BOOK CHAPTER | "Chasing Shadows"

Cloud Computing Forensic Challenges for Law Enforcement

Samuel Opuni Boateng
Information Technology & Law Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mails: Samuel.boateng@st.gimpa.edu.gh
Phone: +233242977837

ABSTRACT

Cloud computing is a relatively new concept that offers the potential to deliver scalable elastic services to many. The notion of pay-per use is attractive and in the current global recession hit economy it offers an economic solution to an organizations' IT needs. Computer forensics is a relatively new discipline born out of the increasing use of computing and digital storage devices in criminal acts (both traditional and hi-tech). In the last decade computer forensics has developed in terms of procedures, practices and tool support to serve the law enforcement community. However, it now faces possibly its greatest challenges in dealing with cloud computing. Through this paper we explore these challenges and suggest some possible solutions.

Keywords: Forensic, Cybercrime, law Enforcement, Digital Universe, Cyberspace, Security

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Samuel Opuni Boateng (2022): Cloud Computing Forensic Challenges for Law Enforcement Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 339-344
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P54

1. INTRODUCTION

Cloud computing has transformed the methods by which digital data is stored, processed, and transmitted. One of the most daunting new challenges is how to perform digital forensics in various types of cloud computing environments. The challenges associated with conducting forensics in different cloud deployment models, which may cross geographic or legal boundaries, have become an issue. Discussing cloud computing forensics, is actually talking about the intersection between cloud computing and network forensic analysis. Cloud computing basically refers to a network service that we can interact with over the network; this usually means that all the work is done by a server somewhere on the Internet, which might be backed up by physical or virtual hardware. In recent years, there has been a significant increase on the use of virtualized environments, which makes it very probable that cloud service is running somewhere in a virtualized environment. There are many benefits of virtualized servers, but the most prominent ones are definitely low cost, ease of use, and the ability to move them around in seconds without service downtime.

A good example of cloud computing is an email service where we don't have to install an email client on our local computer to access our new email and which serves as storage for all email. Instead, everything is already done by the cloud, the email messages are stored on the cloud and, even if we switch to a different computer, we only need to login with our web browser and everything is there. Therefore, we only need an interface with which we can access our cloud application, which in the previous example is simply a web browser.

1.1 Background to the Study

Cloud computing forensics is a subset of digital forensics based on the unique approach to investigating cloud environments. An organisation may have servers around the world to host customer data. However, when a cyber-incident happens, legal jurisdiction and the laws that govern the region present unique challenges. The numerous challenges for the various stakeholders who share an interest in forensic analysis of cloud computing environments can be broadly categorized into technical, legal, and organizational challenges.

These challenges occur when identification and acquisition tasks become impeded or when examination and interpretation by a digital forensic examiner is prevented. Compared to the challenges of traditional digital forensics, those of cloud forensics are considered to either be unique to the cloud environment or exacerbated by the cloud environment. While the goals of first responders and forensic examiners may be the same in the cloud context as in traditional, large-scale computer and network forensics, distinctive features of cloud computing such as segregation of duties among cloud Actors, inability to acquire system and network logs, multi-tenancy, and rapid elasticity—introduce unique scenarios to digital investigations.

On the other hand, challenges associated with, for example, virtualization, large-scale data processing, and the proliferation of mobile devices and other endpoints are exacerbated in the cloud. Cloud forensic challenges cannot be solved by technological, legal, or organizational principles alone. Many of the challenges need solutions from all three areas, and scholars and practitioners have been discussing these challenges.

2. RELATED LITERATURE

According to International Journal of Engineering Research & Technology (IJERT), Forensic frameworks for traditional forensics methods such as static forensics and live forensic can help trace the issue relatively easily especially where data centres are within physical reach. ((IJERT), 29-09-2020).

- A cloud model poses unique challenges like the ones listed below –
- Storage System is no longer local and can violate the jurisdiction laws.
- Each cloud server contains files from many tenants
- Even if data belonging to a particular suspect is identified, separating it from other tenant data is difficult.
- Reconstruction of deleted Data.
- Other than the cloud service provider, there is usually no evidence that links a given data file to a particular suspect.to digital forensics as information is difficult to locate, acquisition is challenging if it cannot be located, and there can be no analysis without acquisition.

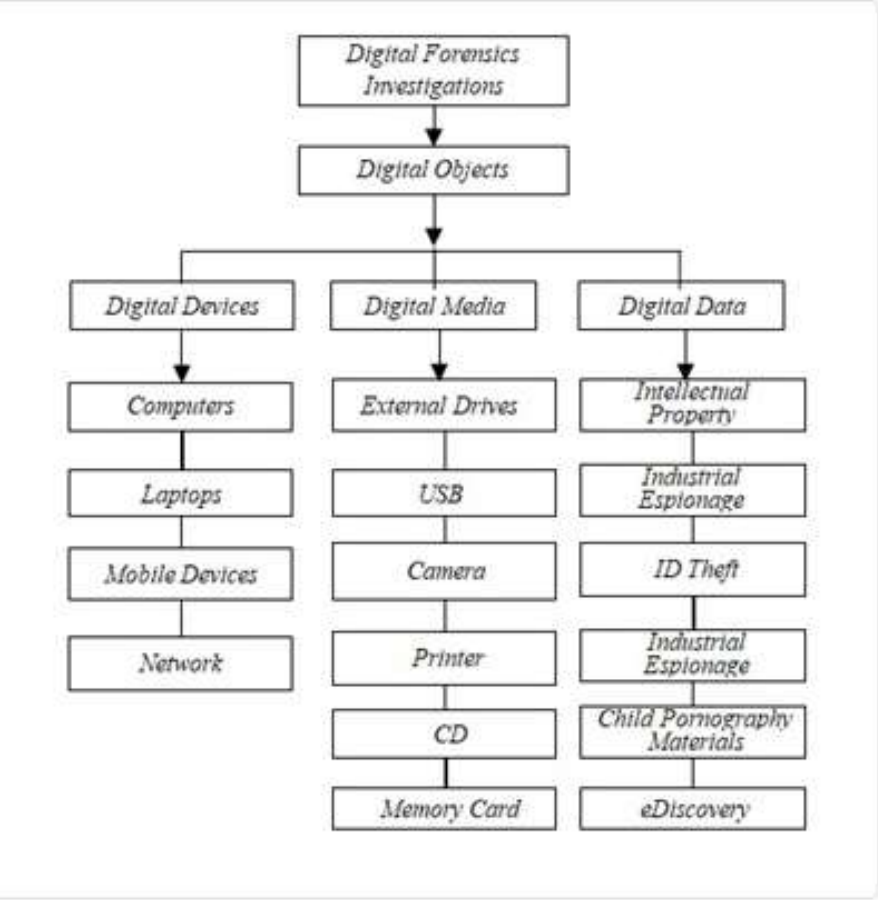

Fig 1: Digital Objects In Digital Forensic Investigations

Source: https://www.heraldopenaccess.us/openaccess/digital-forensics-investigation-jurisprudence-issues-of-admissibility-of-digital-evidence

According to IJERT, there are three sources from which evidence can be extracted in a cloud, i.e., the client side, the network layer and the cloud service provider (CSP) of the three sources the most difficult to gather evidence from is the cloud service provider side. What makes it difficult on the cloud provider side is that the provider is usually outside the jurisdiction of the investigators. International laws and international collaborations have to be taken into consideration, which may be costly and time consuming.

In order to analyze the domain of Cloud Forensics more comprehensively, it is necessary to understand that it is not only a technical issue, but a multi-dimensional one which involves Organizational as well as Legal aspects. While the Technical Dimension consists of tools and frameworks that are required to perform forensic investigations in Cloud Computing

environment, Organizational dimension comes into picture when multiple parties are involved where Cloud Service Provider must communicate with third-parties for their expertise in the Investigation.

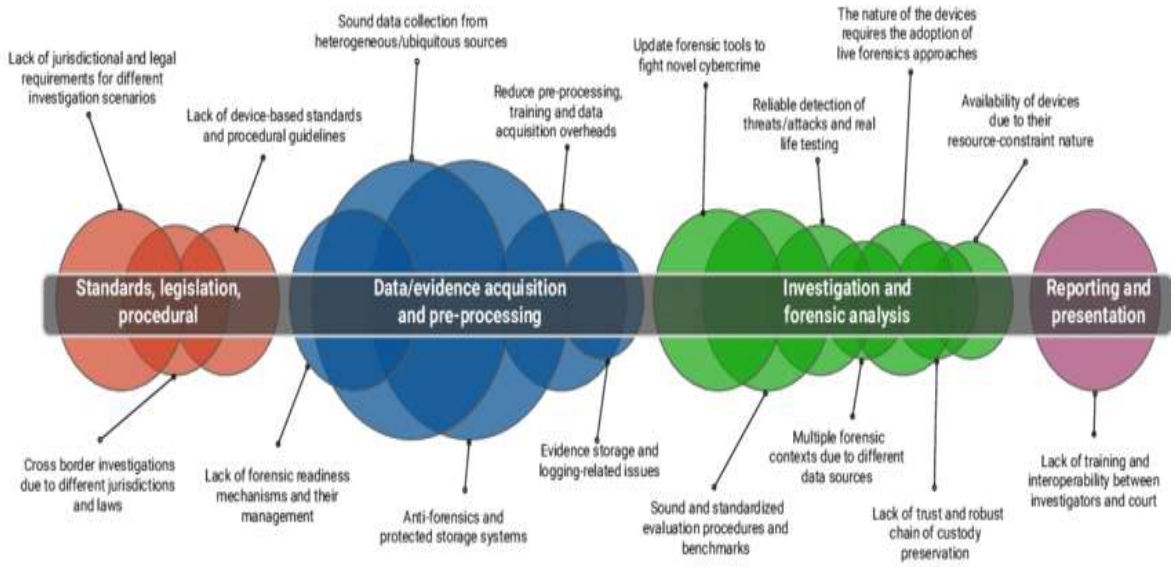

Fig 2: Main digital forensic challenges mapped into different categories
Source: https://www.researchgate.net/figure/Main-digital-forensic-challenges-mapped-into-different-categories-according-to-their_fig3_353818893

Another aspect which is a Legal Dimension requires development of regulations and agreement to ensure that the forensic activities do not breach laws and regulations in the jurisdictions where the data resides. The confidentiality of other clients using the same infrastructure should also not be compromised. The existing tools and framework are limited in terms of their ability to resolve cybercrime related issues mainly due to the distributed and elastic characteristics of cloud computing as the existing tools cannot cope with cloud environment. Tools and procedures are yet to be developed for investigations in virtualized environments especially on the hypervisor level.

According to IEEE Conference Publication below are the deployment models of cloud computing:

- Private cloud—The services of a private cloud are used only by a single organization and are not exposed to the public. A private cloud is hosted inside the organization and is behind a firewall, so the organization has full control of who has access to the cloud infrastructure. The virtual machines are then still assigned to a limited number of users.
- Public cloud—The services of a public cloud are exposed to the public and can be used by anyone. Usually the cloud provider offers a virtualized server with an assigned IP address to the customer. An example of a public cloud is Amazon Web Services (AWS).
- Community cloud—The services of a community cloud are used by several organizations to lower the costs, as compared to a private cloud.

- Hybrid cloud—The services of a hybrid cloud can be distributed in multiple cloud types. An example of such a deployment is when sensitive information is kept in private cloud services by an internal application. That application is then connected to the application on a public cloud to extend the application functionality.
- Distributed cloud—The services of a distributed cloud are distributed among several machines at different locations but connected to the same network.
  The service models of cloud computing are the following
- laaS (infrastructure as a service) provides the entire infrastructure, including physical/virtual machines, firewalls, load balancers, hypervisors, etc. When using laaS, we're basically outsourcing a complete traditional IT environment where we're renting a complete computer infrastructure that can be used as a service over the Internet.
- PaaS (platform as a service) provides a platform such as operating system, database, web server, etc. We're renting a platform or an operating system from the cloud provider.
- SaaS (software as a service) provides access to the service, but you don't have to manage it because it's done by the service provider. When using SaaS, we're basically renting the right to use an application over the Internet.

3. RESEARCH GAPS/FINDINGS

The role of forensic network intelligence in the digital age has received commendable attention in criminal investigation versus the collection of physical evidence. From a forensic point of view, the increasing number of access to cloud computing without it's corresponding security controls poses risk to the organisation. The cloud computing Storage System is no longer local and can violate the jurisdiction laws, each cloud server contains files from many tenants, even if data belonging to a particular suspect is identified, separating it from other tenant data is difficult, Reconstruction of deleted Data and Other than the cloud service provider, there is usually no evidence that links a given data file to a particular suspect.to digital forensics as information is difficult to locate, acquisition is challenging if it cannot be located, and there can be no analysis without acquisition.

4. CONCLUSION

This study highlights many of the forensic challenges in the cloud computing environment for digital forensic examiners, cloud Providers, law enforcement, and others. The information in this document was developed as a result of examining research papers. It provides a definition of cloud computing forensics to scope this area. The document also discusses how the challenges correlate to cloud technology. The categories of challenges include architecture, data collection, analysis, anti-forensics, incident first responders, role management, legal issues, standards, and training. Finally, the results of overcoming each challenge are provided.

5. RECOMMENDATION FOR POLICY AND PRACTICES

To aid in this quest, digital forensics standards and frameworks for digital forensics technologies are required now more than ever in our networked environment. This was also echoed in a more recent literature survey which also identified a number of cloud forensic research and operational challenges, such as the need for a forensic-by-design framework that allows integration of forensic tools into the development of cloud physical system to mitigate risks and enable forensic capabilities.

6. DIRECTION FOR FUTURE

It is also worth to note that, more research is required in the cyber domain, especially in cloud computing, to identify and categorize the unique aspects of where and how digital evidence can be found. End points such as mobile devices add complexity to this domain. Trace evidence can be found on servers, switches, routers, cell phones, etc. Digital evidence can be found at the expansive scenes of the crime which includes numerous computers as well as peripheral devices.

REFERENCE

1. International Journal of Engineering Research & Technology (IJERT)- Cloud Forensics: Trends and Challenges – IJERT
2. Burnette, M.W., 2002. Forensic Examination of a RIM (BlackBerry) Wireless Device June, 2002. URL https//www. rh-law. com/ediscovery/Blackberry. pdf.
3. Schwartz, E., 2010. Network packet forensics. In CyberForensics (pp. 85-101). Humana Press, Totowa, NJ.
4. D. Reilly; C Wren; T. Berry Cloud Computing: Pros and Cons for Computer Forensic Investigations,
   Published 1 March 2011
5. Cloud computing: Forensic challenges for law enforcement | IEEE Conference Publication | IEEE Xplore
6. The three service models of Cloud Computing | OPEN https://www.openintl.com/the-three-service-models-of-cloud- computing/
7. Forensics Plan | Computer Forensics | Digital Forensics https://www.scribd.com/document/144828523/Forensics-Plan
8. Cloud Forensics: What is it And Why is it so important https://www.techstagram.com/2013/03/20/cloud-forensics- importance/ [Online]. Available: https://cloud.google.com/customers/ bnp-paribas-fortis/.
9. Digital Forensics Environment for Cloud https://www.scribd.com/document/168145892/Sibiya-2012