

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/276277307>

Cloud Forensics: A Review of Challenges, Solutions and Open Problems

Conference Paper · April 2015

DOI: 10.1109/CLOUDCOMP.2015.7149635

CITATIONS

3

READS

888

4 authors:



Saad Alqahtany

University of Plymouth

6 PUBLICATIONS 4 CITATIONS

[SEE PROFILE](#)



Nathan L. Clarke

University of Plymouth

126 PUBLICATIONS 1,109 CITATIONS

[SEE PROFILE](#)



Steven Furnell

University of Plymouth

328 PUBLICATIONS 2,920 CITATIONS

[SEE PROFILE](#)



Christoph Reich

Furtwangen University

57 PUBLICATIONS 265 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Federated Authentication Using the Cloud [View project](#)



A Forensically Enabled Cloud Computing Architecture in IaaS [View project](#)

All content following this page was uploaded by **Saad Alqahtany** on 15 May 2015.

The user has requested enhancement of the downloaded file.

Cloud Forensics: A Review of Challenges, Solutions and Open Problems

Saad Alqahtany

Centre for Security, Communications and Network Research
Plymouth University
Plymouth, UK

Saad.alqahtany@plymouth.ac.uk

Steven Furnell

Centre for Security, Communications and Network Research
Plymouth University
Plymouth, UK

Nathan Clarke

Centre for Security, Communications and Network Research
Plymouth University
Plymouth, UK

Christoph Reich

Information and Media Centre
Hochschule Furtwangen University
Furtwangen, Germany

Abstract— Cloud computing is a promising next generation computing paradigm which offers significant economic benefits to both commercial and public entities. Due to the unique combination of characteristics that cloud computing introduce, 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 plenty 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. Furthermore it explores the current research proposals and technical solutions addressed in the respective research. Ultimately, it highlights the open problems that need further efforts to be tackled.

Keywords—Cloud Computing; Digital Investigation; Digital Forensics; Cloud Forensics challenges; Cloud Forensics Solutions

I. INTRODUCTION

In the past few years, cloud computing has become an attractive solution to many Internet users and organizations [1]. Cloud computing offers significant economic benefits to users by providing a highly scalable infrastructure and pay as you go services at low cost and on demand computing. Nonetheless, the same technology also poses a number of threats, including criminal exploitation leaving little evidence behind and carrying out malicious activities very easily. For example, cybercriminals are utilizing existing cloud service as their infrastructure to target the victim. In 2013, a Chinese gang exploited cloud file hosting services and utilizing Dropbox to distribute its malware as a preparation for the initial stage of DDoS attacks [2]. Indeed, the issue of security is listed as the top concern of cloud adoption [3]. Due to the distributed nature and configuration of the cloud computing infrastructure, investigators face several challenges when performing digital investigation in the cloud environment. These challenges are novel and unique to the cloud and 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. Also, little research has been conducted to investigate how digital investigations could be performed in a forensically sound manner within the cloud domain [4]. Moreover, 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 [5]. 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 upon the identification of the issues which digital forensics investigators face when performing digital investigation within the cloud-computing environments. This paper, however, conducts a review based upon a number of scientific papers that were retrieved from well-known academic databases including ACM, IEEE Xplore, Springer and ScienceDirect. Based upon the outcome of the review, this paper identifies the major challenges, existing solutions and open problems in the field of cloud forensics.

The paper is organized in the following manner: section II examines cloud forensic problems and explores the current solutions in each stage of digital investigation process including: identification, preservation, collection, examination, analysis and presentation. Then Section III discusses in details the existing research solutions and highlights the open issues. Finally, the conclusion and future suggestions are presented in IV.

II. CLOUD FORENSICS CHALLENGES & SOLUTIONS

The evolution of cloud forensics is still in its infancy although cloud computing has been utilized in the market for many years [6]. Depending upon each cloud service model which include: Infrastructure as a Service (IaaS), Platform as a

service (PaaS) and Software as a Service (SaaS), different issues can be countered during a digital investigation process [7]. Several researches warned that it would be difficult if not impossible to perform investigation and discovery in the cloud environment without relying on Cloud service providers [8],[9]. Nonetheless, several conceptual solutions were proposed to overcome this difficulty. In general a digital forensics process contains four main stages: identification, preservation and collection, examine and analysis and presentation stage [5]. This section categorizes the cloud forensics issues according to these stages:

A. Identification Stage

An initial identification of machine(s) wherein illegal activities could be carried out and a forensics investigation is required. Due to the dynamic nature of the cloud infrastructure, several obstacles that hinder the investigators to undertake 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 [10],[11],[12]. Indeed, for certain cases, investigators do not even know the location of the data due to the distributed nature of cloud (i.e. data is distributed among many hosts in multiple data centers) [13]. The availability of system statutes and logs files is depending on the cloud service model. It is not feasible in SaaS and PaaS models due to the limited access which 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 [14]. 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 [6]. Nonetheless, the majority of them have focused merely on accessing to evidence in logs in order to trace details of the 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 which collects and correlates logs [14]. Their approach was evaluated within a Eucalyptus cloud environment. Monitoring and analyzing tools (e.g. Snort, Syslog and Log Analyzer) were used in order to monitor the Eucalyptus's behavior and log all internal and external interactions of 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. Beside these, the number of VMs controlled by a single Eucalyptus user can also be identified. Their experimental result shows that cloud forensics will get a better advancement if the cloud service providers (CSPs) could provide a better logging mechanism.

Sang also proposed a log-based model which suits only for the SaaS and PaaS models [7]. This solution aims to keep a separate log in the consumer side locally and synchronise it with the CSP logs using information such as unique IDs and timestamps. Hence, it enables investigators to check user activities on SaaS without the CSP's support. However, the log content is decided by the CSPs 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 of 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 from client side only. Thus, designing and configuring build-in application logs are required in order to log potential evidences such as user communication logs [15]. 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 standardize manner: when, where and what to log [16]. After enabling logging on all infrastructure components to collect logs, a synchronized, reliable, bandwidth efficient, and encrypted transport layer is established to transfer log from the source to a central log collector. According to this proposal, only a minimum number of fields are required to be presented in every log, including the time-stamps record, application and users, session ID, severity, reason and categorization. This proactive approach provides assurance to forensics investigators that the data is reliably generated and collected. However, this framework does not deal with volatile data which may contain potential evidences.

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 [14]. They suggested that a mechanism that prevents potential eavesdroppers from viewing and changing the content of log during the transmission process is required. They also proposed that the CSP can provide network, process, and access logs through a read-only API to get necessary logs from all the three cloud service models.

- Volatile Data

When the power is turned off, volatile data cannot sustain. Likewise, when a VM is turned off or restarted, all the data will be lost unless the image is stored somewhere. Unfortunately, the existing structure of CSPs does not provide a persistent storage to 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 machines [6],[17] [18],[13]. If the inspected cloud hosted virtual machines which do not have persistent storage the only option to conduct inspection and analysis is the live forensics approach [19]. Damshenas et al. proposed the solution that provides persistent storage for the client's data. This extra storage can be utilized in data-recovery, data-safety for client and ease the data collection for investigators. For this reason, it should be globalized between CSPs in order to provide the Clients with their persistent storage. However, it is not common for small and medium scale business organizations to employ this option due to the cost issue.

Furthermore, Birk & Wegener proposed a solution to overcome the problem which is posed by volatile data [14]. They suggested a 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 of the procedures.

- Lack Control of The System

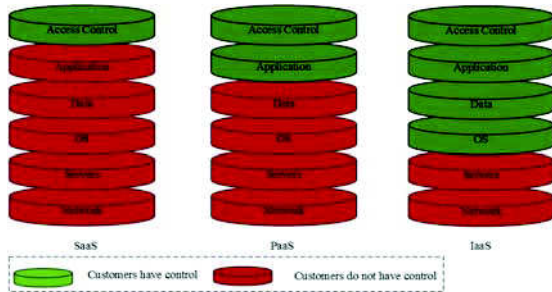


Fig1 Customer Control with Different Service Models [6]

The lack of control of the system poses a number of obstacles to digital investigators when they carry out the evidence acquisition [20]. Indeed, consumers have limited access and control at all levels within the cloud environment (as shown in Fig 1) and have no knowledge where its data is physically located [21]. This effectively removes the opportunity to perform a physical acquisition of the disk, which is a standard practice in computer forensics 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 available to the cloud consumer yet [11].

- Lack of Customer Awareness

Finally, a lack of CSP transparency along with little international regulation leads to loss of important terms regarding forensics investigations in the Service level Agreement (SLA). This issue is applicable to all three services models [22].

B. Data Collection & Preservation

This step is 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 [23]. However, several issues exist when investigators conduct this step in cloud-based investigations and they are listed below:

- Dependence on Cloud Forensics providers

Both customers and investigators are heavily depended upon the CSP in collecting the digital evidence from cloud computing environment as they have limited control on the system. This dependence introduces serious issues of the CSP's trust 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 a timely fashion. These include but are not limited to:

- Due to the sheer volume of data and users within the cloud environment, most CSPs will only keep a limited amount of backups. This can cause problems when recovering deleted data or even overwritten data that is deleted by another user.
- CSPs usually hide the data location from customers for data movement and for replication reasons [22].
- In case of an incident, the cloud provider will focus upon 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 potential damages upon their reputation.
- CSPs do not hire certified forensics investigators to handle cloud-based incidents in a forensically sound manner. Hence, the integrity of evidence could be questioned in the court of law [24].
- The location uncertainty of the data makes the response time to an e-discovery request extremely challenging [25].
- Ultimately, as evidence residing in one CSP, this could lead to a single point of failure and adversely impact on acquisition of useful data [26].

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, they are not designed with forensics 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 [27]. 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 [28]. Furthermore, Dykstra & Sherman proposed a six-layer model for IaaS based upon the amount of trust required: Guest application, Guest OS, Virtualization, Host OS, Physical hardware and Network cloud layer. The further down the stack is, the less cumulative trust is required. For example, Guest application requires trust from all aforementioned layers, whereas network layer only needs trust in the network [29]. Ultimately, they recommended a cloud management plane for using in the IaaS model in the way that customer and investigators can collect vital digital evidence including VM image and logs of network, process and database. However, this approach needs extra level of trust in the management plane.

- Isolating a Cloud Instance

For any forensics process, it is vital to isolate the incident environment in order to prevent any possible evidence from tampering, alteration or adulteration. Hence, it is also needed to isolate particular instance that is connected with the incident in the cloud environment. However, achieving such a task in the cloud environment is not a trivial task due to that 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 digital investigation. Some cloud isolation techniques were proposed by [30] 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 of the evidence while forensic investigations are undertaken in the cloud environment. These techniques are: 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 operating system; Server Farming, which 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, combination of these techniques should be implemented. However, these techniques are mainly theory based without the support of practical experimentation.

- Data Provenance in Cloud

Provenance plays a major role to the success of data forensics in cloud computing. Implementing secure provenance enables the digital investigators to obtain vital forensics data from the cloud environment, such as defining who owns the data at a given time, and when and by whom the data was 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 process history of data objects in cloud computing [31]. They stated that such techniques should satisfy conditional privacy preservation. The technique also provides confidentiality on sensitive documents stored in a cloud, anonymous authentication to cloud servers, and provenance tracking on disputed documents. Cloud computing features was utilized in order to reduce the user's overhead during the process of provenance assumes [31]. They claim that the proposed solution provides trusted evidence in the cloud environment. However, their solution has not been applied to different service models.

- Data Integrity

One of the main issues faced by investigators in cloud based cases is the data preservation [24]. Data integrity is a critical component of the forensic process [21]. It is crucial that the original evidence is not changed at all [13]. 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 carried out procedures [15]. An improper preservation of evidence might become valueless in the court of law [20]. However, it is likely that errors would occur in the data preservation stage in the cloud context due to multiple actors who are involved in the process [6]. Thus, it is a challenging task to prove the integrity of cloud-based evidence to the court in an admissible manner [6]. For example, if the client was involved with the malicious activities, she can claim that her authentication credentials were stolen and might be misused by somebody else. Yet, it is difficult to evaluate the authenticity of that claim [28].

With the aim to preserve the integrity and confidentiality of the data within the cloud environment, a Trust Platform Module (TPM) was proposed [14], [29]. Using the TPM leads

to get preserve the integrity and confidentiality of the data. Furthermore, utilizing TPM solutions provides machine authentication, hardware encryption and signing, secure key storage and attestation [6]. Beside this, it can provide the integrity of running virtual instance, trusted log files and trusted deletion of data to customer [6]. However, the security of the TPM is still questionable due to the possibility of modifying a running process without being detected by the TPM [29]. In the near future, CSPs are unlikely to comply with the TPM as most of current devices are not compatible [6].

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 Virtual Private Network (VPN) can be used together to simply mitigate the issue of the preservation [15]. As the security is a major concern in 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 a Service Level Agreement (SLA) contract should contain all client's privacy data. Yan proposed a framework that images the relative records and files completely [32]. Furthermore, litigation hold or similar freezing mechanism is required to be placed by the CSP on the account and prevent any changes to the data [19]. For example, law enforcement agencies in Australia can make preservation notices to the CSPs according to the Australian Cybercrime Legislation Amendment Bill 2011[33].

- Time Synchronization

The synchronization of time (Stamps) are very important as it can be used as a source of evidence. Nevertheless, the date and time stamps of the data are questionable when they are from multiple systems [6]. 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 a strongly dependent on whether the VM guest OS are using a network protocol to synchronize with a network time server. However, the best strategy recommended by [34] 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 enable investigators to create the time-line analysis and to track multiples log records in different physical locations [15].

- Cloud Literacy of Investigators

Little training materials that can be utilized to educate investigators on the cloud computing technology and cloud forensics procedures are available. Also, current digital forensic training materials are not updated regularly and do not address the major challenges of cloud environments. Moreover, there is lack of standard operating policies for cloud forensics [22]. It is highly needed that members of an investigation team should be trained on law regulations, special tools and

techniques, including programming, networking, communication and negotiation with CSPs [35].

- Chain of Custody

The chain of custody is one of the most critical problems in digital forensics arena [6]. The chain of custody has to illustrate how the evidence was collected, analyzed and preserved at the aim of presenting the evidence in admissible way at the court of law [11]. It is difficult to verify the data chain of custody in the cloud environment, due to the unique combinations of characteristics that the cloud computing has, including the distributed and multi-layered nature [27]. In order to maintain the chain of custody, certain things are required to be clarified, such as the way in which logs were collected, generated and stores along with who had the access to the logs. Moreover, CSPs have to hire trained and qualified specialists [36]. Furthermore, communication and collaborations related to all forensics activities through the chain of CSPs and customer's dependencies need to be clearly written in SLAs [22].

C. Analysis & Examination

It is very challenging to conduct a proper analysis in the cloud due the sheer volume of resources and vast objects to be examined in the digital investigation along with limitation in processing and examining tools. Moreover, there is no standard program for the forensics extraction of data as the customer can access relevant data from various devices such as desktop PC, tablet and mobile phones and a wide range of applications. Furthermore, the data extraction format is varied based on the service model. For example, in the IaaS model, investigators can obtain an image of the virtual machine 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 by using standard forensics tools. Thus, it is important to develop utility applications that translate native cloud data format to a readable and recognizable format by tools [4]. Reconstruction of events of the forensics 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 of the crime might occur in different countries. This will lead to the difficulty in making the logical order of where it took place. Investigators could face a wide range of challenges when they perform the examination and analysis stage, including:

- Lack of Forensics Tools

It is a common understanding that the available forensics tools have various limitations and cannot cope up with the distributed and elastic characteristic of the cloud computing [22], [13], [36]. Also there is a high level of demand upon forensic-aware tools for the CSP and the clients to conduct forensics investigation in cloud environment [22]. Hence, it is crucial to develop tools which can be utilized to identify, collect and analyze cloud forensics data [12]. A combination of computer forensics and network forensics tools is needed at aiming of acquiring forensics data and then analyzing them in a timely fashion. Traditional forensics tools can be used to collect the active data while its integrity is preserved. Network forensics 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, secured in the purpose of using it later in 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, a multi-jurisdiction problem is still a major concern [37]. In a cloud computing, it is less likely that CSPs obey the legal e-discovery obligations due to technical, cost and legal reasons or even to incapability to preserve the original metadata as expected [4]. Furthermore, the response time to an e-discovery is extremely challenging due to uncertainty of data location and the need for assurance of completion of the request [27].

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 visited, extract information stored in cloud, reconstruct Internet activities and search for the online identities that were used. This version is still under development and it only works against Windows XP drives [38]. Furthermore, the management plane was recommended as the appropriate forensics tools for acquiring cloud-based data [29]. They claimed that 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, Dykstar et al. do not recommend them due to the high level of trust they required [29]. Recently, Dykstra et al. developed a management plane forensics toolkit called Forensics Open-Stack Tools (FROST) which is designed to acquire forensics data from virtual disks, API logs and guest firewall logs [21]. It operates at the cloud management plane instead of interacting with the operating system inside the guest virtual machines. FROST is the first forensic tool that be built into any IaaS cloud model [21].

- Evidence Correlation Across Multiple Sources

Correlation of activities across multiple sources can be overwhelming. The resources of evidence 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 [6]. For example, when an adversary shut down her virtual instance after committing certain malicious activities, reconstruction of the crime scene will be impossible. However, regeneration event can be used where a snapshot is done due to occurrence of every attack. Geethakumari & 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 [39]. Ultimately, it is also suggested that incoming and outgoing data through the cloud is visualized by the investigators.

D. Presentaion

The final step of digital forensics investigation is presentation, where the evidence has to be presented to a judicial body in the form of a report or testimony [40]. Several challenges lie in this step in 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 to determine which legal system the case should be heard. Furthermore, it is required that digital investigators have to technically explain to the jury 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 a basic technical knowledge [13].

III. DISCUSSION AND SUMMAY OF CURRENT SOLUTIONS IN CLOUD

It is clear that there are plenty of issues that need to be tackled in order to perform a proper forensics in the cloud environment. Table 1 illustrates challenges and their potential solutions. All proposed solutions were identified from the review conducted in the respective domain. Table 2 summarizes the open problems that need to be resolved.

Table 2 Summary of open issues

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

Table 1 cloud forensics issues and potential solutions

Cloud Forensics challenges/ Process		Apply to Service model			Potential Solution	Ref
		IaaS	PaaS	SaaS		
Identification						
Access to the evidence		√	X	X	Eucalyptus framework OS and the security log	[41]
		√	X	X	a log-based model	[7]
		√	√	X	Extraction of relevant status data	[15]
		X	√	X	A log management solution	[16]
		√	√	X	An encrypted logging model	[14]
Dependence on CSP for	Trust Issue	√	√	X	Layers of Trust Model	[29]
	Data Acquisition	√	√	X	TrustCloud	[28]
	Compliance	√	√	√	Cloud Management Plane	[42]
	Logs	√	√	√	Serve Level Agreement (SLA)	[11],
Lack of customer awareness		√	√	√	--	[22]
Volatile Data		√	√	X	Client Persistent Storage	[15]
		√	√	X	A continuous synchronisation API	[10]
Preservation & Collection						
Data integrity		√	√	√	Trust Platform Module (TPM)	[9], [29]
Time synchronisation		√	√	√	Unified/specific time system	[15]
Cloud literacy of investigators		√	√	√	Developing investigators technical skills	[35]
Chain of custody		√	√	√	Trained staff	[36], [22]
Analysis & Examination						
Lack of forensics tool		√	√	X	FROST, OWADE	[21], [38]
Presentation						
Jury's technical comprehension		X	X	X	Training	[13]

Several solutions were proposed with the aim of mitigating cloud challenges. Despite this, the majority of these solutions are conceptual and not tested in real conditions. So far, traditional tools such as Encase and FTK are still the common tools that are heavily utilised in acquiring the evidence from the cloud despite the difference between conducting digital investigation in the cloud infrastructure and in traditional computer environments. Data acquisition is the first practical required task that digital investigators have to begin with. According to the previous section, there was only one research that evaluated and examined the current tools used in conducting remotely data acquisition. This research conducted by Dykstra and Sherman who developed a set of tools known as Forensics OpenStack tools (FROST). It operates at the cloud management plane instead of interacting with the operating system inside the guest virtual machines. FROST is the first forensics capability to be built into any Infrastructure-as-a-service 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 on the cloud infrastructure is required including the hardware, host operating system, hypervisor and cloud employees. It also assumes that cloud customer is cooperative and involved in the investigation. This work have performed three experiments to acquire forensics data from three different layers namely guest OS, the virtualisation layer and the host OS. All three experiments have succeeded to performing data acquisition remotely from cloud based layer. However, certain amount of trust is highly required in each layer.

Customers and investigators depend on the CSP to conduct this task. Few researchers suggested solutions that would mitigate the issue of the dependence on the CSP such as cloud management plane or API which are provided to the customer in order to get forensics data. However, there are various and crucial forensics data that still reside in the CSP including deleted files from the hard disk and temporary registry logs. In order to acquire this kind of data, relying on the CSP cooperation is inevitable. In turn, many other issues associated with the dependence on the CSP evidence are shown and they are not resolved yet. Such issues are including trust, delay response, inadmissibility of evidence and potential single point of failure. 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 to reconstruct the past state of event with a level of accuracy that the reconstructed information can be admissible in the court of law.

It is clear that there is a big concern with regards to data acquisition and its integrity in the cloud environment. There is a need to provide a solution that will ensure organisations remain in control, take the burden/liability off the CSPs and make it easy to acquire the evidence in a forensically sound manner and in a fashion time. Therefore, the authors are involved in an ongoing project to develop a forensically-enabled IaaS cloud computing architecture. It aims at producing an acquisition and analysis model that fundamentally shifts responsibility of the data back to the data owner rather than relying upon a third party. In this manner,

organisations are free to undertake investigations and will requiring no intervention or cooperation from the cloud provider. The model aims to provide a richer and complete set of admissible evidence than what current CSPs are able to provide.

However, further research is required in order to better understand both the technical implications resulting from such a system on the day to day operation of a cloud system and the financial costs. Furthermore, several difficulties associated with logging data are still not diminished yet. These are including time-line, log review, logging correlation and log policy monitoring. Ultimately, legal issues hinder the smooth performing of forensics investigation due to the lack of guidelines and implementation of global unity to overcome the cross border issue.

IV. CONCLUSION & FUTURE WORK

As there is increasing of cloud computing uses, there is growing need for trustworthy cloud forensics. Several researchers have identified and explored the challenges confronting the digital investigators when they conducting forensics investigation in cloud based cases. Accordingly, few researchers have proposed technical solutions to mitigate these challenges. However, there are still open issues need to be tackled. Dependence on the CSP is a major challenge such as trust issue, delay response, inadmissibility of evidence and potential single point of failure. Furthermore, time line analysis across multiple sources hinders investigators to understand the relationship and data flows between systems. Unfortunately, to date, most studies techniques and tools involving one source of digital evidence at a time for investigation.

This paper identified cloud forensics challenges; matched proposed solutions to these challenges and determined open problems that need further efforts to be tackled.

V. REFERENCE

- [1] S. Zargari and D. Benford, "Cloud Forensics: Concepts, Issues, and Challenges," in *2012 Third International Conference on Emerging Intelligent Data and Web Technologies*, 2012, no. 1999, pp. 236–243.
- [2] K. Higgings, "Dropbox, WordPress Used As Cloud Cover In New APT Attacks," *Dark reading*, 2013. [Online]. Available: <http://www.darkreading.com/attacks-breaches/dropbox-wordpress-used-as-cloud-cover-in-new-apt-attacks/d/d-id/1140098?> [Accessed: 28-Jan-2015].
- [3] C. Hooper, B. Martini, and K.-K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," *Comput. Law Secur. Rev.*, vol. 29, no. 2, pp. 152–163, Apr. 2013.

- [4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology," Gaithersburg, MD, 2011.
- [5] R. Poisel, E. Malzer, and S. Tjoa, "Evidence and Cloud Computing: The Virtual Machine Introspection Approach," *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 4, no. August, pp. 135–152, 2012.
- [6] S. Zawoad and R. Hasan, "Digital Forensics in the Cloud," *CrossTalk*, no. October, pp. 17–20, 2013.
- [7] T. Sang, "A Log Based Approach to Make Digital Forensics Easier on Cloud Computing," in *2013 Third International Conference on Intelligent System Design and Engineering Applications*, 2013, pp. 91–94.
- [8] A. Patrascu and V. Patriciu, "Beyond Digital Forensics . A Cloud Computing Perspective Over Incident Response and Reporting," *Applied Computational Intelligence and Informatics (SACI)*, 2013, pp. 455–460.
- [9] K. Ruan and J. Carthy, "Cloud Computing Reference Architecture and Its Forensic Implications: A Preliminary Analysis," *Digit. Forensics Cyber Crime*, pp. 1–21, 2013.
- [10] D. Birk, "Technical Challenges of Forensic Investigations in Cloud Computing Environments," *Workshop on Cryptography and Security in Clouds*, 2011, pp. 1–6.
- [11] J. Dykstra and A. T. Sherman, "Understanding Issues In Cloud Forensics: Two Hypothetical Case Studies," in *Proceedings of the 2011 ADFSL Conference on Digital Forensics Security and Law*, 2011, pp. 1–10.
- [12] J. J. Shah and L. G. Malik, "Cloud Forensics: Issues and Challenges," *2013 6th Int. Conf. Emerg. Trends Eng. Technol.*, pp. 138–139, Dec. 2013.
- [13] D. Reilly, C. Wren, and T. Berry, "Cloud Computing: Pros and Cons for Computer Forensic Investigations," *Int. J. Multimed. Image Process.*, vol. 1, no. 1, pp. 26–34, 2011.
- [14] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," in *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2011, pp. 1–10.
- [15] M. Damshenas, A. Dehghantanha, R. Mahmoud, and S. Shamsuddin, "Forensics Investigation Challenges in Cloud Computing Environments," in *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*, 2012, pp. 190–194.
- [16] R. Marty, "Cloud application logging for forensics," *Proc. 2011 ACM Symp. Appl. Comput. - SAC '11*, p. 178, 2011.
- [17] S. Zawoad and R. Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," *arXiv Prepr. arXiv/1302.6312*, pp. 1–15, 2013.
- [18] H. Guo, B. Jin, and T. Shang, "Forensic Investigations in Cloud Environments," in *2012 International Conference on Computer Science and Information Processing (CSIP)*, 2012, pp. 248–251.
- [19] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digit. Investig.*, vol. 9, no. 2, pp. 71–80, Nov. 2012.
- [20] S. Zawoad and R. Hasan, "I Have the Proof: Providing Proofs of Past Data Possession in Cloud Forensics," 2012.
- [21] J. Dykstra and A. T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform," *Digit. Investig.*, vol. 10, pp. S87–S95, Aug. 2013.
- [22] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," *Adv. Digit. Forensics VII*, pp. 15–26, 2011.
- [23] G. Sibiya, H. S. Venter, and T. Fogwill, "Digital Forensic Framework for a Cloud Environment," *IST_Africa 2012 Conference proceedings*, 2012, pp. 1–8.
- [24] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic investigation of cloud computing systems," *Netw. Secur.*, vol. 2011, no. 3, pp. 4–10, Mar. 2011.
- [25] K. Ruan, "Designing a Forensic-Enabling Cloud Ecosystem," in *Cybercrime and cloud forensics, USA: IGI Global*, 2013, pp. 331–344.
- [26] M. Crosbie, "Hack the Cloud: Ethical Hacking and Cloud Forensics," in *Cybercrime and cloud forensics, USA: IGI Global*, 2013, p. 17.
- [27] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," *Digit. Investig.*, vol. 10, no. 1, pp. 34–43, Mar. 2013.
- [28] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee,

- “TrustCloud: A Framework for Accountability and Trust in Cloud Computing,” *2011 IEEE World Congress on Services*, 2011, pp. 584–588.
- [29] J. Dykstra and A. T. Sherman, “Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques,” *Digit. Investig.*, vol. 9, pp. S90–S98, Aug. 2012.
- [30] W. Delpont, M. S. Olivier, and M. Kohn, “Isolating a Cloud Instance for a Digital Forensic,” in *ISSA*, 2011.
- [31] J. Li, X. Chen, Q. Huang, and D. S. Wong, “Digital provenance: Enabling secure data forensics in cloud computing,” *Futur. Gener. Comput. Syst.*, Oct. 2013.
- [32] C. Yan, “Cybercrime forensic system in cloud computing,” in *Proceedings of 2011 International Conference on Image Analysis and Signal Processing, IASP 2011*, 2011, no. Dc, pp. 612–613.
- [33] B. Catryna, “Review of the Cybercrime Legislation Amendment Bill,” 2011.
- [34] N. Marangos, P. Rizomiliotis, and L. Mitrou, “Time Synchronization: Pivotal Element in Cloud Forensics,” *Secur. Commun. Networks*, 2014.
- [35] G. Chen, Y. Du, P. Qin, and J. Du, “Suggestions to digital forensics in Cloud computing ERA,” in *2012 3rd IEEE International Conference on Network Infrastructure and Digital Content*, 2012, pp. 540–544.
- [36] G. Grispos, “Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics,” vol. 4, no. November, pp. 28–48, 2012.
- [37] M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, “Digital evidence in cloud computing systems,” *Comput. Law Secur. Rev.*, vol. 26, no. 3, pp. 304–308, May 2010.
- [38] M. Kumar, “Computer Investigations,” *The Hacker News*, 2011. [Online]. Available: <http://thehackernews.com/2011/09/offline-windows-analysis-and-data.html>.
- [39] G. Geethakumari and A. Belorkar, “Regenerating Cloud Attack Scenarios using LVM2 based System Snapshots for Forensic Analysis,” *Int. J. Cloud Comput. Serv. Sci.*, vol. 1, no. 3, pp. 134–141, 2012.
- [40] P. M. Trenwith and H. Venter, “Digital Forensic Readiness in the Cloud,” in *Information Security for South Africa, 2013*, 2013, pp. 1–5.
- [41] Z. Zaferullah, F. Anwar, and Z. Anwar, “Digital Forensics for Eucalyptus,” in *2011 Frontiers of Information Technology*, 2011, pp. 110–116.
- [42] J. Dykstra, “Cybercrime and Cloud Forensics,” in *Cybercrime and cloud forensics*, K. Ruan, Ed. USA: IGI Global, 2013, pp. 156–185.