BOOK CHAPTER | Basking in the Clouds

Integration of Cloud in Mobile Forensics

Michael Acquah Stuff
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: storph@hotmail.com

ABSTRACT

With emerging technology and the connection of electronic devices to the internet, Internet of Things (IoT) has become part of human life. From the development of smartphones to smartwatches and smart-homes, electronic devices now have the capability of performing human activities or aiding humans in performing activities such as turning hall lights on or off with their voice. Although a large number of people use these devices for the greater good, a few individuals or group of people hide behind these devices to perform malicious activities. In order to apprehend and prosecute perpetuators who hide behind smart devices for evil gains, forensic examinations or investigations must be conducted. This review aims to identify digital forensic challenges in IoT. The inclusion criteria for this paper were international journals, articles, conference papers and case studies published from 2019 to 2022. Thematic analysis was used to analyze and synthesis the literature. Three themes emerged from the analysis; automated compromised smart-home tracer; data volatility and reconstruction; IoT forensic investigation framework. This integrative review combines evidence of digital forensic challenges in diverse IoT devices.

Keyword IoT forensics, IoT challenges, Digital forensics, Smart-home forensics.

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

Citation: Michael Acquah Stuff (2022): Integration of Cloud in Mobile Forensics
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 125-130
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P21

1. INTRODUCTION

Cloud computing provides great business opportunities for organizations and IT services providers by introducing scalable infrastructure resources in both hardware and software to push real-time services and minimize the cost of on-demand computing (Ruan, Carthy, Kechadi, & Crosbie, 2011). As much as clouds promote diverse organizations' operations the security and trustworthiness, vulnerability of the integration of the cloud in mobile infrastructure has becomearising concern (Aziz & Fouad, 2017). Clouds can be a target for unauthorized users or as a channel to launch attacks on social networking platforms such as Twitter, LinkedIn, Facebook and WhatsApp helping people to socialize and interact, share information, upload photos and files.

Attacks can also be launched against the cloud when users engage in real-time conversations. Due to the increased usage of smartphones, the use of social networking applications is now common among individuals and organizations. Smartphone users constantly store their personal details including location information, e-mail history, and other confidential documents on their smartphones (Ana - Ramona, 2010). Social networks also promote the interest in users to upload their bio-data involving gender, age, etc. Such a wealth of personal details on social network media facilitates cybercriminals to commit crimes. According to Zareen & Baig (2010), the unknown and diverse nature of social networking sites make smartphones extremely vulnerable to cybercrime. Mobile devices are considered a useful source of forensic evidence that is admissible in the court of law. However, the constant changes in mobile devices mandate the investigators to adopt proper techniques and methods to examine diverse mobile devices.

The source of operating system (OS) in a smartphone can help to develop custom tools for local/traditional digital forensics(Taylor et al, 2010) The social site is mostly hosted on cloud platforms to support scalable solutions. Recent researches focus on forensically analyzing the cloud-based mobile applications and collecting the evidence from the corresponding service provider to identify the suspect(Alobaidli, Nasir, Guimaraes, & Martin, 2017). Mostly, the existing mobile cloud forensic approach supports the forensic investigation of social networking applications. However, effectively tracking down the cloud artifacts based on mobile evidence with reference to social activities is still a difficult task. Therefore, the need to considerably improve the evidence-gathering ability and the accuracy of evidence in the cloud environment in order to be considered forensically sound in the court of law.

1.1 Background to the Study

The Cloud system is made up of the interconnection of various servers that contain files from many users all over the world(Sharma, Arora, & Sakthivel, 2020). In our modern world where privacy is very essential, it is extremely difficult if not impossible to seize servers from a data center without invading on the privacy of the individuals (Zawoad & Hasan, 2013). This results in complicating the cloud forensics.

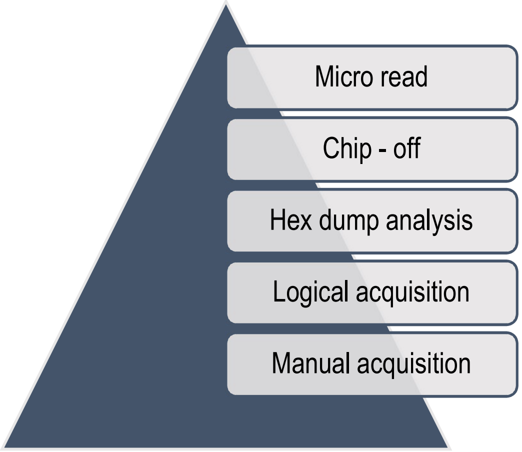

Figure 1 : Levels of Analysis
Source: (Zareen & Baig, 2010)

Some challenges associated with the integration of the cloud to mobile forensics comparatively is that, the old computer forensics analyst has full access and control over the computer which is considered as the evidence. However, in the cloud, access and control over various data sources varies in different software models(Zareen & Baig, 2010). Again cloud computing is a multifaceted system whereas the traditional is a singular(Aziz & Fouad, 2017).

2. RELATED LITERATURE

Digital mobile cloud forensics is the process of detecting and deducing electronic data (Zawoad & Hasan, 2013). The aim of this is to protect available proof in its novel form while undertaking a well systematic enquiry through the identification of the issue, collection of data and authentication of the electronic/digital data with the objective of reconstructing past events(Alobaidli et al., 2017). The context of this is not limited to the law court though it is most used evidentially there. Mobile devices plays a very important role in the life of todays' man and as such plays a major role in investigations (Grispos, Glisson, & Storer, 2013).

The importance of cloud forensics is the ability to reproduce what a user was doing with a mobile device in a period which led to a particular event(Zareen & Baig, 2010). With the modern application software on mobile devices, it is inevitable that individuals do not have any records on such devices(Ruan et al., 2011). There are enormous challenges faced by the mobile cloud forensics that have not been adequately addressed yet by scholars to find the necessary solutions for such challenges. Acquisition of data in the cloud system remains the most dominant with other different difficulties (Alobaidli et al., 2017).

Fig 2: Cloud and Mobile Forensic
Source: https://blog.elcomsoft.com/2019/12/challenges-in-computer-and-mobile-forensics-what-to-expect-in-2020/

3. RESEARCH GAPS

Security password and encryption

The security of data on mobile devices has been the major focus of many manufacturers in the past decade and still remains a priority as issues of privacy and confidentiality has gathered the necessary momentum in most countries. Schemes are been developed by manufactures that practically make it difficult if not impossible for the enforcement agencies to access the data(Aziz & Fouad, 2017).

Operating systems for mobile devices

The ever fast changing operating system of mobile devices is very challenging to the forensics industries. As a result of the variety in most of the operating systems currently available, a lot of feature devices use unique, branded operating systems that are not well known to forensics expect. This is mainly in the cases of terrorism and money laundering (Taylor et al, 2010)

Accidental reset

The integrity of any mobile device data is highly dependent on its handler. If the device is not handled well, it will result in a very devastating effects.

Lack of tools and equipment

With the increase in the numbers of mobile devices, there should to varying tools and equipment's to assist in the cloud mobile forensics (Dillon, Wu, & Chang, 2010) There cannot be single tool that would be efficient for all mobile devices hence having varying tools will assist in the forensics industry during investigations.

Anti-forensic techniques

As stated earlier, privacy and confidentiality is paramount to every household. It is for this reason that some application developers go beyond in their quest to frustrate law enforcement agencies. Techniques against forensics attempt to circumvent cloud mobile forensics investigations (Dykstra et al, 2011)

4. CONCLUSION

Cloud mobile forensics is an emerging force and still remains a gray area for most of the forensic investigators. It is evident that there are several challenges in integrating the cloud to mobile forensics but if the is done and adequate measures are put in place to mitigate fraudsters attempts in frustrating investigations, cloud mobile forensics would assist in eliminating a number of crimes if not eradicating it.

5. CLOUD FORENSICS IMPLICATIONS ON AFRICA

The implication of cloud forensics are enormous, it will bridge the gaps in security in the sub region which is faced with several terrorism threats. Africa would soon have the same voice when it comes to issues related to cloud forensics and its use in evidence in any case. The fallouts should be cross-examined, tested several times to aid in the development of policies and standards that would safeguard Africa and all users of Cloud in its sub region.

A common financial scheme should be espoused and all African countries should contribute to have a wide pool of resources to support the research, policies and practice of the cloud forensics initiatives. As Africa Initiate sound policies, ethics and models under which Cloud services should operate in their region, it will bring a level of systems and structures of cloud forensics in Africa as a whole.

6. RECOMMENDATIONS FOR POLICY AND PRACTICES

The industry needs standardization in order to be a step of criminals. It is necessary to adopt a consolidated standard. There should be guidelines and standards to analyze and interpret digital evidence. Cloud computing security should be observed when designing and establishing metrics and access levels across multiple CSPs and clients.

7. FUTURE WORK DIRECTION

The challenges faced with cloud forensics are enormous and have not been adequately addressed (Meyer & Stander, 2015). It is prudent that measures are put in place to know a standard way to acquire data in a cloud system. Research is encouraged to develop appropriate procedures and measures that would be useful to service providers to extract the needed data by forensic investigators.

The need for a legislation to retrieve necessary evidence in a timely manner across the borders of a third party. There should be a gatekeeping system that restricts unauthorized persons access to certain data. Though we do not see a universal legislation to be adopted globally, given the differences in legislations in various countries, it is prudent that it would be considered sub regionally.

Frequent workshops should be organized by expect in the field including law enforcement agencies and the cloud parties to address the challenging issues and find necessary solutions that be generally accepted.

REFERENCES

1. Alobaidli, H., Nasir, Q., Guimaraes, M., & Martin, S. (2017). Challenges of Cloud Log Forensics.
2. Ana - Ramona, R. (2010). Big Data and Specific Analysis Methods for Insurance Fraud Detection, 30–39.
3. Aziz, A. S. A., & Fouad, M. M. (2017). Cloud Computing Forensic Analysis : Trends and Challenges (pp. 3–23). https://doi.org/10.1007/978-3-319-44270-9
4. Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing : Issues and Challenges, 27–33. https://doi.org/10.1109/AINA.2010.187
5. Dykstra, J., Sherman, A. T., Dykstra, J., & Sherman, A. T. (2011). Understanding Issues in Cloud Forensics : Two Hypothetical Case Studies UNDERSTANDING ISSUES IN CLOUD FORENSICS : TWO HYPOTHETICAL CASE STUDIES, (c).
6. Grispos, G., Glisson, W. B., & Storer, T. (2013). Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services. https://doi.org/10.1109/HICSS.2013.592
7. Meyer, G., & Stander, A. (2015). Cloud Computing : The Digital Forensics Challenge, 285–299.
8. Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Chapter 3 CLOUD FORENSICS, 35–46.
9. Sharma, P., Arora, D., & Sakthivel, T. (2020). ScienceDirect ScienceDirect ScienceDirect Enhanced Forensic Process for Improving Mobile Cloud Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications Traceability in Cloud-Based Mobile Applications. *Procedia Computer Science*, *167*(2019), 907–917. https://doi.org/10.1016/j.procs.2020.03.390
10. Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review*, *26*(3), 304–308. https://doi.org/10.1016/j.clsr.2010.03.002
11. Zareen, A., & Baig, S. (2010). Challenges , Analysis and Tools Classification, (May), 47–55. https://doi.org/10.1109/SADFE.2010.24
12. Zawoad, S., & Hasan, R. (2013). Digital Forensics in the Cloud, (October).