ISSN (Online): 2455-7838
SJIF Impact Factor : 6.093

EPRA International Journal of

# Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed
International Online Journal

Volume: 4, Issue:3, March 2019

Published By
EPRA Publishing

SJIF Impact Factor: 6.093 Volume: 4 | Issue: 3 | March | 2019 ISSN: 2455-7838(Online)

EPRA International Journal of Research and Development (IJRD)

Peer Reviewed Journal

# FORENSIC CHALLENGES: A REVIEW ON FORENSIC CHALLENGES IN MOBILE, NETWORK AND WEB CLOUD COMPUTING

**Chandra Kala J N**

*III BCA, MOP Vaishnav College for Women, Chennai, Tamil Nadu, India*

**Savitha N**

*III BCA, MOP Vaishnav College for Women, Chennai, Tamil Nadu, India*

## ABSTRACT

*Cloud computing is a emerging technology and many users and companies move towards cloud due to its many of its advantages. Though it has many advantages, it has disadvantages with respect to security and also the digital investigator faces many challenges in collecting the evidences that are involved in crime. This paper deals with the security challenges in the different types of forensics in cloud.*

**KEYWORDS**: *Cloud computing, digital investigator, mobile forensics, network forensics, web browser*

## INTRODUCTION

Cloud Computing is an emerging technique with the help of cloud we will be able to manage, store and process data easily using internet. Nowadays, everyone makes use of cloud. However, it has more advantages there are some disadvantages also. Cloud computing is now becoming a battlefield for cyber crimes. This paper deals with the many security challenges in the different types of forensics in cloud. We will see about cloud forensic challenges and types of forensics. The following are the types of forensics mobile forensics, network forensics, web browser forensics, data forensics, enterprise forensics and email forensics.

An little introduction about a cloud forensics challenges**, Mobile forensics** is the technique used by digital investigators for identifying the evidences from mobile devices which are suitable for presenting it in court of law. **Network Forensics** is a sub branch of digital forensics for analyzing and monitoring network traffic for gathering information, intrusion detection or legal evidence. **Web browser** is a tool that helps us to access internet. With the help of a browser we will be able to gather information easily. This paper talks about these forensics and the challenges involved in them.

## LITERATURE REVIEW

Literature review has done on the concepts related to forensics challenges. Basically forensics means the examining the evidences collected for the crime. Due to unique combination of cloud computing that include, rapid elasticity, on-demand self-service, broad network access, measured service and resource pooling digital investigations face various legal, organizational and technical challenges.

**Saad Alqahtany ; Nathan Clarke ; Steven Furnell ; Christoph Reich,** identifies the challenges in the cloud forensics also, it highlights the further problems that need to be tackled. Furthermore, the paper discuss about the challenges in various stages of collecting evidences for the crime.

**Suleman khan, Ejaz Ahmad, Muhammad Shiraz, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa,** talks about the forensics challenges in mobile cloud computing. This paper provide the comprehensive understanding about the mobile forensics challenges and re-direct the investigators to new research areas.

**Pilli, Emmanuel S., Ramesh C. Joshi, and Rajdeep Niyogi,** talks about the forensics challenges in network cloud computing and the various ways in which crime can occur in cloud.

**Muhammad Tallal ,Sheraz Shahid Butt, Momina Abrar Rashid Muhammad Hamza Iqbal,** talks about the forensics challenges in web browsers and how the attack is planned in various types of web browsers.

## CLOUD FORENSICS CHALLENGES

Although the cloud computing is in market for many years, there are cloud forensics exist till now. Several researches have identified, it is not possible to make an investigation without the permission of the cloud service provider. So the cloud forensics can be categorized into following stages,[7]

### Identification:

It is the process of identifying the machine where the illegal activity has occurred and cloud activity required. Due to the cloud infrastructure there are several challenges to the investigators to undertake this step. They include[7]

- *Access to the evidence in logs:*
- *Volatile data:*
- *Lack of customer awareness*

### *Access to the evidence in logs:*

In cloud the identification of evidence is challenging ,because the investigators do not know the exact location of data since the data is distributed in multiple data centers. The availability of log files in SaaS and PaaS is not feasible due to limited access, whereas it is partly applicable in IaaS as client access the virtual machine which act as the real machine. So majority of investigators , depend on log for accessing the evidence.[8]

### *Volatile data:*

Volatile data cannot sustain when the power is turned off. Likewise, when the VM is turned off or restarted, its all the data will be lost unless it is stored in somewhere else[7]. The existing CSP,s structure does not does not provide the persistent storage. Although, the IaaS has some advantages over PaaS and SaaS, volatile storage is a problem if the data is synchronized in persistent storage. The volatile data include temporary internet files and registry entries could be lost when the IaaS customer restart the machine.[9]

### *Lack of customer awareness*

The lack of little international regulation CSP transparency along with leads to loss of important terms regarding forensics investigations in the Service level Agreement (SLA). This issue is applicable to SaaS, PaaS and IaaS.[10]

### Preservation and collection:

It is the process of data collection which act as an evidence for the crime that are considered to be a potential value. It ensures that original data preserved in a way that is accurate, verified and complete. However several issues exist for the investigators in this stage. They include,[8]

- *Data integrity*
- *Time synchronization*
- *Cloud literacy of investigators*
- *Chain of custody*

### *Data integrity:*

This is one of the main issue faced by investigators on data preservation. There is no assurance that the original data is not changed. The information related to the incident has to be listed in the chain of custody register to maintain the integrity of the evidence, including where, how and by whom the evidence was collected, how the evidence was preserved and stored along with any related details of carried out procedures. The improper preservation may lead to valueless in the court. The errors may due to the multiple actors who involved in the project.[9]

### *Time synchronization:*

Synchronization of time(stamps) is very important source of evidence. The difference in time zones between cloud cloud clients and servers cloud clients can affect the admissibility, reliability and integrity of evidence.[7]

### *Cloud literacy of investigators:*

The training material that can educate the cloud investigators about the cloud forensic procedures an cloud computing technique that are available. The current forensic training material is not updated regularly and do not address the major cloud challenges. It is highly needed to train the members of an investigation team on special tools , law regulations and techniques, including networking, communication, programming, , and negotiation with CSPs .[9]

### *Chain of custody:*

Chain of custody illustrates how the evidences collected, analyzed and preserved with the aim of presenting it the court of law. To maintain the chain of custody certain things need to be clarified, they are- how the logs have collected, stored and who access the logs. It is difficult to verify the data chain of custody in the cloud environment, because of unique combinations of characteristics that the cloud computing has, including the multi-layered and distributed nature of cloud.

### Analysis and examination:

It is very challenging for the investigators to make an analysis due to vast volume of resources and objects. Moreover, there is no standard program for the extraction of forensic data as the customers access the relevant data from various devices like PC, tablets, mobile phones etc. Furthermore, the data extraction format varies based on service model. So it is important to have a application that translate the cloud data format to readable format by tools. Due to the distributed nature of cloud, the crime may occur in different countries. So the investigators face the wide range of challenges in this stage, which include[7]

- *Lack of forensics tools:*
- *Volume of data*
- *Reconstruction*

### *Lack of forensics tools:*

The forensics tools which are available have various limitations and cannot cope up with the elastic and distributed characteristics of cloud computing. There is high level demand for forensic aware tools by the CSP to conduct forensic investigation in cloud environment. So it is crucial to develop tools which can be used to identify, collect and analyze the cloud forensic data. The combination of computer forensic and network forensics tools can be used to collect the forensics data. [9]

### *Volume of data:*

Since the volume of data is very large, it becomes difficult for the investigators to analyze the data. It also reduces the processing speed of data. Hence it takes more time to analyze the data.[8]

### *Reconstruction:*

It is crucial to reconstruct the crime scene, to understand how the crime is committed. Unfortunately, it may creates a problem in cloud environment. For example, when an intruder shut down his/her virtual instance, it is impossible to reconstruct the crime scene.[10]

### Presentation:

This is the final step of forensic investigation, where intruders present the evidences for the crime to judicial body in specified format.For instances it is difficult to specify the location of the cloud based crime since the resources are distributed among several countries, which in turn confuses the investigators to determine the legal system for the case. Furthermore, the investigators should explain the jury about how the evidences collected and what they represent. So the investigators comprehensively explain to jury about the evidences, who like to have basic technical knowledge. Here the challenge include,[9]

- ***Jury's technical comprehension***

## MOBILE FORENSICS CHALLENGES

Mobile cloud computing has became a part of everybody's life since users can access the mobile application easily anywhere at anytime and also the increasing growth in the usage of smart mobile phones . In simple, mobile cloud computing is defined as infrastructure where data processing and data storage is performed in cloud rather than smart mobile phones.[13] Being easy to access, the intruders, easily access the mobile networks to get mobile cloud users credential information. Mobile forensics is the technique used by digital investigators for identifying the evidences from mobile devices which are suitable for presenting it in court of law. However, digital investigators face many challenges in collecting evidences, such challenges include[14]

- Data identification
- Multi-tenancy
- Owner of data
- Privacy
- Smartphone OS

### Data identification:

Data identification is the process of identifying the data which act as an evidence. The investigator cannot access the data from the cloud without the permission of the CSP. They must provide the legal documents to the cloud service provider which clarifies the necessity for the investigation. It is a greatest challenge for the investigator since the data is stored in more than one data center which are placed in separate cloud. [15]

### Multi-tenancy:

Many users use a particular resources at a same time. The intruder can alter the resource at that time and it has been a challenging task for the investigator for identifying the intruder's data at the resources among the multiple users.[11]

### Owner of the data:

Service Level Agreement (SLA) is a contract between the user and cloud service provider which specifies till what date and how the cloud services and resources can be used by the clients.

It is one the challenge because it restricts the investigators to access resources due to SLA. CSP does not allow the investigator to access the resources when there is SLA between the client and the service provider. And also the resources are given to other users when the contract ends, so it becomes difficult for the investigator ijn identifying the owner of the data.[11]

### Privacy:

Data of user stored in a cloud can be viewed and accessed by CSP. Most of the companies are conscious about their data privacy and when it is accessed by the CSP it reduces the trust between the user and CSP. So CSP signs the contract with the user for data privacy. Such situation becomes challenges for the investigator to access the data when it is protected by the CSP.[12]

### Smartphone OS:

Many mobile phone companies update their OS after every few months to introduce, value added features. The investigators must be updated and should be knowledgeable about updated versions of OS. So it becomes a challenging task for the investigator in retrieving logs.[16]

## NETWORK FORENSICS

Network Forensics is a category of digital forensics which is used for monitoring the network and detecting whether any intrusions has been occurred or not. Generally network forensics has two uses. Firstly, the security which monitors a network for anomalous traffic and identifies intrusions.

Secondly, law enforcement. This includes identifying the transferred files, keyword searching, emails and chat history.

The following are the challenges in network forensics[1]:

- *Collection and detection*
- *Data fusion and examination*
- *Analysis*
- *Investigation*
- *Incident Response*

### *Collection and Detection:*

Collection and detection involves collecting of network traces and detection of attack over network. The traces involves searched history, firewall logs , applications and packets. The challenge is to identify useful information from network events and keep the records of the events taking place regularly[1].

### *Data fusion and examination:*

The data captured using various network tools (NFATs ,NSM)must be arranged and see for it if any investigation is required. The major challenge is identifying attack traffic from legitimate traffic and malicious network events[1].

### *Analysis:*

The critical step in network forensics is categorizing and analyzing attack data and arriving at an conclusion about what type of attack it is.

We need to classify and order the attack that has been occurred so far ,so that it will be easy to identify the type of attack that has been imposed[1].

### *Investigation:*

Investigation must be held to identify from where the attack has been send. The major challenge in this is to geographically locate the attacker[1].

### *Incident Response:*

An active response must be generated to the network that has been misused. The attacker should not be aware of the response that has been send to the misused network[1].

### Web Browser Forensics:

Web browser is a tool that helps us to access internet. With the help of a browser we will be able to gather information easily. Even though web browsers have more advantages it has some disadvantages like one can view history of our searching and it can be used to perform malicious things.web browsers are used as computer forensics tool. Nowadays, many types of browsers are available we will see some of them and the challenges involved in that browsers[6].

The following are the types of browsers:

- *Internet Explorer*
- *Chrome*
- *Firefox*
- *Safari*

Challenges involved in these browsers are given below:

### *Internet Explorer:*

Challenges in internet explorer are[6]:

- Accessing user's cache and history
- Accessing cookies
- Accessing auto complete data from auto complete forms and password
- Accessing typed url's and form/password data's

### *Chrome:*

Chrome stores its user information and history in SQLite database [6]

Challenges in chrome:

- Downloaded files
- Url's
- Visited sites

***Firefox:***

Challenges in Firefox are [6]:

- History
- Cookies
- Passwords
- Cache

***Safari:***

Safari stores its data in more than one file it stores its files in property list which was introduced by apple to store data. Safari doesn't use database to store data.

Challenges in safari are [6]:

- Bookmarks
- Top sites
- History
- Last session
- Cookies

## CONCLUSION AND FUTURE WORK

Forensics is used for detection of crime. The following are the types of forensics cloud forensics, network, web and mobile forensics. In this paper we have discussed only about these forensics in future work we would deal with more types of forensics and provide solutions for that forensics.

## REFERENCES

1. *Pilli, Emmanuel S., Ramesh C. Joshi, and Rajdeep Niyogi. "Network forensic frameworks: Survey and research challenges." digital investigation 7.1-2 (2010): 14-27.*
2. *Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. digital investigation, 7(1-2), 14-27.*
3. *Pilli, Emmanuel S., Ramesh C. Joshi, and Rajdeep Niyogi. "Network forensic frameworks: Survey and research challenges." digital investigation 7, no. 1-2 (2010): 14-27.*
4. *Pilli, E.S., Joshi, R.C. and Niyogi, R., 2010. Network forensic frameworks: Survey and research challenges. digital investigation, 7(1-2), pp.14-27.*
5. *Pilli ES, Joshi RC, Niyogi R. Network forensic frameworks: Survey and research challenges. digital investigation. 2010 Oct 1;7(1-2):14-27.*
6. *Survey based Project Study of web Browse Muhammad Tallal, Sheraz Shahid Butt, Momina Abrar, Rashid Muhammad Hamza Iqbal*
7. *Khan, Suleman, et al. "Forensic challenges in mobile cloud computing." 2014 International Conference on Computer, Communications, and Control Technology (I4CT). IEEE, 2014.*
8. *Khan, S., Ahmad, E., Shiraz, M., Gani, A., Wahab, A. W. A., & Bagiwa, M. A. (2014, September). Forensic challenges in mobile cloud computing. In 2014 International Conference on Computer, Communications, and Control Technology (I4CT)(pp. 343-347). IEEE.*
9. *Khan, Suleman, Ejaz Ahmad, Muhammad Shiraz, Abdullah Gani, Ainuddin Wahid Abdul Wahab, and Mustapha Aminu Bagiwa. "Forensic challenges in mobile cloud computing." In 2014 International Conference on Computer, Communications, and Control Technology (I4CT), pp. 343-347. IEEE, 2014.*
10. *Khan, S., Ahmad, E., Shiraz, M., Gani, A., Wahab, A.W.A. and Bagiwa, M.A., 2014, September. Forensic challenges in mobile cloud computing. In 2014 International Conference on Computer, Communications, and Control Technology (I4CT)(pp. 343-347). IEEE.*
11. *Khan S, Ahmad E, Shiraz M, Gani A, Wahab AW, Bagiwa MA. Forensic challenges in mobile cloud computing. In2014 International Conference on Computer, Communications, and Control Technology (I4CT) 2014 Sep 2 (pp. 343-347). IEEE.*
12. *Alqahtany, Saad, et al. "Cloud forensics: a review of challenges, solutions and open problems." 2015 International Conference on Cloud Computing (ICCC). IEEE, 2015.*
13. *Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2015, April). Cloud forensics: a review of challenges, solutions and open problems. In 2015 International Conference on Cloud Computing (ICCC) (pp. 1-9). IEEE.*
14. *Alqahtany, Saad, Nathan Clarke, Steven Furnell, and Christoph Reich. "Cloud forensics: a review of challenges, solutions and open problems." In 2015 International Conference on Cloud Computing (ICCC), pp. 1-9. IEEE, 2015.*
15. *Alqahtany, S., Clarke, N., Furnell, S. and Reich, C., 2015, April. Cloud forensics: a review of challenges, solutions and open problems. In 2015 International Conference on Cloud Computing (ICCC) (pp. 1-9). IEEE.*
16. *Alqahtany S, Clarke N, Furnell S, Reich C. Cloud forensics: a review of challenges, solutions and open problems. In2015 International Conference on Cloud Computing (ICCC) 2015 Apr 26 (pp. 1-9). IEEE.*
17. *J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," Digit. Investig., vol. 9, pp. S90–S98, Aug. 2012.*
18. *W. Delport, M. S. Olivier, and M. Kohn, "Isolating a Cloud Instance for a Digital Forensic," in ISSA, 2011.*
19. *J. Li, X. Chen, Q. Huang, and D. S. Wong, "Digital provenance: Enabling secure data forensics in cloud computing," Futur. Gener. Comput. Syst., Oct. 2013.*
20. *C. Yan, "Cybercrime forensic system in cloud computing," in Proceedings of 2011 International Conference on Image Analysis and Signal Processing, IASP 2011, 2011, no. Dc, pp. 612–613.*