Journal of Forensic Research

Chaurasia, J Forensic Res 2015, S3:1
DOI: 10.4172/2157-7145.1000S3-001

Commentary Open Access

Issues in Acquiring Digital Evidence from Cloud

Gaurav Chaurasia*

National law Institute University, Bhopal, India

***Corresponding author:** Gaurav Chaurasia, National law Institute University Bhopal, India-462001, Tel: 9755141800; E-mail: gauravmsclis@gmail.com

Rec date: Nov 24, 2014 **Acc date:** June 27, 2015 **Pub date:** June 02, 2015

Abstract

Now a day cloud computing is grow day by day. We know that today many companies hire the cloud services from the cloud service providers. They are working as a third party. They are providing the software and hardware as a service. Client and the cloud service providers may be belong to the different place.

Because of the nature of the cyber space, there is no physical boundary. If suppose that crime scene occur in this scenario then the investigator face the many problems like collection to the evidence because we know that cloud forensic is the subset of the network forensic. So there is difficulty to identify the source. If suppose that investigator able to find the location, which exist outside the county then the jurisdiction issue will be occur. We know that every country has own jurisdiction. In this paper we will discussed the issues relating to the collection and acquisition the digital evidence with help of the real scenario. And we also discuss the some tool which is help in the collection evidence from the remote location.

Keywords:
Cloud computing; Third party; Cyber space; Crime scene; Network forensic; Investigator; Jurisdiction; Collection; Acquisition; Digital evidence; Tool; Remote location

Introduction

First of all we have to understand the working of cloud computing. Because the knowledge of the cloud is must for doing forensic. If suppose that investigator don't have the knowledge about the cloud then he will not able to collection the evidence. In other words *"where to find?"* means in cloud there is no single resources actually it's exist as distributed. Cybercrime also occur in the cloud environment.

When we talk about the investigation in cloud computing which is a difficult task. In which forensic investigator faces many problems. The forensic of the cloud is not an easy task like window forensic, log analysis etc. It includes many other things. With the advent of cloud computing it also increases the new challenges to digital forensic. So digital forensic investigator must enhance their skills and practice new tool over the cloud environment.

Cloud Computing

According to the researcher cloud computing is a new way to provide the services to the client. In which client does not need to purchase the software and hardware from the market but there is only one major requirement that the user must have the internet connection. In the concept of cloud computing the principle of remote accessing is followed. So client can use the cloud storage for storing the data.

A simple example of cloud computing is Gmail, yahoo, drop box, etc. [1]. In cloud gives the following services like PaaS, SaaS, IaaS. In PaaS (platform as a service) the platform is provided as a service to the client. In SaaS (software as a service) the client uses the software.

So there is no need to purchase the license of software [1,2]. And last one Is IaaS (infrastructure as a service) the cloud service providers give the infrastructure as service to the remote client so there is no need to establish infrastructure. Then have only pay to the cloud service provider and take the services 24×7 times [3].

We know that in cloud environment the client and the service provider are located at different place. In this environment client doesn't have the knowledge about the storage area means where is the data is store? And it is not necessary that the data only stored at the single place it may choose different location for the storage of data. Cloud gives powering growth to the business with a broad cloud computing portfolio and deep cloud expertise [4].

About Cloud Forensic

Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics. Basically, it is a cross-discipline between cloud computing and digital forensics. As per the official definition of NIST: "Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data [5]."

Scenario of the Paper

We know that crime may be has taken place in the cloud environment. Client is locate another place and criminal is located another place and cloud service provider has located another place. So in this paper we are assume a crime scene in the cloud environment and we will see during the investigation which issues will occur (Figure 1).

Figure 1: Cloud computing environment.

Here we can see cloud computing environment suppose cloud service provider give the service from USA and client are locate different-different location. Like victim A is a residence of Australia and criminal is a residence of UK. Then during the process of investigation various issue will be arises.

Issues in acquire digital evidence - there are many issues occur in acquire digital evidence.

- Identify the target – this is the biggest issue in acquire digital evidence from the cloud computing. We know that in cloud computing environment it is difficult to identify the target means where the evidence will be present?
- Jurisdiction problem – if suppose that once the target has been identify. And suppose that resources exist out of the county then how can will you investigate in the other country because we know that every county it has the own jurisdiction. So we can say that jurisdiction is a biggest issue in acquire digital evidence from cloud computing.
- Collection the evidence – when we talk about the collection the evidence from the cloud then there is no specific single source of collection the evidence.
- Legality of evidence – as we know that digital evidence always comes under doubt means is it legal? So legality of the digital evidence most of the time comes under in challenge in the court of law.
- Chain of custody – another issue is chain of custody we know that in digital forensic the concept of chain of custody is important. Who will be holding the evidence and who will be done the analysis and in this concept the responsibilities also differentiate from level to level. Here a document uses between the law enforcement agencies, which consist the information regarding the client and law enforcement? [5]
- Third party issue – we know that in cloud computing third party has involved. And it works as a service provider. If investigator fined the third party resources which are involved in the crime then investigator take the permission to collect the data. If third party live in outside means in other country then investigator face again problem in the investigation process.
- Privacy – when we talk about the data and information then privacy also occur with it. If we put light on the definition of privacy then there are no clear definitions which talk about the privacy. Privacy is differing from person to person.

According to oxford dictionary – "a state in which one is not observed or disturbed other people: she returned to the privacy of her own home [6,7]."

Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations.

Privacy of personal data- Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy' [8].

In investigation process, in first step they collect the data. In this step the privacy issue occurs because in this information not only the information related to the victim but also other user's information also collects. So here privacy of the other user also violate because privacy protected by law. In US the data protection law is available.

So we can say that privacy issues also occur in the acquire digital from the cloud environment.

- Cost factor – if suspected resource is located outside the country then the acquisition of digital evidence is costly process because investigator will go the outside which increase the cost of investigation.
- Time factor – in cloud environment, the resources are distributed so the nature of the cloud also effect on the investigation process because investigator visit each suspected side which will casus the delay in the acquit ion process.

Suggestions

According to researchers point of view there are some suggestions to minimize the impact of the issues.

- I think that there should a law which is providing the harmonization at international level. So the jurisdiction and other issues may be resolved.
- Investigator must have the knowledge about the working of the cloud computing and networking.
- Hash value must be generated by the investigator.
- According to me there should develop some remote forensic tools which will help in the remote evidence collection so time and cost issues will be solved by these tools. For example Helix. Helix provides the remote evidence collection in this scenario we saw that in a network we can make the raw image and sends to the investigator system where forensic investigator extracts this image and analyse the data.
- Proper guidelines must be frame for cloud forensic.
- Coordination among the cyber forensic departments for solving such type of issues which occur in the digital forensic process.

Conclusion

I would like to conclude this paper. We saw that in cloud computing there resources are distributed. If crime scene occurs in this scenario then the forensic investigator phase the various kind of issue which is discussed above in the issues sections these issues we can resolved if we will take appropriate action.

Biography

Gaurav Chaurasia has completed his BCA at the age of 21 years from Punjab Technical University and pursuing postgraduate from National Law Institute University Bhopal (MP). He has published 3 papers in national and International conference. He has done CCNA, MCSE, RHCE form HCLCDC Jhansi (UP). he has qualified the intellectual property online certification form WIPO academy (US) and also got certificate of cyber-crime protection program, data privacy law in India and Facebook law in India form Asian school of cyber law Pune(MH).

References

1. http://www.wikinvest.com/concept/Cloud_Computing visited on 12/01/2014.
2. http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 visited on 18/01/2014.
3. http://www.rackspace.com/cloud/ visited on 20/01/2014.
4. http://www.ibm.com/cloud-computing/in/en/ visited on 20/01/2014.
5. http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics/ visited on 26/01/2014.
6. http://www.computer-forensics.net/FAQs/what-is-a-chain-of-custody.html visited on 22/01/2014.
7. http://www.oxforddictionaries.com/definition/english/privacy visited on 22/01/2014.
8. http://www.rogerclarke.com/DV/Intro.html visited on 23/01/2014.

This article was originally published in a special issue, entitled: **"Analytical Applications in Forensic Sciences",** Edited by Harvey Hou, Alabama State University, USA