THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 9 | Number 4 Article 2

2014

A State-Of-The-Art Review of Cloud Forensics

Sameera Almulla
Khalifa University of Science, Technology and Research

Youssef Iraqi
Khalifa University of Science, Technology and Research

Andrew Jones
University of South Wales, UK; Edith Cowan University, Australia

Recommended Citation

Almulla, Sameera; Iraqi, Youssef; and Jones, Andrew (2014) "A State-Of-The-Art Review of Cloud Forensics," *Journal of Digital Forensics, Security and Law*: Vol. 9 : No. 4 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2014.1190
Available at: https://commons.erau.edu/jdfsl/vol9/iss4/2

A STATE-OF-THE-ART REVIEW OF CLOUD FORENSICS

Sameera Almulla[1], Youssef Iraqi[1], and Andrew Jones[2,3]

[1]Department of Electrical and Computer Engineering, Khalifa University of Science, Technology and Research, UAE
[2]Department of Computing, Engineering and Science, University of South Wales, UK
[3]Edith Cowan University, Australia
[1]{*sameera.almulla, youssef.iraqi*}*@kustar.ac.ae*
[2]{*andy.jones*}*@southwales.ac.uk*

ABSTRACT

Cloud computing and digital forensics are emerging fields of technology. Unlike traditional digital forensics where the target environment can be almost completely isolated, acquired and can be under the investigators control; in cloud environments, the distribution of computation and storage poses unique and complex challenges to the investigators. Recently, the term "cloud forensics" has an increasing presence in the field of digital forensics. In this state-of-the-art review, we included the most recent research efforts that used "cloud forensics" as a keyword and then classify the literature into three dimensions: (1) survey-based, (2) technology-based and (3) forensics-procedural-based. We discuss widely accepted standard bodies and their efforts to address the current trend of cloud forensics. Our aim is not only to reference related work based on the discussed dimensions, but also to analyse them and generate a mind map that will help in identifying research gaps. Finally, we summarize existing digital forensics tools and the available simulation environments that can be used for evidence acquisition, examination and cloud forensics test purposes.

Keywords: digital forensics, cloud computing, cloud forensics, state-of-the-art

1. INTRODUCTION

Cloud computing is an evolved technology that changed the methods by which data is stored and processed. The computing paradigm has shifted from computer and mobile devices to cloud computing. The low entry cost, the saving on capital expenditure and flexibility have made cloud computing an attractive option for many organisations. This introduces several challenges with regard to how to perform digital forensics investigation for cloud based crimes.

Cloud computing has an impact on both the theoretical and practical aspects of digital forensics. The former includes a need for enhancement of the existing digital forensics processes and on how to perform them practically. The latter requires effort by researchers in identifying cloud forensics challenges.

The scope of this paper is to provide a condensed analysis of the cloud forensics literature review by identifying areas that require research attention and pinpointing future needs. "Cloud Computing Forensic Science" is defined in (NIST, 2014b) as

> The application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through

> identification, collection, preservation, examination and reporting of digital evidence.

In this review paper, there are three dimensions that have been used to categorise the cloud forensics literature: survey-based, technology-based and forensics procedural-based.

Survey-based literature covers the challenges that cloud computing introduces in the field of digital forensics. Technology-based concentrates on the literature studies of cloud forensics based on the underpinning technologies such as virtualisation and distributed computing. Also, we propose an additional new classification of literature, namely procedural-based cloud forensics. It includes methodologies and frameworks that target digital forensics procedures, namely identification, preservation, collection, examination and analysis.

Based on our analysis most of the literature tackles more than one procedure e.g., some of the publications focused on proposing solutions for both evidence collection and examination (this includes event reconstruction).

Paper outline An overview of cloud computing and digital forensics is discussed in Section 2. Section 3 discusses the used search criteria and engines. The three main dimensions of the literature are discussed in Section 4. Section 5 discusses the standardisation efforts in cloud forensics. The summary of both conventional or cloud centric tools and test/simulation environments is discussed in Section 6. A discussion on the mind map, research gaps and summary concludes this paper in Section 7.

2. OVERVIEW OF CLOUD COMPUTING AND DIGITAL FORENSICS

2.1 Cloud Computing

Cloud computing has a number of definitions. The National Institute of Standards and Technology (NIST) defines cloud computing as

> A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST, 2014b).

The uniqueness of the cloud environment is a result of its characteristics. In order to analyse and study the opportunities and challenges presented by digital forensics in cloud computing, it is essential to understand these characteristics.

2.1.1 Characteristics

As identified by NIST (NIST, 2014b) there are five characteristics for cloud computing, namely, on demand self-service, ubiquitous network access, resource pooling, rapid elasticity, and pay-per-use business model. Acquiring digital evidence of a suspect whose data is stored in a shared, multi-tenant and elastic pool of resources may result in privacy violation of legitimate users data. Hence, an enhanced digital forensics model is required to collect forensically sound evidence for cloud based incidents. In order to measure the severity of the impact of cloud computing on digital forensics, there must be a clear understanding of the cloud computing service and deployment models (NIST, 2014b).

2.1.2 Service and Deployment Models

Service models are categorised by the type of computing resources provided to the end users.

- Software as a Service (SaaS), applications are delivered as a service over the Internet e.g., Google Mail.
- Platform as a Service (PaaS), the development platform is provided as a service e.g., Microsoft Azure.
- Infrastructure as a Service (IaaS), the server(s), storage and hardware are delivered as a service e.g., Amazon Simple Storage Service (S3).

Deployment models There are four deployment models for cloud computing, namely public, private, community, and hybrid cloud (NIST, 2014b). The deployment models differ based on the users control on the computing resources and their location. For example, public cloud is owned by the Cloud Service Providers (CSPs) and its infrastructure is located within CSP premises. However, in the case of private cloud, the computing infrastructure is owned by the user (e.g., a federal or private company) and it is located within its premises. In each deployment model, cloud services can be provided as SaaS, PaaS and IaaS. In a hybrid cloud, the infrastructure consists of a combination of the private and public models. In the community cloud model, computing resources (server or network) are shared between several organizations of similar interests, needs and requirements.

2.2 Digital Forensics

NIST (2014a) defined digital forensics as

> The application of science to the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody of data.

There is no single process model that can be followed to obtain evidence. As stated by Ruan (2013), there are about four standards for the forensics process, namely Digital Forensics Research Workshop (DFRW), National Institute of Justice (NIJ), National Institute of Standards and Technology (NIST) and Integrated Digital Investigation Process (IDIP). The main difference between the first three and IDIP is the integration of digital forensics process with the physical forensics. Next is a discussion of each process in terms of its definition and how the presence of cloud computing might impact each procedure.

2.2.1 Process

Cloud computing is a dynamic service oriented technology. It creates challenges to the applicability of existing digital forensics procedures. The NIJ process model encapsulates the DFRWS and NIST process models as well as the IDIP. Hence, in our review, the previous works are categorised based on the NIJ forensics process as follows:

Identification Determining the type of crime, software and hardware used by the suspect and possible evidence locations. In a cloud computing environment, identifying the digital forensic requirements to conduct a sound investigation is considered to be the main building block in the process of identification.

Preservation Ensuring evidence integrity by preserving the integrity of the original data. However, in a cloud environment, the challenge is how to preserve the data and then determining whether the existing approaches of measuring data integrity (e.g., using hash functions) are applicable or not.

Collection Extracting the exact bit-by-bit image of the required data. Most of the literature reviews emphasise that collecting the whole target environment might not be possible in the cloud environment. This is due to the fact that the infrastructure is outsourced and owned by the CSP. Also, the variations of cloud service models present a whole new set of challenges on evidence collection.

Examination Studying the collected data and its attributes. Current computer forensics practices examine well-structured storage e.g., hard disks; however, in cloud computing a significant proportion of the target data may be held in memory/network dumps and/or log files.

Analysis An in-depth systematic evidence search is performed on suspect owned devices in two ways: live and/or static systems analysis. To perform the analysis, many tools and applications such as EnCase (EnCase, 2014) and Forensic Tool Kit (FTK) (FTK, 2014) can be used to aid the investigators. In a cloud environment, the analyst must consider the dependencies of a cloud based application either on the service provided within the CSP bound-

aries or outside. In the case where a complete chain of custody is not possible, investigators need to be able to perform analysis on the partial resources in hand (Almulla, Iraqi, & Jones, 2013; Dykstra & Sherman, 2011). Also, there is the need for a digital forensics tool capable of acquiring and analysing cloud-based cases e.g., FROST (Dykstra & Sherman, 2013).

Presentation The findings will be presented to either the management of an organization or a court of law.

2.2.2 Types

Based on the target evidence media, there are two main types of digital forensics;

Static forensic This is the process of obtaining a bit-by-bit copy of powered off digital media. Attaching the media to the forensic machine via a write blocker (before starting the imaging process) preserves the integrity of the original data. In spite of its strengths, there are several limitations of static forensics such as the failure to capture information stored in the Random Access Memory (RAM), which may include encryption keys and network related data.

Live forensic This is a process of collecting volatile network/user related evidence.

Live forensics is becoming increasingly important due to the increase in the size of RAM and the increase in the use of data encryption. RAM might contain valuable credentials such as usernames, passwords and encryption keys.

Another important aspect of live forensics is to define whether the logged on account is in a real or virtual environment. The latter requires further analysis such as the imaging of both the real operating environment and any virtual machines located on the real system.

The main issue with live forensics is that, by virtue of its transient and temporal nature, it will not normally be possible to reproduce the results and as a consequence the reliability of the produced evidence may be questionable.

Most of the literature considers live forensics to be the best fit for cloud forensics. In fact, it is strongly dependent on the cloud service model, CSP cooperation and the target suspect category (client or CSP). In the case of IaaS e.g., Amazon EBS (AmazonEBS, 2014), static forensics may be a more suitable choice. On the other hand, in PaaS or SaaS, live forensics will best suit the situation. However, the feasibility of data access for investigators in the case of the SaaS and PaaS model will differ significantly based on whether the CSP was the victim and based on its Service Level Agreement (SLA) support to digital forensics for incidents.

3. STATE-OF-THE-ART RELEVANT PUBLICATIONS

In our research, we used a scientific database search engine called Summon a product of SerialSolution (Summon, 2014). The Summon solution not only includes a full record of IEEEXplore, Springer, ScienceDirect and Elsevier but also includes Scopus and Web-of-Science databases.

The search keywords "cloud forensics" were used and it was observed that; the total number of 1412 hits takes into account results for either the word "cloud", "forensics" or "cloud forensics". To accurately identify the desired cloud forensics related literature, the results were first filtered by the publication year and the results per year were then manually checked.

Figure 1 shows the system results per year and the actual findings. Although the results from the used search engine showed publications discussing cloud forensics in 2010, the term "Cloud forensics" was first used as a keyword in literature in 2011.

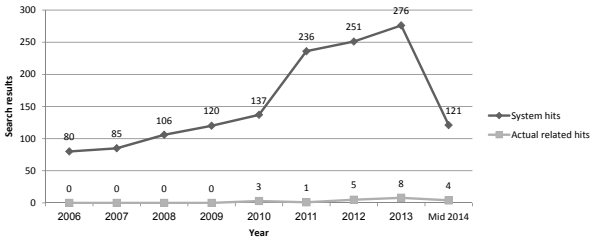

Figure 1 Search Results for "Cloud Forensics" Term

4. STATE-OF-THE-ART CLOUD FORENSICS

In this paper, cloud forensics literature is categorised into three dimensions; survey-based, technology-based and forensics procedural-based. Below is a discussion of the literature review related to each dimension.

4.1 Dimension I: Survey-Based

Researchers who are newcomers to the field of cloud forensics normally start grasping the survey papers where there are results of other researchers, literature review findings and possible challenges that are addressed in this field. In this section, we classify the survey into two categories. the first category includes extensive literature review observations and findings either in technical or legal aspects. The second category includes questionnaires conducted by researchers to picture the current state of cloud forensics among the researchers and practitioners -includes the Law Enforcement Agencies and organizational stakeholders- communities.

4.1.1 Literature Survey

Literature review based papers (Birk & Wegener, 2011; CSA, 2009; George & Mason, 2011; Grispos, Storer, & Glisson, 2012; Hooper, Martini, & Choo, 2013; Marangos, Rizomiliotis, & Mitrou, 2012; Marturana, Me, & Tacconi, 2012; Reilly, Wren, & Berry, 2010; Ruan, Carthy, Kechadi, & Crosbie, 2011; Taylor, Haggerty, Gresty, & Lamb, 2011; Wolthusen, 2009; Zargari & Benford, 2012) pinpointed technical and legal challenges that exist in the cloud computing environment. An additional organizational dimension was discussed by Ruan *et. al.* (2011). The authors discussed the possibility of integrating digital forensics in an organization to respond to the cloud based incidents. It is worth to mention that some of the technical issues have a history in digital forensics, yet present unique challenges in cloud environments.

Technical Issues Most of the computing systems, if not all, consist of two main components namely data and system architecture e.g., OS, hardware, etc. Processing data to generate information is subject to the system functionalities. Changes in the data management, system architecture and data processing result in technology evolution (from personal computers and mobiles to big-data and cloud computing). In the case of digital forensics of cloud computing, not only storing and managing data is different but also the system architecture (distributed computing and virtualisation). These differences pose additional challenges to the practitioners and researchers. Therefore, we categorised the technical challenges either as data or architecture oriented issues.

- **Data related issues**

  Evidence integrity The current wisdom is that the documentation of any process used and the keeping of an audit trail of all actions taken together, where possible, with the use of MD5 hashes, is the best approach to preserving the integrity of evidence. In cloud computing, the integrity needs to be ensured throughout the data lifecycle such as data upload, storage and retrieval. Hence the complexity of methodologies in preserving data integrity has been increased due to the fact that the data has been transmitted over public network (e.g., internet) and stored in distributed facilities.

  Application and software streaming In SaaS and PaaS, application and software streaming can be deployed to optimise the utilization of the network bandwidth and to increase the performance. This can be achieved when the server sends the client the required portion of the application (about 10% of the total program) to launch it and while the client is using the application, the remainder will be streamed to their machines. Once the application license has expired, the CSP will uninstall the software. In such cases, the investigator can look for evidence in the client machine hives (in the case of Windows OS), however if the application was streamed, it is prob-

able that the only source of evidence on the suspected machine will be held in the Random Access Memory (RAM) content.

Time stamps and synchronisation Since the cloud service provider and users may be located in geographically different areas, investigators should bear in mind synchronising the evidence time stamp with the time of data creation. A consistent time source such as Network Timing Protocol (NTP) is important to identify the sequence of evidence and to create a consistent timeline of events across the dispersed parties -client, CSP and the network-.

Data state Collecting data to build the case is the core functionality in a digital investigation. From a technical perspective, data in cloud computing can be in one of three states: at-rest, in-transit or in-execution (Birk & Wegener, 2011). When an incident occurs, the investigator will normally seize the digital device to examine and analyse the evidence. For data at-rest, the investigation process will comply with static forensics model. In a cloud environment this will not normally be possible and the investigator may be reliant on the CSP to collect and provide the relevant data.

While data is in-transit, it might leave traces on the network and on user devices. Unlike data at-rest, maintaining in-transit data integrity is not as simple as the case of data at-rest. Investigators can perform network forensics procedures for incidents occurring within an organization as the network infrastructure is under the control of the organization. However, it is not the case in a cloud environment where the end users are geographically dispersed from the CSP. Finally, in-execution data is when the computer system loads data into the main memory to be processed by the user or another system entity. Investigators can analyse in-execution data such as a running application, process information and machine instructions for current system state through the means of a snapshot.

- **Architecture related issues**

  Shared resources A shared pool of resources is one of the characteristics of cloud computing. Achieving the isolation of the suspected users information from that of an innocent party is a very important and challenging task. In the cloud, the examiners lack of control and knowledge of technical issues may lead to evidence contamination or a breach of the privacy of an innocent third party.

  Seizing cloud computing based equipment Not only the reduced control for the examiner over the information and equipment provided by a CSP but also the an inability to access the valuable information that resides in the cloud could also prevent the investigators from accessing critical information related to the incident.

  Cascaded cloud services In situations where one CSP depends on another, investigators may face the challenge of cascaded services and different service level agreements across different geographical areas.

  Log format In forensic science, different file formats are a challenge for the forensics tools and investigators. Since cloud computing is based on a service oriented architecture, different log formats may be deployed to audit user actions. However, this may introduce challenges on how to unify these logs.

  Tools Insisting on adopting current digital forensics software and application to acquire evidence from the cloud environment might no longer be appropriate. For example, given the distributed nature of the cloud, appropriate forensics tools may be designed in a distributed manner to ensure the consistency of gathered evidences.

  Cloud service models In SaaS, clients are basically using cloud services through

the Internet; hence the main source of evidence is the RAM content. In the PaaS, the application platform is under the client control; as a result, a client can dictate how the application interacts with the underlying infrastructure and system logs can be captured and sent to the service provider to store them. In IaaS, clients have control over the entire virtual machine, virtual storage and virtual network. Also, clients can configure the system to log all critical operations performed and preserve it for investigation (in case an incident occurred).

Digital forensics in/on cloud Using cloud computing resources to serve the purposes of digital forensics is called on-cloud-forensics. However, if the suspect is one of the cloud users or the CSP itself then it is called in-cloud-forensics (Almulla et al., 2013).

To sum up, technical challenges can be categorised either as data oriented or architecture oriented as shown in Table 1.

Legal Challenges

- **Multi-jurisdiction** Cloud computing environments do present significant challenges to forensics. One of the well-known problems is that of jurisdiction. Due to the involvement of multi-jurisdictions in a cloud based investigation, efforts are needed for regulations and agreements in order to ensure that the investigations will not violate any laws or regulations in the jurisdiction where the data is physically stored. Measures must also be taken to ensure that the privacy of other individuals or organization sharing the infrastructure will not be compromised or violated throughout the forensic activity.

- **Service Level Agreement (SLA) and Policies** Cloud users must ensure that the CSPs SLA supports investigations in cases of data breach, a security incident, intrusion or any form of suspicious behaviour. An SLA can be used to define the terms of use between the user and CSP. In Barrett and Kipper (2010), the authors highlighted important points that should be addressed in the SLA which will then support an investigation as follows:

  - State clearly the tools, procedures, access and services provided to cloud users regarding forensics investigation.
  - Roles and responsibilities between client and CSP regarding the forensics investigation.
  - How forensics is to be performed considering different jurisdiction laws and procedures.
  - Availability of an incident response team under the CSP control.
  - The same level of security provisions and forensics preparedness will continue to be carried out if another company takes over the current CSP.
  - Users are able to retrieve data whenever they want and this should be stated under the terms and contract. Also, a format should be available that is easy to read and understand.

- **Readiness and awareness of the legal community** Given the massive uptake of cloud computing services at both the corporate and government levels; law practitioners and decision makers such as lawyers, judges and Law Enforcement Agencies (LEAs) must be aware of the impact of this new technology trend. For instance, looking for alternatives to the bit-by-bit image concept to preserve the original data.

4.1.2 Questionnaire-Based Survey

In order to emphasise the need for cloud forensics and identify particular issues that have to be addressed and eventually resolved; Ruan *et al.* (2013) and Al Fahdi *et al.* (2013) conducted surveys where the participants include

Table 1 Classification of Technical Issues

Data related issues (Affecting factor(s))	Architecture related issues (Affecting factor(s))
Evidence integrity (Data life-cycle, lack of integrity methodologies)	Shared resources (Isolation)
Application and software streaming (Unpackaged software, limitation on logs traces)	Seizing cloud computing based equipment (Geographically dispersed, limited or no physical control)
Data states (Due to different service models)	Cascaded cloud services (Cascaded SLA)
Time stamp and synchronisation (Distributed architecture)	Tools (Distributed nature of evidence)
	Service models
	Log format (Depends on the underpinning technology)

researchers, digital forensics practitioners and organisation stakeholders.

Based on questionnaires conducted in Al Fahdi *et al.* (2013), researchers responded that cloud computing is the first priority among technologies that cause security concerns, whereas, the practitioners ranked it as a third after the anti-forensics and encryption technologies. Overall, participants agreed that cloud computing lacks or has no forensic tools and solutions that are tailored for cloud environment. Finally, 58% of the participants agreed that digital forensics process automation is very important and will be needed to overcome future challenges, e.g., cloud forensics.

Other interesting results were published in Ruan *et al.* (2013), where the survey was designed and focused on cloud forensics. Readers can refer to the original survey for further questionnaire results. Highlights of the results were as follows. Approximately 81% of participants agreed that cloud forensics is an important component of cloud security. Around 80% of respondents selected the investigation of digital crime, civil cases, policy violation, etc. as main cloud forensics usage. About 90% answered that the jurisdiction is the main challenge for cloud forensics. Finally, 87% responded that "Designing forensics architecture for the cloud" should be the main research direction. However, the overall response emphasised that the area of cloud forensics requires significant research effort.

4.1.3 Discussion

Most of the literature studies focused on the IaaS as an investigation target. To the best of our knowledge, no research was conducted to investigate technical findings of the SaaS and PaaS models. Some of the literature discussed three service models -survey based- and others did not identify a particular model for their framework. Considering the service model alone was not sufficient. Hence, the statistics as shown in Figure 2, considered the target service model in relation to the type of the study, either survey or non-survey based, literature.

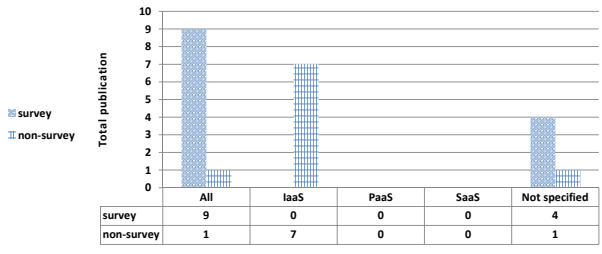

Figure 2 Literature Statistics Based on the Cloud Service Models

Figure 3 shows around 53% of the survey based literature focused on identifying technical issues, while 47% on legal aspects.

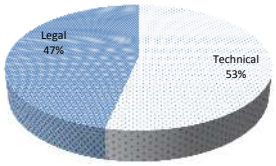

Figure 3 Percentage of Coverage of Technical Issues vs. Legal Issues in Cloud Forensics

4.2 Dimension II: Technology-Based

Many technologies are developed with good intentions, however, individuals can use them to cause harm or hide their malicious activities. Digital forensics need to be dynamic in adopting the changes required to cope with these technologies, especially cloud architecture core components such as distributed computing and virtualisation.

4.2.1 Distributed Computing

In traditional digital forensics, understanding the digital device and operating system is an important skill required by the investigators. In cloud computing, distributed systems are communicating over network channels to receive and respond to client requests. A Distributed File System (DFS) is required to manage the storage and messages in the channels. There are several types of DFSs (Thanh, Mohan, Choi, Kim, & Kim, 2008) such as Client Server Architecture, which is a type of DFS that comes with a communication protocol to allow clients to access files on the server e.g., Sun Network File system. Another type of DFS is Symmetric Architecture File System which is based on peer-to-peer technology (each node acts like a client or as a server) where meta-data is distributed over all participant nodes. It uses a Distributed Hash Table (DHT) based system to distribute data and keys for objects lookup. In contrast, in the Asymmetric Architecture File System, the meta-data is centralized in a single server e.g., Network File System (NFS). In the Parallel Architecture File System, data and its meta-data is block striped in parallel, and distributed across multiple storage devices on multiple servers. It allows concurrent access to the same file. Finally, Clustered Based Distributed File System (CDFS) consists of a single master which controls several hundreds of chunk servers e.g., Google File System (GFS) and HaDoop File System (HDFS). To manage distributed services in the cloud, most of the CSPs such as Google, Yahoo and Facebook have implemented CDFS.

Mulazzani, Schrittwieser, Leithner, Huber, and Weippl (2011) discussed performing forensics analysis on Dropbox application software. Dropbox provides synchronous storage services that are managed by a CDFS. The files are stored in chunks of fixed sizes. The aim of the experiment was to show weaknesses and possible attacks that could be carried out against users. Some of the chunks are marked as deleted and can be overwritten with different user's data. The notion of online slack space was introduced. It is the assigned but unused storage space from end of the file to the end of the chunk. The authors successfully provided evidence that was found in on-line slack space and it can be used to hide files.

Spyridopoulos and Katos (2011) examined the feasibility of developing a digital forensics acquisition tool for the distributed environment. Using Google File System (GFS) and Kosmos File System (KFS)-types of CDFS-; they examined the digital forensics tools based on distributed system requirements published by NIST (2004). In conclusion, the authors emphasise the need to develop forensics-readiness-by-design approaches to handle cloud based crime.

Hegarty *et. al.* (2011) proposed a distributed digital signature detection framework based on the cloud storage platform. It is based on detecting the presence of illicit files in cloud storage through file signatures. The basic process of investigation is as follows: image the storage, compute the hash values of the files in the image and compare the generated hash values with known target malware file signatures.

We observed two schools of thoughts based on aforementioned research. The proposed approaches either can be applied as an add-on solutions as discussed in Hegarty *et. al.* (2011) or by design forensics readiness as in Spyridopoulos and Katos (2011) and Mulazzani *et. al.*

(2011).

Next, we will discuss digital forensics studies related to virtualisation.

4.2.2 Virtulisation

Virtualisation can be defined as a technology that facilitates the efficient use of resources either by integrating or separating systems in a logical manner. Scalability, cost effectiveness and automation in resource management are very important characteristics for the services offered in the cloud. For example, Amazon Elastic Compute Cloud (EC2) provides Virtual Machines (VMs) as a pay-per-use service where a user has full control and root privileges on the VMs.

The digital forensics of virtual environments has been discussed extensively in the literature (Barrett & Kipper, 2010; Birk & Wegener, 2011; Marturana et al., 2012). However, in this section, we target the literature that discusses digital forensics of distributed applications based on virtualisation as in Belorkar and Geethakumari (2011), Delport and Olivier (2012), Dykstra and Sherman (2013), Jawale and Narayanan (2011), Quick and Choo (2013) and Thorpe *et. al.* (2012). Given the correlation between Dimension II and III and to avoid repetition, Delport and Olivier (2012), Dykstra and Sherman (2013) and Thorpe *et. al.* (2012) will be discussed in Section 4.3.

Delport and Olivier (2012) proposed utilizing existing techniques such as Instance Relocation, Server Farming, address relocation, failover, sandboxing, Man-In-The-Middle (MITM) and Lets Hope For The Best (LHFTB) for cloud forensics. The proposed approaches aim to isolate the cloud based computing instances while maintaining the confidentiality, integrity and availability of legitimate users information.

Jawale and Narayanan (2011) studied the private cloud for Hosted Virtual Desktops (HVD) through simulation scenarios. The aim of the paper is to investigate whether current digital forensic procedures are adequate for use in cloud environments. Based on the findings, the authors concluded that to identify and extract evidence from VMs that are configured with persistent storage, current digital forensics procedures are suitable. However, identifying and extracting evidence in a cloud configured as multitenant architecture is not possible using current digital forensics procedures. The differences in the findings are not caused by the actual virtualisation technology but because of inherent characteristics of cloud environment namely multitenancy.

Belorkar and Geethakumari (2011) presented an approach to analyse cloud attacks in a Virtual Network Environment (VNE) using fuzzy clustering techniques. VNE are virtual machines that are connected using virtual network components e.g., virtual switches and virtual Network Interface Cards (NICs) (Kangarlou, Eugster, & Xu, 2009). In order to regenerate the events of an attack, VNsnaps was used to periodically take snapshots of the VNE. The authors concluded that the proposed method can be used to perform attack security analysis and it could be used by a CSP in providing security services.

4.2.3 Discussion

In security and digital forensics practices, it had always been evident that "born by design" solutions can produce the best results in maintaining security measures or to aid in digital forensics practices. One might argue that the forensics discipline can, in general, not select the design of the environments that will have to be investigated; however, to preserve public safety, government might oblige service providers to consider digital forensics while designing different services. As stated earlier in Section 4.1.2, the forensics readiness had been considered as the future research direction. However, Figure 4 shows that about 42% proposed by design solutions and 58% proposed add-on solutions.

To sum up, given the majority of studies of cloud forensics targets IaaS, 75% of technical solutions have been target virtualisation (both distributed and non distributed virtualisation) and 25% targets distributed computing solutions, as shown in Figure 5. Figure 6, shows the correlation between virtualisation/distributed computing and the add-on/by-

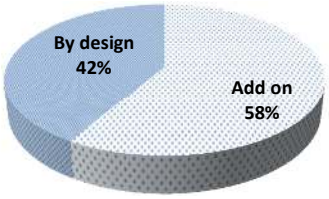

Figure 4 Proposed solution: Add-on vs. by Design

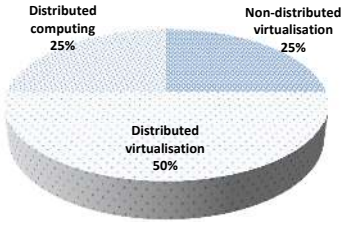

Figure 5 Proposed Solution Targeting Virtualisation vs. Distributed Computing

design solutions.

4.3 Dimension III: Forensics-Procedural-Based

In this section, the literature reviews are categorised based on the target digital forensics procedure as discussed in Section 2.2.1. Identification is defined in terms of whether the researchers identify the target digital forensics requirements they are trying to achieve. These requirements include evidence integrity, consistency and correctness (Vomel & Freiling, 2012). Another challenge is to collect, examine and reconstruct evidence from cloud based services. There are some efforts in proposing framework

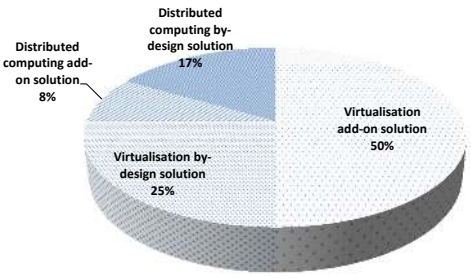

Figure 6 Technology Based vs. Add-on/By-design Literature

or algorithms to achieve forensically sound evidence extraction and reconstruction. In the analysis part, there exists two subgroups based on the target evidence, namely the data or meta-data analysis.

It is worth mentioning that there is no clear cut line between the literature of each section as some of the research aim to achieve multiple goals such as evidence collection and examination.

4.3.1 Identifying Forensics Requirements

There are two issues for which literature is lacking: (1) the ability in identifying the exact requirements and (2) how to formalize these requirements, which can be very challenging.

Vomel *et. al.* (2012) discussed the digital forensics requirements of memory snapshots in a distributed environment, which includes correctness, atomicity and integrity. The authors investigated formalizing these requirements for use later for analysis and testing. The identified requirements are designed for distributed systems at the level of a single computing resource such as CPU. It was distributed in the sense of having multiple processes that are sharing the same CPU and memory.

Patrascu *et. al.* (2013) aimed to achieve evidence correctness of events in a virtual environment. The authors propose a cloud forensics framework to monitor users activities by injecting an additional computational layers into the existing cloud IaaS deployment model.

Mishra *et. al.* (2012) was focused on enhancing the existing traditional digital forensics requirements to meet the needs of cloud forensics. This implies considering its characteristics, service and deployment models.

On the other hand, Sibiya *et. al.* (2013) proposed an incident scene formalization as a forensics requirement. Using a probability algorithm in assigning weights to malicious hosts connected to a victim host, the proposed solution can intelligently identify the resources an attacker requires to a victim host. The proposed solution ranks and prioritise the possible suspected IPs which as a result reduces the

amount of time and resource required to do the full IPs analysis that took place on the victim host.

4.3.2 Preservation

Ideally, if cloud computing entities such as the client, network and CSP could be acquired as per the legal notice, then the preservation, in its current definition, implies that activities of all these parties should be halted until the case is over. Practically, this is not the case in the cloud and it is not achievable.

As discussed by Almulla *et. al.* (2013) and Ruan *et. al.* (2011), because of different types of crime, it is nearly impossible to acquire the complete chain of dependencies in the cloud.

In this review paper, the scope of preservation is limited to utilizing the enabling cloud based technologies such as snapshots in preserving partial resources such as storage -data and/or metadata-, network logs, memory dumps, etc. A snapshot is a point-in-time copy of users storage and network related data.

The snapshot can be either a single VM snapshot e.g., single VM as a victim or distributed e.g., attack performed using distributed application. A distributed snapshot is defined in Chandy and Lamport (1985), as a point-in-time copy of distributed computing objects along with the channel communication messages while ensuring consistency.

The importance of a snapshot (either as storage or network dumps) in cloud forensics was discussed in Birk and Wegener (2011), Dykstra and Sherman (2012, 2011), and Quick and Choo (2013). However, limited efforts have been made to utilize these resources for digital forensics.

Belorkar *et. al.* (2011) (also discussed in Section 4.2.2) presented an approach to analyse cloud attacks based on event recognition using a fuzzy clustering technique. In order to regenerate the events of an attack, VNsnaps was used to periodically take snapshots of the VNE. The authors addressed three important requirements: (1) Snapshots contain detailed information of all components involved or affected by an attack which are globally consistent (Chandy & Lamport, 1985), (2) minimizing the system down-time in order to capture continuous snapshots and (3) ensuring that only the attack vector -files with above the desired threshold- were recorded.

4.3.3 Collection

In spite of requirement identification and digital evidence preservation, evidence collection is another challenge in cloud forensics. Investigators must maintain the "soundness" of the evidence, however, throughout the literature it was evident that digital forensics procedures as they are currently defined might be impractical for cloud based crimes and incidents.

Jawale and Narayanan (2011) developed two case scenarios of Hosted Virtual Desktop (HVD) to evaluate the applicability of current digital forensics procedure when: (1) the suspect was known within the organization, and (2) an unknown suspect and evidence needs to be extracted from a shared resource and multi-tenant environment. The latter drove the authors to draw the conclusion that current digital forensics methodologies require enhancement to be applied to cloud based crimes.

Chung *et. al.* (2012) discussed the impact of cloud services such as Amazon S3, EverNote and Google Docs and possible artefact that can be collected from client PCs and smart phones. Window 2000, XP, Vista, Windows 7 and Mac OS X lion were used as PC OSs. iOS and Android as smart phone OSs. The authors proposed a process model for the forensics investigation of cloud based services.

Similarly, Hale (2013) discussed the digital artefact results after an Amazon Cloud Drive was used either as a desktop or via an internet browser. Based on their findings, the authors propose a forensics method to be followed by examiners to collect the most relevant evidence from these artefacts.

Zawoad and Hasan (2012) discussed evidence collection from a different angle. The aim was to prove the evidence after collecting it from cloud environment. This was achieved using a Proof of Past Data Possession (PPDP) algorithm (Bloom, 1970). To maintain the forensically

sound evidence, authors deployed secured cryptographic scheme in generating PPDP. PPDP is based on Bloom filters where it depends on the probability used to check whether an element is a member of a set or not.

4.3.4 Examination

Once the investigators successfully extract the evidence in a sound manner, the next challenge is to examine the data by reconstructing the evidence and create a time line of events. There have been limited efforts made in proposing solutions for event reconstruction in cloud forensics.

One approach has been discussed in Zowad and Hasan (2012). Another discussed by Dykstra and Sherman (2013), where a cloud forensics tool was introduced to extract and reconstruct the evidence gathered from a cloud environment. The aim was to overcome the non-trivial remote data acquisition challenges, such as integrity, by using hash trees to store logs and using cryptographic hashes for the returned results.

4.3.5 Analysis

There are two categories for collected data from cloud services: (1) actual data or user content data and (2) the information related to the data (meta-data). In an ideal scenario both the data and its meta-data are important for investigations. In the distributed architecture of cloud computing the possibility of evidence acquisition depends on its availability and the access control provided by the CSP. As discussed earlier in this section, most of the studies aim to satisfy more than one forensic procedure. To avoid repetition, we will next discuss studies aimed at evidence analysis based on the two categories;

Content or Data Analysis In some other cases e.g., claim of illegal videos owner-ship by a suspect, both the meta-data and the data are required. Possible approaches to acquire and analyse both data and its meta-data are discussed in Quick and Choo (2013), Hale (2013), Dykstra and Sherman (2012), Dykstra and Sherman (2013), and Martini and Choo (2012). However, to the best of our knowledge, Dykstra and Sherman (2012) was the only research target digital forensics analysis of data.

Meta-data Analysis The majority of research as in Patrascu and Patriciu (2013), Chung *et. al.* (2012), Sibiya *et. al.* (2013), Zawoad and Hasan (2012), Sang (2013), Thorpe *et. al.* (2012) argue for a sufficiency of meta-data for forensics analysis. This is due to a number of reasons. First, the fact that the storage is located on the CSP premises and corresponding legal implications increase the complexity of evidence acquisition and analysis. Second, the characteristics of cloud computing such as scalability and multi-tenancy raise the possibilities of information exposure of other users data. Finally, in most of the cases investigators need to reproduce crime events which requires time stamps to prove or refute a hypothesis. In this case, meta-data can be sufficient to achieve these goals.

4.3.6 Discussion

Given the coherency and the dependency of digital forensics procedures, the literature has been analysed by counting the related studies per procedures. As shown in Figure 7, the majority of the research focused on analysis, where the assumptions were that the data was collected and preserved safely. On the other hand, preservation might be extremely difficult (if not impossible) due to the dynamicity of cloud environment and current practices of digital forensics. Limited research focused on data (the content) analysis and one possible reason might be due to the sensitivity of data, privacy, lack of isolation and higher availability of the meta-data in comparison to the actual data.

Beside the aforementioned dimensions, one interesting result of the analysis is that the majority of the proposed solutions aim to perform digital forensics activities (identification, preservation, collection and examination) for evidence that resides in the cloud (in-cloud) rather than using the cloud resources to conduct digital forensics (on-cloud). (See Figure 8).

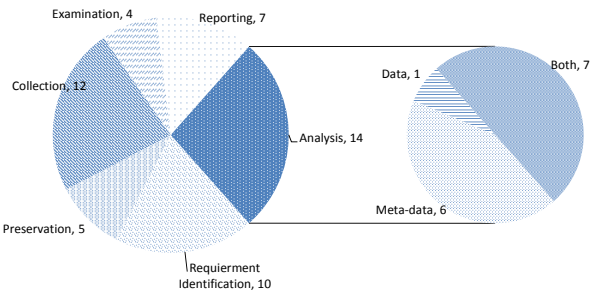

Figure 7 Procedural based Literature Statistics

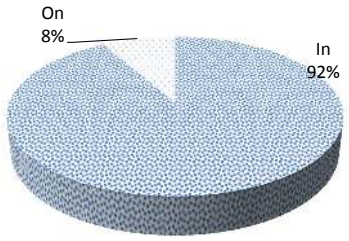

Figure 8 In-cloud vs. On-cloud Statistics

5. CLOUD FORENSICS AND STANDARDISATION

Given that the cloud computing is the current technology trend, several standardisation bodies have initiate a cloud forensics centric working group to cope with the increasing adoption of cloud services.

The initiation can be either by forming a cloud forensics working group or enhancing existing security and digital forensics standards or guidelines. As discussed in Almulla *et. al.* (2013), the Cloud Security Alliances (CSA) (2009), initiated Cloud Computer Emergency Response Team (CloudCERT) to prepare for and respond to vulnerabilities, threats, and incidents in the cloud. The European Network and Information Security Agency (ENISA) (Haeberlen & Dupr, 2012) states the need to research in the field of digital forensics investigations in cloud. The National Institute of Standards and Technology (NIST) (2014b) formed the Cloud Computing Forensic Science Working Group (NCC-FSWG) as an integral part of the overall NIST effort to facilitate adoption of cloud services for the United States Government. In June 2014, a draft NISTIR 8006 "NIST Cloud Computing Forensic Science Challenges" was published (NIST, 2014b).

A recently published report from CSA namely "Mapping the forensics standard ISO/IEC 27037 to cloud computing" discussed in detail the international standards of cloud forensics and its integration to Service Level Agreement (SLA). A detailed discussion was presented in identifying the difference between the traditional and cloud forensics (ISO/CSA, 2014).

The Association of Chief Police Officers (ACPO) group has published a "Good Practice Guide for Computer Based Evidence" (ACPO, 2014) , which contains four main principles that should be used during investigations that may involve digital evidence. Taylor *et. al.* (2011), state that the guidelines must be followed in order to provide proof that the integrity of the presented evidence has not been compromised before coming into the control of the forensics investigator. There were originally five principles, but due to the evolution of the technology involved in crimes, the last two were combined to the current principle number four.

These principles were defined to suit computer based forensics. However, cloud computing has had an impact on these principles and research is being undertaken as to how these principles will be influenced (OShaughnessy & Keane, 2013).

6. AIDED TOOLS AND TEST ENVIRONMENTS

In the process of identification, investigators need to identify the most appropriate tools required to examine evidence efficiently. As discussed earlier, besides widely accepted digital forensics tools such as EnCase (EnCase, 2014) and the Forensics Tool Kit (FTK) (FTK, 2014), there is research required to either modify existing tools or to introduce new tools tailored to meet cloud forensics needs. For instance, outsourcing infrastructure in most of the cloud service models increases the need for tools that are capable of performing analysis and examination using a secure remote connection. Also,

it requires digital forensics tools to acquire and process memory and network dumps. Figure 9 shows that around 95% of the proposed solutions used existing tools.

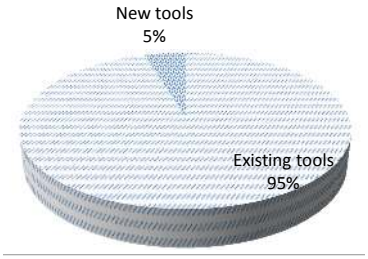

Figure 9 Percentage of using Existing tools vs. Proposing new Tools in the Literature

A summary of most of the tools used to perform digital forensics evidence extraction or analysis are listed in Table 2.

To test the theoretical approaches, researchers need to identify a suitable cloud test environment for their experiment test-bed. Table 3 summarises the test environments that were used that could suit a cloud computing project in general and forensics scenarios in particular. These environments are designed with the cloud computing structure and characteristics in mind.

7. MIND MAP, RESEARCH GAPS AND SUMMARY

7.1 Mind map

The focus of this state-of-the-art review is on publication results for search of "cloud forensics" as a keyword since 2010, a total of 24 publications were identified. However, there are studies (Kangarlou et al., 2009; Bloom, 1970; Vomel & Freiling, 2012) that have been discussed because of the importance of technology in understanding the literature. In this section, the mind map has been divided into two. First, Figure 10 discusses the three dimensions. Second, Figure 11 presents the different forensics tools, standardisation and research gaps.

7.2 Research Gaps

As a result of analysis of the related literature discussed in this state-of-the-art review, we were able to spot areas of weakness and possible research gaps in the study of cloud forensics.

Complete evidence It is a process of seizing all digital devices present in the crime scene. In cloud computing, it is impractical to seize all digital devices due to the massive storage capacity, privacy issues of other legitimate users and the impact on the course of business.

Formalisation Several terms are discussed in the literature which describe the metrics needed for cloud forensics. However, the literature lacks a formal model to describe these metrics. As discussed earlier, sufficiency and necessity need to be formalized to measure sufficiency of a portion of evidence that can be extracted from cloud environment.

Forensics procedures Given different cloud service models, a one size fits all forensics process might not be a solution. Current procedures might fit some of the models, however, the specific characteristics of the other models create challenges for the investigators in acquiring evidence from the cloud. This is due to the variation in the control levels among the user and the CSP in each service model.

Scalability and load balancing The dynamic nature of resource allocation and deallocation creates a serious challenge in the investigation process. How to uniquely identify each resource and whether it is possible to record the history of the resource allocation and de-allocations are some of the questions which need to be researched. In spite of the effectiveness of load balancing to increase the performance and utilisation of data centres resource, it creates challenge when these resources need to be investigated.

Data redundancy In cloud, to increase the availability; multiple copies of user's data will be created and stored around the globe. Given the different methodologies that the CSP used to create these copies and the different retention policies CSP follow in termination of provided

Table 2 Summary of Digital Forensic Tools used in the Literature

Used Tool(s)	Possible usability
Virtual Forensics Computing (GetData, 2014)	To boot a forensics image of a suspect.
WireShark (Riverbed, 2014)	Captures network traffic between VM and the CSP
Microsoft Expression Encoder4 (Microsoft, 2014)	VM windows video recorder
FTK Imager (FTK, 2014) EnCase (EnCase, 2014)	Acquisition of memory and disk images.
FTK Remote Agent (Dykstra & Sherman, 2013) Encase Remote Agent (Dykstra & Sherman, 2013)	Acquisition of evidence remotely
X-Ways (Xway, 2014)	Acquisition of Windows and Linux live system
Sleuth kit HaDoop (Carrier, 2014)	Faster processing of video files for forensics acquisition and analysis (initial stage framework)
FROST (Dykstra & Sherman, 2013)	Digital forensics tools for the OpenStack cloud platform
XenAccess (Xen, 2014)	Xen VM introspection library (Hypervisor level)
VMWatcher (Calavera, 2014)	VMware VM introspection (Hypervisor level)
VMwall (Srivastava & Giffin, 2014)	VMware VM introspection (VM level)

Table 3 Summary of Test Environments used for Cloud Forensics

Cloud test environment	Description	Open-source/ Proprietary
BonFire (BonFire, 2014)	An EU project enables operating a multi-site cloud-based facility on top of different infrastructure testbeds such as Emulab	Proprietary
Eucalyptus (Eucalyptus, 2014)	A software used to build Amazon Work Station (AWS) private and public cloud	Open-source
OpenNebulla (OpenNebula, 2014)	An industry standard used to provide virtual datacentres and IaaS	Open-source
CloudSim (CloudSim, 2014)	A solution to create large scale cloud computing data center, virtual hosts and capability of analysis for network traffic	Open-source
Emulab (Emulab, 2014)	Public facility available for researchers to develop, debug and evaluate their systems	Open-source
OpenStack (Apache, 2014)	A project used to create various IaaS architectures such as storage, compute and network	Open-source
Rackspace (Rackspace, 2014)	Based on OpenStack and provides IaaS	Open-source
Amazon (AmazonS3, 2014) (AmazonEC2, 2014) (AmazonEBS, 2014)	An appropriate solution provide various flavour of IaaS, Amazon Simple Store Service(S3) as storage, Amazon Elastic Comput Cloud (EC2) as a computation required for AWS. Amazon Elastic Block Store (EBS) used for backups	Proprietary

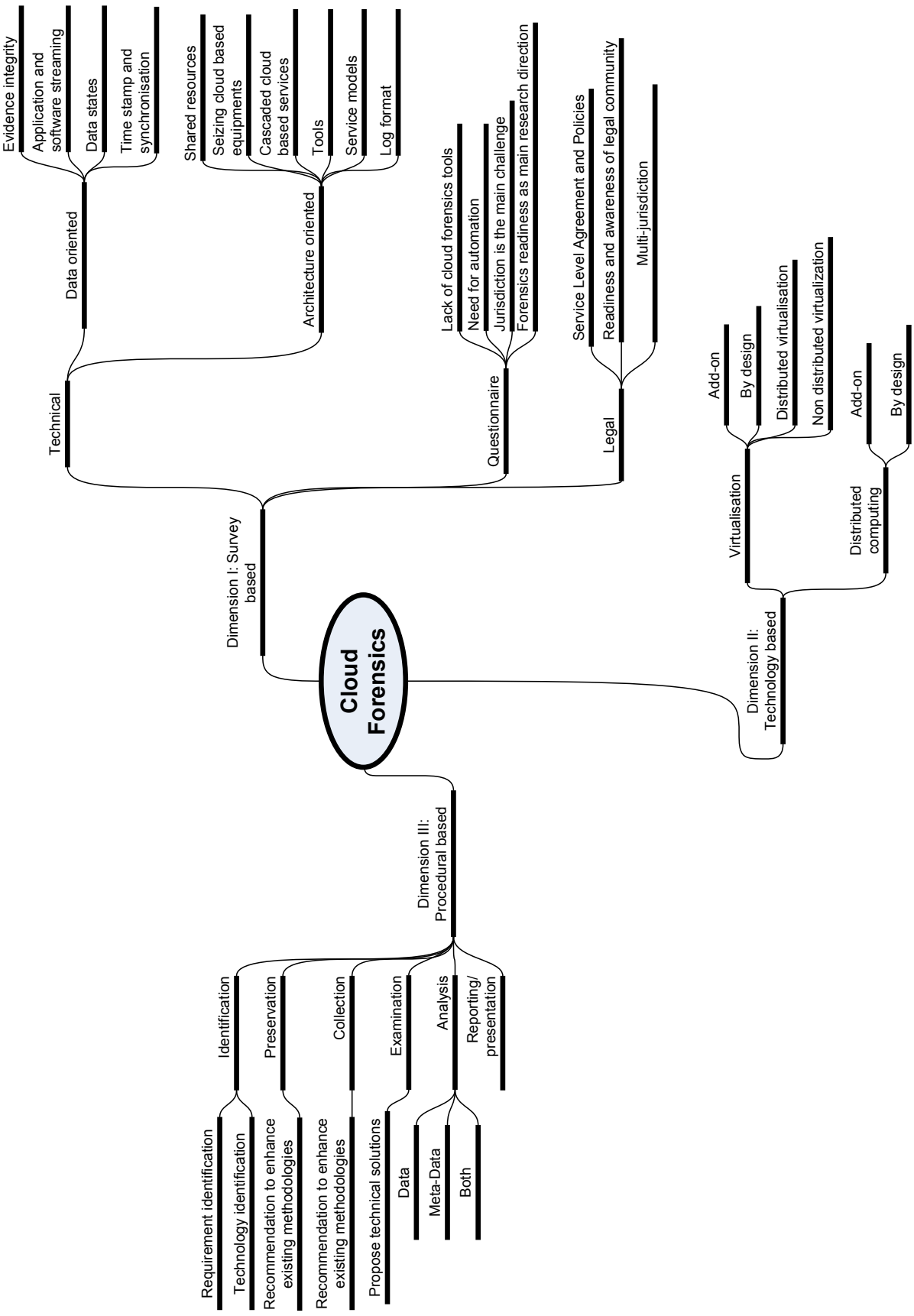

Figure 10 Mind map: State-of-the-art Dimensions

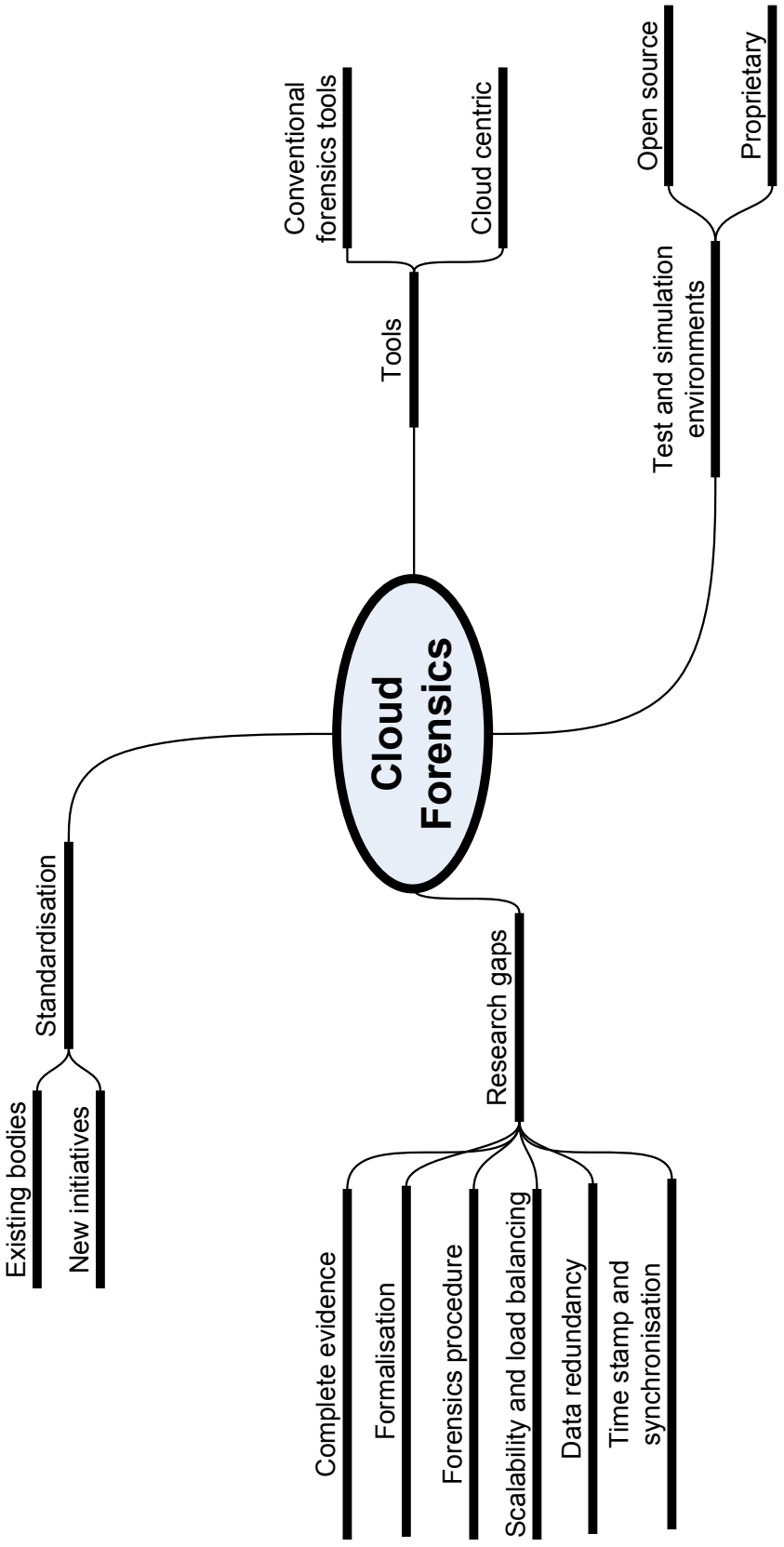

Figure 11 Mind map Tools, Standardisation and Research Gaps

services, it is crucial to research whether or not these copies are traceable?

Time stamp and synchronisation Unlike computer forensics, the evidence is scattered over the participants of cloud services, that includes CSP and users. Time can be considered as a challenge from two perspectives. First, in terms of the time required to collect, examine and analyse the evidences. Second, in terms of the time synchronisation between the gathered digital artefacts.

7.3 Summary

This review paper highlights the state-of-the-art in digital forensics of cloud computing. Recently the term "cloud forensics" has a strong presence in the field of digital forensics. In this state-of-the-art review, we have pinpointed when the term was actually used as a keyword in the literature with aid of search engine SUMMON. This paper categorises the literature in three main dimensions: (1) survey-based, (2) technology-based and (3) forensics-procedural-based. Given the increasing impact of cloud forensics on the standardisation process and its need, this paper presents most of the international standardisation bodies and their efforts to cope with the current trend of cloud forensics. Analysis of the aforementioned categorisation has been discussed to aid in identifying the areas that need more research efforts.

REFERENCES

ACPO. (2014). Good Practice Guide for Computer-Based Electronic Evidence, Official released version. (Retrieved Jul 21, 2013 from `http://www.7safe.com/electronic\_evidence/ACPO\_guidelines\_computer\_evidence.pdf`)

Al Fahdi, M., Clarke, N., & Furnell, S. (2013). Challenges to digital forensics: A survey of researchers practitioners attitudes and opinions. In *Information Security for South Africa.*

Almulla, S., Iraqi, Y., & Jones, A. (2013). Cloud forensics: A research perspective. In *9th International Conference on Innovations in Information Technology (IIT)* (pp. 66–71).

AmazonEBS. (2014). Elastic Block Store. (Retrieved Mar 04, 2014 from `http://aws.amazon.com/ebs/`)

AmazonEC2. (2014). Elastic Compute Cloud. (Retrieved Mar 04, 2014 from `http://aws.amazon.com/ec2/`)

AmazonS3. (2014). Simple Storage Service. (Retrieved Mar 04, 2014 from `http://aws.amazon.com/s3/`)

Apache. (2014). OpenStack. (Retrieved Mar 04, 2014 from `https://www.openstack.org/`)

Barrett, D., & Kipper, G. (Eds.). (2010). *Virtualization and forensics: A digital forensic investigator's guide to virtual environments.* Elsevier.

Belorkar, A., & Geethakumari, G. (2011). Regeneration of events using system snapshots for cloud forensic analysis. In *Annual IEEE India Conference (INDICON)* (pp. 1–4).

Birk, D., & Wegener, C. (2011). Technical issues of forensic investigations in cloud computing environments. In *Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)* (pp. 1–10).

Bloom, B. H. (1970). Space/Time trade-offs in hash coding with allowable errors. *Communications of the ACM*, *13*(7), 422-426.

BonFire. (2014). BonFire. (Retrieved Mar 04, 2014 from `http://www.bonfire-project.eu/services`)

Calavera, D. (2014). VMwatcher. (Retrieved Mar 04, 2014 from `https://github.com/calavera/vm-watcher`)

Carrier, B. (2014). Sleuth kit Hadoop. (Retrieved Mar 04, 2014 from `http://www.sleuthkit.org/tskhadoop/`)

Chandy, M., & Lamport, L. (1985). Distributed snapshots: determining global states of distributed systems. *ACM Transaction of Computer Systems*, *3*(1), 6375.

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud stor-

age services. *Digital Investigation*, *9*(2), 81-95.

CloudSim. (2014). The Cloud Computing and Distributed Systems. (Retrieved Nov 27, 2014 from `http://www.cloudbus.org/cloudsim/`)

CSA. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing. (Retrieved Mar 04, 2014 from `https://cloudsecurityalliance.org/csaguide.pdf`)

Delport, W., & Olivier, M. (2012). Isolating instances in cloud forensics. In *IFIP International Conference Digital Forensics* (pp. 187–200).

Dykstra, J., & Sherman, A. (2011). Understanding issues in cloud forensics: Two hypothetical case studies. *Digital Investigation*, *2011*(3), 19-31.

Dykstra, J., & Sherman, A. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9, Supplement*, 90-98.

Dykstra, J., & Sherman, A. (2013). Design and implementation of FROST: digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, *10*, 87-95.

Emulab. (2014). Emulab. (Retrieved Mar 04, 2014 from `https://www.emulab.net/`)

EnCase. (2014). Guidance Software. (Retrieved Jun 05, 2014 from `http://www.guidancesoftware.com/forensic.htm`)

Eucalyptus. (2014). Eucalyptus Systems, Inc. (Retrieved Mar 04, 2014 from `https://www.eucalyptus.com/`)

FTK. (2014). Forensics tool kit (FTK) computer forensics software. (Retrieved Jun 05, 2014 from `http://accessdata.com/products/computer-forensics/ftk`)

George, E., & Mason, S. (2011). Digital evidence and cloud computing. *Computer Law and Security Review*, *27*, 524-528.

GetData. (2014). Virtual Forensics Computing. (Retrieved Mar 04, 2014 from `http://www.virtualforensiccomputing.com/`)

Grispos, G., Storer, T., & Glisson, W. (2012). Calm before the storm: The challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics*, *4*, 2-11.

Haeberlen, T., & Dupr, L. (2012). *Cloud computing: Benefits, risks and recommendations for information security* (Tech. Rep. No. 2). Heraklion, Crete, Greece: European Union Agency for Network and Information Security.

Hale, S. (2013). Amazon cloud drive forensic analysis. *Digital Investigation*, *10*(3), 259-265.

Hegarty, R., Merabti, M., Shi, Q., & Askwith, B. (2011). Forensic analysis of distributed service oriented computing platforms. In *12th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting.*

Hooper, C., Martini, B., & Choo, K. (2013). Cloud computing and its implications for cybercrime investigations in australia. *Computer Law and Security Review*, *29*(2), 152-163.

ISO/CSA. (2014). Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing : Cloud Security Alliance. (Retrieved Feb 06, 2014 from `https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf`)

Jawale, N., & Narayanan, A. (2011). Organisational preparedness for hosted virtual desktops in the context of digital forensics. In *9th Australian Digital Forensics Conference,* (pp. 65–75).

Kangarlou, A., Eugster, P., & Xu, D. (2009). Vnsnap: Taking snapshots of virtual networked environments with minimal downtime. In *IEEE/IFIP International Conference on Dependable Systems Networks DSN* (pp. 524–533).

Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012). Digital forensics in the cloud computing era. In *IEEE Globecom Workshops*

(GC Wkshps) (pp. 775–780).

Martini, B., & Choo, K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, *9*(2), 71-80.

Marturana, F., Me, G., & Tacconi, S. (2012). A case study on digital forensics in the cloud. In *2012 International Conference on Cyber Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 111–116).

Microsoft. (2014). Microsoft Expression Encoder 4. (Retrieved Mar 04, 2014 from `http://www.microsoft.com/en-us/download/details.aspx?id=18974`)

Mishra, A., Matta, P., Pilli, E., & Joshi, R. (2012). Cloud forensics: State-of-the-art and research challenges. In *2012 International Symposium on Cloud and Services Computing (ISCOS)* (pp. 164–170).

Mulazzani, M., Schrittwieser, S., Leithner, M., Huber, M., & Weippl, E. (2011). Dark clouds on the horizon: Using cloud storage as attack vector and online slack space. In *Proceedings of the 20th USENIX Conference on Security.*

NIST. (2004). Digital Data Acquisition Tool Specification. (Retrieved Mar 12, 2014 from `http://www.cftt.nist.gov/Pub-Draft-1-DDA-Require.pdf`)

NIST. (2014a). Guide to Integrating Forensics Techniques into Incident Response. (Retrieved Jun 05, 2014 from `http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf`)

NIST. (2014b). NIST Cloud Computing Forensics Science Challenges. (Retrieved Jun 29, 2014 from `http://csrc.nist.gov/publications/drafts/nistir-8006/draft\_nistir\_8006.pdf`)

OpenNebula. (2014). OpenNebulla. (Retrieved Mar 04, 2014 from `http://opennebula.org/about/`)

OShaughnessy, S., & Keane, A. (2013). Impact of cloud computing on digital forensic investigations. In *Advances in Digital Forensics* (pp. 291–303).

Patrascu, A., & Patriciu, V. (2013). Beyond digital forensics: A cloud computing perspective over incident response and reporting. In *8th International Symposium on Applied Computational Intelligence and Informatics (SACI)* (pp. 455–460).

Quick, D., & Choo, K. R. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation*, *10*(3), 266-277.

Rackspace. (2014). Rackspace. (Retrieved Mar 04, 2014 from `http://www.rackspace.com/`)

Reilly, D., Wren, C., & Berry, T. (2010). Cloud computing: Forensic challenges for law enforcement. In *International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 1–7).

Riverbed. (2014). Wireshark. (Retrieved Mar 04, 2014 from `http://www.wireshark.org/`)

Ruan, K. (2013). *Cybercrime and cloud forensics: applications for investigation processes.* Information Science Reference.

Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation*, *10*(1), 34–43.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics: An overview. In *Advances in Digital Forensics VII* (pp. 16–26).

Sang, T. (2013). A log based approach to make digital forensics easier on cloud computing. In *Third International Conference on Intelligent System Design and Engineering Applications (ISDEA)* (pp. 91–94).

Sibiya, G., Fogwill, T., & Venter, H. (2013). Selection and ranking of remote hosts for digital forensic investigation in a cloud environment. In *Information Security for South Africa* (pp. 1–5).

Spyridopoulos, T., & Katos, V. (2011). Requirements for a forensically ready cloud storage service. *International Journal of Digital Crime and Forensics (IJDCF)*, *3*(3),

19–36.

Srivastava, A., & Giffin, J. (2014). *Tamper-resistant, application-aware blocking of malicious network connections*. (Accessed 04-03-2014)

Summon. (2014). SpringShare. (Retrieved Feb 22,2014 from `http://www.serialssolutions.com/en/resources/detail/introducing-summon-2.0-discovery-reinvented`)

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security*, *3*, 4–10.

Thanh, T., Mohan, S., Choi, E., Kim, S., & Kim, P. (2008). A taxonomy and survey on distributed file systems. In *Fourth International Conference on Networked Computing and Advanced Information Management (NCM08)* (pp. 144–149).

Thorpe, S., Ray, I., Grandison, T., & Barbir, A. (2012). Cloud log forensics metadata analysis. In *36th IEEE Annual Computer Software and Applications Conference Workshops (COMPSACW)* (pp. 194–199).

Vomel, S., & Freiling, F. C. (2012). Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition. *Digital Investigation*, *9*(2), 125-137.

Wolthusen, S. D. (2009). Overcast: Forensic discovery in cloud environments. In *Fifth International Conference on IT Security Incident Management and IT Forensics (IMF)* (pp. 3–9).

Xen. (2014). XenAcess Library. (Retrieved Mar 04, 2014 from `http://code.google.com/p/xenaccess/`)

Xway. (2014). X-way Software Technology AG. (Retrieved Mar 04, 2014 from `http://www.x-ways.net/`)

Zargari, S., & Benford, D. (2012). Cloud forensics: Concepts, issues, and challenges. In *Third International Conference on Emerging Intelligent Data and Web Technologies (EIDWT)* (pp. 236–243).

Zawoad, S., & Hasan, R. (2012). I have the proof: Providing proofs of past data possession in cloud forensics. In *International Conference on Cyber Security (CyberSecurity)* (pp. 75–82).

