Amanda Bedard

IA5210

Elton Booker

December 2, 2018

Cloud Forensics

Abstract

The goal of this paper is to provide research on the fairly recently emerging field of digital forensics/forensic analysis in the cloud. Research from the proposed sources outlines a history of cloud computing, and how it came to be where it is. It also describes different types of cloud storage, as well as forensic cases where the analysis of data stored in the cloud has been impactful on the result of the case. It will list tools and resources that can be used with forensic analysis of a cloud environment, as well as what makes a case involving cloud storage different from another case that would not involve data/software in the cloud. It will also provide a hypothesis on where the future of forensics in cloud environments is heading.

Introduction

This section provides a detailed introduction on the definition of the cloud and cloud computing, and important features of each. It highlights terms and ideas that are found in later sections to provide the user a general background in order to better understand later concepts brought in.

Being a popular buzzword, if a member of any technological field, one has likely heard of the cloud. Many companies are moving their infrastructure to the cloud for cost savings and virtually infinite scalability. All of this sounds wonderful, but if one does not have a full understanding and background of what the cloud and cloud computing is, its purpose in technology, and why it is so important, then it will be hard to comprehend certain intricacies and difficulties that arise in the field of forensics when it comes to this topic.

According to Amazon Web Services, cloud computing can be defined as "the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing". Basically, if one is to use the cloud, they are paying a company (such as Amazon) to use servers, storage, and/or databases as they are needed[1]. The Cloud Service Provider (CSP) will handle the infrastructure work, such as patching servers and physical security, and the user will handle items such as configuration and data protection when it comes to security. This is usually outlined in the CSP's shared responsibility model[2].

Services on the cloud can be split into three major service models. There is Software-as-a-service (SaaS), which is software delivered through the browser of the user. With this service model, there is no downloading needed and the software is easy to distribute. Another one is Platform-as-a-Service (PaaS), which can be explained as a platform to be used in the creation of software so that the developers do not need to worry about maintaining an operating system, updates, or infrastructure when developing. Finally, there is Infrastructure-as-a-Service (IaaS), which is nothing more than the highly scalable resources made available for companies to provision on their behalf with the CSP. This allows companies to spin up servers in a fraction of the time for use, and shut them down equally as quickly, without worrying about disposal, physical security, and space allocation[3].

Section 1: Fundamental Research

---

[1] Amazon Web Services. "What Is Cloud Computing? - Amazon Web Services." *Amazon*, Amazon, aws.amazon.com/what-is-cloud-computing/.
[2] Amazon Web Services. "Shared Responsibility Model - Amazon Web Services (AWS)." *Amazon*, Amazon, aws.amazon.com/compliance/shared-responsibility-model/.
[3] Watts, Stephen. "SaaS vs PaaS vs IaaS: What's The Difference and How To Choose." *BMC Blogs*, 2017, www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/.

In this section, a brief history of cloud computing is listed with important technological advances that contributed to the cloud as it exists today. It also takes a look at some important legal concepts that contribute to the design and usage of the cloud.

Some argue the birth of cloud computing was in 2006, when it was spoken by Google's prior CEO, Eric Schmidt, but it can be argued to have started in the 1950's with the introduction of mainframe computers. This would have been cloud-like in the fact that it is impractical to have a mainframe per each individual, so companies took a more centralized approach in their management and use. As the years passed, concepts such as virtual machines and virtual private networks were introduced[4].

While the term is first reported used in 1996, cloud computing arguably took off in 1999, where salesforce.com was first launched. Salesforce provided companies with Software-as-a-Service (SaaS), which is a pinnacle offering for any cloud computing company[5]. Cloud computing has launched itself into modern times with companies such as IBM, Google, Amazon, and many, many more big names that have adopted their own platforms and systems, and become major players in offering cloud-based services to consumers.

As it currently sits, there are laws and regulations regarding cloud usage and privacy. This widely varies, pending which service model you are using. Data in the cloud falls under the protection of the Fourth Amendment, which states "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation,

[4] Destefani Neto, Maximilliano. "A brief history of cloud computing." *IBM,* 2014, https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/.
[5] Park, Chi. "The History of Cloud Computing: Some Key Moments." *Inspirage*, Inspirage, 22 Aug. 2018, www.inspirage.com/2015/11/the-history-of-cloud-computing-some-key-moments/.

and particularly describing the place to be searched, and the persons or things to be seized"[6]. This protects CSP's and users from unlawful search and seizure of their data in the cloud. There are various other laws and regulations that will be discussed in *Section 2: Notable Cases and Legal Issues*.

For jurisdiction laws, nothing has been clearly defined yet. Because of the fact that the data can be stored on multiple servers across a plethora of regions and countries, finding the exact location of all the data can be very tedious[7]. Much of the legality of cloud computing is written into the SLA, so that when things go wrong, it is clearly defined who is responsible for the disaster recovery[8]. It's important to note as well, while certain services are compliant with standards such as HIPAA and PCI, it is up to the user to ensure that the software/platform/infrastructure they deploy is complaint as well[9]

Section 2: Notable Cases and Legal Issues

Section 2 outlines important legal decisions that influence the way cloud data is handled and classified. It also describes situations what can be considered cloud data, and when it is considered relevant. Also listed are notable cases involving the forensic analysis of data in a cloud based environment.

In most situations, investigation of data on the cloud is typically performed after some sort of initial investigation where existing evidence (whether it be on a physical machine or through testimony) points to incriminating or decriminating evidence stored within a cloud

---

[6] "U.S. Const., amend. IV."
[7] Wilson, David. "Legal Issues of Cloud Forensics." Expert Reference Series of White Papers. Global Knowledge. 2014.
[8] Wilson, David. "Legal Issues of Cloud Forensics." Expert Reference Series of White Papers. Global Knowledge. 2014.
[9] DePalo, Maki. "Cloud Computing - Legal Issues in the U.S. & International Implication." Law Library Student-Authored Works. Law Library. 2011.

service[10]. As consumers (and even most CSP's) do not have a direct view into the cloud, it is unlikely an initial investigation will contain any cloud forensics.

When it comes to cloud computing and CSP's, privacy is one of the biggest issues in a legal framework. The Stored Communications Act (SCA) addresses voluntary release of stored electronic communications, as a part of the Electronic Communications Privacy Act (ECPA). In the case of Jennings v. Jennings, a husband was suing his wife for accessing emails to his girlfriend, saying it was in violation of his SCA rights. The court ruled that since it was stored for purposes of backup protection, it was still within the SCA[11]. The interesting piece of the SCA is that it does not always require a warrant- if the communication has been in storage for more than 180 days, a court order will suffice[12]. This is big due to the fact most modern electronic communication is stored in the cloud.

Many times, the CSP is hesitant to cooperate with law enforcement, as they wish to prioritize the privacy of their customer's data and do not want to tarnish their reputation. In the situation where law enforcement agents believe an Amazon Echo Device (commonly referred to as 'Alexa') had essentially been a witness to a double murder, the case was prolonged due to the fact Amazon was unwilling to share any data without a binding, legal request served[13].

Unable to keep up with the fast-paced world of technology, laws and regulations tend to fall behind. The Electronic Privacy Information Center (EPIC) had placed a complaint stating

---

[10] Simou, Stavros. "A Survey on Cloud Forensics Challenges and Solutions." Security and Communication Networks, Volume 9, Issue 18. Wiley Online Library. November 8, 2016.
[11] DePalo, Maki. "Cloud Computing - Legal Issues in the U.S. & International Implication." Law Library Student-Authored Works. Law Library. 2011.
[12] "Stored Communications Act, Codified at 18 U.S.C. §§ 2701–2712." The Reporter's Privilege Compendium: An Introduction | Reporters Committee for Freedom of the Press. May 08, 2017. Accessed December 03, 2018. https://www.rcfp.org/electronic-communications-surveillance/iii-electronic-communications-surveillance-authorities/elec-0.
[13] Flynn, Meagan. "Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over." The Washington Post. November 14, 2018. Accessed December 2, 2018. https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/?noredirect=on&utm_term=.bb592a23783f.

that Google is not providing sufficient protection of the confidential information it may receive from users, such as storing personal data in an encrypted form. EPIC states that these security measures are common sense, and that Google is doing their users a disservice by not following the best practice[14]. This brings up an important, unresolved point on whether it should be up to the user to determine if a platform is secure, or if a platform should be required to follow best practices for securing their user's data.

Section 3: Capture and Analysis

In this third section the capture and analysis of cloud data is discussed. The capture of cloud data is outlined, including common challenges that arise with the nature of the data, as well as typical processes. Also listed is some tools and services that can assist in the analysis of such data, along with common processes for handling cloud data.

Capturing data in the cloud for forensic analysis comes with its own set of unique challenges. As there are usually restrictions (or just a general inability) when it comes to physically obtaining the hardware. This requires all data acquisitions on cloud environments to be done live, as opposed to traditional methods. Many times, this requires the use of third party tools, which highlights the concern of integrity, as in order to be presented in court, it must be shown that there is no way the evidence could have been tampered with[15]. Fortunately, since data on the cloud may require some sort of browser interaction, a physical machine analysis can still provide useful information.

---

[14] Buller, Daniel. Wittow, Mark. "Cloud Computing: Emerging Legal Issues for Access to Data Anywhere, Anytime." Journal of Internet Law, Volume 15, Number 1. Aspen Publishers. July, 2010.

[15] Simou, Stavros. "A Survey on Cloud Forensics Challenges and Solutions." Security and Communication Networks, Volume 9, Issue 18. Wiley Online Library. November 8, 2016.

Deleted data is still a concern for investigators, but in a much different light than the typical issues seen by investigators. The user does not have physical access to their data, like they would have for a flash drive or hard disk, so they are unable to physically destroy it, making it readily available for an investigator[16].

On the other side of this, investigators typically find the best evidence mingled in deleted files and unallocated space. The volatile nature of the cloud presents challenges with acquiring this data in an investigation. With Google Services, if data is deleted, not only is it removed from all servers, both active and replication, but all pointers to this data are also removed, making it near impossible to locate any remnants of the data[17]. Multi-Tenancy also provides a plethora of issues, considering CSP's are unwilling to give investigators access to memory that is shared among server tenants, as this could fall in violation of the privacy agreements.

Chain of custody is very important in any forensic investigation. Typically, it begins the second an investigator acquires the evidence and ends either when the evidence is presented to court or the case is closed out. There can be some issues with the integrity of the data, especially considering most cases involve the CSP doing the data acquisition and passing the data on to the investigator. The CSP does not always follow best practices for evidence gathering, so some evidence may not be admissible in court. An investigator usually must take additional steps to ensure that this data is viable in a court of law[18].

---

[16] Grispos, George. Storer, Tim. "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics." arXiv. Cornell University Library. 2012.
[17] Grispos, George. Storer, Tim. "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics." arXiv. Cornell University Library. 2012.
[18] Stephen O'shaughnessy, Anthony Keane. Impact of Cloud Computing on Digital Forensic Investigations. Gilbert Peterson; Sujeet Shenoi. 9th International Conference on Digital Forensics (DF), Jan 2013, Orlando, FL, United States. Springer, IFIP Advances in Information and Communication Technology, AICT-410, pp.291-303, 2013, Advances in Digital Forensics IX. <10.1007/978-3-642-41148- 9_20>.

As stated in sections 1 and 2, jurisdiction issues and privacy rights can make acquisition of cloud based data a daunting task in a public investigation. In certain instances, jurisdiction can delay, or even stop a case in its tracks. Prior to the Cloud Act of 2018, which requires US based providers to adhere to the SCA whether the data is local to the US or not, there were legal issues regarding data stored offshore, where law enforcement agents would have to cooperate with foreign governments to acquire the data[19].

For private investigations, this process is usually much simpler. As many companies take precautions before moving software, services and infrastructure to the cloud, they will not only control the root account, (usually) providing much visibility into the usage, but there is also usually some sort of internet-based data logging system, whether native to the CSP or third party. This will provide the company with logs and information on how the accounts and services are being used so they can easily detect abnormal behavior and narrow it to an account, and even as granular as a date, time, and IP address of access[20]. The only downside to these tools, is that if they are not preemptively configured, or do not capture the correct data, they are essentially useless in an investigation.

Examples of native tools that can be used for the above are Google's Message Log search, and Amazon Web Service's CloudTrail/CloudWatch functionality [21]. Third-party

---

[19] Keane Woods, Andrew, and Peter Swire. "The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems." Lawfare. March 22, 2018. Accessed December 02, 2018. https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

[20] South, Scott, and Adam Krumbien. "The Future of Data Acquisition: Will the Internet's Cloud-Computing Replace the Data Logger?" Thomas Insights - U.S. Manufacturing and Industrial News. August 10, 2010. https://news.thomasnet.com/companystory/the-future-of-data-acquisition-will-the-internet-s-cloud-computing-replace-the-data-logger-581751.

[21] Grispos, George. Storer, Tim. "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics." arXiv. Cornell University Library. 2012.

providers also present users with various tools and functionality they can integrate into their cloud environments. These include companies such as Splunk and DataDog.

Hashing is another very important feature in any investigation. Typically, law enforcement may have to rely on third-party tools to create and provide hashes for their data to ensure it has not been tampered with. One native tool, offered through Amazon Web Services, allows MD5 hashing for resources stored in the Simple Storage Service (S3) buckets. When enabled, this allows investigators to verify the resources in these buckets[22].

Encryption can also pose many challenges for investigators. Companies such as Amazon Web Services allow customers to provide their own key to encrypt their resources. If a resource is encrypted with a customer key and the customer deletes this key, it is near impossible to unencrypt the data, as these companies pride themselves in the strength of their encryption algorithms when it comes to securing data[23].

Date stamps can prove to be unreliable in an investigation involving cloud data. The CSP and customer may exist in separate time zones, which could lead to mismatched and inconsistent timestamps on data[24].

A new service that is beginning to appear within the models is Forensics-as-a-Service (FaaS). In most service models, the CSP is in a position where they would be the ones

---

[22] Grispos, George. Storer, Tim. "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics." arXiv. Cornell University Library. 2012.
[23] Simou, Stavros. "A Survey on Cloud Forensics Challenges and Solutions." Security and Communication Networks, Volume 9, Issue 18. Wiley Online Library. November 8, 2016.
[24] Stephen O'shaughnessy, Anthony Keane. Impact of Cloud Computing on Digital Forensic Investigations. Gilbert Peterson; Sujeet Shenoi. 9th International Conference on Digital Forensics (DF), Jan 2013, Orlando, FL, United States. Springer, IFIP Advances in Information and Communication Technology, AICT-410, pp.291-303, 2013, Advances in Digital Forensics IX. <10.1007/978-3-642-41148- 9_20>.

responsible for the forensic acquisition and hand-off of data[25]. Assuming the CSP could provide court-quality investigations, FaaS would be able to aid in both public and private investigations.

Section 4: Reporting and Predictions

This section reports on the status of digital forensics in the cloud as it exists today, as well as how effective current methodologies are. Some predictions and hypotheses for the future are also outlined in this section, based on the current status and previous trends with cloud computing and usage.

As of current, there exists no toolkit for cloud forensics. This often forces investigators to repurpose existing forensic toolkits for these investigations, which may leave gaps in investigations where existing tools do not offer the complete functionality that is needed for the environment that is being worked on[26]. Due to the nature of cloud forensics, it is often much more expensive to perform an investigation on cloud data than traditional data[27]. Resources such as En-Case and FTK tools can be used, but the user may find themselves relying on other resources to verify[28].

Based on the previous fact, and as more and more users become fluent in utilizing the cloud, there will be a burning need for tools designed specifically for cloud forensics. As

[25] Stephen O'shaughnessy, Anthony Keane. Impact of Cloud Computing on Digital Forensic Investigations. Gilbert Peterson; Sujeet Shenoi. 9th International Conference on Digital Forensics (DF), Jan 2013, Orlando, FL, United States. Springer, IFIP Advances in Information and Communication Technology, AICT-410, pp.291-303, 2013, Advances in Digital Forensics IX. <10.1007/978-3-642-41148- 9_20>.

[26] Stephen O'shaughnessy, Anthony Keane. Impact of Cloud Computing on Digital Forensic Investigations. Gilbert Peterson; Sujeet Shenoi. 9th International Conference on Digital Forensics (DF), Jan 2013, Orlando, FL, United States. Springer, IFIP Advances in Information and Communication Technology, AICT-410, pp.291-303, 2013, Advances in Digital Forensics IX. <10.1007/978-3-642-41148- 9_20>.

[27] Abbas, Zain. Asif, Muhammad. Burney, Aqil. "Forensic Issues in Cloud Computing." Journal of Computer and Communications, 63-69. Scientific Research Publishing. 2016.

[28] Simou, Stavros. "A Survey on Cloud Forensics Challenges and Solutions." Security and Communication Networks, Volume 9, Issue 18. Wiley Online Library. November 8, 2016.

software companies realize this and intend to capitalize on this hole, toolkits of varying costs and functionality will be released to consumers for use on their cloud environments.

As stated in Section 3, FaaS is starting to emerge as a popular methodology, especially when it comes to cloud investigations. With the increasing popularity of cloud services, CSP's will likely offer FaaS services to consumers to prevent them from hiring third party companies to acquire the data, and relieves investigators of tedious administrative tasks. It can be hypothesized that this field will boom once malicious users try to take advantage of the unclear guidelines and restrictions that are currently in place for cloud computing[29].

The field of cloud forensics is still barren of strong resources and services for proper acquisition, and it can be hypothesized that in the near future, with the upsurge of legal cases and companies working in the cloud, many new companies and tools will form to fill this gap and provide high-quality forensic services to individuals and companies who wish to utilize the vast functionality of cloud computing.

Conclusion

In this research paper, various aspects of cloud forensics were discussed. An introduction to cloud, cloud-computing, and cloud terminology was provided to ensure that the reader had a sufficient background before diving into the more advanced topics of cloud forensics. A history of the cloud was then addressed, as well as details on laws and acts relevant to cloud computing and cloud forensics.

[29] Van Baar, R.B. Van Beek, H.M.A. Van Eijk, E.J. "Digital Forensics as a Service: A game changer." Digital Investigation. Elsevier. May, 2014.

Later discussed is when cloud data is relevant and when in an investigation one can typically expect the introduction of cloud data. Also mentioned are a few legal cases with cloud components and important acts were derived from these cases.

In the section regarding capture and analysis, information as well as common issues regarding both these topics are discussed here. Tools, both cloud-native and third-party are mentioned with each topic to provide a deeper insight into how one can implement the various methodologies and controls mentioned.

Finally, for reporting and predictions, a brief summary of current processes of digital forensics in cloud environments on cloud resources is given. Predictions and hypotheses based on the previous sections, as well as the data reported in the reporting section are also presented in this section, especially in regards to the future of cloud forensics, and where it will be within the next few years, as well as standards and practices that may be emerging.

Bibliography

"Stored Communications Act, Codified at 18 U.S.C. §§ 2701–2712." The Reporter's Privilege Compendium: An Introduction | Reporters Committee for Freedom of the Press. May 08, 2017. Accessed December 03, 2018. https://www.rcfp.org/electronic-communications-surveillance/iii-electronic-communications-surveillance-authorities/elec-0.

Abbas, Zain. Asif, Muhammad. Burney, Aqil. "Forensic Issues in Cloud Computing." Journal of Computer and Communications, 63-69. Scientific Research Publishing. 2016.

Amazon Web Services. "What Is Cloud Computing? - Amazon Web Services." *Amazon*, Amazon, aws.amazon.com/what-is-cloud-computing/.

Amazon Web Services. "Shared Responsibility Model - Amazon Web Services (AWS)." *Amazon*, Amazon, aws.amazon.com/compliance/shared-responsibility-model/.

Buller, Daniel. Wittow, Mark. "Cloud Computing: Emerging Legal Issues for Access to Data Anywhere, Anytime." Journal of Internet Law, Volume 15, Number 1. Aspen Publishers. July, 2010.

DePalo, Maki. "Cloud Computing - Legal Issues in the U.S. & International Implication." Law Library Student-Authored Works. Law Library. 2011

Destefani Neto, Maximilliano. "A brief history of cloud computing." IBM, 2014, https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/.

Flynn, Meagan. "Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over." The Washington Post. November 14, 2018. Accessed December 2, 2018. https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/?noredirect=on&utm_term=.bb592a23783f.

Grispos, George. Storer, Tim. "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics." arXiv. Cornell University Library. 2012.

Keane Woods, Andrew, and Peter Swire. "The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems." Lawfare. March 22, 2018. Accessed December 02, 2018. https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

O'shaughnessy, Stephen. Keane, Anthony. Impact of Cloud Computing on Digital Forensic Investigations. Gilbert Peterson; Sujeet Shenoi. 9th International Conference on Digital Forensics (DF), Jan 2013, Orlando, FL, United States. Springer, IFIP Advances in Information and Communication Technology, AICT-410, pp.291-303, 2013, Advances in Digital Forensics IX. <10.1007/978-3-642-41148- 9_20>.

Park, Chi. "The History of Cloud Computing: Some Key Moments." *Inspirage*, Inspirage, 2 2 Aug. 2018,www.inspirage.com/2015/11/the-history-of-cloud-computing-some-key-moments/.

Simou, Stavros. "A Survey on Cloud Forensics Challenges and Solutions." Security and

Communication Networks, Volume 9, Issue 18. Wiley Online Library. November 8, 2016.
South, Scott. Krumbien, Adam. "The Future of Data Acquisition: Will the Internet's Cloud-Computing Replace the Data Logger?" Thomas Insights - U.S. Manufacturing and Industrial News. August 10, 2010. Accessed December 03, 2018. https://news.thomasnet.com/companystory/the-future-of-data-acquisition-will-the-internet-s-cloud-computing-replace-the-data-logger-581751.
Van Baar, R.B. Van Beek, H.M.A. Van Eijk, E.J. "Digital Forensics as a Service: A game changer." Digital Investigation. Elsevier. May, 2014.
Watts, Stephen. "SaaS vs PaaS vs IaaS: What's The Difference and How To Choose." *BMC Blogs*, 2017, www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/.
Wilson, David. "Legal Issues of Cloud Forensics." Expert Reference Series of White Papers. Global Knowledge. 2014.
"U.S. Const., amend. IV."