Calm before the Storm: The Emerging Challenges of Cloud Computing in Digital Forensics

George Grispos

William Bradley Glisson

Tim Storer

University of Glasgow

last revision 2413 by tws on 2011-08-09 10:55:05Z

Abstract

Cloud computing is a rapidly evolving technological phenomenon. Rather than procure, deploy and manage a physical IT infrastructure to host its software applications, organizations are increasingly deploying the same into remote, virtualized environments, which can be hosted and manage by third party providers. This development in the IT landscape has significant implications for digital forensic investigators, toolkit developers and corporate compliance and audit departments. Much of digital forensic practice assumes careful control and management of IT assets (particularly data storage) during the conduct of an investigation. This paper summarises the key aspects of cloud computing and analyses how established digital forensic procedures will be invalidated in this new environment. Several immediate research agendas are proposed to begin addressing these new challenges.

Contents

1 Introduction

Cloud computing technologies have significant potential to revolutionise the way organisations provision their information technology (IT) infrastructure. Migration to cloud computing involves replacing much of the traditional IT hardware infrastructure found in an organization's data centre (including servers, racks, network switches and air conditioning units), with virtualized, remote, on-demand software services, configured for the particular needs of the organisation. These services can be hosted and managed by the user organization, or by third party providers. Consequently the software and data which comprise the service may be physically stored across many different locations, potentially with a wide geographic distribution.

There have been several predictions of substantial market growth in cloud services over the next few years. Gens has speculated that spending on cloud services will grow by 30% in 2011 [Gens, 2010]. A Gartner press release forecast cloud service worldwide revenue to reach $68.3 billion in 2010, an increase of 16.6% from the 2009 revenue of $58.6 billion, and goes on to claim that cloud service revenues will reach $148.8 billion in 2014 [Pring et al., 2010]. A study at the end of 2010 predicted that within the next three years, approximately 40% of small and medium businesses (SMBs) expect to be using three or more cloud services and migrate their data into the cloud [Kazarian and Hanlon, 2011]. There is some speculation that new and SMBs will benefit the most in the coming years, with cloud computing allowing these organizations to utilize critical IT infrastructure that was once only accessible to larger corporations [Schubert et al., 2010].

The use of cloud computing has potential benefits to organisations: flexibility and efficiency. Virtualized services provide greater flexibility over traditional IT infrastructure, because services can be rapidly re-configured or scaled to meet new and evolving requirements, without the need to acquire new and potentially redundant hardware. Complementary to this, the use of cloud computing can reduce the costs of providing IT services, by

eliminating redundant computing power and storage, reducing support requirements and reducing fixed capital commitments. A recent case study found that in certain scenarios a 37% cost saving could be obtained by an organization which migrates its information from a data-centre to a cloud provider [Khajeh-Hosseini et al., 2010].

However, the use of cloud computing presents significant challenges to the users of clouds (both individuals and organisations), as well as regulatory and law enforcement authorities. It has been estimated that cyber-crime will cost the British economy £27 billion per year in the coming years, with businesses accounting for nearly £21 billion of losses largely due to the theft of intellectual property and espionage [Detica, 2011]. It is unlikely that users of cloud computing services and technologies will be less exposed to these risks. The security of confidential corporate and private data remains one of the greatest concerns organizations have when they consider cloud computing [Curtis et al., 2010]. Recent reports have noted Botnet attacks on Amazon's cloud infrastructure [Amazon, 2009] and the compromise of Gmail by (alleged) Chinese hackers [Blumenthal, 2010], illustrating that cloud computing platforms are already a target for malicious activities.

When security breaches, attacks or policy violations occur it may be necessary to conduct a digital forensic investigation. However, existing digital forensics principles, frameworks, practices and tools are largely intended for off line investigation, which assumes that the storage media under investigation is completely within the control of the investigator. Conducting investigations in a cloud computing environment presents new challenges, since evidence is likely to be ephemeral and stored on media beyond the immediate control of an investigator. This paper analyses the potential challenges posed by cloud computing technologies for digital forensics in the context of the Association of Chief Police Officers (ACPO) digital forensic principles, and the DFRW Investigative Process Model (DIP). These two frameworks are commonly cited as the basis of good digital forensic practice, for example Owen and Thomas [2011], Ieong [2006], Hunton [2011].

This paper is structured as follows. Section 2 summarises developments in cloud computing technology, and the main categories of cloud computing, illustrating how these developments differ from traditional computing platforms and infrastructures. Section 3 outlines a number of proposed models for digital forensic investigation processes, and assesses how the adoption of cloud computing may invalidate the assumptions made in these existing frameworks. Section 4 reviews related work on cloud computing and digital forensics. Section 5 discusses some immediate avenues of research to address the issues raised by the analysis. Finally, Section 6 draws some conclusions and summarises the key challenges in conducting digital forensic investigations in cloud environments.

2 Cloud Computing

A cloud has several uses, offering a variety of services and can be deployed in more than one way. Consequently, several definitions of cloud computing have been proposed for a variety of purposes [Mell and Grance, 2011, Wyld, 2009, Schubert et al., 2010]. Schubert et al. [2010] defines cloud computing as:

> "a 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)" [Schubert et al., 2010].

while The Open Cloud Manifesto Consortium [2009] consortium defines the key aspects as:

> "the ability to scale and provision computing power dynamically in a cost-efficient way and the ability of the consumer (end user, organization, or IT staff) to make the most of that power without having to manage the underlying complexity of the technology" [The Open Cloud Manifesto Consortium, 2009].

The key aspects from a digital forensic perspective is that a cloud is defined as a scalable, virtualized, distributed computing platform, whose shared resources are accessed remotely by users through a network.

There are three main levels of service for users of cloud computing [Mell and Grance, 2011]:

- in the *Software as a Service* (SaaS) model, a client can make use of software applications made available from the cloud provider. Typically, users interact with SaaS applications using a web-browser. An example of SaaS is the Google Apps[1] suite offered by Google. Clients can use this service to deploy an email and collaboration platform within their organizations, and make use of Google Docs, Calendar, Gmail and other productivity applications. All data generated by the use of the applications is stored in the cloud;

- the *Platform as a Service* (PaaS) provides an environment for clients to create and host applications. The client does not need to spend capital buying the underlying hardware or the software to develop and host the application. PaaS also includes cloud providers offering database management systems such as Amazon SimpleDB[2]; and

- *Infrastructure as a Service* (IaaS) is the leasing of virtualized computing resources such as processing power, volatile memory and persistent storage space to host virtual machines. IaaS products include Amazon EC2[3] which allows clients to create and launch virtual machines running a variety of operating systems. These can then be loaded with customer-specified applications, just as for any other server. The virtual machine image can be stored and re- deployed, according to the client's requirements.

[1] `http://www.google.com/apps/intl/en/business/index.html`
[2] `http://aws.amazon.com/simpledb/`
[3] `http://aws.amazon.com/ec2/`

The manner in which services are deployed in a cloud can influence the evidence available to an investigator and the way it is collected. For example, IaaS platforms offer an interface to a user (and investigator) that is essentially the same as a remote physical server, although the data which represents the server is inherently more transient. Alternatively, the SaaS and PaaS models restrict the flexibility with which users can interact with a cloud platform, by offering a restricted set of applications, or specifying the constraints within which new software can be created. The storage of data on these services is controlled by the cloud owner, rather than the user.

In addition to the different levels of deployment, Krutz and Vines [2010] have proposed categorising the organizational deployment for clouds, with consequent impact on the geographical location and storage architecture of data held:

- in a *private* cloud, the infrastructure is operated solely by the organization who owns the cloud. This cloud will more likely be found within the same geographical location as the owning organization and be within its administrative control, and include only that same organization's data;

- a *community* cloud is shared between several organizations, either because of a common organisational goal, or in order to pool IT resources. Community clouds may be located within one or more of the community organisation's premises, and will be administered by the community;

- *public* clouds will usually be owned by a provider organization, which will maintain the cloud facilities in one or more corporate data centres. The administrative control of the cloud resources will therefore reside with the provider, rather than the user. Consumers will lease virtual storage and compute resources from the provider as required. A public cloud will therefore likely contain data from more than one user; and

- a *hybrid* cloud is a composition of two or more of the above deployment options. Hybrid clouds can be used to provide load-balancing to multiple clouds. For example, an organization may have exhausted the available resources within its private cloud, and so incorporate resources available on lease from a public cloud.

A consequence of these different organizational configurations may have an impact on the way that data can be collected as evidence. In particular, the data held in a cloud may be physically stored in one or more geographically distributed locations, making the determination of which legal framework and procedures to apply to the evidence gathering process difficult.

In summary, multiple deployment options and the variety of services offered to cloud users introduce new challenges when conducting digital forensic investigations in these environments. The next section of this paper summarises various models used in digital forensics investigations.

3 Digital Forensics in Cloud Environments

ACPO [2007] proposes four principles of digitial forensic practice:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third

party should be able to examine those processes and achieve the same result.

4. The person in-charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The guide is primarily intended for law enforcement investigators, but has also been adopted by the digital forensics community in the United Kingdom (UK). There is an expectation that evidence used in courts produced from a digital forensics investigation will be gathered by following these guidelines (although it is unclear how this determination is made in practice).

Since 2001, various frameworks and process models have also been proposed for conducting a digital forensics investigation [Baryamureeba and Tushabe, 2004, Carrier and Spafford, 2003, 2004, Reith et al., 2002]. The First Digital Forensics Research Workshop (DFRW) defined the term 'digital forensics' and proposed a process model, which they deemed could be applied to all investigations in both research and practitioners [Palmer, 2001]. This was the first attempt to define how a digital forensics investigation should be conducted. The model identifies a linear process, which includes stages of identification, preservation, collection, examination, analysis and presentation. As Palmer noted, the conference agreed that this model still required further work and as such was not deemed to be complete.

The Abstract Digital Forensics Model builds on the work from the DFRW and is effectively an expansion of the DIP Model [Reith et al., 2002]. It adds Preparation, Approach Strategy and Returning Evidence phases to the DIP Model, as well as describing the phases, something which the DIP Model lacked.

Carrier and Spafford [2003] proposed the Integrated Digital Investigation Process, based upon upon "theories and techniques from the physical investigation world". The authors

base their model on 'physical' crime scene principles and methods. The process model is based upon 17 phases which are broken into five groups: readiness, deployment, physical crime scene investigation, digital crime scene investigation and review.

Finally, The Enhanced Digital Investigation Process Model is an enhancement of the model proposed by Carrier and Spafford, consisting of five major phases [Baryamureeba and Tushabe, 2004]:

- the *readiness* is concerned with ensuring the investigator has the correct training and infrastructure to handle an investigation;
- the *deployment* phase specifies means for detecting an incident has occurred and beginning the process of conducting an investigation;
- during *traceback* the crime scene is examined and the devices worthy of investigation are discovered;
- the *dynamite* phase is associated with collecting and analyzing items seized from the crime scene and collecting evidence from these devices; and
- the *review* phase is concerned with reviewing the entire investigation and discovering areas of improvement.

All of these guidelines were developed prior to the advent of cloud technologies and largely assume that the investigator has physical access and control over the target system or device, and in particular, its storage media. This assumption is likely to be invalidated when investigating activity in a cloud environment.

This section analyses the challenges raised by cloud computing with respect to existing models of digital forensics investigations described above. The discussion is based principally on the DIP model. The DIP model provides a comprehensive review of the stages employed in the digital forensic process, and so is convenient for analysing the impact of

phase	**action**	**challenges**
identification	identifying an illicit event	lack of frameworks
preservation	software tools	lack of specialist tools
	sufficient storage capacity	distributed, virtualized and volatile storage; use of cloud services to store evidence
	chain of custody	cross-jurisdictional standards, procedures; proprietory technology
	media imaging	imaging all physical media in a cloud is impractical; partial imaging may face legal challenges
	time synchronization	evidence from multiple timezones
	legal authority	data stored in multiple jurisdictions; limited access to physical media
	approved methods, software and hardware	lack of evaluation, certification generally, but particularly in cloud context
	live vs. dead acquisitions	acquisition of physical media from provider is cumbersome, honerous and time consuming; data is inherently volatile
	data integrity	lack of write–blocking or enforced persistence mechanisms for cloud services and data
examination	software tools	lack of tested and certified tools
	recovery of deleted data	privacy regulations and mechanisms implemented by providers
	traceability and event trace re-construction	events may occur on many different platforms
presentation	documentation of evidence	integration of multiple evidence sources in record
	testimony	complexity of explaining cloud technology to jury

Table 1: summary of challenges to digital forensics

cloud forensics on this process. Other models are also referenced where appropriate, in particular the ACPO principles and guidelines.

The issues raised concerning cloud computing in each of the phases of a digital forensics investigation are summarised in Table 1. The analysis demonstrates that many of the assumptions incorporated into existing models of forensic investigation are not valid in the context of cloud computing.

3.1 Identification

The first step of the DIP model is the determination that a potential criminal, or improper act has taken place involving computer-based systems. These events may relate to traditional crimes or activity augmented by the use of IT, or IT specific crimes. Identification may result from, for example, complaints made by individuals, anomalies detected by intrusion detection systems, monitoring and profiling or as a result of an audit of a computer system. Although the identification phase is not just concerned with digital forensics, it does have an impact on how the investigation is conducted as well as defining the purpose for conducting the investigation.

The detection of suspicious events in a cloud will depend on the deployment model adopted and the form of cloud services (SaaS, PaaS or IaaS) used. The deployment of conventional intrusion detection systems in a cloud has been proposed by several authors [Roschke et al., 2009, Vieira et al., 2010]. Such systems could be deployed by users of IaaS clouds, or by providers in SaaS or PaaS clouds. In a private cloud infrastructure, providers may be better placed to tune the IDS for the particular suite of services deployed which meets the organization's needs. For public clouds, a multi-layered strategy may be necessary. Users can monitor for suspicious events occuring with the services they are using. Providers can monitor the underlying infrastructure used to host the cloud, and therefore detect much larger attacks which could affect a much larger audience.

3.2 Preservation and Collection

A digital forensic investigation is concerned with collecting data from computer based systems that can later be constituted as evidence that a crime or other illicit act has been committed. Legal convention and forensic standards, such as the Daubert principles [Marsico, 2004], require that forensic evidence be testable, and that the methods used to produce evidence be repeatable. Consequently, the preservation phase of the DIP model

defines activities prior to data collection to ensure the integrity of data throughout the investigation life-cycle, i.e. assurance that the evidence is an accurate representation of the data found on the computer system. There are several aspects of the preservation phase which are affected by the use of a cloud environment.

3.2.1 Storage Capacity

In conventional investigations, a pre-requisite of evidence preservation is to have available sufficient secure storage capacity for the data gathered to be archived. Several authors have noted that the growing amounts of data gathered during forensic investigations, driven by increased device capacity and reduced cost, is increasingly challenging for investigators [Sommer, 2004]. This increase imposes extra costs on investigators with the responsibility to store and curate the data, quite apart from the increasing amount of investigator time required to examine it.

The use of cloud environments will likely exacerbate the problem of data storage. An attractive aspect of cloud environments for users is the *elastic* ability to dynamically scale a service's storage capabilities according to on-going requirements. From a user's perspective, a typical public IaaS cloud appears to offer limitless data storage capability as and when the user requires it. An investigator may be faced with gathering an extremely large amount of data placed in a cloud by a user.

One solution investigating authorities could resort to is the using the public clouds to store evidence. This too will bring its own challenges, from both a legal and technical perspective. Investigators will need to address the rules and regulations regarding data protection and privacy issues, and their impact on evidence stored in the cloud.

The adoption of triaging techniques has also been proposed as a means of reducing the amount of data to be analysed by an investigator [Pearson and Watson, 2010] and is already being adopted to reduce backlogs in conventional investigations [Rogers et al.,

2006]. This approach may be particularly appropriate in situations which require urgent responses, such as kidnappings, when the long term integrity and reliability of evidence is less important. The proposed approach permits investigators to conduct examinations of storage devices (see below) in a short period of time in order to identify the most valuable evidence without performing a full forensics investigation.

The Computer Forensics Field Triage Process Model (CFFTM) is a framework proposed to perform triage on digital devices [Rogers et al., 2006]. CFFTM works by accessing information located in a user's 'home directory' on the file system, which contains user–application centric information. Other sources of information used in the CFFTM include the registry, operating system and application logs which can contain timestamp information.

The CFFTM will likely not transfer directly to the context of a cloud environment, since user-centric application data may be stored in the cloud, cached on the user's client computer, or both. Adopting a triage approach may require an investigator to conduct a live examination of this data in the cloud environment while the client is still connected. The implications of a live investigation are discussed further below in the context of data acquisition.

3.2.2 Chain of Custody

During a conventional forensic investigation, accepted practice is to establish and maintain a 'chain of custody' for evidence, defined as:

> "a roadmap that shows how evidence was collected, analyzed and preserved in order to be presented as evidence in court" [Vacca, 2005].

A properly maintained chain of custody therefore provides the documentary history for the entire lifetime of evidence discovered during an investigation. ACPO guidelines

stipulates that the documentation include how the evidence was gathered and managed, by whom and when.

In a conventional investigation, the chain of custody begins when an investigator assumes physical control of digital electronic artifacts (and any incorporated storage devices) that are suspected to be pertinent to the investigation. Subsequently, there are two methods of preserving data on a personal computer [, and Jay G. Heiser(2001]: powering down the computer by issuing a command to the operating system causing a staged shutdown, and removing the power source, causing an immediate halt. Storage devices can then be removed from the computer and examined separately. The chain of custody documentation will typically refer to these devices, which can be isolated and disconnected from a power supply with little risk of loss of evidence.

The remote nature of cloud services means that this assumption is not valid in the context of a cloud environment. Services can be accessed by any system with a network connection to the hosting cloud. Unless an investigator is able to gain control of and disable a service, evidence could be destroyed relatively quickly, either by a service user, or by the cloud provider. To the authors' knowledge there has been little work either by researchers or practitioners to examine the practicality of obtaining control of a cloud service during an on-going forensic investigation. Challenges in this context include the speed with which an investigator can gain control of a service, and the appropriate legal and regulatory framework that should be developed to enable this capability.

3.2.3 Digital Image Acquisition

Assuming control of a service has been established by an investigator, it is necessary to obtain an accurate copy of the data held by the service for later analysis. Both the DIP Model and ACPO Guidelines assume the use of 'forensic imaging' to obtain copies of a storage device's contents without alteration of the source [ACPO, 2007, Palmer, 2001].

Typically, a storage device is connected to an investigator's own computer via a write-blocker. A byte-for-byte copy of the entire device (an image) is then made using a software tool such as AccessData's FTK Imager[4] or the open-source tool dd.[5] If multiple copies of the image are taken, digital hashes of each image can be taken to check whether the source image has been changed.

The collection of evidence from a cloud environment is likely to pose a challenge to investigators. Triage tools, volatile and persistent memory acquisition software, as used in conventional investigations, on a client computer may provide minimal data.

The virtualization of data storage in a cloud makes it complex to identify and isolate the portions of the one or more physical storage devices owned by a cloud provider that represent the user's data that should be gathered for analysis. Virtualized data stored on a cloud may be spread between many different physical devices. For example, Google have employed the Google File System (GFS) to store their customers data in the cloud [Ghemawat et al., 2003]. To customers, data appears to be stored in a single location; however, physically this is not the case. GFS is a "multi-tenant distributed" file system which means that even if two users are within the same organization, their data could well reside in two or more different physical locations [Google, 2010a].

The ACPO guidelines envisage the entire storage device containing relevant information to be collected [ACPO, 2007]. Acquiring all such storage devices from a cloud environment could be both cumbersome and time consuming for the investigator, and disruptive for the provider. The amount of data collected could also be very large, particularly in relation to the amount of relevant data contained. Fundamentally, cloud services only offer remote access to a *logical* representation of data, rather than the underlying *physical* infrastructure. This limitation is likely to be complicated further by the provision of cloud services whose infrastructure is itself virtualized and leased from other cloud providers [**?**]. It appears

[4] `http://accessdata.com/support/adownloads#FTKImager`

[5] `http://www.gnu.org/software/coreutils/`

inevitable that methods will be needed which allow for only a partial recovery of data from any one physical device. Such a method would need to be developed in accordance with accepted forensic principles. In particular, the risk of conducting an investigation with incomplete data must be addressed [Carrier and Spafford, 2004].

This use of virtualization also impacts on the privacy of other users of the cloud, whose data may be inadvertently gathered during the investigation. In some jurisdictions, inadvertent access of non-relevant data from a cloud environment may contravene local privacy and/or data protection legislation.

The preceding discussion has assumed that the investigator conducts a 'dead acquisition' on a physically isolated storage device. However, frequently used data may be stored in volatile memory on the cloud, or be cached by a user's computer during interactions with cloud services. 'Live' acquisitions and investigations are an alternative approach, in which data is examined on the target computer while it is still powered up. This approach enables investigators to gather data that might otherwise be lost if a computer is powered down, particularly:

- data stored in non-persistent memory, such as processes and information on active network connections; and
- temporary data stored in persistent memory, such as application file locks, and web-browsing caches.

The use of live acquisition techniques may increase the amount of information an investigator is able to extract from a cloud client computer, particularly if it has an open connection to a cloud environment. However, digital Image acquisition could be further hampered by the use of encryption in cloud-based environments. With many organizations reluctant to adopt cloud services and storage until concerns about data condentiality and integrity is met [Kamara and Lauter, 2010], cloud service providers are turning towards

encryption as a means of offering this security to their customers. Several cloud storage providers such as SpiderOak have implemented a 'zero knowledge system' such that all data is encrypted client-side before being transmitted and stored in the cloud, furthermore, the keys used to encrypt data are never stored in the cloud [Agudo et al., 2011]. This means serving a cloud storage provider with a court order to decrypt such information could prove fruitless as only the owner of the data can provide the key to decrypt this information. If such an encryption system is deployed by further cloud providers as a means assuring customers their data is safe, evidence in digital images created could reveal encrypted blocks of data of no forensic value to investigators unless encryption keys can be recovered.

3.2.4 Deleted Data

In conventional investigations, data that a user has attempted to delete (but which still resides on a storage device) is often a rich source of evidence. However, the volatility and elasticity of cloud environments make the recovery of deleted data challenging. Some cloud providers maintain that user privacy is a priority within their cloud environments [Google, 2010a]. For example, Google's current policy regarding deleted data is such that once a user deletes their data from Google Services, that data is then deleted from both active and replication servers. Pointers to this data are also deleted, making tracing remnants of user deleted data extremely difficult.

The European Commission is encouraging European Union member states to implement the Data Retention Directive [Union, 2006]. Article 5 of this directive requires member states to ensure that communication providers shall retain certain information about its users, including the "userID", "IP address allocated at the time of the communication" as well "the date and time of the log-in and log- off of the service" [Union, 2006]. Cloud providers are not explicitly mentioned in the directive. However, should they be encompassed by the umbrella definition of 'communication providers', they too will also need to

retain specific information related to clients.

3.2.5 Cross–Organizational Cooperation

If it is not possible for an investigator to obtain personal control of a cloud service, it may be possible to obtain an image of the service's data from the cloud provider. However, this approach is problematic for several reasons. Using the cloud provider to obtain the image means that the chain of custody documentation is not initially controlled by the investigator. A complete chain of custody should identify all individuals who have come into contact with the evidence. Consequently, if the cloud provider is used to obtain the initial image, then the chain of custody begins with the employees assigned to this task. The second principle in the ACPO guidelines states that the individual responsible for acquiring evidence must be competent to do so (although the guidelines are not explicit about what constitutes competency). It is unclear how an investigator would satisfy themselves that the cloud provider's employees were competent to gather evidence on their behalf.

The cross-organizational nature of this approach to evidence gathering from cloud environments has other implications. The investigator may have difficulty establishing the training and experience of the cloud providers employee's assigned to assisting the investigation, particularly if the standards adopted within the provider organisation are not directly comparable to those of the investigator. The use of proprietary technologies by cloud providers may make the involvement of the provider in the investigation essential. For example, parts of the GFS are considered proprietary business information. Investigators may require the cooperation of cloud providers to locate evidence. Consequently, the reliability and quality of the chain of custody may be insufficient for the investigator's purposes.

This problem is exacerbated if the cloud provider is hosted in a different jurisdiction to that of the investigator, since different legal norms and practices may govern the provider's

behaviour. A local search warrant to search and seize evidence may not give the investigator the right to do the same with evidence located in different jurisdictions, even though the evidence is accessible via the Internet [Wang, 2010]. For example, Amazon stores data from customers in the European Union in its cloud services in the Republic of Ireland [Wauters, 2008]. This means that an investigator seeking evidence concerning a cloud user will need to work with the authorities in that jurisdiction. Such a request may take some time, by which time the evidence could be lost or deliberately destroyed.

A partial solution may be for cloud providers to have individuals within their organization, who are trained and qualified to perform forensic investigations should the need arise. These individuals can then begin a chain of custody, which will be passed onto the investigating party. However, it is unclear how the costs of providing this service will be defrayed by the cloud provider. It may be necessary for such services to be mandated by legislation.

The preservation phase also includes the reconciliation of timing information concerning digital evidence, in particular from time stamps in file system meta-data, and from application log files on one or more computer systems. This information can be used to re-construct the sequence of events concerning a suspicious event.

For an investigator to re-construct an accurate time-line of events on the device or system, the correct time and time zone need to be established. In a cloud environments, establishing this information could be challenging. Public clouds will potentially store evidence in a distributed manner across various physical locations. Hence, the physical locations could be in more than one time zone. In addition, virtualized services may also operate according to the time zones of their users, rather than their physically hosted locations.

3.3 Examination and Analysis

Several examination techniques are discussed in the DIP Model once data has been preserved and collected, and there are a variety of software tools available to assist an investigator. Dedicated forensic tool suites such as Forensic Tool Kit[6] or Encase[7] are popular commercial choices. Sleuth Toolkit[8] is an open source alternative .These tool suites can be used to perform 'pattern matching' and 'filtering', which can involve either searching for specific filenames, file types, or content. These tool suites can also be used to discover and recover data that a user has attempted to delete.

During the analysis phase of an investigation, the significance of information artefacts as evidence is evaluated. A narrative is developed, supported by the evidence and a timeline to explain how a crime was committed. Where appropriate, it may be possible to associate particular artifacts with users or user accounts.

Evidence produced during analysis may also be subject to validation, either through comparison with complementary sources, or with previous versions, to gain assurance that the evidence has not be altered as a consequence of some analysis technique.

3.3.1 Types of Evidence in Clouds

Many types of evidence found in clouds, will likely be similar to that found in conventional investigations, including office application documents, emails and images. Several new forms of evidence will also be available, in particular records of activities of users with clouds. Major cloud providers such as Amazon and Google have implemented a number of logging mechanisms tracking use within their services:

- Message Log Search – is a service from Google which allows administrators to make queries on email messages. This search can also be used by forensic investigators

[6] `http://accessdata.com/products/computer-forensics/ftk`
[7] `http://www.guidancesoftware.com/forensic.htm`
[8] `http://www.sleuthkit.org/`

provided they can gain access to the administrator account. Using this tool an investigator can find logs containing information such as: emails sent on a specific date, account ID identification for a specific email, identification of specific email recipients, and the IP address of the sending or receiving Mail Transfer Agent [Google, 2010b].

- Amazon Simple Storage Service Logging – Amongst other logging, Amazon provides logging for buckets created using Amazon Simple Storage Service. Logging can be configured to record requests made against the bucket such as the request type, the resource which the request worked and the time and data the of the request [Amazon, 2010].

To access these logs, an investigator currently needs to access the administrative section of the cloud service under investigation. As such logs will be located in the cloud, the administrative username and password will be required to access them. Cloud providers could assist investigators, although the issues concerning chain of custody discussed above will be present. Marty has proposed a framework for recovering logging information during forensic investigations involving the cloud [Marty, 2011].

3.3.2 Validation using Hashing Tools

Software hashing tools are commonly used in conventional investigations to validate the on-going integrity of data used as evidence. A hash function is an algorithm for converting arbitrary length data strings into fixed length *hash values*, typically a few hundred bytes in length. Hash functions are designed so that any change in the input data should (with high probability) produce a different output hash value. Hash values can therefore be periodically computed for disk images, files or other data representing forensic evidence to gain assurance that the evidence has not been changed by an analysis [Salgado, 2006].

Data stored in a cloud can also be subjected to hashing for integrity checking purposes. For example, Amazon S3 and Web Services (AWS) have both implemented MD5 hashing checksums for objects stored in their services [Amazon, 2010]. In principle, these checksums can be periodically recorded by an investigator to show that any evidence acquired has remained unchanged during the course of the investigation. In addition, this feature may be of future use for investigators wishing to store forensic evidence that they have gathered in a cloud environment.

The use of hashing tools implemented, deployed and controlled by cloud providers does raise some challenges. As in the discussion on forensic imaging above, the use of external facilities draws the provider into the chain of custody. In addition, the investigator has less opportunity to test and evaluate the hashing features in a cloud, compared with tools developed for use on conventional desktop PCs. Typically, an investigator can use a selection of tools which implement the same hash function to compute a hash for some sample data. Any differences between the results produced can be investigated. However, in a cloud environment, the investigator has only a single implementation (the checksum implementation deployed by the cloud provider) to use. Consequently, the investigator's ability to validate the correctness of their tools is limited.

3.4 Presentation

Evidence gathered during a digital forensic investigation can be summarized to explain their conclusions in a number of forms. Evidence may be submitted to a court in the form of a report and an investigator could be asked to provide expert testimony and be subject to cross-examination [Carrier and Spafford, 2003]. Alternatively, the results of an investigation could be used by an organization to improve their corporate policy and could evolve as a form of documentation for future investigations [Wang et al., 2005].

In 1993, the United States (US) Courts made a ruling in the case of Daubert v. Merrell,

which defined the admissibility of scientific evidence [Marsico, 2004]. This admissibility was based upon four criteria as described by O'Connor :

1. Has the scientific theory or technique been empirically tested?
2. Has the scientific theory or technique been subjected to peer review and publication?
3. What is the known or potential error rate? Every scientific idea has error rates, and these can be estimated with a fair amount of precision. There are known threats to validity and reliability in any tests.
4. Has the theory or technique been accepted as a standard in its scientific community?

The conduct of forensic investigations in cloud environments will presumably be subject to the same tests in the so-called Daubert principles, if the resulting evidence is to be acceptable in court. The empirical testing of cloud forensic methods may be challenging due to the rapidly evolving nature of the technology. Empirical testing of forensic tools typically employs standard data sets [Guo et al., 2009], but it is unclear how these could be developed for cloud forensic methods. Certainly, there is a clear need to develop a standard evaluation method and data set for cloud forensics, if results of cloud forensic investigations are to pass the Daubert principles. These criterions affect not only cloud investigations but traditional computer forensics investigation as well. As Marsico notes :

> "...the court does not have a true universally accepted method to reply upon. To further complicate the problem, many self-proclaimed computer forensics experts take what they feel are the best aspects of several approaches and create their own methodology." [Marsico, 2004]

Expert witnesses could be faced with the additional challenge of having to explain the concept of cloud computing to a jury. It must be remembered that juries in the UK are

made up for individuals from the general public, very often, people who only use a personal computer to perform simple tasks. It can be expected that before a judge can allow a jury to listen to evidence retrieved from the cloud, they must understand what a 'cloud' is, and how it works. This could further prolong court proceedings and expert witnesses will be faced with the daunting task of ensuring juries fully understand the concept of the cloud.

The evolution of cloud computing forensics is in its infancy. Currently there is not a standard method or tool set for conducting cloud investigations, or even for evaluating and certifying proposed tools. The presentation of evidence derived from a cloud service will likely be problematic for the near future.

4 Related Work

The potential benefits and challenges of cloud computing for digital forensic investigations have been discussed by several authors [Biggs et al., 2010, Biggs and Vidalis, 2009, Reilly et al., 2010, Wolthusen, 2009, Taylor et al., 2010, Ruan et al., 2011b,a].Reilly et al. [2010] speculate that one potential benefit of cloud computing is having data in a centralized location, which can mean incidents can be investigated more quickly. Wolthusen [2009] notes that when attempting to locate evidence in a distributed environment such as the cloud, major challenges will need to be overcome because evidence could be located across several locations making evidence collection difficult. The distribution of evidence can be across multiple virtual hosts, physical machines, data centres and geographical and legal jurisdictions. The distributed nature of control and storage in a cloud (and the ephemeral nature of virtual instances) will also likely make tracing activity and re-construction of events more challenging [Wolthusen, 2009].

Other challenges identified includes a loss of important forensic information such as registry entries (on Microsoft Windows platforms) temporary files, and metadata which could be stored in the cloud as well as a lack of tools for dealing with investigations involving

cloud data centres [Taylor et al., 2010]. As part of the Cloud Computing & The Impact on Digital Forensic Investigations (CLOIDIFIN) project Biggs and Vidalis [2009] reported that very few High Tech Crime Units (HTCUs) in the UK were prepared to deal with crimes involving cloud computing. Even when HTCUs are prepared to investigate such crimes, current legislation for accepting digital evidence in court presents further challenges [Biggs and Vidalis, 2009].

Ruan et al. [2011b] define cloud computing forensics as a form of network forensics, arguing that cloud environments are essentially a form of public and/or private computer network. However, this definition doesn't incorporate the virtualized nature of clouds, which is likely to have a significant impact on forensic investigations beyond the networked aspect. The paper proceeds to sketch a process model for forensic investigation in a cloud environment, however it is unclear how the model is to be evaluated. Ruan et al. [2011b] reported on a survey of digital forensic practitioners. The survey was conducted with the intention of establishing the views of practitioners concerning the impact of cloud computing on future digital forensic investigations. The results of the survey indicate considerable diversity of opinion within the practitioners surveyed. For example, no answer to the question 'what is cloud forensics?' received more than 60% agreement from the participants.

The legal issues surrounding evidence retrieved from a cloud environment have been extensively examined by Taylor et al. [2010]. Just as in a traditional investigation, any evidence gathered from the cloud should be conducted within local laws and legislation. For example in the United Kingdom, the Data Protection Act 1998 (DPA), the Computer Misuse Act 1990 (CMA) as well as the Criminal Procedure and Investigations Act (CPIA) 1996 and the Criminal Justice Act 2003 (CJA) will presumably all apply cloud computing investigations [Taylor et al., 2010].

The protection of personal data will apply in a cloud computing environment just as

it does in conventional computing environments. If a cloud is used to host a large 'filing system' containing customers personal data then the DPA will apply to investigating this cloud [Taylor et al., 2010]. The investigation of unauthorized access to cloud computing resources could be fairly easy to investigate as digital evidence will probably be found on the suspect's personal computer [Taylor et al., 2010]. The investigation of unauthorized modification of data in the cloud could be more challenging to investigate as per the CMA. Taylor et al. state that unless a confirmation of the modification is sent back to the suspects computer, or unless an audit trail is left behind in one of the many devices used to connect to the victim, then proving the modification actually took place will be difficult to investigate [Taylor et al., 2010]. The CPIA and CJA are laws which concern mainly law enforcement investigators. They require that such investigators identify and recover evidence not only for prosecution but for defence as well, and not ignore one of the two sides in an investigation [Taylor et al., 2010]. This could be more difficult to implement in a cloud investigation. This is largely due to the cloud having no physical boundary, and attempting to investigate such a crime scene with a limited timeframe budget could mean that not every device can be examined for evidence. Courts in the United Kingdom will need to take this into consideration when applying the CPIA and the CJA to cloud-based investigations as investigators will not have the resources nor will it be practically possible to uncover all the evidence from a cloud environment [Taylor et al., 2010].

Cloud computing environments have been suggested by several authors as a basis for *conducting* forensic investigations. Dedicated virtual instances can be ready and waiting on 'stand-by' to assist in gathering evidence from an incident or crime. Cloud storage can be used to store images gathered from investigations, and the extensive compute resources available can also be used to perform brute-force cracking attacks on passwords and encryption keys [Reilly et al., 2010].

5 Future Work

It is clear from the comparison made to a conventional forensics investigation that much further work is required to understand the true impact of the cloud computing on digital forensics. As discussed above, the impact will be on both the procedures followed by investigators on identification of a crime or illict activity and the tools employed to recover evidence.

This section proposes several specific experiments that can be conducted to begin to understand the requirements for tools used in digital forensic investigations in clouds. Only once the results from empirical experiments such as these are obtained can current tools and methodologies used in traditional investigations be properly evaluated and adapted as necessary to the new context.

5.1 Analysis of Cloud Service Usage

With cloud service providers such as Amazon, Google and Dropbox offering an alternative to traditional file storage, email and collaboration solutions, it is likely that the time will soon come when such environments will be probed for evidence. These growing markets have seen many such cloud–based storage solutions emerge and this could lead to many organizations using such services in the near future. Research would focus on how these cloud–based solutions can be investigated and their impact on digital forensics. For example, it is currently unclear what useful evidence could be recovered from cached data created by these services on client computers, or whether data deleted from the service may be cached by the client for some time (or vice versa). Evidence gathered in this way might also contribute to a revised cloud investigation process model, by enabling investigators to concentrate requests for data from cloud providers on specific, known artifacts.

We sketch one such experiment to investigation Google Apps, an email and collaboration solution as follows. Firstly, the client used to connect to Google Apps can be

extensively examined. The investigation can focus around if the client stores a cache copy of any emails on the hard disk drive. During the experiment the client can be used to connect to Google Apps for a period of time. Documents received through Google Apps can be viewed online without downloading local copies to the hard disk. The hard disk of the client computer can then be imaged and the data examined.

The focus of this experiment will be to determine:

- whether it is possible for an investigator to recover email messages including the email body and header information;
- the availability of log files for recovery;
- the recovery of documents viewed using GoogleDocs; and
- how principles of forensic investigation can be applied (i.e. so that evidence is not altered during the course of an investigation).

A second such experiment can investigate the recovery of evidence from cloud–based storage solutions such as Dropbox[9], Wuala[10], Syncplicity[11] and SpiderOak [12]. The experiment can be setup as follows. A selection of files (the data set) can be stored in the cloud using a client computer which has installed on it the one of the above solutions. A number of file manipulations such as storing, moving and deleting files can be performed to mimic the real movement of evidence by a suspect in the cloud. The purpose of this experiment could be two fold. Firstly, to investigate if the data set can be recovered from the client computer used to store them in the cloud and secondly, investigate the artifacts created as a result of the above file manipulations in the cloud. This experiment can also be extended to investigate the clouds affect on digital evidence timestamps. The reality is that the

[9] `http://www.dropbox.com`
[10] `http://www.wuala.com`
[11] `http://www.syncplicity.com`
[12] `http://spideroak.com`

cloud client and cloud storage server will likely be in different time-zones. Timestamps uncovered from evidence gathered from such environments could reveal contradicting results. By observing the time when manipulations are made to the data set during the course of the experiment, the timestamps can be examined and any affects the cloud has on these timestamps can be noted.

5.2 Acquisition Methods for Cloud Environments

A second area of research would be to evaluate current methods of evidence acquisition from the cloud. If these current tools are deemed insufficent then alternative tools can be developed. A cloud test–bed can be used to mimic the main cloud services (SaaS, PaaS or IaaS) offered by cloud providers. The authors believe each of these services will require a unique acquisition methodology and each service will provide a unique set of challenges that need to be overcome. For example in an IaaS environment an acquisition methodology needs to be developed such that forensic 'images' can be acquired from the virtual machines running in this environment. Several other challenges across the different services also need to be addressed due to the properties of cloud computing. Firstly, can the cloud be stabilized to the extent to allow the investigator to take an accurate representation of the evidence at that point in time? With the investigator not having complete control as in the case of a hard drive, which can be isolated from a personal computer, can the investigator be sure evidence is not in the process of being altered in the cloud at that moment in time? Secondly, with cloud storage providers employing a distributed file-system, alternative tools will be required to recognize that such an environment is being used and effectively should 'fetch' all the evidence from various physical locations. Finally, the problem of encryption needs to be overcome such that acquired evidence is not effectively a forensic 'image' of encrypted data. Current evidence acquistion tools can be evaluated using the test bed and alternative tools can also be developed.

5.3 Cloud Forensics Management

A final area requiring further work is to explore the management issues which could arise during a cloud forensics investigation. The idea of using the cloud to host a 'forensic server' used to conduct investigations has already been proposed by [Reilly et al., 2010]. Several issues are raised by this prospect, including, for example, the the forensically sound transfer of evidence from the source of the investigation to the cloud storage. Such a prospect also raises challenges concerning the management of the chain of custody for evidence, and the consequences of a security breach suffered by the cloud provider.

A second area of research in cloud forensics management will examine how to handle and store such a large data set. With evidence from the cloud expected to be much larger than what current investigators are examining presently, how do investigators store this evidence safely and securely? One solution could be the use of the cloud itself. Issues which can be examined include:

- ensuring the evidence is unaltered when transferred to and from as well as when stored in the cloud;
- ensure that by using the cloud, local laws such as data protection are observed if the cloud is used to store evidence;
- be certain that the evidence is secure from unauthorized access, as the evidence can be deleted both wittingly and unwittingly; and
- in the event where sensitive evidence (explicit images and videos) are stored in the cloud, access to this evidence is limited and other users of the cloud do not have access to this material.

Mechanisms to prevent the above such as encrypting the evidence could be used, but due to the large size of the evidence, this could be cumbersome. Therefore research will

need to examine how the cloud can be secured and what options investigators have should they chose to use the cloud to store evidence in it.

6 Conclusion

This paper has argued that conventional methods and guidelines suggested for conducting digital forensics could well be insufficient in a cloud environment. If current forecasts are correct more businesses and organizations will be moving their data to cloud environments. Together with a continued growth in cyber–crime, this transition could mean there will soon be a demand to conduct forensics investigations in such environments. Such investigations would currently be hampered due to the lack of guidance concerning methods and software tools to retrieve evidence in a forensically sound manner. There is also the need for legal issues regarding clouds including data retention and privacy laws to be re-examined, following the widespread adoption of cloud technologies. Finally there is also the need for the digital forensics community to begin establishing standard empirical mechansisms to evaluate frameworks, procedures and software tools for use in a cloud environment. Only when research has been conducted to show the true impact of the cloud on digital forensics, can we be sure how to alter and develop alternative frameworks and guidelines as well as tools to combat cyber-crime in the cloud.

References

ACPO. Good practice guide for computer-based electronic evidence. Association of Chief Police Officers, 7Safe, August 2007.

Isaac Agudo, David Nuñez, Gabriele Giammatteo, Panagiotis Rizomiliotis, and Costas Lambrinoudakis. Cryptography goes to the cloud. In Changhoon Lee, Jean-Marc

Seigneur, James J. Park, and Roland R. Wagner, editors, *Secure and Trust Computing, Data Management, and Applications*, volume 187 of *Communications in Computer and Information Science*, pages 190–197. Springer Berlin Heidelberg, 2011.

Amazon. Zeus BotNet Controller. Security bulletin, Amazon Web Services, December 2009.

Amazon. *Amazon CloudFront – Developer Guide*. Amazon Web Services, November 2010.

Warren G. Kruse (and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Addison Wesley, October 2001.

Venansius Baryamureeba and Florence Tushabe. The enhanced digital investigation process model. In *Digital Forensic Research Workshop*, August 2004. Online Publication. Available at `http://www.dfrws.org/2004/day1/Tushabe_EIDIP.pdf`.

Stephen Biggs and Stilianos Vidalis. Cloud computing: The impact on digital forensic investigations. In *International Conference for Internet Technology and Secured Transactions*, London, UK, November 2009. IEEE Computer Society. Online publication.

Stephen Biggs, , and Stilianos Vidalis. Cloud computing storms. *International Journal of Intelligent Computing Research (IJICR)*, 1(1):63 – 72, 2010.

Marjory S. Blumenthal. Hide and seek in the cloud. *IEEE Security & Privacy*, 8(2):57–58, March/April 2010.

Brian Carrier and Eugene H. Spafford. Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2):–, Fall 2003.

Brian Carrier and Eugene H. Spafford. An event-based digital forensic investigation framework. In *Digital Forensic Research Workshop*, August 2004.

Wendy Butler Curtis, Curtis Heckman, and Aaron Thorp. Cloud computing: ediscovery issues and other risk. ediscovery alert (white paper), Orrick, Herrington and Sutcliffe, June 2010.

Detica. The cost of cyber crime. Detica/Cabinet Office, UK., February 2011. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.

Frank Gens. IDC predictions 2011: Welcome to the new mainstream. White paper, International Data Corporation, 5 Speen Street Framingham, MA 01701 USA, December 2010. URL `http://www.idc.com/research/viewdocsynopsis.jsp?containerId=225878`.

Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. The google file system. In Michael L. Scott and Larry L. Peterson, editors, *19th ACM Symposium on Operating Systems Principles*, pages 125–139, Bolton Landing, New York, USA, October 2003. ACM Press.

Google. Google apps messaging and collaboration products. Security white paper, Google, 2010a.

Google. *Message Log Search*, 2010b. URL `http://www.postini.com/webdocs/admin_msd/wwhelp/wwhimpl/common/html/wwhelp.htm?context=MSDHelp&file=logsearch_about.html`.

Y. Guo, J. Slay, and J. Beckett. Validation and verification of computer forensic software tools–searching function. *Digital Investigation*, 6:S12–S22, 2009.

P. Hunton. A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a uk law enforcement environment. *Digital Investigation*, 2011.

R.S.C. Ieong. Forza-digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3:29–36, 2006.

Seny Kamara and Kristin Lauter. Cryptographic cloud storage. In Radu Sion, Reza Curtmola, Sven Dietrich, Aggelos Kiayias, Josep Miret, Kazue Sako, and Francesc Sebé, editors, *Financial Cryptography and Data Security*, volume 6054 of *Lecture Notes in Computer Science*, pages 136–149. Springer Berlin / Heidelberg, 2010.

Bob Kazarian and Belinda Hanlon. SMB cloud adoption study dec 2010 – global report what will be the impact of cloud serviceson smbs in the next 3 years? White paper, Edge Strategies, March 2011. URL `http://www.microsoft.com/Presspass/presskits/commsector/docs/SMBStudy_032011.pdf`. Sponsored by Microsoft.

Ali Khajeh-Hosseini, David Greenwood, and Ian Sommerville. Cloud migration: A case study of migrating an enterprise it system to iaas. In *3rd International Conference on Cloud Computing*, pages 450–457, Miami, Florida, USA, July 2010. IEEE Computer Society.

Ronaldd R. Krutz and Russell Vines. *Cloud Security A Comprehensive Guide to Secure Cloud Computing*. Wiley, August 2010.

Christopher V. Marsico. Computer evidence v. daubert: The coming conflict. Technical Report 2005–17, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Indianna, 47907-2086, USA., March 2004.

Raffael Marty. Cloud application logging for forensics. In *Proceedings of the 2011 ACM Symposium on Applied Computing*, pages 178–184, TaiChung, Taiwan, March 2011. ACM Press.

Peter Mell and Timothy Grance. The nist definition of cloud computing (draft). Special Publication 800–145, National Institute of Standards and Technology, Computer Secu-

rity Division, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, United States, January 2011.

P. Owen and P. Thomas. An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising acpo & nist guidelines. *Digital Investigation*, 2011.

Gary Palmer. A road map for digital forensic research – report from the first digital forensic research workshop (dfrws), utica, new york, usa, august 2001. Technical Report 001, Digital Forensic Research Workshop, Utica, New York, USA, November 2001.

Stephen Pearson and Richard Watson. *Digital Triage Forensics: Processing the Digital Crime Scene*. Elsevier Science & Technology. Syngress, 30 Corporate Drive, Suite 400, Burlington, MA, 01803, USA, July 2010.

Ben Pring, Robert H. Brown, Lydia Leong, Fabrizio Biscotti, Adam W. Couture, Benoit J. Lheureux, Andrew Frank, Jeffrey Roster, Susan Cournoyer, and Venecia K Liu. Forecast: Public cloud services, worldwide and regions, industry sectors, 2009-2014. Technical report, Gartner, June 2010. URL `http://www.gartner.com/it/page.jsp?id=1389313`.

D. Reilly, C Wren, and T. Berry. Cloud computing: Forensic challenges for law enforcement. In *International Conference for Internet Technology and Secured Transactions*, London, UK, November 2010. IEEE Computer Society. Online publication.

Mark Reith, Clint Carr, and Gregg Gunsch. An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 2002.

Marcus K. Rogers, James Goldman, Rick Mislan, and Timothy Wedge. Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, 1(2), 2006.

Sebastian Roschke, Feng Cheng, and Christoph Meinel. Intrusion detection in the cloud. In Bo Yang, William Zhu, Yuanshun Dai, Laurence T. Yang, , and Jianhua Ma, editors,

Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pages 729–734, Chengdu, Chin, December 2009. IEEE Computer Society.

Keyuan Ruan, Ibrahim Baggili, Joe Carthy, and Tahar Kechadi. Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. In *6th annual conference of the ADFSL Conference on Digital Forensics, Security and Law*, Richmond, Virginia, USA, May 2011a. To appear: Journal of Digital Forensics, Security and Law.

Keyun Ruan, Joe Carthy, Tahar Kechadi, and Mark Crosbie. Cloud forensics: An overview. In , editor, *Advances in Digital Forensics. 7th IFIP International Conference on Digital Forensics*, volume – of *International Federation for Information Processing*, pages ??–??, Orlando, Florida, June 2011b. Springer. to appear.

Richard P. Salgado. Fourth amendment search and the power of the hash. *Harvard Law Review*, 119(38):38–46, 2006.

Lutz Schubert, Keith Jeffery, and Burkhard Neidecker-Lutz. The future of cloud computing: Opportunities for european cloud computing beyond 2010. Expert group report, European Commission Information and Society Theme, January 2010.

Peter Sommer. The challenges of large computer evidence cases. *Digital Investigation*, 1 (1):16–17, 2004.

M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty. Digital evidence in cloud computing systems. *Computer Law & Security Review*, 26(3):304–308, 2010.

The Open Cloud Manifesto Consortium. Open cloud manifesto. Online Publication. Available at `http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf`, Spring 2009.

European Union. Directive 2006/24/ec of the european parliament and of the council. Official Journal of the European Union, May 2006. on the retention of data generated or pro-

cessed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

John R. Vacca. *Computer forensics: Computer Crime Scene Investigation*. Charles River Media, 20 Downer Avenue, Suite 3, Hingham, MA, 02043, second edition, May 2005.

K. Vieira, A. Schulter, C. Westphall, and C. Westphall. Intrusion detection for grid and cloud computing. *IT Professional*, 12(4):38–43, 2010.

Kenny Wang. Using a local search warrant to acquire evidence stored overseas via the internet. In Kam-Pui Chow and Sujeet Shenoi, editors, *Advances in Digital Forensics VI*, volume 337 of *IFIP Advances in Information and Communication Technology*, pages 37–48. Springer Boston, 2010.

Yun Wang, James Cannady, and James Rosenbluth. Foundations of computer forensics: A technology for the fight against computer crime. *Computer Law & Security Report*, 21(2):119–127, 2005.

Robin Wauters. Amazon ec2 now available in europe. TechCrunch. Online Publication. Available at `http://techcrunch.com/2008/12/10/amazon-ec2-now-available-in-europe/`, December 2008.

Stephen D. Wolthusen. Overcast: Forensic discovery in cloud environments. In Oliver Goebel, Ralf Ehlert, Sandra Frings, Detlef Guenther, Holger Morgenstern, and Dirk Schadt, editors, *Fifth International Conference on IT Security Incident Management and IT Forensics*, pages 3–9, Stuttgart, Germany, September 2009. IEEE Computer Society.

David C. Wyld. Moving to the cloud: An introduction to cloud computing in government. E-government series report, IBM Center for the Business of Government, 1301 K Street, NW, Fourth Floor, West Tower, Washington, DC 20005, 2009.