges are novel and unique to the cloud and are not encountered in traditional digital systems. This is due to the unique combination of characteristics that cloud computing introduces, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [7].

According to a survey on cloud and electronic discovery (eDiscovery) disseminated to organizations that are using cloud-based solutions, 26% responded that they do not have an eDiscovery plan in place and 58% responded that they do not even know if a plan exists [8]. This means that in case of litigation and investigation, such organizations will be left scrambling in a reactive manner to collect information from the cloud, leading to greater cost [9]. In addition, little research has been conducted to investigate how digital investigations could

be performed in a forensically sound manner within the cloud domain [10].

The current methodologies, procedures, tools, and architectures are not designed to handle and assist digital forensics in cloud environments even though on-going and proactive investigations are becoming mandatory components for enterprises [11]. Therefore, with great confidence, it can be said that cloud forensic issues have become more and more problematic and solutions that can provide cloud forensics must be sought urgently.

To date, researchers have mainly focused on the identification of the issues that digital forensic investigators face when performing a digital investigation within cloud-computing environments. The survey conducted by [28] which merely focused on cloud forensics, highlighted that 87% of respondents agreed that "Designing forensics architecture for the cloud" is the main research direction.

This paper conducts a review based on a number of scientific papers that were retrieved from well-known academic databases including ACM, IEEE Xplore, Springer, and ScienceDirect. Based on the outcome of the review, this paper identifies the major challenges, existing solutions, and open problems in the field of cloud forensics. Ultimately, a different approach to the forensic acquisition and analysis (FAAS) in an Infrastructure as a Service (IaaS) model is propounded, seeking to tackle the dependency on the CSP issue, which is considered as the main open problem in cloud forensics.

The paper is organized as follows: section two examines cloud forensic problems and explores the current solutions in each stage of the digital investigation process including identification, preservation, collection, examination, analysis, and presentation. Then section three details the existing research solutions and highlights the open issues. The proposed model is then described in section four, and followed by a brief discussion of the model prior to the conclusions and future work.

2 Cloud Forensics: Challenges and Solutions

The evolution of cloud forensics is still in its infancy, although cloud computing has been utilized in the market for many years [12]. Depending on each of the cloud-service models, which include the IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS) models, different issues can be encountered during a digital investigation process [13]. Several researches have warned that it would be difficult, if not impossible, to perform an investigation and discovery in the cloud environment without relying on cloud service providers (CSPs) [14],[15]. Nonetheless, several conceptual solutions have been proposed to overcome this difficulty. In general, a digital forensic process contains four main stages: identification, preservation and collection, examination and analysis, and presentation [11]. This section categorizes the cloud forensic issues according to these stages.

2.1 Identification Stage

The initial identification of the machine(s) wherein illegal activities could be carried out and a forensic investigation are required. Due to the dynamic nature of the cloud infrastructure, several obstacles that hinder the investigators undertaking this step exist:

- Access to the evidence in logs

It is a common understanding that the identification of evidence via various sources could be challenging within the cloud environment [16],[17],[18]. Indeed, for certain cases, investigators do not even know the location of the data due to the distributed nature of the cloud (i.e. data are distributed among many hosts in multiple data centers) [19]. The availability of system statutes and log files depends on the cloud-service model. It is not feasible in SaaS and PaaS models due to the limited access that the client has; whereas it is partly applicable in the IaaS model, as the client has access to the virtual machine (VM), which behaves like an actual machine [20].

A number of tools and procedures which can be utilized to identify and then acquire digital evidence from the cloud have been proposed and developed [12]. Nonetheless, the majority of them have focused merely on accessing evidence in logs in order to trace details of past events.

Zaferullah et al. proposed and developed a standard logging mechanism that ensures the generation and retention of logs along with a log-management system that collects and correlates logs [21]. Their approach was evaluated within a Eucalyptus cloud environment. Eucalyptus is an acronym for "Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems." It is a Linux-based open-source software architecture that implements efficiency-enhancing private and hybrid clouds within an enterprise's existing IT infrastructure without modifying its configuration. Eucalyptus can also leverage a heterogeneous collection of virtualization technologies within a single cloud, to incorporate resources that have already been virtualized [22]. Monitoring and analyzing tools (e.g. Snort, Syslog, and Log Analyzer) were used in order to monitor Eucalyptus's behavior and log all internal and external interactions of the Eucalyptus components. From the log information, it is possible to identify crucial information such as the IP address of the attacking machine, browser type, information on the number of HTTP requests, and content requested. Besides these, the number of VMs controlled by a single Eucalyptus user can also be identified. Their experimental results show that cloud forensics would be advanced if the CSPs could provide a better logging mechanism.

Sang also proposed a log-based model that is only suitable for the SaaS and PaaS models [13]. This solution aims to keep a separate log in the consumer side locally and synchronize it with the CSP logs using information such as unique IDs and time-stamps. Hence, it enables investigators to check user activities on SaaS without the CSP's support. However, the log content is decided by the CSP to ensure comparability. Furthermore, in order to guarantee the authenticity of log data, an incremental Hash code is used to improve the efficiency and to reduce the time for verification. In PaaS, a customized log module can be supplied to the third party for both the consumer and the cloud provider.

Damshenas et al. suggested that it is important to identify potential evidence only from the client side. Thus, designing and configuring built-in application logs is required in order to log potential evidence such as user communication logs [23]. In SaaS, it can be helpful to implement the feature to check the basic logs and the status of the client's usage. However, they did not provide any details on how this application could be implemented.

Marty devised a framework for recovering logging information during an investigation in a standardized manner: when, where, and what to log [24]. After enabling logging on all infrastructure components to collect logs, a synchronized, reliable, bandwidth-efficient, and encrypted transport layer is established to transfer logs from the source to a central log collector. According to this proposal, only a minimum number of fields are required to be presented for every log, including the time-stamp record, application and users, session ID, severity, reason, and categorization. This proactive approach provides assurance to forensic investigators that the data are reliably generated and collected. However, this framework does not deal with volatile data, which may contain potential evidence.

An encrypted logging model that logs data and then sends them to a central logging server under the control of the customer was proposed by [20]. They suggested that a mechanism that prevents potential eavesdroppers from viewing and changing the content of a log during the transmission process is required. They also proposed that the CSP could provide the network, process, and access logs through a read-only API to get the necessary logs from all three cloud-service models.

- Volatile data

When the power is turned off, volatile data cannot be sustained. Likewise, when a VM is turned off or restarted, all the data stored in the RAM will be lost unless the image is stored somewhere. RAM might contain valuable evidence including user-name, passwords and encryption keys. Due to the increase in the size of RAM and the increase in the use of data encryption, live data forensics is becoming increasingly important [25]. Unfortunately, the existing infrastructure of CSPs does not provide persistent storage for the customer. Although IaaS has some advantages over SaaS and PaaS, volatile storage can be a problem unless the data is synchronized in persistent storage. Thus, volatile data that resides within the virtual environment (including registry entries and temporary Internet files) are likely to be lost when the IaaS's customer restarts their machine [12],[26], [27],[19]. If the inspected cloud-hosted VMs do not have persistent storage, the only option to conduct an inspection and analysis is the live forensic approach [28].

Damshenas et al. proposed a solution that provides persistent storage for the client's data. This extra storage can be utilized in data-recovery, in data-safety for the client, and it can ease the data collection for investigators. For this reason, it should be globalized between CSPs in order to provide the clients with persistent storage. However, it is not common for small- and medium-sized business organizations to employ this option due to the cost issue.

Furthermore, Birk and Wegener proposed a solution to overcome the problem posed by volatile data [20]. They suggested continuous data synchronization of the volatile data between the VM and the persistent storage. However, this approach did not provide any guidelines or practical implementation suggestions for the procedures.

- Lack of control of the system

The lack of control over the system poses a number of obstacles to digital investigators when they carry out evidence acquisition [29]. Indeed, consumers have varied and limited access and control at all levels within the cloud environment and have no knowledge where their data are physically located [7]. To elaborate, a tenant administrator has more control over Infrastructure as a Service (IaaS) model and the level of control diminishes as we go towards SaaS model (as shown in Fig 1). This effectively removes the opportunity to perform a physical acquisition of the disk, which is a standard practice in computer forensic investigations. Moreover, the investigator has to obtain vital information from abstracted resources in order to accurately understand the environment including the cloud architecture, hardware, hypervisor, and file system. Unfortunately, in today's cloud architecture, such information is not yet available to the cloud consumer [17].

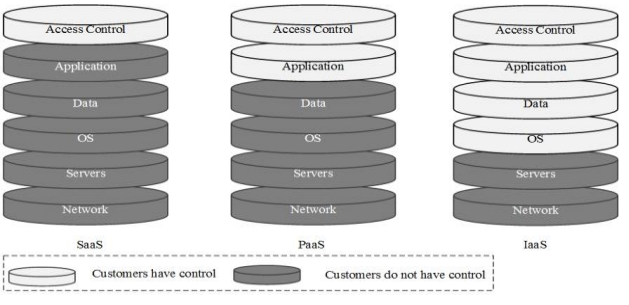

Fig. 1 Customer Control with Different Service Models

- Lack of customer awareness

A lack of CSP transparency along with little international regulation leads to loss of important terms regarding forensic investigations in the Service Level Agreement (SLA). This issue is applicable to all three service models [30].

2.2 Data Collection and Preservation Stage

Data collection is the core functionality in a digital investigation. It is undertaken to collect artefacts of digital evidence and supporting material that are considered of potential value. It ensures that original artefacts are preserved in a way that is reliable, complete, accurate, and verified [31]. However, several issues exist when investigators conduct this step in cloud-based investigations, and they are listed below:

- Dependence on cloud forensic providers

Both customers and investigators are heavily dependent on the CSP in terms of collecting the digital evidence from the cloud-computing environment, as they have limited control over the system. This dependence introduces serious issues surrounding trust in the CSP and evidence integrity. Furthermore, technically there are many reasons that prevent a CSP from providing the consumer with the desired evidence in a forensically sound manner and in a timely fashion. These include, but are not limited to:

i. Due to the sheer volume of data and users within the cloud environment, most CSPs will only keep a limited number of backups. This can cause problems when recovering deleted data or even overwritten data that have been deleted by another user.

ii. CSPs usually hide the data location from customers for data movement and for replication reasons [30].

iii. In case of an incident, the cloud provider will focus on restoring the service rather than preserving the evidence and handling it in a forensically sound manner. Furthermore, some CSPs may not report the incident or cooperate in an investigation due to the potential damage to their reputation.

iv. CSPs do not hire certified forensic investigators to handle cloud-based incidents in a forensically sound manner. Hence, the integrity of evidence could be questioned in a court of law [32].

v. The location uncertainty of the data makes the response time to an e-discovery request extremely challenging [9].

vi. Ultimately, as for evidence residing in one CSP, this could lead to a single point of failure and adversely impact on the acquisition of useful data [33]. However, Investigators may face the issue of cascaded services in situations where one CSP depends on another [25].

Fundamentally, the CSP architecture is designed for operational considerations to provide the most effective use of resources in the most economical fashion. As a result, it is not designed with forensic acquisition and analysis in mind. Currently, cloud customers and investigators have to completely rely on the CSPs to provide digital evidence through centralized administration and management [34]. The lack of transparency between the CSPs and customers might affect their trust relationship.

Ko et al. proposed a detective model called TrustCloud, which consists of five layers of accountability including system, data, workflow, policies, and regulations [35]. Furthermore, Dykstra and Sherman proposed a six-layer model for IaaS based on the amount of trust required: guest application, guest operating system (OS), virtualization, host OS, physical hardware, and network cloud layer. The further down the stack is, the less cumulative trust is required. For example, a guest application requires trust from all of the aforementioned layers, whereas the network layer only needs trust in the network [36]. Ultimately, they recommended a cloud-management plane for use in the IaaS model in such a way that customers and investigators can collect vital digital evidence including VM images and logs of networks, processes, and databases. However, this approach needs an extra level of trust in the management plane. Dependence on CSP is still a serious issue unless the providers offer customers tools or applications that forensically collect their data. From a forensic investigation perspective, a better result of investigation can be achieved through solutions that are designed with forensics in mind. On the contrary, the industrial point of view is that forensic requirements should have no effect on the architecture of environment that might or might not be investigated. However, if such requirements would protect public security, governments might encourage CSPs to set up forensic capabilities while designing cloud architectures [25]. The leading cloud providers have just started embracing such concept. For example, Amazon has recently released CloudTrail logging application that allows the logs to be retrieved using Amazon Web Services (AWS) portal and delivers log files to an Amazon Simple storage Services (S3) bucket that customer specified [37]. Although, this application was designed solely for security purpose, it might provide potential forensic data for Amazon users. However, AWS CloudTrail needs third party tools in order to process analysis and aggregation of log files. Thus, more level of trust is still needed [38].

- Isolating a cloud instance

For any forensic process, it is vital to isolate the incident environment in order to prevent any possible evidence from being tampered with, altered, or adulterated. Hence, the particular instance that is connected with the incident in the cloud environment needs to be isolated. However,

achieving such a task in the cloud environment is not a trivial undertaking due to the data instance sharing storage with multiple instances.

Furthermore, a single cloud node can contain several instances and the nodes have to be cleared when performing a digital investigation. Some cloud-isolation techniques were proposed by [39] that can be used to isolate these cloud instances and mitigate the issue of multi-tenancy in cloud computing. The goal is to prevent any contamination or tampering with the evidence while forensic investigations are undertaken in the cloud environment. These techniques involve instance relocation, where an incident can be moved inside the cloud. The movement can be manually carried out by the cloud administrator or can be performed automatically via the OS. Server farming can be used to re-route the request between user and node. The last technique is to place isolating evidence in a Sandbox. In order to obtain a better result, a combination of these techniques should be implemented. However, these techniques are mainly theory-based without the support of practical experimentation.

- Data provenance in the cloud

Provenance plays a major role in the success of data forensics in cloud computing. Implementing secure provenance enables the digital investigators to obtain vital forensic data from the cloud environment, such as defining who owns the data at a given time, and when, and by whom the data were accessed. Furthermore, it maintains the chain of custody as it provides the time-line of evidence. Li et al. proposed the need for a secure provenance in cloud computing that records ownership and the process history of data objects in cloud computing [40]. They stated that such techniques should satisfy conditional privacy preservation. The technique also provides confidentiality for sensitive documents stored in a cloud, anonymous authentication for cloud servers, and provenance tracking of disputed documents. Cloud-computing features were utilized in order to reduce the user's overheads during the process of provenance [40]. They claim that the proposed solution provides trusted evidence in the cloud environment. However, their solution has not been applied to particular service model.

- Data integrity

One of the main issues faced by investigators in cloud-based cases is ensuring evidence integrity by preserving the integrity of the original data [32]. Data integrity is a critical component of the forensic process [7]. It is crucial that the original evidence is not changed at all [19]. A piece of incident-related information has to be listed in the chain-of-custody register in order to maintain the integrity of the digital evidence, including how, where, and by whom the evidence was collected, how the evidence was stored and preserved, along with any related details of procedures that have been carried out [23]. The improper preservation of evidence might mean that the evidence becomes valueless in a court of law [29]. However, it is likely that errors will occur in the data-preservation stage in the cloud context due to the multiple actors who are involved in the process [12]. Thus, it is a challenging task to prove the integrity of cloud-based evidence to a court in an admissible manner [12]. For example, if the client was involved with the malicious activities, she can claim that her authentication credentials were stolen, and might have been misused by somebody else. Yet, it is difficult to evaluate the authenticity of that claim [35].

With the aim of preserving the integrity and confidentiality of the data within the cloud environment, a trust platform module (TPM) was proposed [20],[36]. Using the TPM leads to the preservation of the integrity and confidentiality of the data. Furthermore, utilizing TPM solutions provides machine authentication, hardware encryption and signing, secure key storage, and attestation [12]. Besides this, it can provide the integrity when running a virtual instance, trusted log files, and the trusted deletion of data to customers [12]. However, the security of the TPM is still questionable due to the possibility of modifying a running process without it being detected by the TPM [36]. In the near future, CSPs are unlikely to comply with the TPM as most of the current devices are not compatible [12].

Furthermore, in order to authorize the client and ensure the confidentiality and integrity of the evidence, multi-factor authentication methods and cryptographic tunneling protocols such as a virtual private network (VPN) can be used together to simply mitigate the preservation issue [23]. As security is a major concern in a cloud environment, researchers have proposed an encryption mechanism to ensure end-user security. While this can increase the complexity of the investigation, it can also be advantageous for investigators. For example, the deployment of the public key infrastructure (PKI) would be used to track down a particular suspect. It is also suggested that an SLA should contain all of the client's privacy data.

Yan proposed a framework that images the relative records and files completely [41]. Furthermore, a litigation hold or similar freezing mechanism is required to be placed by the CSP on the account to prevent any changes to the data [28]. For example, law-enforcement agencies in Australia can give preservation notices to the CSPs according to the Australian Cybercrime Legislation Amendment Bill 2011 [42].

- Time synchronization

The synchronization of time (stamps) is very important, as it can be used as a source of evidence. Nevertheless, the data date-stamps and time-stamps are questionable when they are from multiple systems [12]. Moreover, the difference in time zones between cloud servers and cloud

clients can affect the integrity, reliability, and admissibility of evidence.

Currently, the cloud infrastructure is strongly dependent on whether the VM guest's OS is using a network protocol to synchronize with a network time server. However, the best strategy recommended by [43] is to obtain the time from many servers and keep the most common time value from them.

Furthermore, using a specific time system such as GMT on all entities of the cloud can be helpful in providing a logical time pattern in the way that it enables investigators to create the time-line analysis and to track multiple log records in different physical locations [23].In Addition, a consistent time source such as Network Timing Protocol (NTP) can identify the sequence of evidence and create the time-line analysis of events across CSP and the network [25].

- Cloud literacy of investigators

Few training materials are available that could be utilized to educate investigators on cloud-computing technology and cloud forensic procedures. Additionally, current digital forensic training materials are not updated regularly, nor do they address the major challenges of cloud environments. Moreover, there is a lack of standard operating policies for cloud forensics [30]. It is essential for members of an investigation team to be trained on the legal regulations, the special tools, and the techniques, including programing, networking, communication, and negotiation with CSPs [44].

- Chain of custody

The chain of custody is one of the most critical problems in the digital forensic arena [12]. The chain of custody has to illustrate how the evidence was collected, analyzed, and preserved with the aim of presenting the evidence in an admissible way in a court of law [17].

It is difficult to verify the data chain of custody in the cloud environment due to the unique combinations of characteristics that cloud computing has, including its distributed and multi-layered nature [34]. In order to maintain the chain of custody, certain things need to be clarified, such as the way in which logs were collected, generated, and stored, along with who had access to the logs. Moreover, CSPs have to hire trained and qualified specialists [45]. Furthermore, communication and collaboration related to all forensic activities through the chain of CSPs and the customer's dependencies need to be clearly written in SLAs [30].

2.3 Analysis and Examination Stage

It is very challenging to conduct a proper analysis in the cloud due to the sheer volume of resources and vast number of objects to be examined during a digital investigation, along with limitations in the processing and examining tools. Moreover, there is no standard program for the forensic extraction of data, as the customer can access relevant data from various devices such as a desktop PC, tablet, or mobile phone, and from a wide range of applications. Furthermore, the data-extraction format varies based on the service model. For example, in the IaaS model, investigators can obtain an image of the VM that contains all data uploaded by a suspect. However, the data would be exported in an unstructured fashion, creating difficulties in reading, examining, and analyzing the data format using standard forensic tools. Thus, it is important to develop utility applications that translate the native cloud data format into a readable and recognizable format by the tools [10].

A reconstruction of the events of the forensic investigation produces crucial and valuable analysis in order to logically recreate the crime. However, due to the distributed and shared nature of the cloud, each event relating to the crime might occur in a different country. This will lead to difficulties in deducing the logical order regarding where the event took place.

Investigators can face a wide range of challenges when they perform the examination and analysis stage, including:

- Lack of available cloud forensic tools

It is a common understanding that the available forensic tools have various limitations and cannot cope with the distributed and elastic characteristics of cloud computing [30],[19],[45]. According to survey conducted by [46], participants agreed that there is a lack of forensic tools that tailored for cloud system. Approximately 58% of respondents agreed that digital forensic process automation is needed to tackle future challenges including cloud forensics. Additionally, there is a high level of demand on the forensic-aware tools for the CSP and the clients to conduct a forensic investigation in the cloud environment [30]. Hence, it is crucial to develop tools which can be utilized to identify, collect, and analyze cloud forensic data [18].

A combination of computer forensic and network forensic tools is needed in order to acquire forensic data and then analyze them in a timely fashion. Traditional forensic tools can be used to collect the active data while their integrity is preserved. Network forensic tools can be utilized to collect additional data over the network including activity logs [1]. E-discovery refers to any process in which electronic data are sought, located, and secured with the aim of using them later in a legal case. In the cloud-computing environment, e-discovery can be helpful to conduct offline investigations on a particular computer or network. For example, Encase software has launched their own e-discovery suite; nevertheless, the multi-jurisdiction problem is still a major concern [47].

In cloud computing, it is less likely that CSPs will obey the legal e-discovery obligations due to technical, cost, and legal reasons, or even due to a lack of capability

in terms of preserving the original metadata as expected [10]. Furthermore, the response time to an e-discovery is extremely challenging due to uncertainty regarding the data location and the need for assurance in terms of completion of the request [34].

The open-source software, Offline Windows Analysis and Data Extraction (OWADE), was developed and launched at the BlackHat 2011 Security Conference by researchers from Stanford University in California. This software has the ability to find out which website a user has visited, extract information stored in the cloud, reconstruct Internet activities, and search for the online identities that were used. This version is still under development and it only works for Windows XP drives [48].

Furthermore, the management plane was recommended as the appropriate forensic tool for acquiring cloud-based data [36]. They claimed that the management plane offers the most attractive balance between speed and trust. Despite the fact that some commercial tools (e.g. Encase and FTK) can be used to successfully acquire evidence, Dykstra et al. do not recommend them due to the high level of trust they require [36].

Recently, Dykstra et al. developed a management-plane forensic toolkit called Forensics Open-Stack Tools (FROST), which is designed to acquire forensic data from virtual disks, API logs, and guest firewall logs [7]. It operates on the cloud-management plane instead of interacting with the OS inside the guest VMs. FROST is the first forensic tool that has been built into any IaaS cloud model [7]. Table 1 illustrates a summary of most of the tools used to conduct extraction and analysis within cloud environment.

- Evidence correlation across multiple sources

Correlation of activities across multiple sources can be overwhelming. The evidential resources are spread across multiple digital resources. Handling data evidence from multiple sources introduces a problem for investigators.

- Crime-scene reconstruction

It is crucial to reconstruct the crime scene in order to understand how illegal activities were committed. Unfortunately, this could be a problem in the cloud environment [12]. For example, when an adversary shut down her virtual instance after committing certain malicious activities, reconstruction of the crime scene will be impossible. However, a regeneration event can be used where a snapshot is taken to note the occurrence of every attack. Geethakumari and Belorkar proposed a method allowing investigators to replay the event of the attack and restore the system to the state before the attack by using snapshots [52]. Ultimately, it is also suggested that

Table 1 Summary of current digital forensic tools utilized in the cloud

Utilized tools	General/cloud-Based tools	Functionality	Reference
FTK Remote Agent	General	Remote Acquisition	[36]
Encase Remote Agent	General	Remote Acquisition	[36]
Snort	General	Log all internal and external interactions and monitor Eucalyptus's behavior	[21]
FROST	Cloud-Based	Digital forensics tools for the OpenStack cloud platform	[7]
OWADE	Cloud-Based	What websites a user has visited and whether they have any data stored in the cloud	[48]
CloudTrail	Cloud-Based	Logging in the AWS Cloud	[37]
Wireshark	General	Examines network captures	[49]
Sleuthkit	General	Examines forensic images of hard disk and recover files from them.	[50]
FTK Imager	General	Acquisition of memory and disk image	[25]
X-Ways	General	Acquisition of live system (window & Linux)	[51]
Encase e-discovery suite	General	Offline investigations on a particular computer or network	[47]

incoming and outgoing data through the cloud will be able to be visualized by the investigators.

2.4 Presentation Stage

The final step of a digital forensic investigation is presentation, where the evidence has to be presented to a judicial body in the form of a report or testimony [53]. Several challenges lie in this step in the context of cloud forensics. For instance, it is not clear how to specify the physical location of the cloud-based crime due to distributed and shared resources between multiple clients who are based in different countries. This in turn confuses the investigators in terms of determining under which legal system the case should be heard. Furthermore, it is necessary for digital investigators to explain the technicalities to the jury as to how the evidence was acquired and what it represents. However, the technicalities of a cloud-data center, running thousands of VMs, accessed simultaneously by hundreds of users, are very hard to be comprehended by a jury member who is likely to have only a basic technical knowledge [19].

3 Discussion of Current Solutions in the Cloud

The literature has been analyzed by counting the related studies per stage of digital investigation (discussed in section 2). This review was based on a number of most related scientific papers since the term of Cloud Forensics was first introduced in 2010. These studies have retrieved from well-known academic databases including ACM, IEEE Xplore, Springer, and ScienceDirect. The majority of studies have addressed only the cloud forensics challenges and issues. Several studies have proposed solutions for these challenges in order to perform proper forensics in the cloud environment. Despite this, the majority of these proposals are conceptual and not tested in real conditions. There was only one piece of research that evaluated and examined the current tools used in conducting remote data acquisition. This research was conducted by Dykstra and Sherman, who developed a set of tools known as FROST. So far, traditional tools such as Encase and FTK are still the common tools that are heavily utilized in acquiring the evidence from the cloud—despite the difference between the cloud infrastructure and traditional computer environments.

FROST operates on the cloud-management plane instead of interacting with the OS inside the guest VMs. FROST is the first forensic capability to be built into any IaaS cloud model. However, FROST is deployed by the CSP. Thus, trust in the CSP is still required, but not in the guest machine. Furthermore, trust in the cloud infrastructure is required, including the hardware, host OS, hypervisor, and cloud employees. It also assumes that the cloud customer is cooperative and involved in the investigation. This work involved performing three experiments to acquire forensic data from three different layers; namely, the guest OS, the virtualization layer, and the host OS. All three experiments have succeeded in performing data acquisition remotely from the cloud-based layer. However, a certain amount of trust is still highly required in each layer.

Customers and investigators depend on the CSP to perform data acquisition. Some researchers have suggested solutions that would mitigate the issue of the dependence on the CSP, such as the cloud-management plane or APIs, which are provided to the customer in order to get forensic hard disk and temporary registry logs to acquire data. However, there is various and crucial forensic data that still resides in the CSP, including deleted files and relying upon CSP cooperation is inevitable. In turn, many other issues associated with the dependence on the CSP evidence have been highlighted, and they are not yet resolved. Such issues include trust, delay response, inadmissibility of evidence, and a potential single point of failure.

Amazon, however, has started delivering services that support digital forensics by releasing CloudTrail logging application. This application was designed for security purpose. Despite this, it might provide prime piece of information data for Amazon users. However, one more level of trust on the management console application is still required.

Furthermore, piecing together a sequence of events from multiple sources and different jurisdictions is another major obstacle faced by investigators in the cloud environment. So far, investigators have no valid approach with which to reconstruct the past state of an event with a level of accuracy so that the reconstructed information can be admissible in a court of law.

It is understood that there is a big concern with regard to data acquisition and its integrity in the cloud environment. Furthermore, several difficulties associated with logging data have still not diminished. These include the time-line, log review, logging correlation, and log policy monitoring.

Ultimately, legal issues hinder the smooth performing of forensic investigations due to the lack of guidelines and implementation of a global standard to overcome the cross-border issue.

To conclude this section, Table 2 illustrates cloud forensic challenges and their current potential solutions. All proposed solutions were identified from the review conducted in the respective domain. Table 3 summarizes the open problems that need to be resolved.

However, it has become necessary to identify a solution that will overcome open problems and that would allow the forensic acquisition and analysis of systems within the cloud [54]. While other research has proposed an IaaS solution, it is essentially dependent upon VM images being collected and stored, with credence being placed on the inclusion of the CSP as central to the

solution, thereby ensuring the collection of cloud-management information [7]. CSPs have little motivation to provide assistance with incidents and habitually do not let their customers look behind their "virtual curtains" [23]. They will only cooperate with an investigation of an incident when forced to do so by law-enforcement agencies. Even when they do so, this is dependent on the status of the system at that time, for example, whether the VM remains active, whether the system has been backed up, or whether the data have been overwritten. Therefore, a starting point must be that organizations remain in control of their data and retain the capability to readily forensically undertake an incident analysis/examination of their systems in the event that this becomes obligatory.

The next section presents an on-going project that seeks to tackle the issue of dependence on the CSPs by developing a forensically-enabled IaaS cloud-computing architecture. This research aims to produce an acquisition and analysis model that fundamentally shifts responsibility for the data back to the data owner rather than relying upon the CSPs or a third party.

Table 2 Current cloud forensic issues and solutions

Cloud Forensic Challenges/Process		Applicability to Service Model			Potential Solution	Ref
		IaaS	**PaaS**	**SaaS**		
Identification						
Access to the evidence		√	X	X	Eucalyptus framework OS and the security log	[21]
		√	X	X	A log-based model	[13]
		√	√	X	Extraction of relevant status data	[23]
		X	√	X	A log-management solution	[24]
		√	√	X	An encrypted logging model	[20]
Dependence on CSP	Trust issue	√	√	X	Layers of trust model	[36]
	Data acquisition	√	√	X	TrustCloud	[35]
	compliance	√	√	√	Cloud-management plane	[55]
	Logs	√	√	√	Service Level Agreement (SLA)	[17]
Lack of customer awareness		√	√	√	--	[30]
Volatile data		√	√	X	Client persistent storage	[23]
		√	√	X	A continuous synchronization API	[16]
Preservation & Collection						
Data integrity		√	√	√	Trust platform module (TPM)	[9], [36]
Time synchronization		√	√	√	Unified/specific time system	[23]
Cloud literacy of investigators		√	√	√	Developing investigators technical skills	[44]
Chain of custody		√	√	√	Trained staff	[45], [30]
Analysis & Examination						
Lack of cloud forensic tools		√	√	X	FROST, OWADE	[7], [48]
Presentation						
Jury's technical comprehension		X	X	X	Training	[19]

Table 3 Summary of high-level open issues

	Open Issues
1	Tackle the dependence on the cloud service providers
2	Time-line analysis across multiple sources and evidence correlation
3	Overcome the cross-border issues
4	Lack of control of the system
5	Jury's technical comprehension

4 A Model for Forensic Acquisition & Analysis in the Cloud

The proposed approach in this research seeks to omit the involvement of the CSP, while handing over control of the forensic acquisition process to the cloud customer, using an *agent-based* approach that is held in each VM and sending the required information to a central *Cloud Forensic Acquisition and Analysis System* (Cloud FAAS). By using agent-based acquisition, all cloud-management data (e.g. VM start time, stop time) are recorded, and the need for lower level data that are only accessible via a CSP is omitted, such as physical storage locations for the VM data. Further, this innovative approach allows an image to be recreated of the VM hard drive at any point in time and ensures every file is accessible in its entirety, thereby overcoming the current restriction of partially overwritten files being inaccessible. Limitations arising from data carving and fragmentation are therefore removed and the forensic investigator is provided with an increased level of insight.

As Figure 2 illustrates, there are two contributing factors: the agent coordinator and the Cloud FAAS. The agent coordinator manages agents installed within an individual VM system, whereas the Cloud FAAS is the central processing point for forensic data:

i) The agent coordinator: Different agents that hold responsibility for various forms of the acquisition. An acquisition policy, defined by the cloud customer (from here on in referred to as the organization), will be housed within the Cloud FAAS and there will be a request to enable or disable, which will be achieved by the use of different agents. The following agents will be available:

- Non-volatile memory agent—responsible for logically imaging the hard drive associated with the VM
- Volatile memory agent—responsible for logically imaging the live memory of the VM
- Network traffic agent—responsible for logging and storing network traffic (both egress and ingress)
- Activity log agent—acquiring system and application logs

Along with the nature/responsibility of the VM, organizational requirements will dictate the agent utilized. For example, in a 3-tier web application, to avoid the replication of the network data store, the *network traffic agent* will only be operated on the web front-end system, as the back-end server will communicate with the web server. Additionally, the *activity log agent* is expected to be the least used, as information can be generated from the other agents. To elaborate, its role will be to provide high-level log information to an investigator where the overhead and cost of operating the other agents is not deemed compulsory.

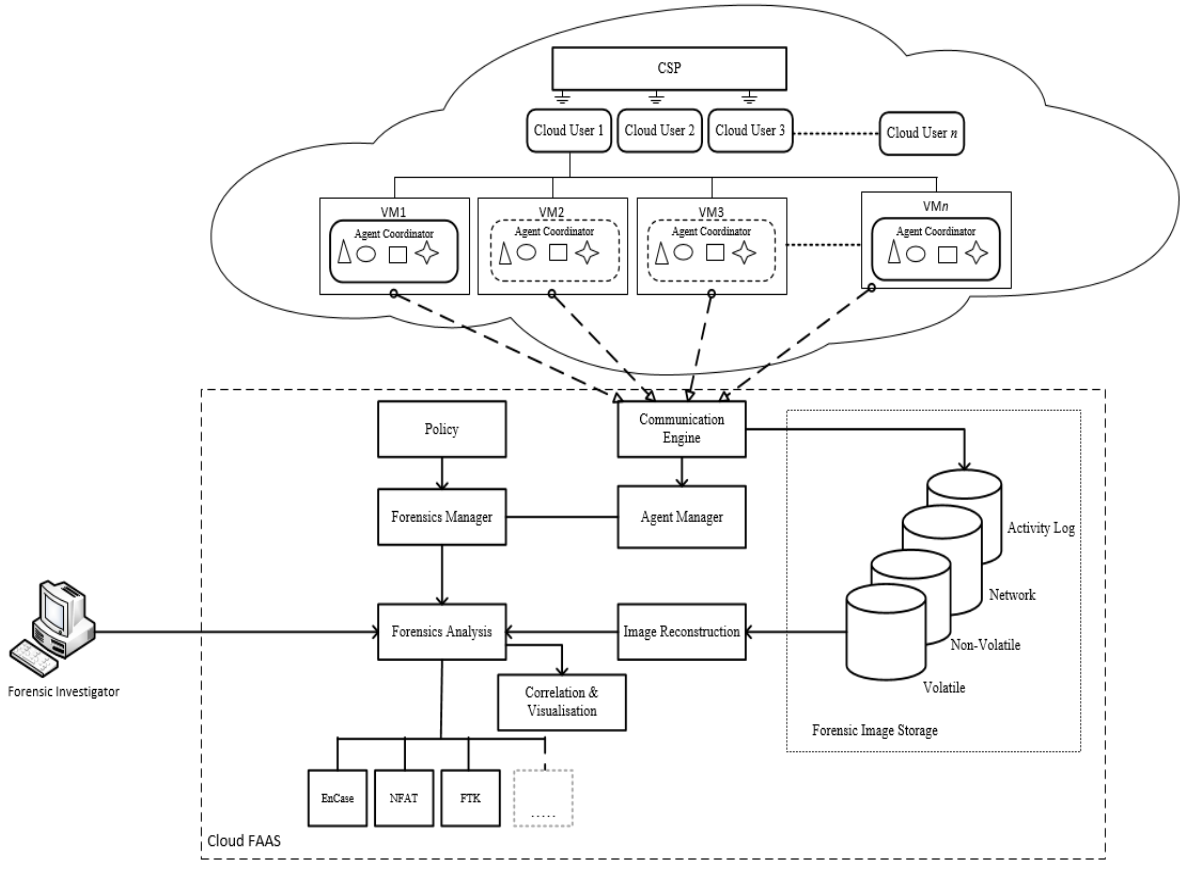

Fig. 2 A novel model for data acquisition within an IaaS

ii) Cloud FAAS: Forensic acquisition policies for the VMs are defined by the access provided to the management information, and will influence its effectiveness and budgetary implications. The policy is an essential component of the approach. Therefore, it is flexible and the set of standard templates may be adapted to suit the organizational risk assessment. It has been developed with the user in mind and is based on standard templates derived from server roles—critical systems monitor all changes across all agents, whereas those that are less critical will incorporate a less granular acquisition approach.

The interaction between the two contributing factors is provided by a *communication engine*, which facilitates the communication by the *agent coordinator* and the Cloud FAAS. This communication is cryptographically secured, thereby ensuring data confidentiality and integrity. To ensure the continuity of control and data integrity throughout the acquisition, the *agent coordinator* and *agent manager* ensure that image data are forensically hashed at all levels, including complete images to files. Once completed, the information is stored in the *forensic image storage*.

The responsibility for managing the overall system lies with the *forensic manager*, including providing an interface to the forensic investigator, the ability for the investigator to select the system to be analyzed, and the timeframe in which that is to be examined. Information will be taken from the image repository and the image(s) reconstructed using the *image reconstruction module*; the policy will impact upon what data and the extent of their granularity is to be reconstructed. Once images have been reconstructed, data will be sent to undergo forensic examination and analysis. Figure 2 illustrates that industry de facto tools, such as EnCase or FTK, will be utilized to complete this analysis. To provide a higher level of abstraction in comparison to an individual system, and to ensure that investigators can understand the relationship and flow between systems, a correlation engine and visualization component will be provided.

4.1 Acquisition & data handling

It is acknowledged that the storage of data could become extremely expensive for organizations due to the VM non-volatile storage range being 100GBs and there being GBs of network activity; solutions must address this while retaining an acceptable forensic standard.

The introduction of a policy-based approach is an attempt to mitigate information overload and address this concern. Figure 3 shows the two main steps of the proposed data-handling approach, with the first step being the acquisition of the forensic image of the non-volatile memory (i.e. the hard drive as seen by the VM). Operating at this logical layer on a VM means it is not possible, nor is it permissible due to the nature of the cloud, to map this data to a physical drive. As such, step 2 is operationally akin to an incremental backup, recording all file system changes to the drive. The data clusters of those files are also stored, which ensures the forensic value of the data, allowing the image reconstruction engine to reproduce a forensic image of the drive at any point when required, including information on the deletion and overwriting of files.

It is not normally possible to obtain access to deleted files; however, this approach overcomes that barrier as the files are stored by the system, which, in turn, reduces the volume of data communicated and stored as well as providing the investigator with full access to deleted files.

The approach set out in the research is to assist in investigating incidents in a relatively short (6-month) timeframe; it is not intended to provide a replacement for organizational backup of data. The policy will define data retention, however, by considering the volume of storage required in the Cloud FAAS, and this is likely to be short, in terms of weeks or months. A re-image of the drive will be essential in the future for computation and storage requirements, as illustrated in Figure 3, where it shows the changes that have occurred since initial imaging in terms of volume and complexity.

The policy defines many factors, such as frequency of reimaging, the granularity of file system changes, frequency of volatile memory captures, and resolution of the network-traffic captures. There will be an increase in demands placed upon agents and the Cloud FAAS, in particular the *forensic image storage*, by higher levels of resolution and frequency, and lower granularity of data capture. It is possible to minimize the adverse effects on the core operation by optimizing the transmission of data from the *agent coordinator* to the Cloud FAAS at times of low network usage. However, it is accepted that in the absence of the most rigorous policy, the forensic value of data will not be impeccable, however, it will be no less than that of current forensic systems where there can be a direct impact due to the time taken to acquire data compared to the point in time the incident occurred.

The organization has control over the proximity of the operation of the Cloud FAAS, although there are advantages and disadvantages as to the choice of location. If hosted within the same CSP as its operational servers, and if running a cloud service in its own right, this could be advantageous in terms of having high bandwidth local-area connections, yet it would be at risk from being reliant upon the flawless running of the CSP. However, the organization may choose to host it locally so that ownership and access to data are as strong and reliable as possible. A cloud-based deployment more generally would certainly be advantageous from a data-processing and forensic analysis perspective. Both of these aspects are computationally very intensive, yet unpredictable as to when they will be required. An elastic and flexible computing environment would allow for this—whether that is a public or private cloud.

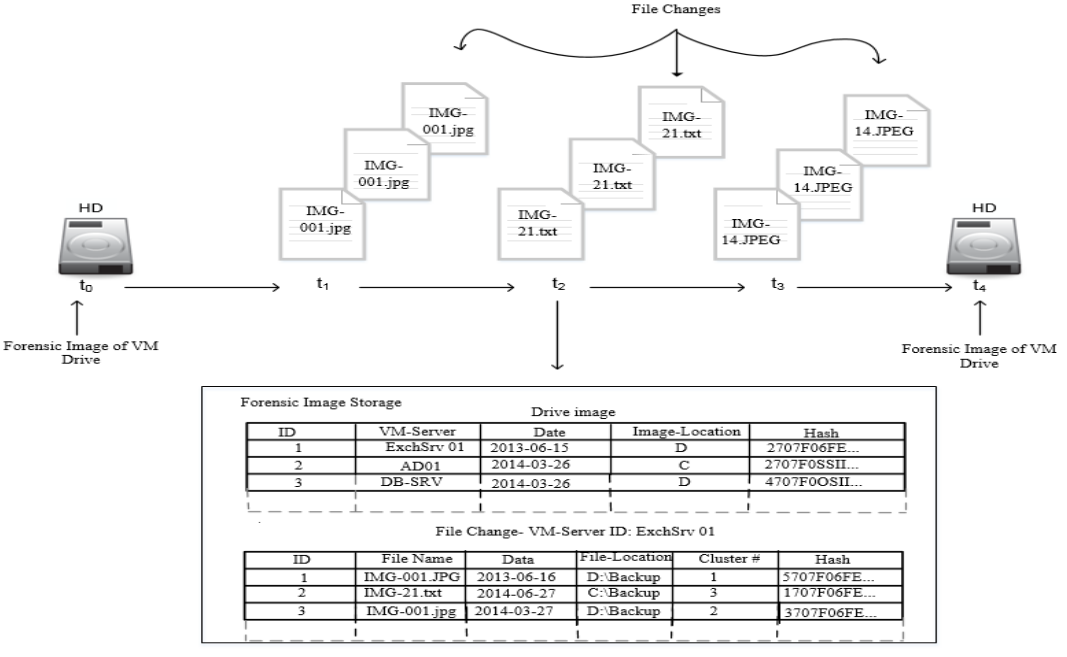

Fig. 3 File changes at given times

4.2 Performance and Scalability Analysis

Despite the fact that proposed model is still merely conceptual, indeed, ensuring the performance of FAAC model is a major concern. Following the development of the (FAAS) prototype, a complete system will be evaluated against the following issues:

1- Performance Overhead: collecting the relevant material from different systems (VMs) across all agents and send them to the FAAS causes the additional overhead. Adding such new mechanism can slow down running VMs and then affect running services. Furthermore, all communication is undertaken in a cryptographically secure manner – to ensure the confidentiality and integrity of the data in transit. The Agent Coordinator and Agent Manager also include the forensics hashing of all image data (at all levels of data object – complete images to files) to ensure chain of custody and data integrity is maintained throughout the acquisition phase. This will require some techniques such as encryption and hashing which adds more workload to the running services as well.

2- Network Overhead: it is vital to keep network overhead to a minimum. However, the volume of data being recorded – VMs data and Network activities- and sent via network activities resulted in an impact on the network traffic.

3- Granularity: it refers to the level of data which is being collected and stored. Although finer level of integrity is important to digital investigators, it can affect the level of performance overhead.

4- Quality of Reconstructed Image: the constructed image retrieved from Forensics Image Storage must gain acceptance from both the judicial and technical communities.

5- Performance of Forensics Analysis: some cases are high profile, such as a child abduction, which must be processed as quickly as possible in order to provide investigators with time sensitive information that may be vital to the outcome of the situation. Unfortunately, some of these cases can take hours or even days to finish on larger evidence. The average amount of data per case, as experienced by FBI's 15 Regional Computer Forensics Laboratories, has grown 6.65 times (from 84 GB to 559GB) in eight years (2003–2011) [56]. Thus, it is imperative to reduce the overall processing time of large quantities of data by leveraging the power of a high performance computing platform and adapting existing tools to operate within this environment.

Ultimately, in order to mitigate aforementioned issues and gain a better result, the best balance between the various issues has to be taken in account. Thus, developing this proposed model, examining and analyzing it with real and live data will practicably give better insight about its feasibility and value in solving the research problem.

5 Conclusions and Future Work

As there are increasing cloud-computing uses, there is a growing need for trustworthy cloud forensics. Several researchers have identified and explored the challenges confronting the digital investigators when they conduct forensic investigations in cloud-based cases. Accordingly, some researchers have proposed technical solutions to mitigate these challenges. However, there are still open issues that need to be tackled.

This paper identified cloud forensic challenges, matched proposed solutions to these challenges, and determined open problems that need further efforts to be tackled. With the on-going success of the ever-expanding cloud, it is found that the concern surrounding the integrity and acquisition of data must be addressed. It is imperative that organizations retain control of data to ensure that they can be forensically examined in a timely manner, and thereby releasing the CSPs of that burden. The solution outlined above can help overcoming the concerns; however, further research would provide a greater understanding of the technical implications of the day-to-day operations of a cloud system as well as the financial implications arising therefrom.

References

1. Zargari, S., Benford, D.: Cloud Forensics: Concepts, Issues, and Challenges. In: 2012 Third International Conference on Emerging Intelligent Data and Web Technologies. pp. 236–243. Ieee, Bucharest (2012).

2. Higgings, K.: Dropbox, WordPress Used As Cloud Cover In New APT Attacks, http://www.darkreading.com/attacks-breaches/dropbox-wordpress-used-as-cloud-cover-in-new-apt-attacks/d/d-id/1140098?

3. Dzombeta, S., Stantchev, V., Colomo-palacios, R., Brandis, K., Haufe, K.: Governance of Cloud Computing Services for the Life Sciences. Ieee Comput. Soc. (2014).

4. Hooper, C., Martini, B., Choo, K.-K.R.: Cloud computing and its implications for cybercrime investigations in Australia. Comput. Law Secur. Rev. 29, 152–163 (2013).

5. Stantchev, V., Colomo-Palacios, R., Niedermayer, M.: Cloud Computing Based Systems for Healthcare. Sci. World J. 2014, 1–74 (2014).

6. Ruan, K., Carthy, J.: Cloud Forensic Maturity

Model. In: Digital Forensics and Cyber Crime. pp. 22–41. Springer Berlin Heidelberg (2012).

7. Dykstra, J., Sherman, A.T.: Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Digit. Investig. 10, S87–S95 (2013).

8. Murphy, B.: e-Discovery in The Cloud Not As Simple As You Think, http://www.forbes.com/sites/jasonvelasco/2011/11/29/e-discovery-in-the-cloud-not-as-simple-as-you-think/.

9. Ruan, K.: Designing a Forensic-Enabling Cloud Ecosystem. In: Cybercrime and cloud forensics. pp. 331–344. IGI Global, USA (2013).

10. Mell, P., Grance, T.: The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technolog. , Gaithersburg, MD (2011).

11. Poisel, R., Malzer, E., Tjoa, S.: Evidence and Cloud Computing : The Virtual Machine Introspection Approach. J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl. 4, 135–152 (2012).

12. Zawoad, S., Hasan, R.: Digital Forensics in the Cloud, (2013).

13. Sang, T.: A Log Based Approach to Make Digital Forensics Easier on Cloud Computing. In: 2013 Third International Conference on Intelligent System Design and Engineering Applications. pp. 91–94. Ieee (2013).

14. Patrascu, A., Patriciu, V.: Beyond Digital Forensics . A Cloud Computing Perspective Over Incident Response and Reporting. In: Applied Computational Intelligence and Informatics (SACI). pp. 455–460. , Timisoara (2013).

15. Ruan, K., Carthy, J.: Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis. Digit. Forensics Cyber Crime. 1–21 (2013).

16. Birk, D.: Technical Challenges of Forensic Investigations in Cloud Computing Environments. In: Workshop on Cryptography and Security in Clouds. pp. 1–6. , Zurich, Switzerland (2011).

17. Dykstra, J., Sherman, A.T.A.: UNDERSTANDING ISSUES IN CLOUD FORENSICS : TWO HYPOTHETICAL CASE STUDIES. In: Proceedings of the 2011 ADFSL Conference on Digital Forensics Security and Law. pp. 1–10 (2011).

18. Shah, J.J., Malik, L.G.: Cloud Forensics: Issues and Challenges. 2013 6th Int. Conf. Emerg. Trends Eng. Technol. 138–139 (2013).

19. Reilly, D., Wren, C., Berry, T.: Cloud Computing : Pros and Cons for Computer Forensic Investigations. Int. J. Multimed. Image Process. 1, 26–34 (2011).

20. Birk, D., Wegener, C.: Technical Issues of Forensic Investigations in Cloud Computing Environments. In: 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. pp. 1–10. Ieee, Okland,CA (2011).

21. Zaferullah, Z., Anwar, F., Anwar, Z.: Digital Forensics for Eucalyptus. In: 2011 Frontiers of Information Technology. pp. 110–116. Ieee, Islamabad (2011).

22. Wolski, R.: https://www.usenix.org/conference/lisa-09/eucalyptus-open-source-infrastructure-cloud-computing, https://www.usenix.org/conference/lisa-09/eucalyptus-open-source-infrastructure-cloud-computing.

23. Damshenas, M., Dehghantanha, A., Mahmoud, R., Shamsuddin, S.: Forensics Investigation Challenges in Cloud Computing Environments. In: Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. pp. 190–194. Ieee, Kuala Lumpur (2012).

24. Marty, R.: Cloud application logging for forensics. Proc. 2011 ACM Symp. Appl. Comput. - SAC '11. 178 (2011).

25. Almulla, S., Iraqi, Y., Jones, A.: A STATE-OF-THE-ART REVIEW OF CLOUD. 2014 ADFSL. 9, 7–28 (2014).

26. Zawoad, S., Hasan, R.: Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. arXiv Prepr. arXiv1302.6312. 1–15 (2013).

27. Guo, H., Jin, B., Shang, T.: Forensic Investigations in Cloud Environments. In: 2012 International Conference on Computer Science and Information Processing (CSIP). pp. 248–251. Ieee, Xi'an, Shaanxi (2012).

28. Martini, B., Choo, K.-K.R.: An integrated conceptual digital forensic framework for cloud computing. Digit. Investig. 9, 71–80 (2012).

29. Zawoad, S., Hasan, R.: I Have the Proof : Providing Proofs of Past Data Possession in Cloud Forensics. (2012).

30. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud forensics : An overview. Adv. Digit. Forensics VII. 15–26 (2011).

31. Sibiya, G., Venter, H.S., Fogwill, T.: Digital Forensic Framework for a Cloud Environment. In: IST_Africa 2012 Conference proceedings. pp. 1–8 (2012).

32. Taylor, M., Haggerty, J., Gresty, D., Lamb, D.: Forensic investigation of cloud computing systems. Netw. Secur. 2011, 4–10 (2011).

33. Crosbie, M.: Hack the Cloud: Ethical Hacking and Cloud Forensics. In: Cybercrime and cloud forensics. p. 17. IGI Global, USA (2013).

34. 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. 10, 34–43 (2013).

35. Ko, R.K.L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., Lee, B.S.: TrustCloud: A Framework for Accountability and Trust in Cloud Computing. In: 2011 IEEE World Congress on Services. pp. 584–588. Ieee, Washington, DC (2011).

36. Dykstra, J., Sherman, A.T.: Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digit. Investig. 9, S90–S98 (2012).

37. Amazon Web Services: AWS CloudTrail : User Guide. (2014).

38. Pichan, A., Lazarescu, M., Soh, S.T.: Cloud forensics: Technical challenges, solutions and comparative analysis. Digit. Investig. 13, 38–57 (2015).

39. Delport, W., Olivier, M.S., Kohn, M.: Isolating a Cloud Instance for a Digital Forensic. In: ISSA (2011).

40. Li, J., Chen, X., Huang, Q., Wong, D.S.: Digital provenance: Enabling secure data forensics in cloud computing. Futur. Gener. Comput. Syst. (2013).

41. Yan, C.: Cybercrime forensic system in cloud computing. In: Proceedings of 2011 International Conference on Image Analysis and Signal Processing, IASP 2011. pp. 612–613 (2011).

42. Catryna, B.: Review of the Cybercrime Legislation Amendment Bill. (2011).

43. Marangos, N., Rizomiliotis, P., Mitrou, L.: Time Synchronization : Pivotal Element in Cloud Forensics. Secur. Commun. Networks. (2014).

44. Chen, G., Du, Y., Qin, P., Du, J.: Suggestions to digital forensics in Cloud computing ERA. In: 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content. pp. 540–544. Ieee, Beijing (2012).

45. Grispos, G.: Calm Before the Storm : The Challenges of Cloud Computing in Digital Forensics. 4, 28–48 (2012).

46. Al Fahdi, M., Clarke, N.L., Furnell, S.M.:

Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In: 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference. pp. 1–8 (2013).

47. Taylor, M., Haggerty, J., Gresty, D., Hegarty, R.: Digital evidence in cloud computing systems. Comput. Law Secur. Rev. 26, 304–308 (2010).

48. Kumar, M.: Computer Investigations, http://thehackernews.com/2011/09/offline-windows-analysis-and-data.html.

49. Raghavan, S.: Digital forensic research: current state of the art. CSI Trans. ICT. 1, 91–114 (2012).

50. Sleuthkit: Open Source Digital Forensics, http://www.sleuthkit.org/index.php.

51. X-Ways: X-Ways technology, http://www.x-ways.net/.

52. Geethakumari, G., Belorkar, A.: Regenerating Cloud Attack Scenarios using LVM2 based System Snapshots for Forensic Analysis. Int. J. Cloud Comput. Serv. Sci. 1, 134–141 (2012).

53. Trenwith, P.M., Venter, H.: Digital Forensic Readiness in the Cloud. In: Information Security for South Africa, 2013. pp. 1–5 (2013).

54. NIST: NIST Cloud Computing Forensic Science Challenges NIST Cloud Computing. , USA (2014).

55. Dykstra, J.: Cybercrime and Cloud Forensics. In: Ruan, K. (ed.) Cybercrime and cloud forensics. pp. 156–185. IGI Global, USA (2013).

56. Thethi, N., Keane, A.: Digital forensics investigations in the Cloud. 2014 IEEE Int. Adv. Comput. Conf. 1475–1480 (2014).