Abstract

The increased use of cloud technology in today’s business, educational and personal computing environments has created several challenges when it comes to digital forensic examinations. Cybercriminals and hackers are exploiting this technology and attacking and infiltrating systems in ways that have not been seen before. Digital forensic examiners, law enforcement officials and cybercrime investigators are facing new hurdles when performing examinations and investigations that involve cloud technology. This study performed research in the form of a review of existing literature related to cloud technology and its impact on the field of digital forensic investigations. The research confirms that the continued development and use of cloud computing technology has a very strong impact on forensic investigations. Investigators will be faced with new hurdles and challenges when performing investigations in cloud-based systems and a new set of standards, guidelines, policies, practices and regulations will have to be put in place to ensure the success of cloud-based forensics.

CHALLENGES OF DIGITAL FORENSIC INVESTIGATIONS IN THE CLOUD ENVIRONMENT

by

Candice E. Torres

A Capstone Project Submitted to the Faculty of

Utica College

Spring 2012

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Cyber Security – Intelligence and Forensics

Table of Contents

Acknowledgments

I would like to thank the faculty and staff of the Utica College Master of Science in Cybersecurity program for developing a dynamic, educational, and informative curriculum which challenged our Cohort throughout our journey. A special thank you to my Capstone instructor, Paul Pantani and my subject matter expert, Vernon McCandlish, for all your edits, comments and constructive criticism that helped make this project a success.

Thank you to my fellow classmates in Cohort 1; it is not an understatement to say that I might not have made it all the way through without your collaboration and support. A special thank you to Kerry Mildon, Carilyn Fennell, and Laura Meagher (we miss you!) for the many phone calls, emails, and Skype sessions while we worked on assignments.

To my wonderful family, Mom, Mike, Joseph, Nikki and Santino, I thank you for all your support, not just through this program, but always. Your faith in my abilities and support for my decisions has always been extremely important to me and I love you all so much. I could not have gotten through this without all your encouragement!

Last, but certainly not least, I'd like to thank Andrew Totman, for being my number one fan. Thank you for always understanding when I had to spend countless hours working on papers, for cooking me dinner at night, and finding ways to keep busy on your own. Your endless support and encouragement has meant the world to me as I completed my "Ironman." We will cross the next 140.6 mile finish line together in 2014. I love you.

Challenges of Digital Forensic Investigations in the Cloud Environment

While cloud computing technology has been around for over a decade, its popularity has only recently begun to increase. It is estimated that by the year 2013, the cloud computing market will reach over $150 billion. The number of cloud users, including individuals, businesses, and government entities, will likely increase in the future, as companies are transitioning to more Internet-based applications, mobile applications and off-site data storage (Ingthorsson, 2011).

Cloud computing is a model for technology that allows its users convenient and on-demand access to shared resources (including, servers, networks, storage, and applications). These resources can be made available to users with minimal interaction by the cloud provider over broad networks, such as the Internet, and can be pooled with other resources to serve multiple consumers. Providing users with a shared pool of resources increases speed and efficiency and allows for greater mobility of data (Mell & Grance, 2011). End users can access applications through the cloud (through web browsers, desktop applications, or mobile applications). Unlike traditional computing products, all data is stored on remote servers located off-site. These servers are not operated and cannot be freely accessed by the end users. Instead, they are controlled and maintained by the cloud providers.

The increased use of cloud technology will inevitably mean that law enforcement investigators, cybercrime investigators, and computer forensic examiners will encounter a greater amount of data that is stored in the cloud than data stored on local servers and on-site computers. With increased use, cloud environments will likely contain an increased amount of evidence of criminal activity (Lawton, 2011). Because this is a relatively new area of examination, law enforcement, forensic examiners and cybercrime investigators will face an array of new challenges in their investigations.

The purpose of this study was to examine and evaluate several of these challenges that investigators face when dealing with data stored as part of cloud technology.

- How are criminals using cloud technology to their benefit?
- In what specific ways does cloud computing pose a challenge for cybercrime investigations?
- Are the current laws, policies, procedures and best practices for cybercrime investigations effective when dealing with cloud computing technology?
- Should changes be made to current policy to aid in the effectiveness of digital cybercrime investigations?

As the use of cloud technology increases, it is more likely that criminals and cybercrime organizations will exploit this technology and use it to their benefit. Criminal activity in the cloud provides a myriad of challenges to cybercrime and digital investigators. According to Thomas Hurbanek, Senior Investigator for the New York State Police Computer Crime Unit, "…cloud computing technologies… could create an environment where entire segments of business activity could be conducted outside the reach of law enforcement" (Sternstein, 2010, par. 6).

A study conducted by McKinsey & Company in 2009 showed that requests for electronic discovery increased by fifty percent annually. The demand for forensic investigations is increasing and an influx of cloud-related cases heavies the burden on digital forensic investigators. Law enforcement officials and other digital investigators must adhere to laws and policies that are currently in place when performing investigations. Because cloud computing is a relatively new technology, current standards and laws are not sufficiently inclusive of the new cloud model and can limit the effectiveness of cyber forensics investigations (Lawton, 2011).

Like with traditional forensics, digital forensic investigators must adhere to a strict set of best practices and guidelines when collecting and analyzing digital evidence. When an investigation involves criminal activity and criminal charges will possibly be filed, an investigator must do the utmost to ensure that all data is admissible in a court of law and has been obtained through the proper protocol. United States courts are becoming increasingly involved with the issue of cloud technology and the digital evidence that can be gathered from the cloud. Proper forensic collection methods must be followed to ensure the efficacy of evidence collected and data must be collected, preserved, analyzed and presented in a manner which follows appropriate protocols (Lawton, 2011).

In 2010, United States District Court Judge Shira Scheindlin imposed sanctions on over a dozen parties that did not effectively meet the proper obligations for electronic discovery (Lawton, 2011). Judge Scheindlin wrote:

> Courts cannot and do not expect that any party can meet a standard of perfection. Nonetheless, the courts have a right to expect that litigants and counsel will take the necessary steps to ensure that relevant records are preserved when litigation is reasonably anticipated and that such records are collected, reviewed and produced to the opposing party. (Pension Committee, 2010)

The cloud provides a specific challenge to investigators in that it is much more difficult to make sure that appropriate measures are taken to preserve data and evidence. When it comes to the cloud, law enforcement will not generally have the ability to physically seize any media on which data or evidence resides. Since many users have access to a specific cloud server, it becomes challenging for an investigator to seize only a section of the virtual media where he or she believes data resides. It would also be nearly impossible for an investigator to ensure that the section of media seized contained all the data needed for a proper investigation from start to finish. It can also be difficult for investigators to attribute activity to any specific cloud user (Lawton, 2011). These obstacles can compromise the integrity of an investigation.

While the use of the cloud model has grown, research on the forensic investigation aspect of this technology has not kept up. Much attention has been paid to the issue of data security and privacy, while further study into how forensic investigations are impacted by the cloud has seldom been addressed. Although investments into advancing cloud technology continue to occur, studies into the impact this technology has on digital investigations have been insignificant. Moreover, as of 2009, there were no studies that focused on the impact that cloud computing has on digital forensics and data acquisition (Birk, 2011).

Currently, there is little legislation in place that is broad enough to encompass cloud computing technology. The Electronic Communications Privacy Act (ECPA), enacted in 1986, extended the government restrictions on wire taps from telephone calls to electronic data transmissions via computer. However, the law made no specific mention about data stored on the Internet, or in the cloud. Because the law was written at a time before cloud technology was as widespread as it has become, there has been confusion amongst law enforcement personnel, consumers and the business community on the privacy of information stored in cloud-based technology. The ECPA can serve as an example of why legislation should be reviewed as technology changes occur (Sternstein, 2010).

Upon determining the policy limitations that are currently in place, it is important to examine and predict what policy changes need to be made in order to increase the effectiveness of forensic investigations that involve cloud technology. It is necessary to evaluate the process for obtaining a warrant for digital forensic evidence. A comprehensive assessment should determine whether current laws and cloud usage policies are enabling investigators to follow proper protocol for collecting, preserving, analyzing and presenting digital evidence (Lawton, 2011).

Examining cloud technology and its challenges to digital investigations should provide law enforcement personnel and cybercrime investigators more clarity regarding what type of obstacles they may face during an investigation. Policymakers could also benefit from further research on cloud technology and investigations, as the data presented could affect future policy change and determine the direction of new laws and amendments to current legislation. In addition, cybersecurity experts, IT professionals and developers might use this research to develop new facets of existing cloud technology and improve its security for users and consumers. A thorough review of the policies and legislation in place that affect investigations in the cloud is necessary for the future success of those investigations, the eventual prosecution of cyber-criminals and ultimately, the safety and privacy of cloud consumers and their data.

By evaluating previous research on cloud computing and digital forensic investigation, this study will answer the above research questions and determine if cloud computing provides any challenges to investigators. Based on the research findings, this study will propose suggestions as to what changes, if any, should be considered in order to make cybercrime investigations more effective and efficient.

Literature Review

With the use of cloud computing technology rapidly increasing, cybercrime and digital investigators will be tasked with a greater number of cases that involve the use of this technology. Data created and stored through the use of cloud technology provides a new set of challenges to investigators. These challenges, including criminals exploiting the cloud, the difficulty for investigators to gather, analyze and present evidence from the cloud, and a lack of standards and guidelines for practitioners, decrease the efficiency of cloud forensic examinations.

There is a large amount of research on cloud computing, its background, and its security. The sources for this project were selected because each dealt specifically with how cloud computing affects digital forensic investigations. Additional research was chosen on the topics of cybercrime and cybercriminals exploiting the cloud. The sources chosen were scholarly and peer-reviewed and provide credibility to this project. The combination of the data gleaned from these resources has allowed the author to formulate and discuss the notion that cloud computing provides a great challenge for digital forensic investigators.

Cloud Computing Technology

Cloud Service Models. The cloud environment is comprised of one of three service models: Software as a Service, Platform as a Service and Infrastructure as a Service. These models are used to deliver shared services to users. The three types of models specify which services are provided to cloud customers, allowing for users to customize their cloud experiences.

In the Software as a Service (SaaS) model, a service (or application) is housed in one location, namely a data center, and accessed by users over a network (the Internet, Intranet, a Virtual Private Network, or Local Area Network). A central network provides “access”, “rental” or “subscription” to users, often on a fee-based schedule. SaaS serves to provide users access to a commercially available application and benefit the consumer by lowering operational costs, streamlining their operations and making processes more efficient (SIIA, 2001). SaaS is the most commonly used cloud service model for business applications and sales for SaaS products in 2010 reached $10 billion (McCall, 2011).

Platform as a Service (PaaS) differs from SaaS in that an entire developing platform can be accessed via a network, and not just one piece of software. Developers using a PaaS model have access to virtual developing environments (often complete with toolkits configured for the specific environment), application standards and distribution environments at their fingertips. By utilizing PaaS, developers can lower operational budgets by avoiding costs associated with buying, maintaining and managing the hardware and software used for hosting purposes, since the PaaS model supports the entire software development life cycle. Because the target audience for the PaaS model is developers rather than end users, PaaS is a less widely used model for cloud computing than SaaS (Cloud platform, 2012).

Infrastructure as a Service (IaaS) delivers computer infrastructure as a service, along with storage and networking. IaaS is often known as a virtualization environment and its objective is to provide a standardized foundation for SaaS and PaaS models. IaaS users can forego the expenses of maintaining data centers, software, servers and equipment by choosing to house all this in the cloud. IaaS users can also control customization of the operating system, database and software for their own specific needs. Virtualization of the infrastructure, its availability and its performance are all sustained by the cloud service provider (Loeffler, 2012).

Cloud computing users are generally only required to pay for the resources they use, making all three of the cloud models viable alternatives to traditional computing technology. Each model is targeted towards a specific audience and many consumers will have familiarity with using SaaS, as it has a broader market than the other models. PaaS and IaaS have a much smaller target clientele but are much more customizable, allowing for increased efficiency for their niche users. While the consumer for each model may vary, all three serve to make end users pay less and have a more efficient, flexible and reliable computing experience. The Appendix provides a comparison of the three cloud service models (Loeffler, 2012).

Cloud Deployment Models. Cloud technology must be comprised of one of four deployment models: public cloud, private cloud, community cloud, and hybrid cloud. These deployment models serve to distinguish specific types of cloud environments by ownership and size. Each model serves to support the needs of a user or organization in its own specific way (Mell & Grance, 2011).

In the public cloud deployment model, the cloud infrastructure can be used by the general public, but can be owned and managed by a business, corporation, and/or government entity. The infrastructure itself resides at the location of the cloud provider. Users can use the public cloud model to develop their own services in the cloud at a significantly reduced cost versus developing and deploying that service outside of the cloud (Dialogic, 2010).

A private cloud model specifies that the cloud infrastructure is used exclusively by a single organization. It can be owned by that organization or a third party and can reside on or off-premises. Users of a private cloud are responsible for building the infrastructure because it is specific to a single organization. Because of this, private cloud models are sometimes not cost-efficient solutions for an organization (Haff, 2009).

Like the private cloud model, the community cloud is authorized for use by a single entity. Instead of being a single organization, the community cloud allows for use by a specific group of organizations with like concerns and needs (such as schools). One or more of the organizations in the community may own and operate the cloud, or a third-party may maintain ownership. The community cloud can exist on or off-premises of any of the organizations (Mell & Grance, 2011).

Hybrid cloud infrastructure is composed of two distinct cloud infrastructures (public, private, or community). The individual infrastructures remain distinct entities but are joined together in the hybrid cloud by "standardized or proprietary technology" that allows for portability between the two infrastructures (Mell & Grance, 2011, p. 3). An organization may function under a private cloud model for its daily operational activities but use a public cloud model, like Amazon Simple Storage Service, for archiving of data. The use of these two cloud deployment models would constitute a hybrid cloud (Mell & Grance, 2011).

Criminals and the Cloud

Security is often cited as one of the primary reasons that corporations eventually switch over to storing their data in the cloud as opposed to on local servers (Ingthorsson, 2011). However, cloud technology has issues with security. It can be challenging for cloud providers to maintain data security and integrity, web application security, and manage vulnerabilities with virtualization, all while maintaining the availability and flexibility for which the cloud is known. These security deficiencies within cloud technology can be shown to benefit criminals and criminal organizations (Williams, 2010).

The physical location of cloud data servers can make investigating and prosecuting criminal activity more difficult. According to Garfinkel (2011), some cloud vendors promote “geographical diversity” (par.9), which allows for the ability to create virtual machines in a variety of physical locations. Criminals can use this “geographical diversity” to their advantage by using a cloud provider with servers located in another country, outside of the jurisdiction of the United States, to launch cyber-attacks against the United States. This can make conducting investigations challenging for an investigator because of a variety of political, technical and legal obstacles (Garfinkel, 2011).

The same virtualization technology that makes the cloud attractive to business and consumers also makes it more difficult for investigators to trace criminal activity back to an individual or group. In an organization using cloud technology, a single machine connected to a network might have its data spread amongst several cloud servers. When this machine is shut down, the storage allocated to the virtual machine’s disks is almost immediately used by other machines in the cloud. If both legitimate users and criminals are a part of the same cloud, investigators will have difficulty recovering useful forensic data and attributing it to a specific user (Garfinkel, 2011).

Cybercrime in the Cloud. Despite the growing popularity of cloud computing technology and the predictable nature of cybercrime, there is little research devoted to linking the two topics together. The majority of research on the subject focuses on securing the cloud computing environment with little discussion of how cybercriminals are exploiting the cloud. Gold (2010) discusses the new breed of cyber-criminal, who is well-versed in larger scale attacks on cloud computing systems. Gold paraphrases Richard A. Clarke, chairman of Good Harbor Consulting, saying that law enforcement "continues to make arrests for various offences, including hacking and out-and-out fraud involving Internet credentials. But the arrests involve only the … 'little people' and never the… criminal masterminds" (p. 10).

The cloud environment is a high-value target with a large potential payload for criminals. The cloud servers often contain an enormous amount of data, especially when compared to any given organization's traditional on-site server. Jerome LeCat, CEO of Paris-based Information Technology company, Scality, predicts that the amount of data stored in the cloud will increase by 800% in the next five years (Gold, 2010).

Because of the virtualized environment of the cloud, business users' and personal users' data can often be found together (Kavitha & Subashini, 2010). Criminals need only compromise one website to potentially gain access to huge amounts of data. A 2007 attack on the website Monster.com yielded millions of contact details of the website's users for the person or persons who were successfully able to hack the website and its cloud servers (Mansfield-Devine, 2008).

Eighty-five percent of successful attacks on a company's IT resources are done by hackers with low or moderate skills (Gold, 2010). Prior to the influx of cloud computing applications traditional cyber-attack methods, such as denial of service (DoS) attacks were prevalent. DoS attacks are used by hackers to prevent legitimate users of a service from using the service (CERT, 1999). Investigators and IT professionals are now seeing more exploitation of web-based vulnerabilities. The majority of SaaS applications are web-browser based, which is a benefit for criminals. Now, instead of having to compromise an entire system, criminals can exploit vulnerabilities within the browsers themselves to achieve their goals (Mansfield-Devine, 2008).

Cloud Security. One area of research that is well documented regarding cloud computing and cybercrime is the discussion of security vulnerabilities in the cloud. Kavitha and Subashini (2010) illustrate where vulnerabilities can exist in the Software as a Service, Platform as a Service and Infrastructure as a Service models of cloud computing. As discussed previously, all SaaS applications are web-based and typically run in a browser. Any security issues in any Internet browser can cause vulnerabilities to the SaaS applications themselves (Kavitha & Subashini, 2010).

Platform as a Service providers, such as the popular Salesforce.com, offer their users robust Application Programming Interfaces (APIs). These APIs allow developers to customize applications to their own specifications as well as modify code provided on the site to fit their needs. With hundreds of third parties developing code and customized applications via PaaS providers, it is virtually impossible for a cloud provider to check all programming code for any potential security flaws or vulnerabilities. Because of these vulnerabilities, PaaS providers are an obvious target for cybercriminals and hackers (Mansfield-Devine, 2008).

Virtualization in the cloud, or Infrastructure as a Service, provides another significant security risk for cloud service providers. All virtualization software has been found to contain some amount of vulnerability that can be exploited by criminals or hackers. These vulnerabilities can be used to bypass security restrictions or gain unauthorized access to a system. Once a hacker has access to the IaaS system, it can be used for whatever illegal purposes he or she desires (Kavitha & Subashini, 2010).

Digital Investigations in the Cloud

To perform a successful digital forensic investigation, investigators typically follow a process of identification, extraction, analysis, and presentation of evidence found. Whether the data is housed on a computer, a local server, mobile device or in the cloud, it is important that investigators follow this linear process with their investigations. Cloud technology provides very real challenges for the investigator using the standard computer forensic process (Taylor, Haggerty, Gresty, & Lamb, 2011).

Identification and Preservation of Data. Much research has been done on the challenges of identifying potential sources of evidence located in the cloud. The term digital evidence encompasses a wide variety of data, including files stored on a hard drive, items stored in memory, digital video or audio, file fragments, or packets transmitted via a network. In most investigations, the quantity of digital evidence is quite large (when considering the number of files on a single computer and up to an entire network). Evidence can also be easily changed; a simple reboot of a computer system can remove all traces of evidence. It is also possible for digital evidence to implicate a vast number of potential suspects (especially when data is transmitted over a network or via the Internet) (Reilly, Wren, & Berry, 2011).

There are several potential considerations an investigator must make before identifying evidence in the cloud. The very nature of cloud environments allows for evidence to be less static. In a typical computing environment, data (such as registry entries, temporary Internet files or cached web pages) is often written to a computer's hard drive. Data in the cloud is much more dynamic and will reside in a virtual environment. This data can also be lost when a user leaves the cloud (Taylor, Haggarty, Gresty, & Hegarty, 2010).

Data can be transferred numerous times between computers and across continents at any given time (Mason & George, 2011). Because of this dynamic nature, it is difficult for an investigator to truly maintain a proper chain of custody on data in the cloud (Reilly et al., 2011). As data moves from device to device, it has the potential to be copied (leaving copies stored on each device it touches) or deleted (leaving no copies in existence). The existence of multiple copies of data on various numbers of servers across the globe could clearly affect an investigator's ability to identify the pertinent evidentiary data and where it originated (Grispos, Glisson, & Storer, 2011).

To accurately identify potential evidence stored in the cloud, a digital investigator must determine if the cloud system is a public or private cloud. Since a private cloud is designed for use with and for a single organization, its maintenance is often taken care of by the organization itself, though it can be run by a third-party. In this instance, potential evidence sources like servers, data repositories and applications should be easily accessible by an investigator working on behalf of the organization, or with sufficient authority given by a third-party to access this information. Additionally, investigators can potentially have access to suspects or other persons who may be instrumental in helping to identify pertinent data (Taylor et al., 2010).

When dealing with a public cloud model, identifying data becomes more challenging for an investigator. Because a public cloud is managed by a cloud service provider and access is provided through remote interfaces, identifying potential evidence is not an easy task. Cloud providers aim to deliver applications and data seamlessly to their users, and this dynamic environment makes data identification problematic. Data in the public cloud is constantly moving and interacting with other data, making the existence of evidentiary data more difficult to identify (Taylor et al., 2011).

The physical and logical location of the cloud service provider can add a level of difficulty to a digital forensic investigation. In many forensic investigations, in order to identify data, an investigator will physically seize device(s) from the premises to determine if any relevant data is housed within those devices. Reilly et al. theorizes that the main stumbling block to cloud computing forensics is that it is extremely difficult for investigators to gain access to physical devices that contain valid evidence (2011). Since many cloud providers have data repositories and servers located off-site, this type of seizure is not practical.

Data Extraction. The issues that investigators have in identifying evidentiary data in the cloud also extend to the extraction of that data. According to Taylor et al. (2011), "[c]loud computing impacts upon the ability of law enforcement agencies to physically seize computing assets in order to pursue an investigation" (p. 6). Even if an investigator is able to identify evidentiary data with minimal difficulty, extracting the data in a timely manner could prove difficult. The nature of cloud computing has data changing rapidly and it is unlikely that the seizure of pertinent data or systems could be done before any significant changes could occur.

Physical Extraction. Investigators will have to develop computer forensic practices for extracting data from web-based SaaS applications. Because web-based applications differ from many traditional computing applications, not all traditional data extraction methods will apply. Though SaaS applications in the cloud are relatively new technology, investigators can draw on their knowledge and experience gained from conducting investigations involving web-based email servers like Microsoft Hotmail and Google's Gmail (Taylor et al., 2011).

Platform as a Service cloud models provide a challenge to investigators because it is difficult to gain physical access to the servers where data is housed. Physical access is often necessary for the purpose of creating a disk image for analysis of data. Some cloud service providers offer a forensic analysis service to their customers, which could reduce the challenges to digital investigators. If an organization uses virtual machines, an investigator can also create locally-stored snapshots of these machines to extract evidence in a forensically sound manner (Taylor et al., 2011).

The nature of virtualization allows for a physical resource to be shared amongst a number of users (Reilly et al., 2011). For virtualization technologies, like those that occur in IaaS cloud models, the challenge for forensic examiners and analysts is whether the concern should be with the client computer operating system (OS) or the host computer operating system. An investigation can be made much less complex if the analysis is mainly concerned with the client OS, as this can be done from the host OS with much less difficulty (Taylor et al., 2011).

Attribution of data. The issue of identifying actual suspects and assigning computing activities to them can prove to be extremely difficult in the cloud environment. Traditional computer forensics offers investigators the benefit of linking a computer or server that has been seized to a suspect or suspects by obvious physical links. The computer may be located in a person's place of residence or work environment, or a suspect's finger prints may reside on the keyboard. When evidence is stored in the cloud, these types of clear physical links are not as frequent. (Taylor et al., 2011).

Within a cloud network, machines are in constant interaction with one another, with no knowledge by the users. Because there is a lack of a physical machine for each cloud user, a username and a password can be all that identifies a given user. Criminals who can obtain the credentials for a user can perform illegal activities under that user's identity. Investigators have no real foolproof means to attribute data or activity to a specific user (Taylor et al., 2011).

Analysis of Data. An important challenge that digital forensic investigators face in analyzing data during an examination is the lack of standardization amongst cloud virtual platforms. In traditional computer forensics, there are relatively few operating systems that an investigator might encounter. Commercially available analysis software, such as Guidance Software's EnCase or Access Data's Forensic Toolkit can be used to analyze most computer systems that an investigator will encounter. In contrast, the mobile phone market has a much larger variety of operating systems. If an investigation is concerned with mobile device forensics, the examiner must have the appropriate means of analyzing the data gathered from the mobile device. Cloud computing data analysis can be even more complex than mobile device analysis (Reilly et al., 2011).

Presentation of data. According to Taylor et al. (2011)

> [a]ny computer forensic investigation should keep within the appropriate guidelines for computer-based electronic evidence within the jurisdiction concerned. That is to show a court, if required, that the digital evidence produced is no more and no less than when it was first taken into the possession of the forensic examiner. (p. 9)

Challenges exist for investigator in maintaining precise, forensically sound digital evidence. This is in part because of the challenges identifying, extracting and analyzing this evidence, as discussed prior, but also because of the lack of an industry standard specifically for cloud computing forensics. Investigators must still do their best to adhere to the standards of traditional computer forensic examinations, which can often prove difficult in a cloud environment (Taylor et al., 2011).

In criminal cases, the presentation of forensic data collected during an examination is of the utmost importance. If evidence is not collected by sound forensic means it may not be admissible in a court of law. In cases involving cloud technology, it may not always be possible for an investigator to gather data from the cloud while maintaining standards on data collection that were developed for traditional computing environments (Taylor et al., 2011).

A large number of cybercrime cases involve the details of an investigation to be presented to a jury. This can prove challenging when dealing with traditional computing technology and even more so when an investigation involves the complex nature of a cloud environment. Investigators will often have to explain the technical nature of how evidence was acquired and analyzed and what the evidence suggests, to a jury made up of people who may only have average knowledge of technology (Reilly et al., 2011).

Where digital and computer forensic investigations might typically use time-lining, or reconstructing a series of events based on timestamps associated with integral pieces of data, cloud computing forensics might not allow for this useful presentation format. If an investigator is involved in a case involving cloud computing as well as more traditional forms of computing and he or she is unable to gather sufficient evidence from the cloud, the creation of a timeline would be near impossible. A timeline created without all the evidence necessary would have large gaps which could jeopardize a case in court (Reilly et al., 2011).

Some cloud computing applications and providers have implemented an audit trail for their data, which allows for tracking of changes of application in SaaS environments. Audit trails in IaaS and PaaS cloud environments can maintain logs of users' activities. Unless a cloud provider maintains audit trails, the data that forensic investigators gather from the cloud, if they are able to gather any at all, may not be admissible (Taylor et al., 2010).

Cloud Computing to Aid in Forensic Investigations

While cloud computing technologies can provide hindrances to digital investigators, Reilly et al. discuss the alternative possibility: that cloud computing can be used to an investigator's advantage (2011). The use of a virtual machine (VM) in cloud computing can be used as an asset during a forensic examination if a snapshot of the VM can be taken. This snapshot can provide an investigator with an identical image of the computer's hard drive (including data stored there, VM configuration and BIOS configuration) at the time of the snapshot. The question does exist though, as to whether a snapshot provides an accurate picture of what is occurring in such a globally distributed network such as a cloud environment (Paul, Anvekar, Jacob, & Sekaran, 2012). Whether these snapshot images can be used as true forensic evidence in court is still questionable, but they have the potential to gather important pieces of evidence to assist in building a case (Reilly et al., 2011).

Forensic investigators could also certainly make use of cloud technology and the flexibility it provides to perform digital forensic examinations. By taking advantage of cloud technology, investigators can build a dedicated virtual forensic server in the cloud, eliminating the need to carry forensic tools on portable hard drives, thumb drives and disks. This virtual server could be accessed when needed by a forensic investigative team (Grispos et al., 2011).

The availability of seemingly endless amounts of storage in the cloud could also be used to a forensic investigation team's advantage. The cloud has the potential to store petabytes (1 million gigabytes) of data and can also house resource-intensive applications. Instead of an investigator having to store a large number of hard drive images on physical devices, storage in the cloud could be a viable alternative (Reilly et al., 2011). The cloud's extensive resources could also be used in brute force password cracking attempts and decrypting of encryption keys (Grispos et al., 2011).

Standards for Cybercrime Investigations in the Cloud

Cloud computing forensics and legal issues.

The nature of cloud computing allows a single instance of a piece of software to run on a cloud server and be accessed by numerous users. This multi-tenancy is perhaps one of the biggest legal concerns with cloud forensic investigations. Adding to the concern of multi-tenancy is the issue of multi-jurisdiction. Because cloud users can be located in any country world-wide, the differences in the jurisdictions can determine what data can be accessed during an investigation and how the data should be retrieved (Ruan, Carthy, Kechadi, & Crosbie, 2011).

Multi-tenancy. The subject of multi-tenancy in the cloud brings up the issue of users' expectation of privacy. In the cloud, a given user's individual data is often intermingled with other users' data. During the course of an investigation, investigators must take the appropriate steps to make sure that the data that he or she is extracting is pertinent to the case and does not involve any information on an uninvolved third-party. This is especially difficult considering the dynamic, virtualized nature of the cloud environment (Ruan et al., 2011).

Privacy issues on data in the cloud have been addressed in several United States court cases. The courts have had to consider whether or not data seized from the cloud violates a person's Fourth Amendment rights. The Fourth Amendment protects individuals (and their personal information and effects) against unreasonable searches and seizures. It also states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to the third parties" (U.S. Const. amend. IV). There is much debate on whether or not this language applies to data in the cloud, and a general consensus has not been reached. Instead, decisions are being made on a case-by-case basis. This lack of consensus can be harmful to cloud forensic investigations (Barnhill, 2010).

***Multi-jurisdiction*.** Cloud computing forensics is unique in the field of digital forensics in that data can reside in a jurisdiction on the other side of the world from the user. According to Ruan et al. it is important to develop regulations and standard in the legal realm regarding cloud forensics. These regulations are necessary to ensure that forensic examinations and investigations are complying with all laws and regulations in the various jurisdictions in which evidentiary data resides (2011).

It can be shown that the use of cloud technology provides real challenges to those performing digital forensic investigations. The literature review presented here provides an overview of the issues facing cloud forensic investigations. A thorough discussion of these challenges will follow.

Discussion of the Findings

As discussed previously, the purpose of this study was to determine what specific challenges law enforcement personnel, cybercrime investigators and digital forensic examiners face when performing investigations involving cloud computing. The obstacles to investigations in the cloud are unique and can hinder an investigation. Criminals exploiting the cloud, difficulty in adhering to the standard computer forensic process, and a lack of standards, policies and laws regarding cloud forensics can all cause challenges for an investigator.

An array of sources was used to conduct research on this topic. Sources varied from research projects from educational institutions to law reviews and scholarly articles in professional journals. The amount of research on these topics was not overwhelming, and sources had to be chosen carefully to ensure credibility. These sources were chosen for their knowledge and thoughtful discussion of cloud computing technology, cloud computing and cybercriminals, cloud computing investigations, digital and computer investigations, and cloud computing security. Most of the findings were consistent with the premise that cloud technologies provide a unique set of challenges for investigators.

Criminals Can Exploit the Cloud

A 2009 survey of Information Security professionals conducted by Arbor Networks' Worldwide Infrastructure Security indicated that nearly 35% of respondents were worried about attacks on cloud services and applications. The sheer volume of information stored in the cloud (including sensitive personal data like Social Security numbers, credit card information and bank account numbers) make it a prime target for criminals (Network Security, 2010).

As technology improves, cybercrime attacks from criminals and hackers will have to become more sophisticated in order to meet the advances in technology. According to Hawthorn (2009), cybercrime has surpassed the illegal drug trade in revenue with a $100 billion market. Cloud computing technology and the virtualization that accompanies cloud platforms provide a new medium for cybercrime.

Reports have noted botnet attacks on Amazon's cloud infrastructure as well as a compromise of Google's Gmail servers in 2009 (Grispos et al., 2011). Botnets, which are systems of computers that are infected with remotely-controlled software, are dangerous because they allow the infected computers to be controlled by hackers (Puri, 2003). By combining new and improved tactics with more commonly employed attacking methodologies, such as viruses, worms and Trojan horses, hackers and criminals have been able to maintain a level of success in this new environment (Hawthorn, 2009).

Traditional means of attack for cybercriminals still play an important role when discussing attacks in cloud environments. Malware injection, in which an attacker deliberately deposits malicious software on a system in order to disrupt operation of a computer, is still a “weapon of choice” for hackers and cybercriminals (Hawthorn, 2009, pg. 19). The problem becomes much more widespread when malware injection occurs via the Internet or cloud environment. A Sophos Labs threat report from 2008 indicated that 90% of web-based malware was found on trusted sites, such as Google. Cybercrime attacks can affect a larger audience when perpetrated through trusted sites with a large amount of traffic (Hawthorn, 2009).

Hackers and criminals without immediate means to access a cloud server can still gain access to the cloud. Cybercriminals are still using botnets and all varieties of malware to directly access companies’ servers. With unrestricted access to a company’s server, hackers can use these botnets and malware to steal administrator credentials that will allow them to access cloud-based resources. Once hackers have access to the cloud, they can gain access to potentially sensitive data (Gold, 2010).

Cloud Security Deficiencies

The virtualized nature of cloud computing introduces a distinctive batch of security challenges. All three deployment models, SaaS, PaaS, and IaaS have unique issues which can make them insecure. These security vulnerabilities can provide access to criminals and hackers who are looking for ways to exploit the cloud.

Though SaaS applications are run from a network, they provide a challenge for security professionals, as typical network security measures are not enough to keep them secure. Traditional network defenses, such as firewalls, network intrusion detection systems and network intrusion prevention systems cannot adequately safeguard SaaS applications. These applications should be protected at the application level and are vulnerable to a variety of threats (Kavitha & Subashini, 2010).

PaaS and IaaS deployment models also have security risks. With numerous developers using PaaS systems and coding and uploading their own data, cloud providers should have increased security checks in place to ensure that the data being stored there is valid and safe. Salesforce.com has over 40,000 customers and 800 applications (Mansfield-Devine, 2008). With this much data being stored, it is possible that a hacker could upload malware hidden in the code of an app.

The IaaS model is generally the most secure of the cloud deployment models, but also has issues. Many IaaS providers, such as Amazon Elastic Compute Cloud (EC2) split the responsibility for security between the vendor and the customer. The vendor will control security up to the hypervisor, or virtual machine manager. The hypervisor is essentially the interface for the IaaS model (IBM, 2007). In these instances, the vendor could control security of the virtualization environment, but the customer would maintain security for the IT system, including the applications and data (Kavitha & Subashini, 2010). With security being divided between parties, the potential for vulnerabilities exists, since different entities might have different security measures and standards in place.

Offering a different opinion on cloud security, Gold counters that sufficient security is already being built directly into the infrastructure of most cloud computing systems. This allows security to be a foundation for all users of a given cloud system or application and mitigates the amount of damage that can be done by hackers (Gold, 2010). Gold also suggests that they key to successful security in the cloud is the automation of processes to protect users' sensitive data and activities and recommends that cloud providers start offering security as a service.

Cyber Investigation in Cloud Environments Cannot be Performed Effectively

The principles for forensically sound investigations require that the data collected be authentic, reliable, complete, believable and admissible (Reilly et al., 2011). Adhering to these principles is a challenge in cloud environments, as the nature of the cloud means that data is constantly being moved and changed. Since it is not always possible for investigators to gather data in a forensically sound manner, cloud investigations are not as efficient or effective as most traditional digital investigations.

While cloud investigations may not follow the same procedures as conventional digital investigations, it is possible that the very nature of the cloud may require them to follow a different set of standards. It may not be feasible for an investigator to gather evidence from the cloud exactly the same way an investigator might gather evidence from an actual computer. Even so, evidence gathered from the cloud may still be usable in much the same way that evidence gathered during a live analysis of a running machine is usable. As long as the evidence is gathered in a way that adheres to a best evidence rule, and the investigator can be sure that the original source material was not altered in a meaningful way, cloud data may be usable in an investigation.

Typical digital forensic investigations involve data gathered from many sources compiled together to form an accurate picture of an incident or event. When the data is in the cloud, it may be difficult for an investigator to gather nearly enough data to form a complete case (Taylor et al., 2011). The outcome of this can be an incomplete picture of events and the evidence may not always form a clear indication of what type of activity actually occurred.

When data can be accurately gathered from a cloud environment, attributing this data to a specific user can be a challenge for an investigator. The lack of physical evidence to associate a specific user to that data cannot always be found. The cloud's dynamic nature allows for data to be continually moving from location to location. Data that might implicate a suspect in an investigation could easily be mingled with other users' data and determining ownership of specific pieces of evidence is extremely challenging.

The lack of standardization in cloud environments makes investigations more difficult. Standard analysis tools and suites of commercially available programs are not specifically designed with cloud forensics in mind. Investigators will have to be more creative in their acquisition and analysis techniques since they may be unable to rely on more traditional analysis methodologies and tools. Cloud forensics will likely need to combine both static and live analysis methodologies in order to be successful. Acquisition of cloud data must utilize "next generation forensic tools… [to] visualize the physical and logical data locations" (Zimmerman & Glavach, 2011, p. 6). There are several virtualization platforms that can be used by cloud service providers, and an investigator should have familiarity with them and the means to analyze data from them (Paul et al., 2012).

While a standardized analysis protocol would make cloud forensics easier, it would be difficult to achieve. The cloud environment is extremely customizable and there are many variations on platforms that serve the needs of specific cloud consumers. Additionally, the sheer volume of activity in the cloud ensures that it is constantly changing. Because the platforms used in the cloud are not consistent, developing one standardized protocol for analysis is not possible. An investigator should have the means to analyze data from any type of cloud platform that may be encountered (Paul, et al., 2012).

An important part of standard computer forensic investigation often involves live analysis on running machines. From a running computer, an investigator can gain important evidentiary data, such as registry entries, temporary files and metadata. While this data can be stored in the cloud, it is nearly impossible for an investigator to analyze this data because of the constant state of change the cloud is in (Grispos et al., 2011). Additionally, the amount of data in the cloud can be a hindrance to investigators. In any given case, an investigator might need to download terabytes (one thousand gigabytes) of data. The time necessary to download this data might end up being prohibitive to an investigation; by the time the data is downloaded, there will likely have been many, many changes made to the cloud environment in which the investigator is working.

The presentation of data gathered from the cloud must be done in such a way that maintains the integrity of the investigation. Investigators must do all they can to ensure that their data is forensically sound, especially in cases involving potential criminal activity that may be presented in a court of law. In order for the data to be considered forensically sound, it will be necessary for an investigator to ensure that the data collected adheres to best evidence standards: Data should be obtained in a well-document manner that doesn't alter the original source material any more than is essential and is able to be justified.

A 1993 United States Supreme Court case, Daubert v. Merrell Dow Pharmaceuticals defined the admissibility of scientific evidence to be based on four criteria (collectively referred to as the Daubert principle):

1. Has the scientific theory or technique been empirically tested?
2. Has the scientific theory or technique been subjected to peer review and publication?
3. What is the known or potential error rate?
4. Has the theory or technique been accepted as a standard in its scientific community?

Grispos et al. (2011) contend that forensic investigations in cloud environment will be required to adhere to the same tests as in the Daubert principle if the evidence is to be admissible in court. Because cloud technology changes so rapidly, adhering to these standards may be difficult for forensic examiners.

In criminal investigations, it is of the utmost importance that data collected and analyzed be admissible in a court of law. Without a strict, widely-accepted set of guidelines, perhaps developed by a committee of industry leaders and experienced digital cyber investigators and legal experts, it can be difficult for an investigator to collect evidence from the cloud in a manner which allows for it to be admissible during a trial.

Prosecutors may need to base their cases solely on evidence gathered from a suspect's computer and not from data discovered in the cloud environment. This could jeopardize a case and lead to a lower percentage of successful prosecutions of cybercriminals and hackers (Taylor, et al., 2011).

Standards for Cloud Forensics Should be Instituted

In order to ensure that cloud based evidence adheres to the Daubert principle, a standard for digital forensic examinations in the cloud will need to be developed (Grispos et al., 2011). Currently, a standard specifically designed for cloud investigations does not exist. The creation of a universal standard for cloud forensics, or a set of best practices on which investigators could base their proceedings, would positively affect the efficiency of cloud forensics.

Traditional computer and digital forensics have an industry accepted best practices for performing cybercrime and computer forensic investigations as well as evidence handling and presentation. These standards encompass everything from photographing a scene and storing hard drives in anti-static bags to details on performing live analysis on a running machine. While some of the same principles would apply to cloud investigations, many of the steps taken in computer forensics could not be applied to the cloud. For example, evidence guidelines, such as the proper handling of physical material like hard drives and disks would not apply to cloud data. It also may not be possible to ensure that the original state of the virtualized cloud system remains exactly the same. In live analysis, investigators use tools such as a cryptographic hash value to demonstrate that the data they gathered is the same as the original data on a machine. With the cloud environment changing so rapidly, it may not be possible for to ensure that the system is in the exact same state before and after data acquisition. In this instance, an investigator should attempt to document that steps were taken to ensure as little effect on the system as possible. An industry accepted standard for cloud computing forensics should be developed to effectively standardize cloud forensic investigations (Shields, Frieder & Maloof, 2011).

When discussing cloud forensic policy, it is important to also address legal issues that arise during cloud forensic investigations. Because cloud forensics is a relatively new field, there are no real laws in place that deal with the specific legal issues that affect cloud investigations. Among these problems are jurisdictional, tenancy and privacy issues as well as contract issues between cloud providers and consumers.

The active, moving nature of the cloud allows for data to be stored in a variety of different locations. Many cloud consumers utilize the cloud for this very reason; data can be stored off-site and require fewer resources on the consumer's part. In many cases, data housed off-site (physically or logically) is also subject to jurisdictional rules and laws. A cloud provider can be located in a different state or even country from where the investigation is based.

It is typical for a large cloud provider, such as Yahoo, to house much of its data in one location (such as the United States) while the data appears to the user to be stored locally (especially in the case of Yahoo's "country specific" sites) (Taylor et al., 2010). This is done in part to ensure proper load balancing of resources. Load balancing allows a cloud provider to distribute Internet protocol traffic amongst many servers to ensure optimal efficiency, productivity and utilization for consumers and clients. If an investigation was taking place in the United Kingdom and the data in question was stored via Yahoo on a US server, it could be necessary for UK government or law enforcement agencies to interact with their US counterparts in order to gain access to data. In a large enough case, this might be a reasonable course of events, but for the smaller digital forensic examinations and even criminal cyber investigations, going to these lengths might not be feasible.

The differences in laws in different jurisdictions mean that what is considered a crime in one location may not be in another, and access to server data might not be easily obtained by an investigator (Taylor et al., 2010). These types of inconsistencies can hinder an investigator from completing an accurate, thorough, and forensically sound investigation. Countries will need to develop their own sets of laws to determine how jurisdictional issues in cloud forensics should be handled. Ideally, these laws would help to aid investigators in dealing with cases involving multiple jurisdictions. Different countries might consider treaties that allow for digital cloud investigators to obtain access to pertinent data that exists outside of their normal realm of jurisdiction.

Even if a cloud server is not located in another jurisdiction, legal issues could arise with an investigator obtaining access to the data. Cloud providers often maintain server farms, or web farms, which are clusters of servers that allow them to store massive amounts of data. If a cloud service provider is not willing to provide blanket access to the data stored on their servers, an investigator would have to go through the proper legal channels to obtain access to that data, including obtaining warrants if necessary. This course of action could mean that critical data needed for an investigation is lost. Metadata stored in the cloud environment can change very quickly and could easily be lost by the time an investigator has gained the proper authority to access data.

Cloud service providers may show some hesitation upon releasing data to investigators without a warrant or other order from a legal entity or law enforcement agency. This may be due in part to contract legalities that could arise between the cloud service provider and its consumer. Most consumers are very interested in how their private data is maintained and protected and are very likely to have a contract with a cloud provider that protects their rights. As such, cloud providers have to make sure that they are taking every step to ensure the satisfaction of their clients. A cloud provider is unlikely to breach a contract by providing full access to their server data to an investigator without having the proper documentation or warrant that requires them to do so.

Multi-tenancy in the cloud brings up privacy issues which are very important to many Americans in the post-9/11 world. There has been no clear consensus in cases involving cloud forensics to determine whether an individual's privacy extends to data stored in a third-party cloud. A district court in the state of Oregon found that e-mail stored in the cloud with a third-party is not protected under the Fourth Amendment, stating:

> Subscribers are, or should be, aware that their personal information and the contents of their online communications are accessible to the ISP and its employees and can be shared with the government under the appropriate circumstances. Much of the reluctance to apply traditional notions of third party disclosure to the email context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our emails. Some people

> seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not. (Barnhill, 2010)

However, in the case of Quon v. Arch Wireless, a Ninth Circuit court found that the defendant’s text messages, though stored in the cloud and accessible by the service provider, were in fact protected by his Fourth Amendment rights. Similarly, in United States v. Cioffi, it was determined that the defendant, a hedge fund manager had an expectation of privacy regarding his personal Web-based e-mail account (Barnhill, 2010).

The lack of consensus by U.S. Courts on whether data in the cloud is protected by the Constitution creates an area of confusion for cloud forensic investigators. To perform a complete investigation, it is imperative that investigators know that they are following the law in gathering data in and not infringing on the rights of any suspects or other parties involved. Without knowing whether data is protected or able to be used in an investigation it is difficult for an investigator to complete an investigation with integrity and success.

Comparison of the Findings

While many researchers have chosen to focus on one important issue regarding cloud computing and cloud forensics, such as security vulnerabilities, jurisdictional issues, or cybercrime in the cloud, there were no available sources that discussed a variety of issues related to forensic investigations in the cloud. It is important to look at the challenges that cloud forensic examiners face from many angles to determine what the most effective solution is for increasing the success of investigations. By taking a comprehensive look at several factors involved, a more accurate determination on changes to be made can occur.

Limitations of the Study

The nature of this research was such that it lacked a true methodology for gathering original data on the subject of cloud computing and forensics. As such, it is comprised from data gathered from other scholarly sources used to determine the true nature of a problem and a potential solution. Because of this limitation, much of the information and data presented can be found as theoretical and may not be found to apply to a practical situation. The practical application of this research is a good basis for future studies on this topic. Further recommendations on what specific steps should be taken will follow.

Recommendations

In order to experience a high-level of success, the field of cloud forensics will have to undergo some important changes. Increases in cloud security at the most basic level will help to protect the cloud and its data from cyber attacks by criminals and hackers. Improvements in security in all three cloud models, SaaS, PaaS, and IaaS will go a long way to help minimizing cybercrime in the cloud.

In addition to securing the cloud from possible attacks, cloud forensic investigations would benefit from a standardized set of guidelines and procedures. Establishing an industry recognized protocol is essential for ensuring that cloud forensic investigations consistently gather forensically sound or best evidence. These guidelines should include a methodology for effectively gathering evidentiary data from the cloud while minimizing the impact to cloud virtual systems.

With the proper standards in place, analysis and presentation of cloud data gathered during an investigation will become easier as well. Like with traditional computer forensics, a basis for analysis of evidentiary data should be included in the standards created. This could include the creation of new analysis tools and software specifically designed for cloud forensic evidence, or more simply, a set of recommended procedures on analyzing cloud-specific data.

When investigators are confident that they have gathered and analyzed evidence in a precise and structured manner, they will then be able to present the results of their investigation in a formulated way and illustrate that they have followed a methodology that is consistent across the industry. Ideally, the methodology created would be such that if another investigator were to simultaneously perform the same investigation, the results would be comparable.

In addition to an industry accepted standard, law enforcement personnel and policymakers should be involved in ensuring the future success of digital forensic investigations. Multi-tenancy and multi-jurisdiction issues are critical to forensic investigations. Investigators should take care to protect users' data and the privacy of uninvolved cloud users during cloud investigations. Additionally, data should be collected in the most time-efficient manner possible in order to minimize the loss of critical data and metadata. This can be difficult when terabytes of data are potentially stored on a multitude of servers world-wide. Lawmakers can be involved in establishing treaties and rules between jurisdictions in order to expedite the process while still keeping consumer and individual privacy in mind.

In the United States, forensic investigators can benefit from clarity on existing laws and acts that are currently in place which could affect cloud forensic investigations. The Fourth Amendment of the U.S. Constitution and the ECPA have both been applied to data stored in the cloud. However, judges have been inconsistent in their rulings in cases involving cloud data. This lack of consistency impedes forensic investigators and a clear consensus from U.S. lawmakers and officials would provide much needed clarity to the field of cloud forensics.

This research into cloud forensic challenges could easily be expanded by changing the methodology to include original data gathered directly from cloud providers, forensic investigators, policymakers, lawmakers and cloud consumers. A more hands-on approach in gathering data from the entities involved in cloud forensics directly could provide a new and interesting vantage point to this field of study.

Additionally, each area discussed in this research could be expanded to become a new focal point. There are many issues with cloud security that could be researched in-depth and become the center of another study that solely discusses how cloud security itself impedes cloud forensic investigations. Likewise, one could focus specifically on the multi-jurisdictional aspect of cloud forensics, or privacy issues and extend that research into a complete study. For an individual who is currently working in the field of digital forensics, actually developing and implementing a standard procedure for investigation would be a project that could be put to use by others in the field.

Because cloud forensics is a relatively new field of study, there is not a large amount of research dedicated to the challenges investigators face. This lack of research hinders cloud investigators and prevents developments in the field. Technology develops rapidly and it can be difficult for research to keep up with the rate of growth. As cloud technology forensics continues to develop and become more mainstream, it will likely become the focus of more studies which will help to reveal the unique challenges investigators are encountering.

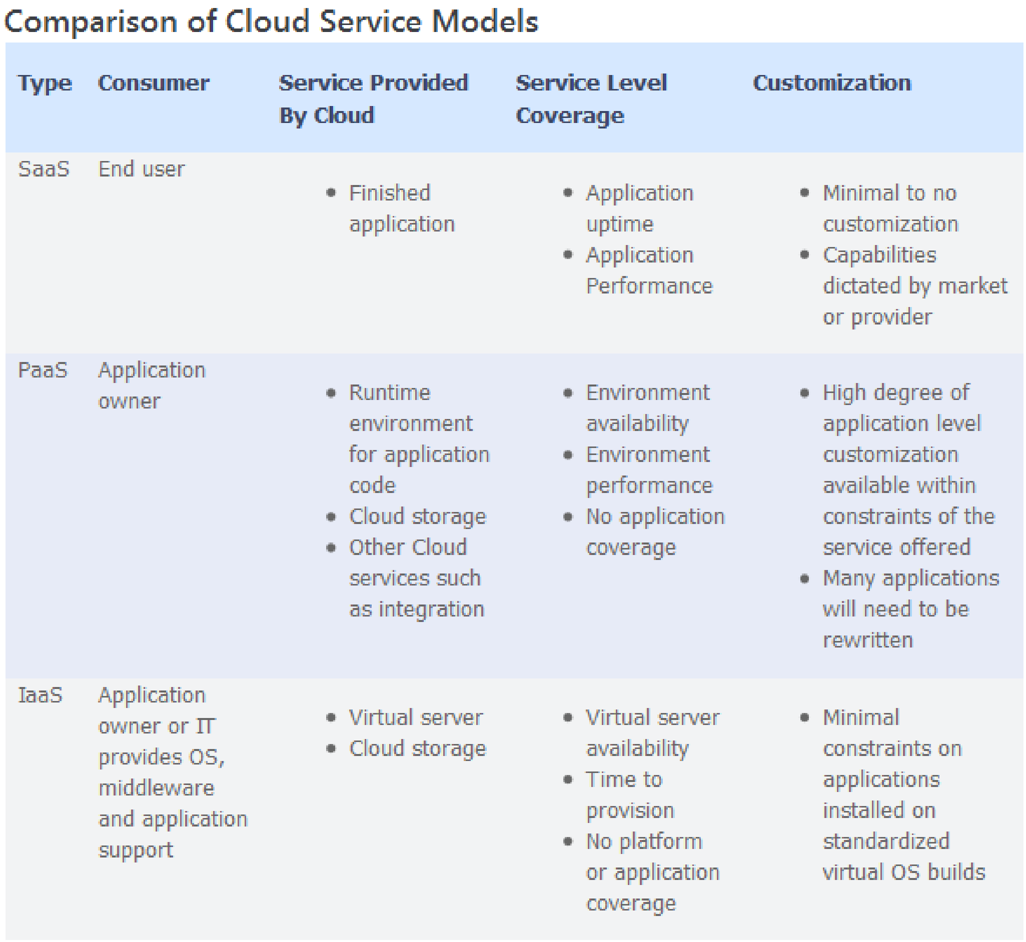
Conclusions

The purpose of this study was to examine and evaluate several of these challenges that investigators face when dealing with data stored as part of cloud technology.

- How are criminals using cloud technology to their benefit?
- In what specific ways does cloud computing pose a challenge for digital forensic investigations?
- Are the current laws, policies, procedures and best practices for digital forensic investigations effective when dealing with cloud computing technology?
- Should changes be made to current policy to aid in the effectiveness of digital forensic investigations?

For as long as cloud computing remains a part of the technology landscape and hackers and criminals continue to exploit it, there will be a place for digital forensics in the cloud. Digital investigators working in a cloud environment will benefit greatly from improvements to the cloud forensic process; namely, increased cloud security, the development of a comprehensive procedure for cloud forensics and clarification on existing laws and policies that affect cloud technology. If this can be accomplished, the cloud can become a more secure environment for consumers and a more difficult target for hackers and criminals. As more research is conducted in this field of study, the author is hopeful that the issues facing cloud investigators will become more of a concern to the industry and steps will be taken to ensure the continued success of digital forensics and cloud-specific forensics.

Appendix



Comparison of Cloud Service Models

Type	Consumer	Service Provided By Cloud	Service Level Coverage	Customization
SaaS	End user	• Finished application	• Application uptime • Application Performance	• Minimal to no customization • Capabilities dictated by market or provider
PaaS	Application owner	• Runtime environment for application code • Cloud storage • Other Cloud services such as integration	• Environment availability • Environment performance • No application coverage	• High degree of application level customization available within constraints of the service offered • Many applications will need to be rewritten
IaaS	Application owner or IT provides OS, middleware and application support	• Virtual server • Cloud storage	• Virtual server availability • Time to provision • No platform or application coverage	• Minimal constraints on applications installed on standardized virtual OS builds

Bibliography

Barnhill, D. (2010). Cloud computing and stored communications: Another look at Quon v. Arch Wireless. *Berkeley Technology Law Journal (2010).*

Birk, D. (2011, January 12). *Technical challenges of forensic investigations in cloud computing environments* [PDF]. Retrieved from http://www.zurich.ibm.com /~cca/csc2011/submissions/birk.pdf

CERT/CC. (1999). Denial of service attacks. Retrieved from http://www.cert.org/ tech_tips/denial_of_service.html

Cloud platform as a service (PaaS) in cloud computing services. (2012). Cloud computing: Understanding legal best practices. Retrieved from http:// cloudcomputingsec.com/296/cloud-platform-as-a-service-paas-in-cloud-computing-services.html

Dialogic Corporation. (2010). Introduction to cloud computing [PDF]. Retrieved from http://www.dialogic.com/solutions/cloud-communications/build/~/media/ products/docs/whitepapers/12023-cloud-computing-wp.pdf

Garfinkel, S. (2011, October 17). The criminal cloud. MIT technology review. Retrieved from http://www.technologyreview.com/business/38720/

Gold, S. (2010, December). Protecting the cloud: attack vectors and other exploits. *Network Security*. Vol. 2010, No. 12. pp. 10-12. doi:10.1016/S1353-4858(10)70146-X

Grispos, G., Glisson, W., & Storer, T. (2011, August 9). Calm before the storm: The emerging challenges of cloud computing in digital forensics. Retrieved from http://www.dcs.gla.ac.uk/~tws/papers/grispos11calm-rev2425.pdf

Haff, G. (2009, January 27). Just don’t call them private clouds. CNET. Retrieved from http://news.cnet.com/8301-13556_3-10150841-61.html

Hawthorn, N. (2009, October). Finding security in the cloud. *Computer fraud & security*.

Ingthorsson, O. (2011, November 30). 5 cloud computing statistics you may find surprising [Weblog post]. Cloud computing topics. Retrieved from http:// cloudcomputingtopics.com/2011/11/5-cloud-computing-statistics-you-may-find-surprising/

IBM. (2007). Virtualization in education [PDF]. Retrieved from http://www-07.ibm.com/solutions/in/education/download/Virtualization%20in%20Education.pdf

Kavitha, V. & Subashini, S. (2010). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications.* doi:dx.doi.org/10.1016/j.jnca.2010.07.006

Lawton, G. (2011, January). Cloud computing crime poses unique forensic challenges. Retrieved from SearchCloudComputing: http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges

Loeffler, B. (2012, January). What is infrastructure as a service? Microsoft TechNet. Retrieved from http://social.technet.microsoft.com/wiki/contents/articles/4633.what-is-infrastructure-as-a-service.aspx#Infrastrcuture_as_a_Service

Mansfield-Devine, M. (2008, December). Dangers in the cloud. *Network Security*. doi:10.1016/S1353-4858(08)70140-5

Mason, S. & George, E. (2011). Digital evidence and ‘cloud’ computing. *Computer law and security review*. Vol 27 (2011) 524-528. Doi:10.1016/j.clsr.2011.07.005

McCall, T. (2011, July 7). Gartner says worldwide software as a service revenue is forecast to grow 21 percent in 2011. Retrieved from http://www.gartner.com/it/ page.jsp?id=1739214&M=6e0e6b7e-2439-4289-b697-863578323245

Mell, P. & Grance, T. (2011, September). The NIST definition of cloud computing [PDF].National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Network Security (2010).Online criminals replacing brawn with brain. Volume 2010(1), 20.doi:10.1016/S1353-4858(10)70018-0

Paul, A., Anvekar, M., Jacob, R. & Sekaran, K. (2012). Cyber forensics in cloud computing. *Computer engineering and intelligent systems*. Vol 3(2).

Puri, R. (2003, August 8). Bots & botnets: An overview. Retrieved from SANS Institute at http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299

Reilly, D., Wren, C., & Berry, T. (2011, March). Cloud computing; Pros and cons for computer forensic investigations. *International journal of multimedia and image processing.*1 (1).

Ruan, K., Carthy, J., Kechadi, T. & Crosbie, M. (2011). Cloud forensics: An overview [PDF]. Retrieved from http://cloudforensicsresearch.org/publication/ Cloud_Forensics_An_Overview_7th_IFIP.pdf

Shields, C., Frieder, O. & Maloof, M. (2011). A system for the proactive, continuous, and efficient collection of digital forensic evidence. *Digital investigation.* 8(2011) S3-S13. doi: 10.1016/j.diin.2011.05.002

Software & Information Industry Association (SIIA). (2001, February). Software as a service: Strategic backgrounder [PDF]. Retrieved from SIIA.net at http://www.siia.net/estore/pubs/SSB-01.pdf

Sternstein, A. (2010, September). Debate heats up over police access to data in the cloud. NextGov. Retrieved from http://www.nextgov.com/nextgov/ng_20100924_5567.php

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer law and security review*. Vol 26 (2010) 304-308. doi: 10.1016/j.clsr.2010.03.002

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011, March). Forensic investigation of cloud computing systems. *Network Security.* Vol 2011 (3) 4-10. doi: 10.1016/S1353-4858(11)70024-1

U.S. Const. amend. IV.

Williams, A. (2010, April 19). The largest cloud in the world is owned by a criminal network. Read Write Web. Retrieved from http://www.readwriteweb.com/cloud /2010/04/the-largest-cloud-in-the-world.php

Zimmerman, S. & Glavach, D. (2011). Cyber forensics in the cloud. IA Newsletter. Vol 14 (1). Retrieved from http://iac.dtic.mil/iatac/download/Vol14_No1.pdf