Cybercrime and Cloud Forensics:
Applications for Investigation Processes

Keyun Ruan
University College Dublin, Ireland
Cybercrime and cloud forensics: applications for investigation processes / Keyun Ruan, editor.
p. cm.
Includes bibliographical references and index.
Summary: "This book presents a collection of research and case studies of applications for investigation processes in cloud computing environments, offering perspectives of cloud customers, security architects as well as law enforcement agencies on the new area of cloud forensics" -- Provided by publisher.
363.25'968--dc23
2012033552

Library of Congress Cataloging-in-Publication Data
Cybercrime and cloud forensics: applications for investigation processes / Keyun Ruan, editor.
p. cm.
Includes bibliographical references and index.
Summary: "This book presents a collection of research and case studies of applications for investigation processes in cloud computing environments, offering perspectives of cloud customers, security architects as well as law enforcement agencies on the new area of cloud forensics" -- Provided by publisher.
363.25'968--dc23
2012033552

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.
Chapter 1

Digital Forensic Investigation and Cloud Computing

Joshua I. James
University College Dublin, Ireland

Ahmed F. Shosha
University College Dublin, Ireland

Pavel Gladyshev
University College Dublin, Ireland

ABSTRACT

This chapter aims to be a high-level introduction into the fundamental concepts of both digital forensic investigations and cloud computing for non-experts in one or both areas. Once fundamental concepts are established, this work begins to examine cloud computing security-related questions, specifically how past security challenges are inherited or solved by cloud computing models, as well as new security challenges that are unique to cloud environments. Next, an analysis is given of the challenges and opportunities cloud computing brings to digital forensic investigations. Finally, the Integrated Digital Investigation Process model is used as a guide to illustrate considerations and challenges during an investigation involving cloud environments.

INTRODUCTION

Cloud computing is a topic that has been gaining popularity with businesses and end users in recent years. A certain level of hype and inconsistent definition has lead to some confusion about what cloud computing is, and what services it can provide. Along with general confusion, some concerns have been raised about the security of cloud environments. As seen with traditional computing, a growing concern for security leads to consideration of incident response and eventually digital forensic investigation capabilities. This work endeavors to examine the implications of cloud computing on digital forensic investigations.

To accomplish this, a high-level introduction into fundamental concepts of both digital forensic investigations and cloud computing for non-experts will be given. A brief overview of
the history and advancement of digital forensic science, legal considerations surrounding digital forensic investigations, the current state of digital crime, types of digital forensic examinations, and an introduction into current digital forensic investigation process models will be given to build the reader’s understanding of digital forensic science. Next, fundamental concepts of cloud computing, such as service and deployment models, will be covered. Once fundamental knowledge of cloud computing is established, some cloud computing security issues will be examined, followed by an analysis of the challenges and opportunities cloud computing brings to digital forensic investigations. Finally, a digital forensic investigation model will be used as a guide to illustrate digital forensic investigation challenges when applied to cloud environments.

DIGITAL FORENSIC SCIENCE

This section is a brief overview of the history and advancement of digital forensic science. Legal considerations surrounding digital forensic investigations, primarily focused on law in the United States, are discussed as well as the current state of digital crime and how digital investigators are addressing this global problem. Key digital forensic definitions, types of digital forensic examinations, and an introduction into current digital forensic investigation process models are given to build the reader’s understanding of the field.

History and Advancement of Digital Forensic Science

Digital forensics is a branch of the forensic sciences that deals with the analysis of digital evidence from digital sources (Palmer, 2001). Unlike traditional forensic sciences, a digital forensic analysis attempts to analyze non-physical evidence, or evidence that cannot be directly observed by humans without interpretation. It is because digital evidence cannot be directly observed that the admissibility of such evidence in court is under constant scrutiny (Casey, 2004). To help establish digital forensics as a credible forensic science, digital forensic science was defined at the first Digital Forensics Research Workshop (DFRWS) in 2001 as:

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions show to be disruptive to planned operations.

Digital investigation, however, predates this academic definition. Several notable but less developed definitions were previously proposed, such as those submitted by McKemmish (1999) and Civie and Civie (1998). Likewise, beyond academic definitions, research and digital investigations were already taking place prior to 2001. For example, Pollitt (1995) claimed that “[f]or a number of years now, law enforcement agencies have been seizing computers and other electronic devices.” A growing interest in digital forensic investigation is confirmed by looking at other works of the early 1990s (Collier & Spaul, 1992a, 1992b; Clede, 1993; Spafford & Weeber, 1993). Hannan (2004) claims “forensic computing origins lay in the late 1980s…,” which is when computer-based evidence was encountered more often by police (Jones, 2004), and is perhaps true for forensic computing as a field or separate science (Garfinkel, 2010), but from a legal perspective computers and computer evidence were topics of concern before then. For example, the U.S. Computer Fraud and Abuse Act was first enacted in 1984 (USDoJ, 2002), and also in the early 1980s Computer in Court - A Guide to Computer Evidence for Lawyers and Computing Professionals (Kelman & Sizer,
1982) was published that considers fundamental legal issues in relation to computer evidence. Even prior to this work, the admissibility of computer evidence from digital devices has been discussed as early as 1974 (Tapper, 1974), with references to computer technology in trials appearing as early as 1962. In the mid-1970s computer evidence became more of a focus (Roberts, 1974; DeHetre, 1975; Jenkins, 1975) rapidly evolving through the late 1970s when the computer was compared to an expert witness (Teubner, 1978), and the basic tenants for admissibility of computer evidence were explored (Connery & Levy, 1979); most of which is still relevant today. This increased interest in the mid-1970s correlates to the increasing reliance on computer systems in business, and an increasing availability and usage among the public (Polsson, 2011). Even with a considerable amount of evolution and previous work, Wilsdon and Slay (2005) claim that there are issues when it comes to implementation of past research and development in digital forensic investigations; a claim reiterated by Pollitt (2007) and Garfinkel (2010).

Despite a multitude of technological, and in some ways philosophical, changes to the field of digital investigation, the DFRWS definition is still widely accepted. Alternatives, or amendments, have been proposed (Hannan, 2004; Kent, et al., 2006), but the DFRWS definition has remained popular. Since the time of this definition, the areas of evidence preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation have been continually developed, and various process models and standards for each phase of digital investigations have been proposed. However, no one standard has yet to see global acceptance (Wilsdon & Slay, 2005; Hunton, 2012; Lim, et al., 2012), and according to James and Gladyshev (2010) the majority of organizations are creating their own Standard Operating Procedures (SOP), which are not always directly based on a common standard. But regardless of the process used, when considering digital forensic investigations, the resulting evidence must be admissible in court (Carrier, 2006). As stated by Cohen (2010), “[o]n a global level, the most commonly applied standards are similar to the U.S. Federal Rules of Evidence and the Daubert decision.” In the United States, the admissibility of scientific evidence was primarily examined using the Frye standard—from Frye v. United States, 293 F. 1013 (1923)—where accepted scientific evidence is based on the scientific community’s general acceptance of the employed technique. The Frye standard was superseded in 1993 by the Daubert standard (Daubert v. Merrell Dow, 509 U.S. 579 [1993]; General Electric Co. v. Joiner, 522 U.S. 136 [1997]; Kumho Tire Co. v. Carmichael, 526 U.S. 137 [1999]), although not without criticism (Gutheil & Bursztajn, 2005; Giannelli, 2006). The Daubert standard allows a judge to determine the reliability of scientific evidence during what is called a “Daubert Hearing,” usually before the trial. Four general categories are used as guidelines when assessing a scientific technique: testing, error rate, publication of the technique, and acceptance from the scientific community (Carrier, 2003). The Daubert standard was introduced to reduce the misuse of scientific evidence, but still not all states in the U.S. have adopted the Daubert standard; either keeping with the Frye standard or opting for their own testing methods (O’Connor, 2010). For additional information on global legal considerations concerning digital crime, digital forensic investigations, and admissibility of digital evidence, please see the Additional Reading.

The field of digital forensic investigation has had to cope with the rapid creation and adoption of digital devices. A growing number of interconnected devices can be exploited from almost anywhere in the world, but law enforcement still struggle with the concept of jurisdiction in an online world without borders, sometimes resulting in illegal, or at least questionable, cross-border actions by law enforcement (Lemos, 2001; Anderson, 2012). While research, legal and even practical
foundations of digital forensics have been slowly forming, a continuing lack of communication between government, corporate and academic entities worldwide has been a limiting factor in the effectiveness of investigating global digital crimes (Broadhurst, 2006; Jang, 2012).

Continued Lack of Communication in an Increasingly Connected World

According to Internet World Stats (2011), from late 2000 to late 2011 there has been an estimated 528.1% worldwide growth in Internet users, numbering 361 million in 2000 to 2.267 billion at the end of 2011, a trend which is expected to continue (IBTimes, 2010; Meeker, 2012). Cisco (2012) estimates that there will be over 10 billion mobile-connected devices by 2016. Further, traditional and non-traditional digital devices - such as TVs and kitchen appliances - are expected to be increasingly connected to the Internet, contributing to a forecasted 50 billion devices connected by 2020 (Higginbotham, 2010). This growth in users, devices, and associated services has given rise new possibilities for business and communications, as well as digital crime. Statistics from the Internet Crime Complaint Center (IC3) (IC3, 2011), a US-based organization, show that there was a 3.4% increase in complaints filed from 2010 to 2011, with 303,809 and 314,246 complaints per year, respectively. McAfee (2010) gives an overview of the growth of digital crime from 2000 to 2010, claiming that the cybercriminal community evolved from hackers simply looking for a challenge, to organized gangs looking to profit off the rapidly increasing use of connected devices and services. Some gangs are well established, and in 2011 a single highly-organized gang was suspected of being responsible for up to a third of all data thefts (Williams, 2011). Digital forensic investigators, however, not only need to deal with booming online criminal activity, but also the use of digital devices related to more traditional crimes. For example, Gogolin (2010) claims that most investigations today involve some sort of digital component. Cisco (2012) estimates that “[b]y the end of 2012, the number of mobile-connected devices will exceed the number of people on earth.” In more saturated regions when a crime happens, both criminals and bystanders are likely to be producing digital information, which may be of use in the investigation of a non-digital crime. Amateur pictures and videos taken by cell phones have captured abuse, and even murder (Barnard, 2009; CNN, 2009), and have been used as evidence in court (Nguyen, 2012). Further, text messages, cell phone logs and geo-location services are also commonly analyzed by law enforcement in digital and non-digital crime investigation. This presents a difficult situation for digital forensic investigators. The field of digital forensic science is relatively new, technologies are rapidly advancing, and the scope of the digital investigator’s job continually expands. Yet funding for digital investigators in law enforcement is slow to increase (Gogolin, 2010). This may change with the perceived growing threat of a full-scale “cyber war,” and some countries may begin to focus budgets on digital investigation and security (Paul, 2012). Regardless, digital forensic investigators must attempt to keep up with rapidly advancing digital, as well as traditional, criminals while ensuring the integrity of the science of digital forensics. Rapid changes in digital forensic science, however, cannot come from digital forensic investigators alone. Improved collaboration and communication is needed between the currently siloed digital crime investigation players—military, law enforcement, corporate, and academia—and must be focused at a global, not national, level (Jones, 2012).

Digital Forensic Investigation

Carrier (2006) differentiates between ‘digital investigations’ and ‘digital forensic investigations,’ claiming that “[a] digital investigation is a process to answer questions about digital states and events,” while “[a] digital forensic investiga-
tion is a special case... where procedures and techniques that are used will allow the results to be entered into the court of law.” Under this definition, when an investigator is conducting a digital forensic investigation, the focus is on ensuring that the overall investigation process is able to produce evidence that is admissible in court. While this is a requirement for law enforcement, non-LE entities do not always consider the admissibility of evidence when beginning an internal investigation. This may lead to administrators or technicians unknowingly overwriting data of evidential value that may later be unusable by law enforcement once it was found that the case needed to be escalated to a criminal investigation. It is for this reason that all digital investigators should be competent, and able to consider how their actions could affect future legal recourse (ACPO, 2008). “[A]ny case involving computer forensics should always be treated as though it were going to court, and that any documentation and evidence will eventually be turned over to a prosecuting attorney” (Shinder and Cross 2008).

Digital forensic investigations are comprised of many different sub-fields. The general sub-fields include computer forensics, network forensics and cellular phone, or mobile device, forensics: each of which is comprised of more specific forensic studies, e.g. file system, memory, and software analysis. Further, specific sub-fields are forming with the advancement of technology, such as critical infrastructure investigations (Purdy, 2010) and Cloud forensics (Ruan, et al., 2011). While the technical aspects of an investigation may be specific to the suspect device, the examination and investigation process models can be generically applied.

**Digital Forensic Investigation Phases**

When considering digital forensic process models, there are essentially two layers of abstraction that are discussed: the depth of digital forensic examination, and the process phases of each type of examination. The depth of forensic examinations was not always considered, and each piece of suspect storage media normally received a fully in-depth analysis. Since the capacity of common data storage media has, and still is, growing rapidly—combined with a growing number of cases involving digital storage devices—some investigators are finding it impractical to conduct in-depth analysis on each piece of media. “[F]ew [Digital Forensic Laboratories] can still afford to create a forensic duplicate of every piece of media and perform an in-depth forensic examination of all data on those media… It makes little sense to wait for the review of each piece of media if only a handful of them will provide data of evidentiary significance” (Casey, et al., 2009). This philosophy has led to the growing acceptance of digital forensic triage (Rogers, et al., 2006; Koopmans, 2010; Mislan, et al., 2010), as well as the concept of a preliminary analysis; both of which will be discussed further.

Casey, Ferraro et al. (2009) described a three-tiered model of forensic examination to enable the “tailoring [of] forensic examination[s] of digital evidence to the type of crime or case under investigation.” This model includes a survey/ triage forensic inspection, a preliminary forensic examination, and finally an in-depth forensic examination. Many law enforcement agencies are currently considering, and even implementing this model (Goss, 2010). Though, corporate and contract-sector digital forensic analysts are currently more likely than law enforcement to use triage and preliminary analysis techniques (James & Gladyshev, 2010).

**Triage Forensic Inspection**

Koopmans (2010) proposed a definition of digital forensic triage that is derived from the definition of triage in the medical context:

*A process for sorting injured people into groups based on their need for or likely benefit from...
immediate medical treatment. Triage is used in hospital emergency rooms, on battlefields, and at disaster sites when limited medical resources must be allocated.

Koopmans then applies the medical definition to computer forensics, resulting in computer triage being defined as: “A process of sorting computer systems into groups, based on the amount of relevant information or evidence found on these computer systems.” Casey et al. (2009) defines triage as a “[t]argeted review of all available media to determine which items contain the most useful evidence and require additional processing.” In Rogers et al. (2006), and later expanded by Mislan et al. (2010), triage is a process, normally performed on-scene, that is used to:

1. Assess the severity of a crime and prioritizing it accordingly;
2. Assess the offender’s possible danger to society;
3. Obtain actionable intelligence in exigent circumstances (e.g., missing person, military operations, risk of evidence destruction);
4. Identify the richest sources of digital evidence pertaining to an investigation;
5. Identify victims that are or may be at acute risk;
6. Identify potential charges related to the current situation; and
7. Determine whether a certain item requires deeper inspection, such as recovery of deleted information or decoding of encrypted data.

Generally, the key point with digital forensic triage is that triage can be used to identify the ‘richest sources’ of digital evidence at the scene, allowing the detected media’s in-depth examination to be focused and expedited. Triage is an extremely high-level examination, designed to be fast, not thorough. Under this philosophy, and Koopmans’ definition, triage is not designed to normally remove media from needing further examination, and only allows for a shallow, focused view of found evidence—aka low hanging fruit—that helps in the prioritization of all the exhibits. However, some organizations, such as ADF Solutions (2011), claim that “triage can identify and eliminate negative computers with the same degree of confidence as can full forensic examinations.” Differences in definition have caused some confusion within the digital forensic community. This claim, however, is very different technically and philosophically from triage as previously defined, and should instead be considered as a preliminary forensic examination.

Preliminary Forensic Examination

A more in-depth examination than triage, preliminary forensic examinations have “the goal of quickly providing investigators with information that will aide them in conducting interviews and developing leads” (Casey, et al., 2009). Depending on the results found during triage, the type of case, and the policy of the department, a preliminary analysis might be deep enough to justify discontinuing analysis on that particular media if nothing was found. Because preliminary analysis is more in-depth than triage, it usually takes longer, and as such may or may not be conducted on-scene. Several tools with various preliminary analysis workflows exist, such as SPEKTOR, ADF Triage-Examiner, and Cybercrime Technologies’ Rapid Evidence Acquisition Project. Most are designed to be easy to use, and are highly automated. This allows first responders with minimal training to be able to conduct preliminary analysis. Again, depending on the organization’s policy, if suspect traces are found during a preliminary analysis, the media will continue to receive an in-depth analysis with a focus on the already discovered traces. If no suspect traces were found, then further analysis may not be necessary.
In-Depth Forensic Examination

An in-depth forensic examination is usually analysis conducted with media that has been seized, and is much more thorough than the previous tiers of examination. Because of this, in-depth forensic examination also takes a considerable amount of time longer (Goss, 2010). This is also the most manual level of analysis; however, some tasks can be automated. Casey et al. (2009) defines an in-depth forensic examination as a “[c]omprehensive forensic examination of items that require more extensive investigation to gain a more complete understanding of the offense and address specific questions.” This can be considered the standard depth of analysis. The type of case and the used digital forensic investigation process model dictates if the previous two tiers of examination will be used, but there will rarely, if ever, be a case where an in-depth analysis is not necessary to answer questions about suspect media.

Digital Forensic Investigation Process Models

“[T]he reality is that there is no single process for digital forensics” (Carrier, 2008). Various process models have been proposed, and commonly used models will be briefly discussed; however, as stated before, there is no one accepted standard, and the majority of organizations are creating their own SOP, which may or may not be based on an existing process model. For a comprehensive overview of other proposed models, see Additional Reading.

Digital Forensic Research Workshop 2001

In 2001 the Digital Forensic Research Workshop identified an investigative process for Digital Forensic Science (Palmer, 2001). This process included identification, preservation, collection, examination, analysis, presentation, and decision phases (see Figure 1). In Figure 1, the items in gray were the most agreed upon, and “were identified by the attendees as core processes [of digital forensic investigations]” (Pollitt, 2007).

National Institute of Justice

The U.S. Department of Justice (DoJ) National Institute of Justice (NIJ), created an electronic crime scene investigation guide for law enforcement in 2001. In this work, a four-phase process model was proposed. This model, however, was later expanded in the second edition of the guide (NIJ, 2008). The overall model consists of preparation, preservation, documentation, collection, examination, analysis, and reporting.

- **Preparation:** Knowledge about the types of devices commonly encountered, potential evidence sources, investigative tools, and equipment for collection, packaging and transportation of electronic evidence.
- **Preservation:** Securing and evaluating the crime scene; ensuring the safety of persons and protecting the integrity of all evidence.
- **Documentation:** Documentation of the scene, and electronic evidence.
- **Collection:** “The search for, recognition of, [and] collection of… electronic evidence.”
- **Examination:** “Helps to make the evidence visible and explain its origin and significance.”
- **Analysis:** “Looks at the product of the examination for its significance and probative value to the case.”
- **Reporting:** “A written report that outlines the examination process and the pertinent data recovered completes an examination.”

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) proposed a four-phase model in the special publication 800-86 (Kent, et al., 2006). This model includes collection, examination, analysis and reporting phases (see Figure 2).
In this model each phase is defined as such:

- **Collection:** “Identify potential sources of data and acquire data from them”
- **Examination:** “Assessing and extracting the relevant pieces of information from the collected data”
- **Analysis:** “Study and analyze the data to draw conclusions from it”
- **Reporting:** “Preparing and presenting the information resulting from the analysis phase”

**Integrated Digital Investigation Process**

Carrier and Spafford (2003) proposed a investigation process model that considered the physical investigation along with the digital investigation.
Digital Forensic Investigation and Cloud Computing

Figure 3. Integrated digital investigation process phases (Carrier & Spafford, 2003)

Figure 4. Integrated digital investigation process breakdown of physical crime scene investigation phase (Carrier & Spafford, 2003)

(see Figure 3). This model, named the Integrated Digital Investigation Process (IDIP), takes a holistic approach to crime scene investigation, where the physical crime scene reconstruction (see Figure 4) effects, and is affected by, the digital crime scene reconstruction (see Figure 5) to form a complete theory of happened events. Unlike the previous models, the IDIP feeds back between the physical and digital investigation phases. However, the overall model can be described as: Readiness, Deployment, Preservation, Survey, Documentation, Search, Reconstruction, Presentation, and Review.

All of the previously discussed process models have a common core. While each model has components that will continue to be debated, each model generally attempts to secure suspect data, analyze the secured data, and report on the findings in a way that is admissible in court. To accomplish this, preparation beforehand is necessary, as is meticulous documentation throughout the entire process. A particular model may be better suited to a certain organization, but generally each model will accomplish these main goals. One issue is in the standardization and verification of models used. Ensuring that the investigation and examination processes are valid is a topic of concern that can only begin to be alleviated when rigor is introduced into each phase of a digital forensic investigation.

Formal Methods

The concept of digital forensics as a science has been debated, and a call for formalizing digital forensic investigations has been proposed by academics and practitioners alike (Stephenson, 2003;
The digital investigation process can be considered scientific if it formulates and tests hypotheses that are scientific” (Carrier, 2006). Various formal models have been proposed for digital investigation processes, such as the computer history model (Carrier & Spafford, 2006), finite state machine models (Gladyshev, 2004; James, et al., 2010), and others (Willasen, 2008; Rekhis & Boudriga, 2010). Research into the formalization of digital investigations is increasing, but these techniques are usually still too theoretical to be practically applied. Going forward, however, newly implemented digital investigation processes must be based on formal methods in order to ensure validation and integrity of the process, and to guarantee the field is backed by scientific, rather than improvised, methods.

**Digital Evidence**

The Scientific Working Group on Digital Evidence (SWGDE) define digital evidence as “[i]nformation of probative value that is stored or transmitted in binary form” (SWGDE, 2009). There are two states of data that digital forensic investigators must work with: live (non-persistent) data and post-mortem (persistent) data. Live data is data in a system that is powered on, and is more prone to change. Persistent data is data available when the system has been shut down. It must be said that all data has a degree of volatility, or susceptibility to change, and the speed in which data is likely to change, ordered from fastest to slowest, is known as the Order of Volatility (OoV). Farmer and Venema (2005) give an example of a “rough guide” for the order of volatility for different locations of data storage, assuming a live system (see Table 1).

Digital investigators must consider the implications of collecting each type of data, and be able to prioritize the data by the order of volatility. The order of volatility, and even availability of data, differs between a live system and an offline system.

**Post-Mortem Data Forensic Acquisition and Verification**

Many digital investigators have been taught to physically disconnect the power, or “pull the plug,” on a suspect computer that is powered on at a crime scene (NIJ, 2008). Disconnecting the power would ensure that evidence would not be modified by processes running on the suspect system. Pulling
the plug became standard practice until relatively recently when investigators, and the legal system in general, started considering volatile data, such as data in Random Access Memory, that was being lost. Once the power had been removed, a digital investigator was able to copy the persistent data, such as data written to the hard drive before powering down. Because persistent data is static, it is relatively easy to verify that the data has not changed over time. Verification of static data for digital forensic investigation purposes is normally done using a cryptographic hash.

“A hash function (H) is a transformation that takes an input \( m \) and returns a fixed-size string, which is called the hash value \( h \) (that is, \( h = H(m) \))” (Public-Key Cryptography Standards, 2009). Hash values are used in digital forensic investigations to verify the integrity of data. Hash value in the context of digital forensics are defined as “numerical values, generated by hashing functions, used to substantiate the integrity of digital evidence…” (SWGDE, 2009).

Once a suspect’s device is shut down, an examiner can make a bit-by-bit copy of the storage media, known as a ‘forensic image’ (Shipley & Door, 2012). A common way to acquire the suspect’s storage media is by removing the suspect hard drive, and attaching it to a workstation using a hardware or software write-blocker to ensure no data can be written. Once connected, many tools exist to make a bit-by-bit copy of either the whole physical disk, known as a physical disk image, or to make a copy of specific partitions on the disk, known as a logical disk image.

By hashing the suspect bit-level data on the media before acquisition, the resulting hash value becomes the standard with which to compare to ensure 1) the data on the suspect disk has not changed through actions of the examiner, 2) the created forensic image is an exact copy of the original suspect media, and 3) the suspect data can be verified by a third-party. Hashing static data at the time of acquisition allows investigators throughout the chain of custody to verify that any previous, or current, processes have not altered the data they are working with. Persistent data may be verified by utilizing the fact that the data should not change over time. Because of this, a hash of the data can be compared with the original, even years later. In the case of a post-mortem data analysis, the hard drive of a suspect computer can be removed and hashed, and a forensic disk image, or exact copy of the data, could be created. The disk image could then be hashed. If both hash values are exactly the same, then the data on the hard drive, and within the disk image, can be said to be the same. Hashing and Imaging is normally done after powering down the suspect computer. The hashing process is not instantaneous, and shutting down ensures that no data changes while hashing process is taking place. In many situations, however, powering down a critical server may not be feasible, or data that is relevant to the case may not be persistent. In these cases, live data forensics may be the only alternative.

### Live Data Forensic Acquisition and Verification

Live data forensics has been proposed to “provide additional information that is not available in a disk-only forensic analysis” (Adelstein, 2006). Live data forensics is conducted on a running suspect system, and is used to collect volatile data—such as the contents of RAM—that may contain encryption keys, chat fragments, active network connections, active processes, cache, etc.

#### Table 1. Approximation of the lifespan of data by order of volatility

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Time Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registers, peripheral memory, etc.</td>
<td>nanoseconds</td>
</tr>
<tr>
<td>[Random Access Memory]</td>
<td>nanoseconds</td>
</tr>
<tr>
<td>Network state</td>
<td>milliseconds</td>
</tr>
<tr>
<td>Running processes</td>
<td>seconds</td>
</tr>
<tr>
<td>Disk</td>
<td>minutes</td>
</tr>
<tr>
<td>Floppies, backup media, etc.</td>
<td>years</td>
</tr>
<tr>
<td>CD-ROMs, printouts, etc.</td>
<td>tens of years</td>
</tr>
</tbody>
</table>
Live forensic imaging of a suspect drive may also be done on critical systems that cannot be shut down. There are a number of benefits and drawbacks to live data forensics. Sometimes live data forensics is necessary because the system may be critical to business continuity, shutting down may create legal liability for examiners, or the system may have encrypted media that will be inaccessible when dismounted (Bilby, 2006). In these situations, live data forensics may be the best way to collect evidence, although not ideal. Several challenges with live data forensics must be considered.

First, the suspect system is still running, and data is likely to be changing as it is being collected. Because of this, it is impossible for a third party to verify that the data collected is correct. This is similar to previously discussed fingerprint extraction methods. Acquiring a copy of the fingerprint alters the original, making it impossible to be verified by a third party. In the case of digital forensics, to acquire RAM (from the suspect machine) a program must first be loaded into the suspect RAM. Meaning that to collect the data, some data must be altered. Further, acquiring RAM takes time, and during that time processes may be starting or stopping and users may be connecting and disconnecting from the suspect system. By the time the entire contents of RAM have been acquired, the state of the RAM has changed from when collection began. Hashing methods for verification of live data are only useful for the data that has been collected and is no longer changing. Data that has been collected cannot be verified after acquisition since the original data is constantly changing, and is no longer the same as at the time of acquisition. In addition, there is a possibility of crashing the suspect system when attempting live data forensics, which has potential to disrupt, or even corrupt, critical business data.

Second, when conducting live data forensics, the investigator will make changes to the system. However, in order to collect volatile evidence, the suspect’s computer must remain on, and the suspect’s operating system must be used to access the needed data. When retrieving information from RAM, for example, a program must be loaded into the running memory, changing its contents. Even just inserting a USB key into a running suspect system will alter the system. However, Principle 2 of the ACPO guideline states:

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.

Principle 2 essentially allows the use of live data forensics in extraordinary situations, as previously mentioned, as long as the investigator is both competent, and knows the full impact of his or her actions.

Finally, live data forensics usually relies on the suspect system. Alternative methods of RAM acquisition, such as the so-called ‘cold boot attack’ (Halderman, et al., 2009) and FireWire acquisition methods (Martin, 2007; Gladyshev & Almansoori, 2010) have been proposed, but these methods also have associated risks. Carrier (2006) claims that the suspect system cannot be trusted. Rootkits or other malware in the suspect system can provide various anti-forensic functions, resulting in unreliable evidence (Bilby, 2006). To minimize the reliance on the suspect system, Carrier suggests that analysis applications should use their own file system code rather than relying on the kernel and system calls, and to use trusted binaries on write-protected media; a technique most live data forensic tools, such as Microsoft’s Computer Online Forensic Evidence Extractor (COFEE) (Mansfield-Devine, 2010; Microsoft, 2010) are using. These techniques do not completely remove the risk of malicious code on the suspect system affecting a forensic investigation, but, assuming Principle 2 of the ACPO guideline has been met, they do reduce the risk to a level that tends to be accepted in court.
Regardless of the drawbacks, live data forensics is sometimes the only option for collecting evidence. Live forensic data has been accepted in court (Adelstein, 2006), and since computer systems are becoming increasingly more distributed, data center oriented, and services are becoming more ‘Cloud’ based, traditional post-mortem data forensics becomes less of an option.

CLOUD COMPUTING: SECURITY AND DIGITAL FORENSICS

This section introduces cloud computing, related terminology, and service and deployment models. Once fundamental knowledge of cloud computing is established, some key cloud computing security challenges will examined, followed challenges cloud computing brings to digital forensic investigations.

What is the Cloud?

The concept of cloud computing, and the services provided via the “Cloud,” has received increasing interest from the public, private companies and even government organizations (Paquette, et al., 2010; Russell & Hammons, 2012), and as such are introducing more opportunities for cyber criminals and new challenges for law enforcement (Biggs & Vidalis, 2009). Many believe cloud computing is a computing paradigm shift, while others believe that cloud is a collection of old technologies with a new name for marketing purposes (Johnson, 2008; Armbrust, et al., 2009; Ellison, 2009). An obscure understanding of both the underlying technologies and new business model opportunities—and where each begin and end—has lead to some confusion in the definition of cloud computing. This confusion in definition appears to come from the fact that cloud computing is primarily comprised of three service layers\(^5\): infrastructure, platform, and application (Mell & Grance, 2011), each of which can be completely, or even partially, provided by any number of Cloud Service Providers (CSP).

Cloud computing encompasses each of these three service layers, which will be discussed further, but some layers are neglected when definitions focus on particular technologies rather than cloud computing as a whole concept (Vaquero, et al., 2008). Armbrust et al. (2009) submit that “cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services.” NIST (Mell & Grance, 2011) has proposed an arguably more comprehensive definition for Cloud Computing that is gaining in popularity:

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

Further, NIST identifies five ‘essential characteristics’ of cloud computing, these being on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. When each of these essential characteristics are met, it allows for “the illusion of infinite computing researches available on demand… [as well as] the ability to pay for the use of computing resources on a short-term basis as needed” (Armbrust, et al., 2009). In other words, computing resources can be sold to customers as a utility, much like water or electricity, where the customer is able to use as much as they want, when they want, and only pay for what they have used.

Armbrust, Fox et al. (2010) claim that when computing resources can be sold as a utility, there are at least three use cases that “favor utility computing over conventional hosting.” The first is when a company must build their data center to be able to serve the peak load. At times when...
load is less than peak, infrastructure is being underutilized. They claim that “cloud computing lets an organization pay by the hour for computing resources, potentially leading to cost savings even if the hourly rate to rent a machine from a cloud provider is higher than the rate to own one.”

The second case is when a customer does not yet know the demand for their services. Since computing resources in the Cloud can be provisioned as needed, as a user base rises or falls, so too can the amount of computing resources provisioned by the customer be added and removed. Rapid provisioning allows a customer to be more flexible in situations where load may be highly variable or rapidly increase as popularity grows.

The third case is for batch processing needs. Since the cost of processing using one machine for 1,000 hours, and 1,000 machines for one hour is the same, companies who require batch processing can potentially save time on their processing needs.

Choo (2010) expands on these points, considering the benefit of “avoid[ing] the expense and time-consuming task of installing and maintaining hardware infrastructure and software applications,” claiming that hardware investments and administrative costs may be reduced when utilizing cloud infrastructure.

Although cloud computing may provide a number of benefits, it is not without potential drawbacks. Risks in terms of security and investigation will be discussed in later sections, but many potential risks, to both the CSP and the cloud customer, are dependent on the service and deployment models utilized.

Cloud Computing: Service Models

Cloud computing is primarily comprised of three service layers (Mell & Grance, 2011). These three layers are also essentially business models, or the level at which cloud services are normally sold by a Cloud Service Provider.

**Infrastructure as a Service**

The first of the three primary service layers is the infrastructure layer, which is comprised of computing hardware, and a software abstraction layer. Computing hardware in the Cloud is relatively unchanged from pre-cloud infrastructures; datacenters, for example, still largely use the same hardware. Some companies are attempting to market their hardware as specifically ‘for cloud’ (Duffy, 2009; Myslewski, 2009), which focus on faster delivery, convergence or multi-processing, but these technologies may also be useful for non-cloud infrastructures.

Still in the infrastructure layer, but on top of the hardware, is a software layer, termed hypervisor. “[The hypervisor] provides an abstraction layer that allows each physical server to run one or more ‘virtual servers,’ effectively decoupling the operating system and its applications from the underlying physical server” (Xen, 2011). For cloud services, at this layer is also a management stack that allows resource pooling. Many separate servers can then be added to the resource pool, creating the illusion of an infinite amount of resources. This concept is quite similar to distributed, or grid, computing6. The difference is in resource allocation for a task. With cloud computing the customer is allocated “a small fraction of the total cloud resource pool” (Eucalyptus, 2010), allowing multiple customers to use separate fractions of resources from the pool at the same time. In traditional distributed systems, a customer’s task will attempt to utilize most, if not all, of the resource pool until their task is complete. This means other customers must wait in a queue until tasks before them are complete (McGuigan, 2011).

With cloud computing, a company effectively has a large pool of processing and storage of which a small portion of the whole can be rented to customers when needed, usually on a pay-per-usage scheme. This is referred to as Infrastructure as a Service (IaaS). To create the illusion of infinite resources IaaS requires a considerable investment...
Digital Forensic Investigation and Cloud Computing

in hardware, and has high associated running costs. Hobson (2010) claims that “Cloud Service Providers like Amazon, Google and Microsoft are driving the push, because they have excess capability to spare.” As described previously, an attractive feature of IaaS to many companies is a possible operating cost reduction by letting an IaaS provider handle the hardware and maintenance, rather than buying and maintaining more hardware than they need, or running the risk of having too few resources during a spike in customer activity.

Platform as a Service

The second of the three primary service layers is the platform layer. The platform layer relies on the previously mentioned infrastructure layer, and has the goal of providing a Web-accessible platform for customers. The customer, however, normally has no control over the infrastructure layer that the platform is built upon. “This cloud computing model provides a platform for developers to code, test and experiment [with] new software without the complexity of setting up and maintaining test, development and production servers” (Brennels, 2010), and is known as Platform as a Service (PaaS).

The platform provided is usually either a base operating system or a full software stack used to deliver a solution. Whatever the platform, the reason for it is generally storage, application development, and hosting, especially for providing services to many concurrent users. Some platform services, for example, are Google Apps, Microsoft’s Azure, and Amazon’s EC2. By utilizing the flexibility of the resource pool at the infrastructure level, the provided platform can quickly be allocated more or less resources, or multiple platforms—sometimes referred to as instances—can be created and configured, allowing the “increase or decrease [of] capacity within minutes, not hours or days” (Amazon, 2011).

Software as a Service

The third of the three primary layers is the software layer. At the software later, a provider’s applications are provided to the customer. This is known as Software as a Service (SaaS). As the top tier, the software layer relies on both the platform and infrastructure layers for both hosting, and to allocate more or less resources for the application based on the application’s needs. The customer, however, normally has no control over the platform and infrastructure layers that the application is running on. Google Docs and Apple’s icloud are examples of software as a service (Wang, et al., 2011). The applications are hosted by a provider, and are delivered to a client through a gateway. The client, in the case of Google Docs, for example, does not install any applications locally, and can save user data either locally or to available storage provided by the infrastructure and application layers.

Other Service Models

Other service models exist which are built on top of some, or all, of the three previously mentioned primary layers. One such example is Recovery as a Service (RaaS), which is essentially a backup of servers and data to a cloud that can be made live in case of failure or emergency. Gartner (Pettey, 2011) defines RaaS as “the managed replication of virtual machines and production data in a service-provider’s cloud, together with the means to activate the VMs to support either recovery testing or actual recovery operations.” Failing over to backed-up systems that can immediately be made live in the Cloud has a potential benefit of being faster than receiving and recovering from tape backups, with possibly less data loss in the process (Brennels, 2010).

Another proposed model is Security as a Service (SecaaS). The Cloud Security Alliance (2011) define Security as a Service as “the provision of security applications and services via the Cloud either to cloud-based infrastructure and software
Digital Forensic Investigation and Cloud Computing

or from the Cloud to the customers’ on-premise systems.” In the same way cloud computing potentially reduces computing costs for companies, SecaaS may “… enable enterprises to make use of security services in new ways, or in ways that would not be cost effective if provisioned locally.”

A final example is Forensics as a Service (FaaS). When conducting digital forensic investigations, large amounts of data must be processed. Efforts have begun to utilize the resources cloud computing provides, and apply them to digital forensic processing needs (Didone & de Queiroz, 2011; Carrier, 2012). The majority of work thus far has focused on utilizing processing capabilities, normally for law enforcement or consulting companies. But just like other described service models, cloud-based forensic services as software, or even a platform, could potentially be provided to users cloud-based infrastructure or on-premise systems. Potentially reducing the time from incident detection to forensic investigation.

These are only a few examples in a trend towards what Hewlett-Packard (2011) describes as “Everything as a Service” (XaaS).

Cloud Computing: Deployment Models

Organizations have a wide range of needs, and are looking to cloud computing to reduce operating costs. An organization, however, may not feel comfortable entrusting their entire infrastructure, hosting and storage needs to an off-site, uncontrollable CSP. Likewise, some organizations, such as government entities, may have higher security standards and requirements than average cloud customers. Three primary deployment models are commonly used to meet the almost endless combination of needs from organizations that still want to receive the benefits of cloud computing.

Private Cloud

NIST (Mell & Grance, 2011) defines a private cloud as “infrastructure [that] is provisioned for exclusive use by a single organization…. This allows the organization to utilize some of the benefits of cloud computing, such as resource pooling, hardware abstraction, robustness and fast instance deployment and configuration, while still keeping both physical and policy level control of all hardware, software and services. The resources in a private cloud are utilized only for the single organization, referred to as ‘single tenant’ environment. Operating a private cloud, however, still requires an investment in infrastructure and knowledge. Because of this, over or under provisioning of resources is still possible, and costs associated with infrastructure, running and maintenance may still be a burden on the organization. Since this model is single tenant the costs are not distributed, making it the most expensive model.

Public Cloud

Public clouds are cloud services offered to the public via a CSP. Unlike a private cloud, the organization running the cloud service does so to offer cloud resources to external customers. Multiple customers then lease resources from a shared resource pool, referred to as a ‘multi-tenant’ environment. The CSP then takes on the burden of installing, running, and maintaining the provided infrastructure. Since the infrastructure/platform/software security concerns are managed by the dedicated CSP, some organizations may benefit from better security practices than they would be able to create and implement in-house. Since this model is multi-tenant, the costs are distributed over a large number of customers, making it the least expensive model. With this model, cloud customers may trust the CSP for hosting, storage and general access to the customer’s data—all of which could be revoked or removed by the CSP, e.g. if the customer stopped paying, or the CSP went out of business (Kravets, 2012). CSPs offer comprehensive Service Level Agreements (SLA) to define what they are and are not responsible for. While the customer may have some control
Digital Forensic Investigation and Cloud Computing

over whether their data is stored nationally or internationally, they do not generally have physical access to their host, and can lose a great deal of policy-level control. Lower running costs and increased ease of deployment, however, are attractive for many organizations regardless of this loss of control.

Community Cloud

A community cloud is a deployment where multiple organizations pool their resources to achieve a common goal. By pooling the resources for the community, costs are distributed between the members, allowing for the benefits of a cloud while being less expensive than a private cloud. A community cloud works when each member has similar task, policy, and security needs, but liability, internal security, and distribution of investment and maintenance costs are all challenges with this deployment. For these reasons, this model may not be ideal for business critical hosting needs since a business may have less physical or policy control of their data without the assurance of an SLA.

Hybrid Cloud

For this work, the hybrid cloud deployment model will not be considered one of the primary models; however, it is a noteworthy, often used extension to the primary cloud deployment models. This model also has yet to see a widely accepted common definition. The debated definition from NIST (Mell & Grance, 2011) is:

*The [hybrid] cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).*

This definition is also sometimes referred to as a combination cloud. Under this definition, two or more of the previously described deployment models are joined together, but still remain unique entities. The benefit of this model is one of flexibility, and also potential cost savings. Two common methods are normally used to achieve this goal, cloud bursting and cloud brokering.

“Cloud bursting combines existing cloud infrastructure with remote resources from one or more public clouds to provide extra capacity to satisfy peak demand periods” (Moreno-Vozmediano, et al., 2012). For example, an organization that has its own private cloud may temporarily exceed its internal capacity. Instead of increasing investment in infrastructure for a temporary overutilization, some services can be expanded to a public CSP. To take advantage of cloud bursting, an organization must first identify mission critical and non-critical data. The organization, then, could control what data is hosted on the public cloud, ensuring that mission critical data never leaves their area of physical or policy level control.

A cloud broker, according to Grivas et al. (2010), has knowledge of existing cloud service offerings from multiple CSPs, and the relation between business processes and the cloud services. A cloud customer is able to request a business process change, and the broker discovers and binds new services from one or more CSPs to provide the desired process changes for the customer. This allows customers to focus on their business processes instead of devoting time and resources towards discovering, testing and comparing the plethora of cloud service offerings. A cloud broker could potentially broker services for only one CSP or cloud deployment, but normally brokerage occurs across multiple CSPs (Bloomberg, 2011), potentially resulting in a hybrid cloud deployment for the customers.
Cloud Computing Security and Investigation Challenges

New concepts in cloud computing have created new challenges for security teams and researchers alike (Vouk, 2008). Cloud computing service and deployment models have a number of potential benefits for businesses and customers, but security and investigation challenges—some inherited from ‘traditional’ computing, and some unique to cloud computing—create uncertainty and potential for abuse as cloud technologies proliferate. This section looks at security challenges relating to cloud computing. Further, challenges cloud computing poses to digital forensic investigation will also be given.

Cloud Computing and Security Challenges

According to a survey from Ponemon Institute (2011), only 35% of IT respondents and 42% of compliance respondents believe their organizations have adequate technologies to secure their IaaS environments. The report shows that respondents believe IaaS is less secure than their on-premise systems, however, “[m]ore than half (56 percent) of IT practitioners say that security concerns will not keep their organizations from adopting cloud services.” A drive towards cloud service offerings is reiterated by Gartner (2012), who forecasts that spending on cloud computing at each service model layer will more than double by 2016. At the same time Ernst and Young (2011) found that there is a perceived increase in risk by adopting cloud and mobile technologies, and many respondents believe that these risks are not currently being adequately dealt with. However, North Bridge (Skok, 2012) suggests that confidence in cloud computing is increasing, even though maturity of the technologies remains a concern.

An increased confidence in cloud computing and a drive to improve business processes while reducing costs are leading to security of such systems being a secondary concern. This attitude has been carried over from traditional computing, which could possibly result in the same, or similar, security challenges, such as those presented by the Computer Research Association (2003) in the Four Grand Challenges in Trustworthy Computing.

If both security and insecurity from traditional computing are inherited by cloud computing, both may be augmented with the increased complexity of the cloud model, the way that services are delivered, and on-demand extreme-scale computing. Each cloud deployment and service model has its own considerations as far as security and liability are concerned. For example, in a private, single-tenant cloud where all services may be hosted on-premise, the risks are similar to on-premise, non-cloud hosting. The organization has end-to-end control, can implement and target security systems, and can control critical data flow and storage policies. A challenge with this model is that the organization must have the expertise to be able to create, implement, and maintain a comprehensive security strategy for increasingly complex systems.

Several works have previously examined some cloud security concerns (Armbrust, et al., 2009; Jansen, 2011; Balduzzi, et al., 2012; Kui, et al., 2012; Zissis & Lekkas, 2012). The majority of these works can generally be classified as using a Confidentiality, Integrity, and Availability (CIA) model, extended by introducing the concept of ‘trust.’

Confidentiality

In the CIA model, confidentiality is used to describe the limitation of access to data (or information) to only authorized users. Cloud computing introduces a number of confidentiality concerns. Some reasons for this include multiple—possibly competing—customers utilizing the same hardware, the remote and dispersed nature of the cloud service provider, possible layering of services from multiple CSPs, the legality of data disclosure to...
a third-party, and general access management, among others. Gellman (2009) states that “[c]loud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information,” claiming that a user’s privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider, and potentially along with the jurisdiction in which the data is physically stored.

Messmer (2011) claims that access control in cloud environments is somewhat difficult, and may not meet data protection regulations. Kui et al. (2012) identify access control in outsourced cloud environments as ‘critical,’ defining secure identity authentication as a challenge when data is outsourced to a CSP. “[The] data users and cloud servers aren’t in the same trusted domain; the server might no longer be fully trusted as an omniscient reference monitor for defining and enforcing access control policies and managing user details.” Kui et al. suggest that user authentication may be untrustworthy when outsourced due to server compromise beyond the customer’s domain of control, or potential insider attacks from the CSP.

Balduzzi et al. (2012) demonstrated that potential confidentiality risks exist for users who create and distribute images for use in the Cloud, claiming that, for example, “an attacker can gather SSH private keys [from a virtual machine image] to break into other machines, or use forgotten Amazon Web Services (AWS) keys to start instances at the image provider’s cost.” In their research they were able to recover forgotten AWS and SSH keys that were immediately usable to start new instances at the key owner’s expense; last login information that could be used to collect usernames, target machines, and potentially passwords; browser history, from which they found traces of a user’s company and personal email login information; authentication credentials and potentially interesting commands to extract user and database login information, credit card information, VNC authentication, etc, by examining shell history; and in some cases they were also able to recover deleted files, such as the aforementioned keys and history logs.

Kui et al. (2012), Balduzzi et al. (2012), and Zissis and Lekkas (2012) all identify multi-tenancy as a confidentiality risk with cloud computing. Kui et al. claims, “side-channel attacks present new risks to cloud users’ information in the multi-tenant environment.” It has been shown that an attacker can force a machine under their control to co-locate on the same hardware as a victim, allowing for the possibility of side-channel attacks9 (Ristenpart, et al., 2009). From this, stolen cryptographic keys and passwords, and general spying are possible. Likewise, Balduzzi et al. gave an example of scanning other VM instances on the network, and determining open ports and potentially vulnerable services. Zissis and Lekkas, on the other hand, submit, “Data [persistence] may lead to the unwilling disclosure of private data,” claiming that “a user may claim a large amount of disk space and then scavenge for sensitive data.”

While some confidentiality considerations can be reasonably remedied by choosing a reputable CSP that provides an SLA that suits the organization as well as “certifications of quality and operational control” (Ingthorsson, 2010), other implications, such as legal requirements of the CSP to produce details of customer activities to law enforcement may not be able to be avoided. For example, in some cases in the United States, the government may demand customer details from Internet Service Providers unbeknownst to the customer. “There have been thousands of such requests lodged since the [the Patriot Act] was passed, and the F.B.I.’s own audits have shown that there can be plenty of overreach…” (Zittrain, 2009). Legal, liability, and other jurisdiction issues are not necessarily new privacy considerations brought on by the use of cloud computing, but the level of outsourcing, and the possibly global dispersion of the CSP raises new concerns on the ease of information leakage.
Most of these privacy issues stem from the fact that an organization essentially loses control when their data is given to a third party. Cloud computing adds to this risk by introducing the multi-tenant and service-layering aspects, which could possibly be abused.

Integrity

Integrity in the CIA model normally refers to the trustworthiness of data or information. Jansen (2011) claims that using cloud services, especially in multi-tenant environments, may increase risk to the integrity of data, both in storage and processing. “Multi-tenancy in VM-based cloud infrastructures, together with the subtleties in the way physical resources are shared between guest VMs, can give rise to new sources of threats.” For example, malicious code may circumvent VM isolation methods, and interfere with the hypervisor or other guest VMs. IBM (2010) claims that 35% of known vulnerabilities in server virtualization allow an attacker to escape from a guest virtual machine to either another guest or the hypervisor itself. Even without circumventing isolation methods within the CSPs infrastructure, Balduzzi et al. (2012) showed that traditional software vulnerabilities, such as non-updated software, may still lead to malware infection that could result in questionable integrity of stored data and running services.

Another area that may have an impact on the integrity of data is computation outsourcing. Kui et al. (2012) submit that “the Cloud’s operational details aren’t transparent enough to users. Consequently, various motivations can cause the Cloud to behave unfaithfully and return incorrect results.” Hardware problems, software bugs, or outsider or insider attacks could potentially compromise the integrity of processed data.

Zissis and Lekkas (2012) focus instead on the social aspect of integrity, claiming “the cloud model presents a number of threats including sophisticated insider attacks on [customer data].” They cite authentication as an issue in cloud environments “due to the increased number of entities and access points…” that could potentially lead to a manipulation of software that can affect the integrity of customer data.

Availability

Cloud computing resources are designed for high availability, however, Jansen (2011) submits that cloud service providers “can and do experience outages and performance slowdowns.” Temporary outages have occurred with Amazon (Kosner, 2012), Google (2012), and Microsoft (Parnell, 2012) cloud services, caused by software, hardware or external issues. In these cases, service was eventually restored, but each left customers without access to services and data for a period of time.

Jansen also claims, “It is possible for a service provider to experience serious problems, like bankruptcy or facility loss, which affect service for extended periods or cause a complete shutdown.” Cloud providers have gone out of business before, being bought by other companies that may allow current users a short period of time to retrieve their data (Scheier, 2009), while in other cases massive, irrevocable data loss has occurred (Bright, 2008). Missing a payment could be as drastic, and the only assurance of what will happen to a customer’s is if the consequences are specified in an SLA with the CSP. However, an SLA may not always ensure data can be returned. For example, Megaupload, a once popular file-sharing portal, had company assets seized by New Zealand authorities, denying customers service since the seizure. Although the seizure and international sharing of seized data were deemed to be illegal by a New Zealand High Court (Chirgwin, 2012), service has not resumed, and customers are being denied access to legitimate data (Kravets, 2012).

Armbrust et al. (2009) believe that for high-availability, there should be no single point of
failure. However, they claim, “the management of a Cloud Computing service by a single company is in fact a single point of failure,” again citing hardware and software issues or CSPs going out of business. Further, Jansen and Armbrust, Fox et al. mention Distributed Denial of Service attacks (DDoS) that could potentially cripple cloud services, claiming that with enough computers, even cloud services could become saturated. Since multiple cloud service layers are used, each layer could be a potential point of attack to disrupt service to the client.

Jansen further claims that there is a ‘value concentration’ when data from multiple companies is hosted in the Cloud. This potentially means that cloud services may be more enticing to hackers since one CSP is likely to host data for multiple clients. If the hacker is able to penetrate the CSP, they may then gain data from multiple companies without targeting each of the companies individually.

The CSP is not the only potential point of failure. The client side that relies on cloud services may also be targeted. For example, anti-virus software is increasingly utilizing cloud computing for analysis of code. The response to cloud-based malicious code analysis was viruses that filter client-side network traffic to prevent the anti-virus agent from communicating certain information to the cloud service (Microsoft, 2011). Since client-server communication is a requirement the access cloud-based services, denial of service can be achieved by attacking any point of communication.

The distributed nature of cloud computing can allow for high availability if deployed correctly. A major challenge, however, is not only the traditional challenges of availability of data, but also the dependence on external third parties to be able to access critical data.

**Trust**

Some of the challenges mentioned previously are not unique to cloud computing, but a recurrent point in most work dealing with security in cloud computing is the concept of trust. In the traditional CIA model, critical data and services were normally under physical and policy control of the owner. In this case—except for insider threats—trust is implicit. The owner had a considerable amount of direct control over confidentiality, integrity, and accessibility. If any of these areas were lacking, the owner could make infrastructure or policy changes to improve, and for these reasons, the owner questioning their own level of trust was not explicitly stated. “In traditional architectures, trust was enforced by an efficient security policy, which addressed constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people” (Zissis & Lekkas, 2012). Trust in the Cloud, however, is not implicit. Many articles have been written questioning if data in the Cloud is more secure than on-premise systems (Kaufman, 2009). This is because many companies do not so easily trust external groups, even well known CSPs, to store and process critical data. For example, Ernst and Young (2011) found that “almost 90% of respondents believe that external certification would increase their trust in cloud computing.”

Jansen (2011) claims that cloud customers are relinquishing direct control over many aspects of security. This “confers an unprecedented level of trust onto the service provider.” This trust assumes that the CSP—and every CSP that is providing a service supporting the CSP the cloud customer is using—has proper controls and auditing in place to mitigate threats such as insider access, and vulnerabilities that each used cloud service introduces.

Zissis and Lekkas (2012) claim that in cloud computing the concept of perimeter security becomes “fuzzy.” With traditional security, a perimeter of trust is created, and entities outside of this perimeter are considered suspicious. In the cloud model, critical data and business processes are outside of the perimeter of trust. For this rea-
son, “the ability to clearly identify, authenticate, authorize, and monitor who or what is accessing the assets of an organization is essential to protecting an information system from threats and vulnerabilities.” Zissis and Lekkas also propose that organizations should consider hybrid approaches, where critical systems, processes and data are isolated, and may be provided where the infrastructure is trusted, while non-critical systems, process and data maybe hosted by less-trusted CSPs.

Cloud computing is sold as a utility, or pay-per-use, service. Kui et al. (2012) identify that “because users might have little or no visibility into the cloud infrastructure, they’re often unable to directly connect their actual cloud resource consumption and the usage charges.” Without a guarantee on resource consumption measurement, and the ability to verify and audit charges, charges may be undisputable. For example, issues for which the customer should not be liable could cause excessive charges against which the customer may not be able to dispute. Further, charges could also potentially be falsified by the CSP. Without verifiable resource metering, a customer has no way to prove or disprove a claim.

When services are hosted in a public, multi-tenant, cloud, for example, the customer trusts the CSP for service. The customer is trusting that the CSP is able to competently create, implement and maintain a security strategy, not just for external attacks, but also from other tenants in the same cloud, and that their multi-tenant blanket approach to security will be adequate for all customers. Likewise, the customer must trust the CSP itself to not misuse the customer’s data. Security comparisons of cloud deployments, and even between cloud and non-cloud infrastructures, is somewhat a moot point because “it is possible to deploy a private cloud in a way that is far less secure than the current batch of public clouds just as it is possible to deploy any infrastructure in an insecure way” (Wolski, 2010). Ultimately, it comes down to the organization’s realistic evaluation of their capabilities and what amount of risk they are willing to take.

Other Cloud Security Concerns

Beyond the previously mentioned challenges, data and vendor lock-in is a concern with cloud services (Armbrust, et al., 2009; Kim, 2012). Data and vendor lock-in can become a challenge when Application-Programming Interfaces (API) are not standardized. If interfaces are not standardized, it may become difficult for cloud customers to move from one CSP to another, or even utilize multiple CSPs for data redundancy purposes.

Armbrust et al. also identify ‘reputation fate sharing’ as a risk. They state that “reputations do not virtualize well,” claiming that one customer can impact the reputation of the CSP and all co-hosted users. For example, a spammer using the CSP’s IP range, may get those IP addresses blacklisted (Kerbs, 2008). This could potentially disrupt service of legitimate cloud customers if they are later assigned an IP address that has been blacklisted.

Ernst and Young (2011) claim that “a company’s physical boundaries are disappearing as more of its data is transmitted over the Internet.” Because of the distributed nature of cloud computing, the physical location of data and the jurisdiction in which the data is located is a major concern that is seeing an increase in research (Ward & Sipior, 2010; Hu, et al., 2012; Vaciago, 2012).

The essence of the jurisdictional challenge is that a CSP may have data centers in multiple countries, each with unique laws about how and what data can be imported, exported, stored, and accessed. Depending on the CSP, and the underlying CSPs used to support the services, it may be difficult for a cloud customer to specify and audit the jurisdiction(s) in which they will allow their data to be stored. A customer having adequate knowledge of each of the legal systems where their data may be stored is a challenge that would require considerable resources for research.
Digital Forensic Investigation and Cloud Computing

on the side of the cloud customer. A mistake could allow critical data to be stored in countries with lax cybercrime and/or data privacy laws (Choo, 2010). Ruan et al. (2012) submit that service level agreements should define the level of control the cloud customer over the jurisdiction(s) in which customer data is allowed to reside, as well as allow the cloud customer or trusted third-party the ability to audit such restrictions. An SLA with the initial CSP must also include the ability to control and audit data stored on underlying CSP services.

Many of the previously discussed security considerations normally placed the cloud environment as the target of an attack, however, cloud services may also be used as the originator of attacks (Choo, 2010). For example, a proof of concept cloud-based DDoS infrastructure has been developed to conduct large-scale DDoS attacks using cloud resources for less than a similar criminal botnet would cost (Bryan & Anderson, 2010; Lemos, 2010).

Further, Roth (2011) demonstrated that the large amount of compute available in the cloud environment may be used as an extremely fast, and relatively inexpensive means of cracking passwords. Cloud computing allows the ability for a customer to design massively parallel and GPU assisted environments, applying the cost and time benefits of cloud computing to brute force password cracking.

This work has described a number of security concerns for both CSPs and cloud customers. However, even though these are concerns, Kui et al. (2012) identify that “designing security into cloud benefits users and CSPs, [and] inevitably increased overhead for both.” They submit that additional overhead (such as increased processing requirements) could increase the cost of the cloud services, which may conflict with the economic benefits that companies are hoping to realize by using these cloud services.

Finally, within organizations and between cloud customers and CSPs the ownership for security in the Cloud is not always precisely defined (Ponemon, 2011; Ruan, et al., 2012). If security tasks are not precisely assigned, a customer may be unwittingly vulnerable, and determination of liability when an incident occurs may be difficult.

For more security challenges in the Cloud see Additional Reading.

Cloud Computing and Investigation Challenges

Many of the technologies that make up cloud services, such as virtualization, have existed since before the utility computing business model was practical on a large scale. Because infrastructure, platform, and software hosting technologies have existed for business and personal use for some time, techniques for digital investigation of incidents relating to these technologies may be well known. For example, forensic acquisition and verification of hard drives is a common task in digital forensic investigations. Many times the same acquisition methods for a physical disk may also work for virtual disks associated with a virtual machine. Many of the digital forensic acquisition, verification, and analysis techniques may be able to be applied to cloud investigations, but cloud does pose some new challenges for digital forensic investigators. The following are a few of the many potential challenges cloud computing brings to digital investigation.

In traditional investigations, the suspect or victim’s computers may normally be the main source of information about an incident. For example, in a child exploitation case, a suspect may have stored illicit images on their local hard drive. By finding and analyzing the images, the investigator may be able to determine that the images were, in fact, illegal. Other information, such as the recently opened files list, may be used to support that the suspect had knowledge of the images. However, if the suspect is using cloud-based storage, the images may not be stored locally. In this case, the investigator may be able to show that the suspect had knowledge of the images, but not
whether the images were actually illegal. Saliba (2012) claims that cloud services may reduce the amount of direct evidence available on a suspect’s disk, but sometimes provide more information about the user and cloud service that would help in acquiring a subpoena or warrant. As more data is stored in the Cloud, and services reduce the client-side impact, fewer evidential traces may be found. Instead, investigators will have to rely on more cooperation from CSPs that may not be in the same jurisdiction.

When suspect data is stored in the Cloud the data may be in one jurisdiction while the suspect machine connecting to the service may be in another jurisdiction. This scenario is becoming a challenge for law enforcement in many countries, especially with mobile cloud-attached devices. In many countries, investigators may access data stored remotely if given permission by the suspect (verbal confirmation, entering the password, etc.). However, there has been very little definition of what to do if data is stored on a non-national cloud service that is currently connected while the investigator begins a live analysis of the suspect system. If the data is accessible, an investigator may save a considerable amount of time by acquiring the data from the connected service rather than waiting for international requests. However, authority on this matter is not always clear. In the author’s experience, a lack of definition on the scope of acquisition of data on non-national remote connections sometimes depends on the country, and many times depends on the investigator’s preliminary analysis of the remotely stored data as well as the likelihood of receiving the data if an international request was made.

Investigators physically accessing the CSP may also be more difficult, and may be impossible if the data is distributed over several geographic locations (Taylor, et al., 2011). In traditional investigations, a computer or server may possibly be taken down, and its physical disks imaged. Taking down production servers is increasingly rare for server environments since law enforcement may be liable for damages while the server is down. Taking servers down in a cloud environment may have an impact on many customers, creating more liability. Further, data may be stored on virtual storage spanning multiple servers, or even geographic locations, meaning that hard disk acquisition may not be practical, or even produce the desired data. Liability and reconstruction of virtual storage in cloud environments from physical disk images remains a challenge.

Storage in the Cloud is attractive to users because it is highly accessible and relatively cheap. As previously mentioned, the amount of data on personal hard drives is becoming too large for most law enforcement agencies to acquire and store all the data. Cloud services, however, are currently offering Gigabytes of space for free with the option to pay for more storage. The amount of stored data could quickly add up across multiple cloud service offerings, resulting again in too much data for law enforcement to process and store.

Since acquisition of a whole physical disk may not be practical or possible, and the quantity of data may be too large to effectively process and store, selective data acquisition may be required. Selective data acquisition implies a preliminary analysis, or some prior knowledge, to reduce the overall dataset an investigator is interested in. The challenge with this method is an intrinsic challenge in digital forensic investigations; how do we know what we do not know? In other words, even if all possible data could be acquired, how do we know that no evidence has been missed? If this question cannot be easily answered when all data is available, how can an investigator justify reducing the dataset, and potentially excluding inculpatory and/or exculpatory evidence? Some investigators are currently focusing on data sources that they believe are likely to provide the richest sources of information, but justifiable exclusion remains a challenge.

Because of the distributed, multi-layered nature of cloud computing, chain of custody for the data may be impossible to verify (Barbara, 2009).
Without strict controls it may be impossible to determine where exactly the data was stored, who had access, and was leakage or contamination of data possible. If data is stored in a cloud where multiple users and CSPs potentially have access, association of the data to the suspect is a challenge to establish beyond a reasonable doubt.

When an incident occurs on the side of the CSP, the CSP may be more concerned with restoring service than with preserving evidence. Further, the CSP may begin its own investigation into an incident without taking proper precautions to ensure the integrity of potential evidence. In more severe cases, CSPs may not report or cooperate in investigation of incidents for fear of reputational damage. The challenge in this case is with the competence and trustworthiness of the CSP. A CSP would be an effective, immediate first-responder, but questions about the integrity and chain of custody of the acquired evidence may make admissibility difficult. To meet this challenge law enforcement should work with CSPs, and ensure proper documentation is being created and forensically sound processes are being used.

Another challenge is with feature of rapid elasticity in cloud environments. Data associated with newly created virtual machine instances may only be available for a limited time. To this author’s knowledge, no research has been conducted on determining available data associated with removed VM instances. If a new VM instance is created and either compromised or used to attack, evidential traces may be available in the VM. If the VM instance is then de-allocated, investigators currently do not know whether evidential traces or the entire VM instance cloud be recovered.

The final challenge in this non-comprehensive list is the issue of international communication. As mentioned previously, cloud computing blurs physical, policy, and jurisdictional boundaries globally. However, law enforcement at a global level has yet to find effective, timely, and efficient international communication and cooperation channels. Conferences such as the International Symposium on Cybercrime Response specifically discuss international law enforcement communication and collaboration efforts. Such conferences allow law enforcement to create informal communication channels, and sometimes help in the creation of bilateral agreements for cooperation, but these channels have their limits. Global law enforcement communication channels, such as INTERPOL’s I-24/7 network or the G8 24/7 network, connect many countries, but are limited by their structure and bureaucracy. Many officers have found the global networks to be somewhat effective if the request was not overly urgent, however, these networks have failed to address real-time requests for help from countries under DDoS attack. Many times, law enforcement will prefer faster, informal channels to begin an international investigation, rather that traversing such networks. However, multi-country operations, such as “Operation Unmask” (Norton, 2012), show the potential of these networks to assist in large-scale coordination efforts. Overall, users, businesses and even criminals are utilizing technologies, such as cloud computing, to be able to rapidly find and share (and exploit) new ideas. These groups are no longer considering physical and political borders. Law enforcement, however, is currently restricted by a lack of effective global communication channels, political issues, and jurisdiction that make policing in a globally connected world even more of a challenge.

**DIGITAL FORENSIC INVESTIGATION AND CLOUD COMPUTING**

As more businesses and users adopt cloud computing, security challenges, such as those previously discussed, will be increasingly targeted and exploited. There are many technological and political challenges where investigation of potentially criminal incidents in the Cloud are concerned. Investigators, however, must still be able to acquire and analyze data in a methodical, rigorous, and
forensically sound manner. This section explores the general application of a current digital forensic investigation process model—specifically the Integrated Digital Investigation Process—to cloud computing, and describes cloud investigation considerations at each phase of the model.

### Readiness Phase

Carrier and Spafford (2003) state that “the goal of the readiness phases is to ensure that the operations and infrastructure are able to fully support an investigation.” The operations readiness phase involves the on-going training of personnel, such as first responders and lab technicians, and the procurement and testing of equipment needed for the investigation.

Operation readiness should include education in cloud-related technologies, such as hypervisors, virtual machines, and cloud-based storage. Personnel should have general knowledge of how to interact with cloud technologies at the infrastructure, platform, and software layers, and understand the effect their actions have on the environment. They should understand the methods and tools available to collect investigation-relevant data in each layer of the Cloud. Different CSPs may have proprietary systems, so training on the use and investigation of these proprietary systems should be considered, if possible. Finally, personnel should have the hardware and software necessary to acquire relevant data from the Cloud.

Infrastructure readiness is an on-going process to ensure that investigation-relevant data is available when an incident occurs. Infrastructure readiness is a responsibility of the CSP, the level of which may be defined in the SLA between the CSP and the cloud customer. Because of the different in operations between CSPs, and the differing level of logging and data retention requested by cloud customers, law enforcement may have difficulty considering the type and amount of data that may be available.

The training of personnel, identification of potential risks, and identification of potential data sources before an incident occurs can greatly help in efficient incident response, and with the timely and sound acquisition of relevant data. For this reason, this work recommends that CSPs and law enforcement work together to model threats, their potential impact, and potential evidential trace data sources before an incident occurs. This will assist the CSP in preserving potential evidence during incident response, and will help law enforcement have a better idea of what data will be available, and how to handle such data, if a particular incident occurs.

To help in the identification of threats, their impact on a system, and their potential evidential traces, this work proposes an extension to the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) model (Swiderski & Snyder, 2004). The STRIDE model is used to help understand the result of a specific threat being exploited in a system, and has previously been applied to probabilistic risk assessment in cloud environments (Saripalli & Walters, 2010). In this work, we propose to extend the STRIDE model beyond risk assessment and potential exploitation results, to add the identification of possible investigation-relevant traces produced by the exploitation. We term this the ‘Investigation STRIDE model,’ or I-STRIDE.

As shown in Figure 6, the I-STRIDE process is conducted by first deconstructing a service into its dependent components. A risk assessment is conducted per component, and risk mitigation techniques are derived. This work proposes that each risk identified by I-STRIDE, has associated investigation-relevant data sources. When a threat to a component has been identified, an investigator may determine what data is likely to be effected by the threat. From this subset of effected data, specific data sources that may be of evidential value can be identified. These potential evidential data sources may then be used for pre-investigation planning and data targeting purposes.
Application of I-STRIDE to a Deployed Cloud Architecture

To show the applicability of the I-STRIDE model to cloud environments, assessment of a small cloud computing infrastructure based on the Open Source distribution of Eucalyptus (2011) will be given as an example. The components of this platform will be explained, and an analysis using the I-STRIDE model will be conducted against this deployment.

The Eucalyptus architecture is composed of five high-level components that are essentially standalone Web services (Eucalyptus, 2010). These components include:

- **Cloud Controller (CLC):** The cloud controller is the main entry point for the cloud environment. CLC is responsible for “exposing and managing the underlying virtualized resources.”
- **Cluster Component (CC):** CC is responsible for managing the execution of VM instances.
- **Storage Controller (SC):** Provides block-level network storage that can be dynamically attached by VMs instances.
- **Node Controller (NC):** Executed on every node that is designated for hosting and allows management of VM instances.
- **Walrus:** Allows the storage and management of persistent data.

Figure 7 shows the Eucalyptus components and their connection and communication channels.

The scope of this case will be limited to asset-centric threat modeling. The assets in this case are will be defined as each of the Eucalyptus components, and will also include a cloud client. In this experiment, threats (see Table 2) were identified and exploited in the deployed Eucalyptus architecture. An analysis of which assets were affected and how, was conducted. After, an investigation was conducted to determine potential evidential data sources. Identified threats, their description, the affected asset, the impact on the asset, and the location of potential evidential data sources are listed in Table 2.

Using the I-STRIDE model could help CSPs and law enforcement identify an investigation starting point if a specific incident occurred. This level of readiness would potentially allow for improved pre-planning, first response and cooperation once an incident occurred.

**Figure 6. The I-STRIDE process model for risk assessment, mitigation, and investigation**
Deployment Phase

The deployment phase of the IDIP is split into detection and notification and confirmation and authorization phases. In the detection and notification phase, an incident is detected, and the appropriate people are notified. In the case of cloud, detection and notification may come from the CSP, cloud customer or a third party.

Once an investigator has been notified of an incident, they may then need to confirm the incident, and must get authorization to conduct an investigation. Authorization depends on the investigator’s affiliation, and where the incident took place. For example, an investigator for the CSP may already have authorization from the CSP to investigate, where a law enforcement officer would need authorization to begin the case, and may need to procure warrants. Similarly, if the owner of the system in which the incident took place gives consent for the investigation, that may be all the authorization that is necessary, but if consent is not given, then other legal approval may be required.

Physical Crime Scene Investigation Phase

The IDIP includes a physical crime scene investigation phase. The purpose of the physical crime
scene investigation is to extract physical evidence, and reconstruct the physical scene. Information from the physical crime scene investigation may later feed into, and provide context for, the digital crime scene.

When considering cloud computing, identification of where the relevant physical crime scene may be is a challenge. For example, if a hacker remotely accesses a cloud service to exploit another remote user, the physical crime scene may or may not be at the CSPs data center, depending on the exploit. The crime scene instead may be both at the suspect and victim’s side, and possibly in different countries or jurisdictions.

The physical crime scene investigation phase is comprised of sub-phases including preservation, survey, documentation, search and collection, and reconstruction. These will be discussed further in the context of the digital crime scene investigation. However, “the search and collection phase of the physical crime scene is where the digital crime scene investigation begins” (Carrier & Spafford, 2003). The search and collection phase is used to collect evidence and provide more information that may be relevant.
Digital Crime Scene Investigation Phase

From the physical crime scene search and collection phase begins the digital crime scene investigation. Similar to the physical crime scene potentially being spread out among multiple physical locations, so too may the digital crime scene. For example, evidence may be on both the CSP’s infrastructure as well as the victim’s computer.

The first sub-phase on the digital scene investigation is preservation of the scene. If the crime scene can be identified, for example, where an incident occurred and evidential traces are likely to be found, then the scene must be preserved. If the crime scene is a victim’s computer, preservation may be as simple as removing the computer from the network, or creating a forensic disk image. If, however, the crime scene is ‘at’ a cloud service, preservation becomes a challenge since many users may be accessing the service, potentially changing the scene. With a cloud service, and investigator should consider the best way to preserve the current state of the service, while having a minimal impact on the system.

Once preservation has taken place, as well as possible, a survey and acquisition of potential evidentiary sources takes place. Again, if the scene is a suspect or victim computer, traditional imaging and post-mortem triage and acquisition may be possible. Taking a cloud service offline, however, may not be possible. In the case where the scene must remain ‘live,’ live data forensics is necessary. The survey phase attempts to extract obvious pieces of digital evidence that will potentially give the investigator an idea about the suspect and crime. At this stage, the I-STRIDE model could be used to assist in conducting a targeted survey of the system. Once potential evidential sources have been identified, they are then forensically acquired. Depending on legal and technological restrictions, a computer’s full physical disk may be acquired, or a targeted acquisition may be required.

The IDIP then proposes a documentation phase to document all digital evidence when it is found. Thorough documentation, however, should be conducted in parallel with all other phases in the IDIP. Thorough documentation can later be referred to if any part of the process is questioned. The documentation phase also includes data verification tasks, such as verifying the hash of acquired data. In the cases where live data forensics is necessary, some acquired data may not be able to later be verified. In these cases, precise documentation acts as verification for the investigator’s actions.

Next is the search and collection phase. This phase is a thorough analysis of data and information acquired in the survey phase. If the data has been acquired in the survey phase, then data analysis should be similar irrespective of whether the data sources were acquired from a cloud environment or not. Some cloud-related challenges, however, might be in the analysis of unknown or proprietary data structures. This challenge is not unique to data acquired from cloud environments, but since cloud software that creates proprietary data structures would only be hosted in the Cloud, reverse engineering the data structure may be more difficult.

Once relevant data has been extracted, then the crime scene is reconstructed. “[The reconstruction phase] uses the scientific method to test and reject theories based on the digital evidence” (Carrier & Spafford, 2003). The reconstruction phase is where an investigator determines what the observed data means in relation to the investigation. This is also the phase where an investigator attempts to determine if there is sufficient evidence to support the theory, or whether more evidence would be necessary.

Based on the results from the reconstruction phase, survey and acquisition of the digital crime scene may again be required to collect data determined by the analysis to potentially be relevant. Otherwise, the digital crime scene theory is fed back into the physical crime scene investigation.
model, where more physical evidence may need to be acquired and analyzed, potentially starting another digital crime scene investigation.

**Review Phase**

The final phase of the IDIP involves reviewing the process and results, attempting to determine what worked, what did not, and what changes to the process need to take place. The review phase should be used to guide education, research and tool development efforts that feed back into the readiness phase. From the results of the review phase, new methods may be created to deal with before unknown situations that are specific to cloud environments.

**CONCLUSION**

Cloud computing has a number of benefits, such as high availability, potentially lower cost, and potentially improved security. However, cloud computing also has a number of associated risks. Some of these risks have been inherited from traditional computing models, while the cloud business model introduces others. As more businesses and end users move their data and processing to cloud environments, these environments will increasingly become the target, or even the originator, of malicious attacks. For this reason, digital forensic investigation methods must be tested against cloud computing environments with the help of CSPs to ensure digital evidence is available, and integrity can be maintained and verified.

This work has shown how current digital forensic investigation process models may be used to derive cloud-specific considerations when planning an investigation. In addition, in investigations of cloud environments the CSP will likely be involved. This work has proposed a risk and investigation assessment model (I-STRIDE) that can act as a base for CSPs and law enforcement to more effectively work together before and during the investigation of incidents in cloud environments.

Much more research is necessary concerning digital forensic investigations in cloud environments, but beyond technical challenges cloud computing is already testing the limits of communication and collaboration between international law enforcement. As cloud computing blurs geographical borders for businesses, end users and even criminals, law too must begin to look to a more open, global system; a system where everyone—law enforcement, private sector, academia, and even the public—can play a role to detect, research and reduce digital crime. Cybercrime affects every Internet connected country, and without effective international collaboration, laws, and efficient communication channels that support international collaboration, cybercrime will continue unchecked.

**REFERENCES**


**ADDITIONAL READING**


Finley, K. (2010). 5 cloud-oriented operating systems available now. ReadWrite Cloud.


**ENDNOTES**

1. Also known as Computer Forensics or Cyber Forensics.

2. Some researchers believe various groups have exaggerated the threat of a cyber war (Schneier, 2010).

3. “Cyberwar is a form of war which takes places on computers and the Internet, through electronic means rather than physical ones” (Smith, 2011).

4. Some data, such as imaging Random Access Memory, can be acquired directly from an external FireWire connection (Gladyshev & Almansoori, 2010).

5. The layers of Cloud Computing can also be described in depth by using the Open Systems Interconnection (OSI) model.

6. Distributed computing—computing systems in which services to users are provided by teams of computers collaborating over a network (Arms, 2000).

7. A combination of programs that work together to produce a given result.

8. In this survey, 35% or respondents were customers and 65% were vendors. For these statistics, separation between customer and vender was not shown, and inclusion of venders could potentially bias results in favor of confidence in cloud services.

9. A side channel attack uses physical aspects of a system as sources of information about digital data or processes, such as power consumption, sound, and electromagnetic waves.

10. Brute-force password cracking is essentially attempting every possible key combination until the correct password is found.

11. Asset-centric threat modeling first identifies an organization’s assets, and then focuses on identification of threats to the identified assets.

12. XSS is not specific to Eucalyptus, and is added to illustrate a threat to an asset—the cloud client—that will likely have no in-house traces associated, but is an in-house security issue.