Group 4

Professor Micheal D’Angelo

CIS 4093

May 15th 2023

**Emerging Cloud Computing/Cloud Forensic Challenges**

As technology has evolved over the years, we have been introduced to concepts like cloud computing and digital forensics. These two play a major part in any field, any career and especially in evolving the way we examine investigations. We will be discussing what cloud computing and digital forensics are, how they came to be and much more in detail about their effects.

Cloud computing was invented by Joseph Carl Robnett Licklider in the 1960s, and his purpose was to connect people and data from around the world. Licklider developed APRANet and helped work on Project MAC (Project on Mathematician and Computation) - goal was to allow users to program a single computer from various locations. Within 6 months of Project Mac being launched, 200 users were able to access their systems in 10 different MIT locations. This method of virtual computing started being used in the 90’s and businesses started developing their own cloud service that they offered to consumers.

* AWS was launched in 2006
* Google cloud was launched in 2008
* Microsoft Azure was launched in 2010.

Cloud Computing allows you to access multiple computer resources, data storage, development tools and more. It is managed by the cloud service providers which is then delivered over the internet. Cloud computing is divided into three categories which are Infrastructure as a Service (IaaS), Platform as a service (PaaS), Software as a service (SaaS).

Cloud Computing works by allowing clients access to cloud applications over the internet. The companies that provide Cloud services are AWS, Microsoft Azure, Apple, IBM, Google, and Oracle. There are many advantages of Cloud computing which include the following: It can be cheap since you don’t have to use/pay for more hardware to store your data, cloud Services can be reliable since your data is stored on multiple servers instead of one. Meaning that if a Hardware failure happens then a consumer's data is not at harm, your data can be backed up and restored on Cloud, cloud can also offer more storage if needed.

Although there may be many advantages of cloud computing, it also comes with its many flaws. These include the following users have limited access, meaning that their data is owned, managed, and monitored by the service provider, cloud is depended on internet connection. Without a good internet connection it is hard to access data stored on the Cloud.

Digital forensics is a very new field which means it does not have a defined beginning, middle and end compared to cloud computing. However, since it is new, there are always advancements that need to be made to increase its accuracy, reliability, and mobility.

When it comes to being a forensic investigator, it is crucial to have a system that can handle large amounts of data, in other words where they can be stored. Thanks to cloud computing, forensic investigators can store more data on cloud storage, and they can store more than a terabyte. If they were to store that amount of data on physical storages then it would be costly, especially investing in CPU and RAM. It can be accessed anywhere as long as they have a good internet connection.

As the internet grows there are more cyber crimes committed in this day and age. To investigate these matters, data has to be recovered within a computer. But what if that data is stored on cloud storages? Cloud forensics would be appropriate in this field. It involves collecting, analyzing, and preserving data from cloud based systems. But the problem is that the Cloud service provider has control over the data needed for investigation, making it difficult for forensic investigators. Plus cloud services encrypt their data which is another obstacle for them. ([Linkedin Cloud Forensic](https://www.linkedin.com/pulse/cloud-forensics-understanding-investigation-process-jayadev-paleri?trk=pulse-article_more-articles_related-content-card#:~:text=Data%20fragmentation%3A%20Data%20in%20the,access%20and%20analyze%20the%20data).)

The latest technology that developers and cloud service providers like AWS and Microsoft are interested in is quantum computing. Quantum computers use the principles of quantum physics to speed up the processing of big data sets and difficult algorithmic tasks. Network security can be improved by using a supercomputer, which can offer strong encryption capabilities for electronic communications. Quantum computing in the cloud has the ability to revolutionize industries, similar to different rising technology which includes AI and machine learning.

In response to the expansion of 5G, Internet of Things (IoT) devices, and latency-sensitive applications, cloud providers are pushing closer to the edge. Although edge computing is not a new concept in the computer world, it is more commonly used by businesses. Edge computing allows systems to bedecentralized and brings processing and data closer to users. This method reduces latency, lowers bandwidth costs, and improves connectivity.

With the digital transformation of businesses, security is moving to the cloud. By consolidating with SASE, enterprises can reduce costs and complexity, provide centralized orchestration and real-time application optimization and help secure seamless access for users. It can also enable more secure remote and mobile access by restricting access based on user, device, and application identity, improve security by applying consistent policy and increase network and security staff effectiveness with centralized management.

The vast infrastructure, power, and cooling requirements related to cloud computing greatly impact an organization's environmental impact. Data centers are responsible for 2% of all electricity use in the US, according to the US Department of Energy. The typical energy consumption per floor of a commercial office building is 10 to 50 times lower than that of a data center. The effectiveness of hardware and software is something that cloud providers are constantly striving to improve. Long-term energy savings from even modest adjustments and enhancements can be significant. A major problem is e-waste, which is produced in large quantities annually by outdated hardware. This is driving the demand for improved computer hardware recycling.

In the Cloud Forensic Process Flow, four steps must be completed before performing digital forensics. These steps include, identification, collection & preservation, examination & analysis, and presentation.

**Identification:** The first step in computer forensics is case identification. This includes two important steps: Identification of evidence and incidents that help prove that the events described in the case study actually occurred.

**Collection & Preservation:** The second step is to collect evidence from digital sources such as cell phones, emails, hard drives, and other digital media, and protect this evidence so that it can be processed later without tampering with it.

**Examination & Analysis:** In the final phase, digital cues are analyzed and evaluated by the device used in the previous phase. Collecting and reviewing relevant data is the starting point of any investigation. Second, researchers tend to make sense of the data and decide if the evidence is sufficient to reach conclusions.

**Presentation:** Finally, the investigator will prepare a report based on the findings and ensure that the report contains sufficient evidence to be admissible in court.

While researching cloud forensics, it was discovered there have been many challenges as well as solutions regarding the cloud computing process. These include, maintaining logs, having a separate plan for retrieval, and legislative solutions.

Log maintenance is a big challenge in cloud computing. Several models have been proposed for log management in cloud computing. One option is to record in detail every action taken on an instance and use specially designed transport logs to upload those records to a central cloud-based log repository.

Anotherbig challenge is data collection. It is possible that the difficulty of data collection in Cloud Forensics could be alleviated by creating a separate plane that would be used to manage the data server required by researchers. Reliable organizations must maintain this cloud infrastructure layer.

The solution to the problems caused by the lack of cloud law is to create a specific service level agreement (SLA) between customers and cloud service providers (CSP). A SLA should clearly describe the legal requirements to be followed during a criminal investigation.

**Cloud Forensics**

Cloud computing is having a significant impact on digital forensics as it becomes more widely adopted for both business and personal use. In the following paragraphs I will outline some of the major pros and cons of cloud computing as it relates to digital forensics. This is also called cloud forensics.

One of the pros is the potential to gather data in real time. So even though you may not have access to a suspect’s machine, you can still monitor their activity if they are interacting with cloud services. This has major implications as it allows a suspect to be investigated without their knowledge. Another one of the pros is scalability for things such as storage and computing power. Forensic investigations typically deal with large amounts of data. If that is the case, it is easier than ever to increase computing power and storage via the cloud to accommodate your needs. This will allow for faster and more efficient processing of data. Lastly, cloud computing allows for investigators to easily access forensic tools and create virtual environments from a remote location. If investigators have the need to create virtual machines to mimic certain environments as a part of their investigation, this is now easier than ever with cloud computing as an option.

One of the cons of cloud computing as it relates to digital forensics is the issue of preservation. In traditional digital forensics the focus is to isolate suspect computers from the internet and then preserve any data on them. While you can still preserve a suspect’s machine in a cloud forensic investigation, you may not be able to store important data that is stored remotely.

Another major roadblock when it comes to cloud forensics is investigators also have to rely on cloud companies to acquire and preserve data in a manner that fits the standards and regulations of digital forensics. In addition to this, they will need to rely on cloud companies for things like documentation and chain of custody, which are vital for ensuring evidence will be admissible in court. If the chain of custody is not properly documented, evidence can be thrown out in court as a result. Adding an extra party in the chain of custody leaves more room for error, especially when that party is not familiar with the standards for digital forensics.

We’ve already discussed IaaS, PaaS, and SaaS, but it is also relevant when it comes to cloud forensics. In the SaaS model, where a client doesn’t have any control over the software infrastructure they use, an investigator will have to completely rely on the cloud service provider to obtain evidence such as system logs. PaaS also proves difficult for an investigator because the client really only has control over the applications they use, making acquiring relevant data very difficult for investigators. IaaS provides the most potential for an investigator as the client is responsible for the software infrastructure and can more easily track user activity. Regardless of the type of cloud service a client employs, obtaining the necessary data in cloud forensics is much more challenging for an investigator than it is in traditional digital forensics.

Lastly, data in the cloud is dispersed by nature, making it difficult to locate and extract in general. Data can be spread out across multiple servers and drives, and it can be hard for an investigator to know where to look. Because each cloud system is different, an investigator will have to learn where and how to extract data from each time, decreasing the chances of maintaining the integrity of the data.

While cloud computing has provided both advantages and disadvantages for digital forensics, it seems as if the disadvantages outweigh the advantages. The advantages it provides are more along the lines of quality of life, making digital forensics more convenient at times. However, the disadvantages have the potential to completely railroad an investigation depending on the cloud services that are being employed by the client.

* AWS and its services
* Microsoft Azure and its services
* GCP and its services

Amazon offers a cloud computing platform called AWS, or Amazon Web Services. It provides a variety of services, including database administration, networking, storage, and computation. AWS offers a number of prominent services, including:

* **Simple Storage Service (Amazon S3):**
* Multiple versions of an object can be stored in the same bucket thanks to S3's versioning features. Versioning makes it possible to trace and audit any modifications made to an item, which is helpful in forensic investigations.
* Server access logging: All requests made to an S3 bucket are recorded using the server access logging feature offered by S3. This contains information about the request, such as the date and time, the requester's IP address, and the request parameters. In forensic investigations, server access logging can be used to monitor who accessed an object and when.
* Object-level logging: Object-level logging offered by S3 keeps thorough access logs for each object in a bucket. This includes information about the date and time of the access as well as the user agent and IP address of the requester. Forensic investigations can make advantage of object-level logging to determine when and by whom a particular item was accessed.
* Server-side encryption: Server-side encryption for data at rest is offered by S3. The confidentiality of sensitive data may be maintained in forensic investigations due to this, which helps ensure that data is protected from unauthorized access.
* Object tagging: S3 provides object tagging capabilities that allow you to add custom metadata to an object. Object tagging can be used to add additional information to an object that can be useful in forensic investigations, such as the reason for the object's creation or its relevance to a particular investigation.
* Amazon CloudTrail
* Log file integrity validation: Digital signatures for each log file are produced by CloudTrail using the SHA-256 hash methods. This can be helpful in forensic investigations to protect the integrity and validity of the log data and helps to confirm that log files have not been altered or tampered with.
* Encryption: For your AWS account, CloudTrail records all management activities, such as deploying instances, changing security groups, or removing things. This might be helpful in forensic investigations to determine who and when executed a specific action.
* Logging of management events: CloudTrail logs all management events for your AWS account, including actions such as creating or modifying security groups, launching instances, and deleting objects. This can be useful in forensic investigations to track who performed a particular action and when.
* Multi-region support: In order to record API events from many AWS regions into a single S3 bucket, CloudTrail provides multi-region logging. To make sure that all pertinent log data is gathered in one location, this might be helpful in forensic investigations.
* Event notification: When particular events in your account happen, CloudTrail can send event notifications to AWS Lambda or Amazon Simple Notification Service (SNS). Automating log data processing and generating alerts when specific events take place might be helpful in forensic investigations.
* Amazon GuardDuty:
* CloudTrail integration: For your account, GuardDuty works with CloudTrail to record API events. GuardDuty is able to identify and notify users when suspicious API calls occur, such as those that originate from unexpected locations or use unusual parameters.
* Network traffic analysis: In order to identify potential threats, such as port scanning, attempts to exploit known vulnerabilities, and communication with known malicious IP addresses, GuardDuty monitors network traffic to and from your AWS resources.
* Threat intelligence: GuardDuty leverages threat intelligence feeds to find compromised accounts and endpoints as well as known malicious IP addresses and domains.
* Cross-account support: In order to monitor several AWS accounts for potential risks from a single account, GuardDuty provides cross-account analysis.
* Security findings: With regard to potential vulnerabilities found in your AWS environment, GuardDuty generates security findings. Security findings contain thorough information regarding the threat, such as the resource that was impacted, the threat type, and repair suggestions.

Microsoft Azure is another cloud computing platform that provides a range of services for building, deploying, and managing applications and services through Microsoft-managed data centers. It offers a wide range of services for computing, storage, networking, and database management, among others. Some of the popular services provided by Microsoft Azure are:

**Virtual Machines (VMs):** Users are able to run apps on virtual machines and it offers scalable cloud computing capability.

**Blob Storage:** Users can store and access unstructured data with this scalable object storage service from any location on the internet.

**SQL Database:** It is a managed database service that makes relational databases like SQL Server and PostgreSQL easy to set up, scale, and maintain.

**Azure Functions:** It is a serverless compute service that autonomously controls the underlying processing resources while running your code in response to events.

**Content Delivery Network (CDN):** It is a globally dispersed network that offers fast data transfer rates and minimal latency for both static and dynamic content.

**Azure Kubernetes Service (AKS):** It is a Kubernetes service that is fully managed and streamlines the deployment, administration, and scaling of containerized applications.

**Azure Active Directory (Azure AD):** It enables users to manage user access and permissions and offers safe access management for Azure resources.

**Azure DevOps:** This service offers models for controlling and deploying infrastructure as code.

**Azure Stream Analytics:** Users can evaluate and process streaming data from numerous sources with this real-time data stream processing service.

GCP (Google Cloud Platform) is a suite of cloud computing services provided by Google, offering a wide range of services and tools for building, deploying, and managing applications and infrastructure in the cloud. GCP offers a variety of services in different categories, including:

**Compute:** Developers can execute applications and workloads in the cloud using a variety of computing services provided by GCP, such as Virtual Machines, Kubernetes Engine, App Engine, and Cloud Functions.

**Storage and Databases:** Users can store, manage, and analyze their data in the cloud using the various storage and database choices offered by GCP, including Cloud Storage, Cloud SQL, Cloud Spanner, Cloud Bigtable, and Cloud Datastore.

**Networking:** GCP provides a range of networking services that assist businesses in connecting, scaling, and securing their network infrastructure, including Virtual Private Cloud (VPC), Cloud Load Balancing, Cloud DNS, Cloud CDN, and Cloud Interconnect.

**Big Data:** BigQuery, Cloud Dataflow, and Cloud Dataproc are just a few of the big data technologies offered by GCP that let customers process and analyze enormous amounts of data.

**Artificial Intelligence and Machine Learning:** A number of machine learning services, including AI Platform, AutoML, and Vision API, are offered by GCP. These services enable businesses to create intelligent applications and gain insights from their data.

**Security:** The security services offered by GCP, such as Cloud IAM, Cloud Security Scanner, and Cloud Armor, assist businesses in defending their infrastructure and data from potential threats.

**Management Tools:** GCP offers a suite of management tools, including Stackdriver, Cloud Deployment Manager, and Cloud Console, to assist businesses in managing their cloud resources and keeping an eye on their infrastructure and apps.

These are just a few of the many services offered by the top cloud platforms. AWS, Microsoft Azure, and GCP provide highly scalable and reliable platforms for businesses to run their applications and services, and they have become the go-to platform for cloud computing in recent years. These top three companies make up about 66% of the cloud user market share.

There are multiple methods of protecting the cloud which include using cloud services that encrypt, reading user agreements when purchasing apps, using unique passwords and updating them frequently, not sharing personal information, not storing sensitive information, and using a strong malware program. Other methods include using a limited amount of public Wifi but when it is used, install a VPN app, regularly updating your system, and using two-factor authentication.[[1]](#footnote-0)

Some services available for the protection of Cloud include the following:

* Data Encryption
* Firewall Detection
* Monitoring
* Isolated Networks
* Anomaly Detection [[2]](#footnote-1)

In recent years, there have been many attacks regarding cloud computing which include the following:

**FlexBooker Data Breach:**

A digital scheduling website had 3.7 million users suffer a data breach where names, email addresses, phone numbers, and even password hashes and credit card information were stolen. This happened because a secured security measure was not installed. A solution could be to implement better protocols, an improved system and use multiple forms of data verification systems.

**The Biggest Data Leak in the History of China:**

1 billion Chinese citizens had their data stolen from a database located in Shanghai. The hackers had tried to extort $200000 from the department holding names, phone numbers, government ID numbers and police reports as their leverage. This attack occurred because the department had a secure database but not a secure network. The database was accessible using an open internet that made it possible for hackers to enter into the system. Since the issue was a network issue, a solution could be to use a private internet source that requires a password and two-step verification from the department.

After extensive research, we were able to find some case studies regarding digital forensics which are the following:

**The BTK Killer**

In the early 2000’s, a man named Dennis Rades was finally caught for the murder of more than 10 people. He was never caught and was let loose to remain free for almost 30 years until he started repetitively irritating the Police Department. He would send the officers messages speaking about his crimes which caused the department to investigate his messages thoroughly. Because of his messages, he “sent the police a Microsoft Word document on a floppy disk. Digital forensics experts were able to trace the metadata contained within the disk, helping unveil the BTK Killer’s true identity. Rader was finally arrested and imprisoned shortly after this.”

**The CraigsList Killer**

CraigsList is a website like eBay, where customers can buy or sell items. In 2009, in Boston, Massachusetts, a woman was found dead in her hotel room. In that same city, another woman reported she was assaulted and robbed while being held at gunpoint. Both of those women had both bought from a man under the name of Andy on CraigsList who was actually connected to the crime in a way no one could imagine. Digital forensics experts went through the women’s emails to investigate exchanges between Andy. They discovered IP addresses that traced back to a 23 year old man named Philip Markoff, who was a medical student. Through the use of technology, digital forensics played a huge part in uncovering the culprit behind the crime.

All in all, digital forensics and cloud computing are both ever changing fields that need constant improvement over the years. As technology has grown and improved, crime has increased and become more complex which is why digital forensics must be stronger than ever.

*All research and information was paraphrased from the following links.*

Works Cited

*What Is AWS CloudTrail? - AWS CloudTrail*, docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html. Accessed 15 May 2023.

*Concepts and Terminology - Amazon Guardduty*, docs.aws.amazon.com/guardduty/latest/ug/guardduty\_concepts.html. Accessed 15 May 2023.

*What Is Amazon S3? - Amazon Simple Storage Service*, docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html. Accessed 16 May 2023.

Simonesavi. “Computer Forensics Chain of Custody in Azure - Azure Example Scenarios.” *Azure Example Scenarios | Microsoft Learn*, learn.microsoft.com/en-us/azure/architecture/example-scenario/forensics/. Accessed 15 May 2023.

“How to Use Live Forensics to Analyze a Cyberattack | Google Cloud Blog.” *Google*, cloud.google.com/blog/products/identity-security/how-to-use-live-forensics-to-analyze-a-cyberattack. Accessed 15 May 2023.

*A Comprehensive Review of Cloud Forensics and Blockchain Based ...*, www.researchgate.net/publication/367194110\_A\_Comprehensive\_Review\_of\_Cloud\_Forensics\_and\_Blockchain\_Based\_Solutions. Accessed 16 May 2023.

“Advantages of Cloud Computing - javatpoint.” *Javatpoint*, https://www.javatpoint.com/advantages-and-disadvantages-of-cloud-computing. Accessed 15 May 2023.

Carter, Anthony. “Where is Cloud Data Physically Located?” *VIRTUS Data Centres*, 24 April 2019, https://virtusdatacentres.com/item/381-where-is-cloud-data-physically-located. Accessed 15 May 2023.

Chai, Wesley. “What is Cloud Computing? Everything You Need to Know.” *TechTarget*, https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing. Accessed 15 May 2023.

Delvadiya, Devang. “Impact of Cloud Computing on Digital Forensic.” *Tutorialspoint*, 14 March 2023, https://www.tutorialspoint.com/impact-of-cloud-computing-on-digital-forensic. Accessed 15 May 2023.

Lawton, George. “The future of quantum computing in the cloud.” *TechTarget*, 17 April 2020, https://www.techtarget.com/searchcloudcomputing/tip/The-future-of-quantum-computing-in-the-cloud. Accessed 15 May 2023.

O'Shaughnessy, Stephen & Keane, Anthony. (2013). “Impact of Cloud Computing on Digital Forensic Investigations.” IFIP Advances in Information and Communication Technology. 410. 291-303. 10.1007/978-3-642-41148-9\_20.

Ot, Anina. “Top 16 Cloud Computing Companies & Service Providers 2023.” *Datamation*, 22 February 2023, https://www.datamation.com/cloud/cloud-service-providers/. Accessed 15 May 2023.

Pedamkar, Priya. “History of Cloud Computing | Brief Overview of Cloud Computing.” *eduCBA*, https://www.educba.com/history-of-cloud-computing/. Accessed 15 May 2023.

Perry, Yifat. “The Future of Cloud Computing: 5 Trends You Must Know About.” *NetApp BlueXP*, 24 June 2022, https://bluexp.netapp.com/blog/cvo-blg-the-future-of-cloud-computing-5-trends-you-must-know-about. Accessed 15 May 2023.

Pyfer, James, and William L. Hosch. “Project MAC | computer science | Britannica.” *Encyclopedia Britannica*, https://www.britannica.com/topic/Project-Mac. Accessed 15 May 2023.

Richter, Felix. “Infographic: Big Three Dominate the Global Cloud Market.” *Statista*, 28 April 2023, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/. Accessed 15 May 2023.

“3 Famous Cases Solved Through Digital Forensics.” *Eclipse Forensics*, 1 July 2021, https://eclipseforensics.com/3-famous-cases-solved-through-digital-forensics/. Accessed 15 May 2023.

“What is cloud computing?” *IBM*, https://www.ibm.com/topics/cloud-computing. Accessed 15 May 2023.

“What Is Cloud Computing?” *Microsoft Azure*, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing. Accessed 15 May 2023.

“What Is SASE - Secure Access Service Edge?” *Cisco*, https://www.cisco.com/c/en/us/products/security/what-is-sase-secure-access-service-edge.html#~sase-overview. Accessed 15 May 2023.

Zhang, Mary. “Top 10 Cloud Service Providers Globally in 2023.” *Dgtl Infra*, https://dgtlinfra.com/top-10-cloud-service-providers-2022/. Accessed 15 May 2023.

1. https://us.norton.com/blog/how-to/secure-your-info-in-the-cloud# [↑](#footnote-ref-0)
2. https://www.educba.com/cloud-security-services/?source=leftnav [↑](#footnote-ref-1)