Security and Digital Forensics in Cloud Computing

Marcellus Williams II
Department of Computer Science
Hampton University
marcellusawilliams2@gmail.com

Chutima Boonthum-Denecke
Department of Computer Science
Hampton University
chutima.boonthum@hamptonu.edu

ABSTRACT

This paper will be discussing the importance of digital forensics in cloud computing. As cloud computing evolves and become a more prevalent factor in our use of technology, so do the risks and security vulnerabilities that can potentially cause a lot of harm to a larger range of people. Digital forensics is a way to gather data, and intelligence of how to make cloud services more secure and effective at distributing resources. Digital forensics is the process of gathering data, and analyzing it to support a scientific purpose. This purpose could be trouble shooting the cloud architecture or recovering lost data due to an inefficient computational algorithm. When using cloud computing it would be beneficial to incorporate some form of digital forensics techniques and tools to gain a better understanding of how the data is stored and secured.

CCS CONCEPTS

• **Applied computing** → Computer forensics; • **Computer systems organization** → Cloud computing

KEYWORDS

Cloud Computing, Cloud Services, Digital Forensics

ACM Reference format:

M. Williams, C. Boonthum-Denecke. 2017. Security and Digital Forensics in Cloud Computing. In *Proceedings of 2017 ADMI Symposium*, Virginia Beach, Virginia USA, March 23-26, 2017.

1 INTRODUCTION

As the field of cloud computing begins to grow and evolve into a viable form of rapid accessibility computing so do the security vulnerabilities associated with it. Digital forensics is a way to gather data, and intelligence of how to make cloud services more secure and effective at distributing resources. Digital forensics is the process of gathering data, and analyzing it to support a scientific purpose. This purpose could be trouble shooting the cloud architecture or recovering lost data due to an inefficient computational algorithm. When using cloud computing it would be beneficial to incorporate some form of digital forensics techniques and tools to gain a better understanding of how the data is stored and secured.

This paper will be broken into 4 components, the background review, the discussion, any future work with the topic, and finally the conclusion, which will wrap up the topic and summarize the key points. Within the background review this paper will be discussing what cloud computing is so that the reader will have an understanding of what cloud computing is and how attackers can negatively impact it. Once the reader has a full understanding of what cloud computing is the paper will focus on specific examples of exploits that have impacted cloud-computing architectures, and have done a lot of damage to people. Next, we will discuss what digital forensics is and how digital forensics has worked to solve cybercrimes and deter cyber criminals from conducting attacks on networks and information systems. In the discussion portion we will be discussing how digital forensics can be beneficial to cloud computing, and aid in making cloud architecture more secure by helping with investigation purposes and deterring potential criminals. This paper will also analyze the different forensic tools available on the market to conduct a comparison and determine which tools are best for implementation in a cloud environment. We will be using the tools, and comparing their effectiveness in different competency areas to determine which one is the most effective at investigating cloud-based incidents. This paper will also cover the limitations of digital forensics in the cloud so you can have an understanding of why cloud forensics is such a difficult task to conduct and implement when it comes to cloud security. A lot of the limitations come from a legal standpoint as a result of the cloud spanning multiple geographic locations. It makes it difficult to know where to draw the lines of jurisdiction and responsibility. In the future we plan to do vulnerability assessments in the cloud, and conduct digital forensics on various cloud services.

2 BACKGROUND

2.1 Cloud Characteristics

In order to understand the importance of digital forensics as it relates to the cloud we must first understand what cloud computing is, and what security vulnerabilities put it at risk. The National Institute of Standards and Technology defines cloud computing as a form of computing that allows for convenient, consistent, and quick access to computing resources that allow for the development of applications, the ability to store and access data and items, and the ability to manipulate data and rapidly implement complex algorithms for the benefit of society.

Cloud computing has 5 essential characteristics that must be maintained through effective security controls in order for the cloud to maintain functionality. The characteristics are: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

On-demand self-service means that the subscriber or user can alter their service to fit their needs without the intervention of the service provider. The simpler the cloud implementation, the more reliable and effective it is for use. *Broad network access* means the cloud can be used by a variety of different network based devices. The devices consist of thick clients such as desktops and laptops, or thin clients such as tablets, and phones. *Resource pooling* is the ability for the computing resources to be used by consumers and serve multiple purposes using virtual and physical resources. *Rapid elasticity* meaning the services can be scaled based on an as needed basis. The user can decide how many resources they need for their project or application, and can increase or decrease them at will. The final characteristic of cloud computing is *measured service*, where the computing service uses some type of abstraction algorithm to optimize the experience. The computing service uses some type of analytics to analyze the efficiency of the resource use and leverage the resources for more effective and efficient, whether it is storage, computing, or application development [6]. It is worth noting that security is one of concerns in cloud computing.

Cloud Computing Pros vs Cons	
Pros	**Cons**
Agility	Customization Costs
Cost Efficient	Usability
Fast Deployment	Connectivity
High Scalability	Security

Figure 1. Pros and Cons of Cloud Computing

2.2 Cloud Services

Now, we need to understand the type of services available and what value the offer to potential cloud computing users. There are three types of services available for cloud computing architecture: Software-as-a-service, Platform-as-a-service, and Infrastructure-as-a-service. Software-as-a-service is the use of cloud based applications for storage, computation, network management, and other future provided by the service provider. The consumer does not control, or administer this architecture but simply uses them for computational functions. An example, Google Docs, is an application distributed by the cloud that allows for users to create documents with their peers and store them on the cloud for constant peer based review. The user does not control or manage this application, and instead simply enjoys the cloud resource provided. The documents are created and stored seamlessly in the cloud, thus increasing the need for security and protection.

Platform-as-a-service is the use of cloud for application building classes, where the provider grants the consumer access to languages, libraries, and tools to create and publish their own applications for personal use, or consumption. An example of a platform-as-a-service is Microsoft Azure, which provides languages, and classes for easy and sophisticated application building and deployment. It is compatible with a multitude of languages, and provides classes and tools for easy implementation.

Finally, *infrastructure-as-a-service* is the use of cloud services for storage, processing, and network uses outside of software development. These applications provide for the storage of data to be manipulated and utilized in customer applications. They provide essential features such as cloud databases, and even cloud virtual networks that can be used and distributed different organizations. These types of services all prevent different security risks that must be addressed and mitigated. If an incident occurs it is important to consider digital forensics to find the culprit, and deter others from causing similar incidences. [6]

2.3 Deployment Models

The final basic component of cloud computing is the deployment model. This is critical to understanding what type of security controls need to be implemented, and the type of risk your data is exposed to. There are 4 deployment models: private, community, public, and hybrid. A private cloud is a cloud where a single entity uses the cloud, which may be distributed by that organization or a third party cloud provider. Only those connected to this organization are capable of using the private cloud computing resources. This is the most secure form of cloud computing, because the computing resources are kept secure within a single network, and not broadcasted over a wide area.

A *community cloud* is the exclusive use of cloud computing services by a group of consumers from organizations with the same interests. These organizations tend to share stakeholders, and work together to meet the demands of their stakeholders. This deployment model is still fairly secure as it restricts the use of cloud resources, but the permitted user amount is much larger than that of the cloud meaning authentication is critical to keeping this cloud secure. There are more people with access to this cloud, which increases the risk. The trade off with private and community-based clouds is you trade some of the availability, and ease of use for a more secure architecture where use is fairly limited. This is the opposite of the public cloud deployment model. The public cloud deployment model is an open use deployment model where the cloud resources are distributed

openly to the public for a fee. A public cloud is not owned, managed, and distributed by a private entity and is available for all paying customers. This form of cloud deployment is the least secure, because it is readily available via wide area networks, and the Internet meaning more people have access to it. The more people that have access to the cloud, the more likely it is for someone to exploit a security vulnerability and cause harm using cloud computing. The final deployment model is the hybrid cloud. A hybrid cloud is any combination of the other three cloud deployment models for a more customized use of the service. The consumer of a hybrid cloud deployment model can use a public cloud for deployment of applications, but a private one for data storage, and network management. This form of cloud deployment provides consumers with the ability to modify their use of cloud services to fit their individual security, exposure, and availability needs. [6]

2.4 Cloud Vulnerabilities

This section will discuss on how these cloud characteristics add different vulnerabilities to cloud computing. Understanding these vulnerabilities associated with the cloud facilitate understanding why digital forensics in the cloud is a growing field of importance. We understand the characteristics of the cloud, the services provided, and how they are deployed. Now we must understand how each of those elements contributes to the vulnerability of the cloud. Cloud computing provides a variety of different services, and benefits but each benefit has its individual drawbacks or vulnerabilities that must be considered by consumers before using the cloud. Among those benefits is a readily deployable virtual environment, which also contains risks.

A cloud virtual server, or network is hosted similar to a physical server; the difference is the virtual servers contain software to support Virtual Machine functionality. If there is vulnerability in the virtual machine software it could potentially infect the physical servers and cause a massive amount of damage. One such vulnerability is hypervisor vulnerability, which is similar to an unauthorized elevation of privilege. With the hypervisor exploit an attacker can execute code and gain control of all virtual machines running on the host. This would disrupt the on-demand service characteristic of the cloud, because the virtual machine resource available on the host server would be unavailable to consumers. This type of attack can lead into a denial of service attack where the virtual host is flooded with fake traffic resulting in the server to overflow and deny service to legitimate traffic hindering the consumers' access to the service. [3]

A common concern for cloud computing is data security. For the software-as-a-service architecture data is often processed and stored in plaintext in the cloud, with the service provider being the one responsible for the security. The data is also stored in backups by the provider, which raises additional concerns since the confidential data is stored in multiple locations where it can be compromised through multiple avenues. Accessibility is an additional concern, because through broad network access more devices are able to access the cloud's data. If any of the devices are compromised it could compromise the entire storage service in your cloud for all other devices. Basically, if you use your phone that contains some form of malware it can be used as a vehicle to gain access to the cloud and compromise your data or your customer's data.

The platform-as-a-service architecture contains vulnerabilities, because they typically rely on third-party relationships and tend to inherit the vulnerabilities of those third party platforms. Infrastructure-as-a-service is usually vulnerable through virtualization, and a concept called Virtual Machine Migration. An attacker can target a virtual machine and migrate it to a malicious server, thus compromising all the data within that virtual machine. This can be done if the attacker elevates his or her privileges to hypervisor, which is responsible for virtual machine isolation.

Infrastructure-as-a-service also provides virtualized network capabilities for organizations, and should that virtualized network be compromised all the data contained in the organization's network could be compromised. They could easily migrate the network to where it travels through a malicious server feeding confidential information to the server, thus providing the attacker with access to that information. [2]

2.6 Cloud Exploits

A recent cloud attack against Dropbox has resulted in the theft of passwords for 68 Million accounts for the online software-as-a-service cloud storage platform. Dropbox is a digital media storage platform that contains sensitive photos, and videos among other things. These passwords are often sold on the Dark Web marketplace, where photos and videos can be used for multiple fraudulent purchases, and online identity theft. An additional danger from this compromise to the cloud service Dropbox is that additional accounts that use similar credentials are also threatened, such as bank accounts and email accounts. [5]

Another recent attack on cloud services is the ransomware attack on Apple's iCloud services. The attack gains access to the lost iPad or iPhone mode and locks the device before posting a ransom note in Russian demanding $30 to $50 dollars sent to the referenced email. [7] A corporate cloud email service provider was also attacked by a spear phishing attack that resulted in the services being halted. The attack was a result of an attacker repeatedly sending emails with malicious links to the company's email. This malicious link would result in the attacker gaining access to the company's cloud based email service known as Mimecast. A lot of organizations use cloud services like Mimecast to host their company email suites. This provides administrators with the ability to monitor conversation, and allow for network collaboration. This collaboration can be compromised if the attacker gains access to the virtual server containing the emails. Confidential information about projects and consumer data can be compromised with ease. [1] Whenever an incident occurs dealing with computing or data manipulation, an organization typically uses some form of digital forensics tools and techniques to investigate the crime and hold someone accountable. These investigations stop the attacker from being able to repeat success

in the attack by either capturing the culprit, or providing enough insight to fix the vulnerabilities. A successful investigation also deters other attackers from attempting the same exploit given the increased possibility of their capture.

2.6 Digital Forensics

Digital forensics or computer and network forensics is the application of science to aid in the identification, collection, examination, and analysis of data while preserving the integrity of the information and adhering to a strict chain of custody for the evidence so it can be considered admissible in court. Cloud computing relies heavily on data, and data manipulation, which could be beneficial to implementing a digital forensics program to gather evidence against physical, and digital crimes. Digital forensics consists of four basic phases: collection, examination, analysis, and reporting.

Collection is the identifying, recording, and acquiring of data relevant to what has occurred, and what is being investigated. For cloud computing purposes, it could be active or inactive malware that contains identifiable characteristics.

Examination is the process of determining the value of the collected evidence to suit the investigation's intent, while maintaining the data's integrity.

Analysis is deriving the critical details that would corroborate or support the intent of the evidence or data. It addresses all the necessary questions to paint a clear picture of what has occurred.

The final phase is *reporting*, which consists of describing what the evidence intends to prove, and how it was obtained to determine its validity and if it can be admissible in court.

Digital forensics has become critical due to the increase in use of computer to commit various types of crimes. Attackers have grown heavily invested in using cloud architecture to distribute viruses, or take advantage of security vulnerabilities to compromise confidential data. The digital forensics process will help provide insight on how to protect cloud computer services, and make cloud computing more secure for the consumers. Digital forensics provides multiple forms of added benefits outside of supporting investigations. It provides such benefits as: operational troubleshooting, log monitoring, data recovery, data acquisition, and regulatory compliance.

Digital forensics tools and techniques can be applied to troubleshoot operational issues related to the virtual machine host of a cloud server, or resolve functional issues with a software-as-a-service application to prevent the exploitation of a serious flaw before it can even become a threat. Log monitoring is the process of collecting and analyzing logs or system audits for accountability purposes. This can be useful outside of an investigation, because it can allow for organizations to build a profile on an individual that could compromise their cloud or correct dangerous behavior before it can cause damage or compromise of data stored in the cloud servers. One of the biggest fears about cloud computing is the loss of data due to everything being stored virtually, instead of at physical data centers within an organizations reach.

Digital Forensics is the science of recovering or acquiring data; meaning data that is lost can be recovered using the right forensic techniques. This adds a little bit of reassurance to organizations that make the switch to cloud computing as their primary means of storing, and manipulating data to be readily accessible. Data acquisition is also useful when hosts are retired or no longer used. The data can be retrieved from the hosts and stored in the cloud to be used again as needed. A lot of organizations that use the cloud are government agencies, or have government standards that require them to meet a security standard. Some healthcare facilities utilize private or public clouds to speed up the process of disseminating protected health information so they can help patients faster. They can utilize digital forensics to assess their ability to protect confidential health information, as it is stored in cloud architecture. Failure to protect this information could result in detrimental legal action that puts the entire organization in jeopardy. [4]

2.7 Cloud Forensics

Cloud computing is a new transformative way of computing similar in impact to the introduction of the World Wide Web, and fourth generation smart phones. This technology is radically changing how information services are created, delivered, accessed and managed. Cloud computing services is growing at an alarming rate making it urgent that we address the security concerns and redefine how security is maintained for the cloud. The term for digital forensics in the cloud is called cloud forensics, which focuses on the broad network access element of cloud computing environments.

Cloud forensics is complicated, because cloud computing allows for resources to cover and span multiple geographic areas blurring the lines of traditional jurisdictions for investigation purposes. This makes it extremely important that investigators collaborate with each other to determine who takes the lead, and how they can facilitate a successful cloud forensics investigation. What makes cloud digital forensics extremely importance is the multiple dimensions that are required in the investigation. These dimensions are: technical dimension, organizational dimension, and legal dimension. The technical dimension refers to the tools and procedures utilized to complete the forensic process in the cloud-computing environment. This includes the data collection process, live forensics analysis, and evidence segregation.

The data resides in two locations, the client-side or area of the cloud that the consumer typically utilizes, and the provider-side or area of the cloud that the provider is responsible for maintaining. The client-side sends requests to the provider-side for access to the cloud resources. Rapid elasticity must also be extended to forensic tools as needed when dealing with cloud forensics. This means forensic tools must be dynamically allocated as needed to facilitate the investigation process.

Another essential characteristic of cloud computing that must also be extended to the forensic process is the use of resource pooling. Resource pooling from a forensics standpoint allows for the compartmentalization of evidence to serve multiple purposes. The next dimension is the organizational dimension, which deals

with the personnel components that contribute to cloud computing architecture. This includes the cloud service provider, the customer, and any third-party that helps implement the cloud service. The organization must issue a service level agreement to facilitate collaboration in cloud computing between law enforcement, the cloud service provider, third parties and academia. Third parties can aid in compliance, while academia can provide the technical experts to facilitate the data collection as a part of the technical dimension. The organization must also ensure the fulfillment of the following roles via internal staffing or external participation and collaboration: investigators, IT professionals, incident handlers, legal advisors, and external assistance. Investigators examine the allegations and work with law enforcement to build the case to be taken to court and obtain a conviction. IT professionals provide expert support for the facilitation of data collecting, and cloud vulnerability testing.

Incident handlers respond to incidents and initiate the appropriate actions for business continuity. Legal advisors provide the regulatory guidelines for the cloud forensics process so the digital evidence is admissible in court, and not thrown out due to procedural issues or wrongdoing. Finally, external assistance is important in cloud forensics to aid in the audit process. The final dimension is the legal dimension, where it deals with how the case is built legally to ensure the evidence is admissible and the evidence corroborates the story to prove guilt in cloud related crimes. [8]

2.8 Limitations

One of the most difficult challenges to overcome in the field of cloud forensics is using the cloud to collect forensic data. Depending on the implementation the customer can have maximum control over their data, or little to no control over the physical location of their data. Infrastructure-as-a-service provides unhindered access to the physical location of data, whereas software-as-a-service provides almost no access to the physical location of the data. Without access to the physical data it is difficult to conduct a data acquisition, and requires a lot more collaboration with the cloud service provider, which would lengthen the process.

Another challenge is data recovery. Since the data is stored virtually, once it is deleted it is not possible to recover the data unless the cloud service data has redundant storage for the deleted data. This is due to the fact that the data is not physically stored anywhere on hand, and once the data is deleted it can be rapidly overwritten deleting it from memory completely. This hinders the process of event recreation to aid with the investigation and painting the picture of occurrence for the court. Another challenge is evidence segregation, or separating the relevant data from the other items stored in the cloud. Since multiple tenants use the same host to collect and store data, audits may of multiple tenants are often stored in one audit log making it difficult to find the relevant data to assist in the investigation.

Another limitation is dealing with the lack of policies and procedures when it comes to hypervisor attacks. A hypervisor is to a virtual operating system, as a kernel is to a traditional operating system. Hypervisors are big targets for attackers, and the lack of policy makes it difficult to conduct forensic investigations, due to the lack of knowledge and techniques of how to investigate hypervisor attacks. Another issue is with the redundant data stored over multiple jurisdictions creates legal issues, because investigators are not sure who is responsible for data stored in what location. Investigators can unknowingly violate laws leading to the evidence not being admissible in court resulting in a case being thrown out due to procedural error. [8]

Table 1. The limitations associated with digital forensics in cloud computing.

Cloud Forensics Challenges Categories				
Architecture	Multi-Tenancy	Data Segregation	Origin	
Data Collection	Data Integrity	Data Recovery		
Analysis	Metadata Logs	Metadata		
Anti-Forensics				
Risk Management	Identity Management			
Legal	Contract	Jurisdiction	Privacy	Ethical
Standards	Interoperability	No Single Process		
Training	Qualifications	Certifications		

3 EXPERIMENTAL AND RESULTS

Because of the difficulty of conducting digital forensics experimentation in cloud forensics, we started our research on comparing current market digital forensics tools to determine which tools would be the most effective for cloud digital forensics analysis. The three applications we used for this experiment are: *EnCase*, *ProDiscover*, and *FTK Imager*.

The system we used to conduct the digital forensics imaging is a 2013 MacBook Pro Retina with a 2.3 GHz Intel Core i7 with 16 GB of RAM. The Operating System was a Windows 7 virtual environment opened using VMware Fusion. The experimental data were found in exercises from Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, and Christopher Stewart. The data was stored on a disk, which we extracted onto an external hard drive along with free versions of EnCase, ProDiscover, and FTK Imager. This experiment will measure each application's ability to obtain documents, allocated picture files, unallocated picture files, emails, and encrypted files.

Table 2 illustrates the results of the different digital forensics tools in recovering data in five areas of competency. These areas are especially critical to cloud computing as they are the most commonly stored data types used in cloud computing architecture.

Table 2: Digital Forensics Tools Comparison

Digital Forensics Tools Comparison			
	EnCase	**FTK Imager**	**ProDiscover**
Documents	5	5	5
Allocated Pictures	8	6	5
Unallocated Pictures	3	0	3
Emails	10	6	3
Encrypted Files	0	2	2

Based on the results of this experiment the best digital forensics tool to use for cloud architecture is EnCase, because of its ability to uncover the highest amounts of data in each respective competency except one. One of the deciding factors was its ability to uncover the highest amount of pictures and emails. Most picture applications, and email applications use cloud-computing architecture so uncovering emails and pictures are critical to the success of digital forensics in the cloud. ProDiscover is the most balanced, because it is able to be moderately decent at all of the competency areas, but when it comes to security you want to have the highest quality of security controls and data acquisition applications as possible. Encrypted files is the least critical form of data when it comes to cloud computing because even if the data is recovered the file is not accessible unless it is decrypted, which could take days, hours, or even years to complete.

4 CONCLUSIONS

In this paper we discussed cloud computing in general including the five characteristics of cloud computing, the services available, and the different deployment methods that deliver the resources to the consumer. The cloud is a very complex form of computing where resources are provided quickly and efficiently through network access to perform a variety of different functions. As one of the most rapidly developing form of computing it has become a target for many forms of attack and espionage. As these attacks occur it is critical that cloud service consumers investigate the cause of these attacks to attempt to capture the culprit, and mitigate the vulnerability.

We discussed some of the basic vulnerabilities that are inherent to cloud computing that consumers should be cognizant of. One of the vulnerabilities occurs because of the broad network access characteristic of cloud computing. Many devices are allowed to access the cloud meaning it provides more avenues of attack. We also included specific examples of cloud attacks that caused moderate damage to organizations, and consumers; as well as what digital forensics is from a standard traditional computing standpoint so the reader can have an understanding of the basics of digital forensics. Then we discussed about how digital forensics impacts cloud computing, and becomes an asset to securing the cloud. It facilitates the release of patches to fix vulnerabilities, and gathers data that can be used to investigate incidents. We also talked about the limitations when dealing with digital forensics in the cloud. The limitations are due to the lack of techniques and procedures due to the rapid development of the cloud. These limitations will become less prevalent once an adequate amount of research is done in how to effectively incorporate digital forensics into cloud computing.

In the future we plan to conduct digital forensics investigations on some of the cloud services and then investigate whether existing penetration testing and digital forensics techniques can minimize the intrusion.

ACKNOWLEDGMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant no. DGE-1303409 (PI/co-PI: Dr. Chutima Boonthum-Denecke, Dr. Jean Muhammad).

REFERENCES

[1] "Cloud service provider has its email networks hacked | Hexis", *Hexiscyber.com*, 2015. [Online]. Available: https://www.hexiscyber.com/news/hot-topics/cloud-service-provider-has-its-email-networks-hacked. [Accessed: 07- Dec- 2016].

[2] K. Hashizume, D. Rosado, E. Fernández-Medina and E. Fernandez, "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications*, vol. 4, no. 1, p. 5, 2013.

[3] Hussain, Z. & Gummadi, A. (2013). *Vulnerabilities in Cloud Computing* (1st ed., pp. 8-10). Fairfax, Virginia: George Mason University. Retrieved from http://www.chinacloud.cn/upload/2013-05/13050613111874.pdf.

[4] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response* (1st ed., pp. 16-17). Gaithersburg, MD: The National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

[5] Khandelwal, S. (2016). *Dropbox Hacked — More Than 68 Million Account Details Leaked Online. The Hacker News*. Retrieved 5 December 2016, from http://thehackernews.com/2016/08/dropbox-data-breach.html.

[6] Mell, P. & Grance, T. (2011). *Special Publication 800-145: The NIST Definition of Cloud Computing* (1st ed., pp. 5-7). Gaithersburg, MD: The National Institute of Standards and Technology. Retrieved from http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

[7] Ragan, S. (2016). *Apple devices held for ransom, rumors claim 40M iCloud accounts hacked*. *CSO Online*. Retrieved 5 December 2016, from http://www.csoonline.com/article/3093016/security/apple-devices-held-for-ransom-rumors-claim-40m-icloud-accounts-hacked.html.

[8] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud Forensics. *Advances In Digital Forensics VII*, 35-46. http://dx.doi.org/10.1007/978-3-642-24212-0_3