International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 7– No.10, October 2014 – www.ijais.org

An Overview of Cloud Base Application Forensics Tools for Mobile Devices

Muhammad Faheem
Abdul Wali Khan University
University College Dublin

Tahar Kechadi, PhD
University College Dublin
Ireland

Nhien An Le Khac, PhD
University College Dublin
Ireland

ABSTRACT
With the increased use of mobile devices, the respective data is stored and maintained over the remote clouds. In case of any data crimes at the cloud, the existing forensic tools are not capable of data recovery and thus lot of research was being proposed at this level. A detailed review of the existing forensic tools used for the digital and mobile analysis will be reviewed and the respective literature gaps with respective to cloud forensic will be evaluated. Literature gaps with respective current digital and mobile forensics tools against required data acquisition, investigation, preservation, examination and analysis are identified. With the increased usage of mobile apps like Facebook, Google plus and Viber, data of the users is stored across the remote clouds. The main challenge for the mobile forensics tools in this context is that to acquire the remotely located data of mobile locations. Based on the research gaps identified the actual methodology of the research is proposed, where a new approach will be proposed against the mobile forensics which can integrate with the existing tools, that can acquire and analyse the remote data storage from the clouds.

Keywords
Cloud forensics, Mobile cloud forensic applications, and Cloud forensics tools

1. RESEARCH BACKGROUND
With the increased demand of mobile applications, even cloud service providers are expanding their business area towards the respective applications. Global connectivity with the Smartphone has opened the doors for remote storage of data across the clouds similar to any of the regular cloud data storage options which include both the public and private clouds [1]. As per the reports of Cisco, the data traffic received from the mobile is around 597 petabytes per month in 2011, which is almost eight times more when compared to the year 2000 and this value may touch ten Exabyte's per month by 2016 [2]. With the increasing data traffic from millions of Smartphone and tablets, the data is being migrated to cloud storage since few years.

Billions of files are saved across the clouds using the respective services from various users and organizations which belong to different business areas like retail, healthcare, IT and finance [3]. It is observed over few years that cloud computing is aggressively integrating with the business operations against improving growth, scope and optimizing the risk of infrastructure and resource maintenance as well [4]. Thus cloud computing and the respective storage options have become a part of Smartphone and other mobile devices like with the advantages with mobile devices and respective cloud storage, there are potential threats like intruder attacks and theft of mobile data stored over remote clouds [5].

Traditional mobile forensics are limited to a particular device, memory SD cards or SIM and now the scope of respective forensic tools should be extended, where the cloud service providers need to investigated as well [6]. Thus investigating the cloud service providers have gained lot of research importance and opened lot of research challenges and issues as well. As the data of the mobile devices is stored over a remote location, investigating and applying the traditional forensics tools is a tedious task [7]. Still there are chances to get the remotely located cloud data against mobile forensics investigation, thus the actual problem statement identified is discussed as below.

2. PROBLEM STATEMENT
The data which placed at remote locations is needful whenever required whether for investigation purpose or for a person who leads crime for his own purpose .Cloud computing and the respective services are widely used across different applications which includes web applications and mobile applications as well [8]. In general a cloud service can be defined as the application, data, resource or infrastructure maintained or offered by third party service providers against the actual needs of individual person or business organizations [9]. Data of a user or an organization is managed and maintained over a remote location across the cloud storage models and the respective security architecture and policies are imposed to ensure the data integrity, reachability and reliability. Thus securing the cloud services is a tedious job and many security models were discussed over literature with respect to mitigation policies as well [10].

Mobile devices have completely replaced the usage of traditional desktops or laptops to access the respective cloud services, where with a required internet connection any sort of public or private cloud resources or data can be accessible with respective to the authentication procedures[11]. Mobile forensics is an evaluating research subject area, where many tools and techniques were proposed in this context. Mobile forensics is a specific type of typical computer or digital forensics, where the source of evidence will be the mobile device, SIM card or memory SD card [12]. There are many existing mobile forensics tools proposed over literature and from the primary analysis, it is observed that mobiles accessing the cloud services are becoming the source of evidences for mobile forensics since few years.

Data stored across the remote clouds is being accessed at the mobiles or data from the mobile is being accessed with the respective cloud services, which leads to security vulnerabilities. Thus mobile forensics with respective cloud

services has gained ample importance these days by the researchers and good amount of research was proposed in this subject area [13]. From the primary analysis of the research against the cloud based mobile forensics, it is clear that there are some identifiable gaps over the literature across the aspects like data acquisition, examination and analysis and the traditional mobile forensic tools may not be suitable at all the configuration levels of cloud based mobile forensics [14]. Thus an integrated model is required in this context to enhance the respective forensics analysis process, which can result in better mobile data acquisition, examination and analysis.

Data extraction from the remote clouds is the main challenge with mobile forensic tools and in general this extraction process will include both physical and logical data. Low level data extraction is followed at physical level and higher level data extraction is done using the communication protocols at the logical data. Both the approaches have equal advantages and disadvantages. Disadvantages with these data extraction process include encryption/decryption complexity, data synchronization and time issues. Oxygen Software Company introduced an improved logical data extraction in 2004, where special applications are installed which can access the mobile OS API's , temporary files, cached files and deleted data. Later this tool have raised lots of doubts and forensic compliance with respect to the access of mobile OS files and encrypted files. Thus still there is scope of designing a prototype of mobile forensic tool and acquiring the required source of evidence from remote clouds [13].

Thus the main aim of the current research is to propose a mobile forensic analysis model that can properly integrated with the existing tools and acquire, examine and analyse the data stored over the local mobile devices or across the remote cloud services like Amazon, Google or Facebook data. Mobile apps are being uploaded or downloaded from the third party service providers aggressively with the level of mobile OS support and thus the mobile forensic analysis with respective to the cloud services plays a crucial role. Proposed cloud based forensic analysis can follow the typical phases of forensic analysis like remote cloud data acquisition, examination and analysis using the lightweight operating system components and database components of the respective mobiles itself and thus reducing the complexity of the entire forensics analysis as well.

3. LITERATURE REVIEW

As per the literature survey analysis, investigation of remote cloud data is a complex task against forensics analysis when compared to normal or regular data. The term cloud forensics can be defined as a special subject area which combines both the traditional digital or computer forensics and mobile forensics. Investigating the remote cloud data is complex in nature, as the data is accessed virtually and gaining physical access to the respective data is a tedious job and thus gained lot of importance over researchers. Traditional digital and mobile forensic tools are inefficient and ineffective over cloud forensics and thus a new model or methodology of forensics analysis and investigation is required in this context [15].

There are many challenges across the cloud forensics analysis and investigation and the key among are to create the required forensic images over recovery process of the remote mobile cloud data. If the existing tools are capable of recovering the respective data, they can be used for the cloud based mobile forensics and due to lack of the required capabilities and they are not applied [16]. One and only benefit with the mobile cloud data forensic investigation is that, the required source of evidence or data is located at a centralized location and thus the forensic analysis can run quickly. The potential limitation with this approach is that even the irrelevant data of organizational individual is also considered for the forensic analysis across the respective physical locations [17].

The increased use of Smartphone make them gold mine for investigation purpose. And through conducting experiments it results that data can be recovered for forensic detection. As day by day crime is increasing whether it is on social networking or it can be any forge case through which robbery can be held. The different OS phones required different test procedure as software differs. Iphone, iOS, blackberry etc. have different configuration but each can recovers there back data. If any accident occurs then easily the crime is traced and the data can be read. The recovered data can be helpful for the crime spot [21.

Even there are chances to lose the required forensic evident data at the remote clouds when the users clears the sessions and thus recovery is the complex task identified over applying the cloud based mobile forensic analysis. Thus to meet the respective challenges researchers are striving a lot to propose sophisticated techniques to recover the forensic evidence data stored remotely over the mobile clouds service providers [18]. When the case with few existing forensic tools like FTK (Forensic Tool Kit) and Encase is considered against the mobile cloud forensic analysis, it is proved that they are capable to acquire the required evidence data from specific types of clouds like Infrastructure-as-a-service (IaaS) and the respective instances [19].

Still there is ample gap against applying the existing forensic tools over different types of cloud services. Legal issues surrounding the cloud service providers' policies are also a potential barrier to the respective forensic evidence recovery or investigation and thus proved to a potential problem again [20]. All the existing issues as discussed are multiplied when the number of mobile devices accessing the same cloud increases and it is the common case observed over many scenarios. There are some mobile forensic tools that can be used to recover or investigate the remote cloud data; still the scope is limited to only the interactions of the respective mobile devices with the cloud data.

4. AIMS, OBJECTIVE, RESEARCH QUESTION

4.1 Aims:

To analyse and evaluate various mobile forensic tools used to investigate and examine the remote data stored over the clouds and propose a new mobile forensic framework that can integrate with the existing tools and used for better forensic analysis and examination.

4.2 Objectives:

Research objectives are as listed below

a) To review the existing mobile forensic tools and discuss various forensic analysis cases with respective to evidences from mobile devices.

b) To evaluate the mobile data storage across clouds and review various cloud storage models.

c) To review different mobile applications like Facebook, Google Maps, Google Plus, Twitter and the methods of storing the data over remote clouds.

d) To review various mobile cloud data service providers and the typical storage architecture followed at the more servers.

e) To review various existing remote data acquisition, prevention, examining and analysing tools against implementing the mobile forensic tools.

f) To review various mobile forensic cases against remote cloud storage area and compare the techniques proposed at this level.

g) To analyse the typical mobile forensics tools and study their implementation over the remote cloud data storage

h) To propose a mobile forensic framework that can consider the remote cloud storage as the required forensic evidence for the further investigation process and compare the physical data vs. logical data acquisition processes, which can be integrated with the existing mobile forensic tools for better forensic evidence acquisition and examination.

4.3 Research Questions

Below are the research questions

a) How can the existing mobile forensic tools be used to investigate the cloud data storage as the respective evidence?

b) To what extended the meta-data services of the remote cloud data can be used across the mobile forensic investigation?

c) How the does the mobile data stored over the remote clouds and what architecture is used to save the data?

d) What type of mobile applications data is stored or retrieved from the remote clouds data storage and how it is important against mobile forensics tools analysis and examination?

e) What are the key features of the Smartphone's that are helpful in recovering the remote cloud data?

f) What level of mobile user activities like file upload or download can be used across the cloud based mobile forensic tools for respective analysis process?

5. RESEARCH METHODOLGOY

Quantitative research methodology can be applied for the current research as it needs experimental analysis. Proposed research with the required experiments can be done at six different stages and they are as listed below

a) Literature analysis will be done to analyse the existing mobile forensics tools, their features and limitations

b) A detailed study on impact of the cloud storage over the mobile applications and the respective cloud storage

c) Detailed analysis of various mobile applications like Viber, LinkedIn, senspace.com, 4shared.com, Picasa, Google drive and Google plus and the respective cloud storage mechanism will be done to understand the storage requirements and mechanisms

d) Study few mobile forensics case studies with respective remote cloud data misuse or theft and analyse the role of existing mobile forensic tools over data recovery and investigation

Based on the analysis of existing mobile forensic tools over remote cloud data acquisition and investigation, a new framework will be proposed by considering and integrating the architecture of existing mobile forensics tools like FTK Image and Encase. Proposed architecture will be explained by comparing with the existing mobile forensic tools and framework will be proposed that can integrated and isolated with the existing mobile forensic tools.

5. CONCLUSION

Aim of the current research is to investigate and propose mobile cloud data forensic tool. From the literature study it is clear that, there are many digital and mobile forensic tools and they are not suited for recovery and investigation of the cloud data of mobile devices and thus a new approach is required in this context. In general data of the mobile applications like Facebook, Viber, Google plus, Google drive, 4shared.com and other file sharing database applications is stored over the remote cloud storage. Ensuring data security of the individual mobile users has significant importance against success any application. Thus in case of any data lost or corrupted, mobile forensic tools should be able to acquire, examine, investigate and recover the data. There are some existing tools with respective to the requirement and still suffer from many limitations.

This paper presents a very high level overview of what is involved in future research papers the actual research methodology and the proposed mobile forensic tool architecture attributes used over the proposed research is discussed and based on the results from the experiments, the actual methodology of forensic recovery and analysis of mobile cloud data storage will be analysed.

6. REFERENCES

[1] Vidalis, S., 2009. Cloud Computing: The Impact on Digital Forensic Investigations. International Conference for Internet Technology and Secured Transactions, 3(1), pp.16–23.

[2] Crosbie, M., 2011. Cloud Forensics. Advances in Digital Forensics VII, 12(3), pp.35–46.

[3] Hegarty, R., 2010. Digital Evidence in Cloud Computing Systems. Computer Law & Security Review, 26(3), pp.12–18.

[4] Vidalis, S., 2010. Cloud Computing Storms. International Journal of Intelligent Computing Research, 1(1), pp.63–72.

[5] Glisson,T. 2012. Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics. International Journal of Digital Crime and Forensics, 4(2), pp.28–48.

[6] Reilly, D., 2010. Cloud Computing: Forensic Challenges for Law Enforcement. International Conference for Internet Technology and Secured Transactions (ICITST), 13(2), pp.1 1–17.

[7] Dykstra, J., 2012. Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques. Digital Forensic Research Workshop (DFRWS), 43(12), pp.12–19.

[8] Delport, W., 2011. Isolating a Cloud Instance for a Digital Forensic Investigation. Information Security for South Africa, 4(2), pp.16–23.

[9] Glisson, T., 2011. A Comparison of Forensic Evidence Recovery Techniques for a Windows Mobile Smart Phone. Digital Investigation, 8(1), pp.23–36

[10] Mayall, G., 2011. Electronic Retention: What Does Your Mobile Phone Reveal About You? International Journal of Information Security, 10(6), pp.37–49.

[11] Johnson, D., 2011. Third Party Application Forensics on Apple Mobile Devices. System Sciences (HICSS), 2011 44th Hawaii International Conference on, 14(5), pp.11–12.

[12] Hoog, A., 2012. Iphone and Ios Forensics - Investigation, Analysis and Mobile Security for Apple Iphone, Ipad and Ios Devices. Syngress, 1(1), pp.10–12.

[13] Richard, B., 2010. Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? The Journal of Digital Forensics Security and Law, 5(3), pp.13–29.

[14] Breeuwsma, M., 2013. Forensic Imaging of Embedded Systems using JTAG (boundary-scan). Digital Investigation, 3(1), pp.32–42

[15] Mislan, R., 2009. Hashing Techniques for Mobile Device Forensics. Small Scale Digital Device Forensics Journal, 12(2), pp.19–24.

[16] Dankar, S., 2009. Hashing Techniques for Mobile Device Forensics. Small Scale Digital Device Forensics Journal, 32(12), pp.18–24

[17] Mellars, B., 2004. Forensic Examination of Mobile devices. Digital Investigation, 1(4), pp.66–72.

[18] Reiber,L. 2008. SIMs and Salsa, MFI Forum, Mobile Forensics, 13(2), pp.15-20

[19] Willassen, S., 2005. Forensic Analysis of Mobile Phone Internal Memory. IFIP WG 11.9 International Conference on Digital Forensics, National Centre for Forensic Science, Orlando, Florida, February 13-16, 2005, in Advances in Digital Forensics, 194(14), pp.19–23.

[20] Distefano, A.2008. An Overall Assessment of Mobile Internal Acquisition Tool. Digital Investigation, 5(1), pp.12–27.

[21] Mutawa, N. L., Baggili, I. and Marrington, A. (2012) 'Forensic analysis of social networking applications on mobile devices', Digital investigation, 9, pp. 524-533