International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

Review on Forensics in Cloud Computing

Miss Sneha Shete

Lecturer, Computer engineering Department, V.P.M's Polytechnic, Thane, Maharashtra, India.

Abstract*: This paper will discuss the need for computer forensics to be practiced in an effective and legal way, outline basic technical issues, and point to references for further reading. It promotes the idea that the competent practice of computer forensics and awareness of applicable. Network administrators and other computer security need to understand issues associated with computer forensics. Forensics essentially refers to the process of in depth analysis of information that exists in the present, in order to reconstruct past events or objects, with the proffered interpretation being subject to scrutiny by others.*

Key Words: *Forensic Process, Digital Forensic, Cloud Computing etc.*

1. INTRODUCTION

If you manage or administer information systems and networks, you should understand computer forensics. Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive. Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. As a result, it is not yet recognized as a formal "scientific" discipline. We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

1.1 CYBER FORENSICS

Cyber forensics, also called computer forensics or digital forensics, is the process of extracting information and data from computers to serve as digital evidence for civil purposes or in many cases to prove and legally prosecute cyber-crime. With technology changing and evolving on a daily basis cyber forensic professionals must continually keep pace and educate themselves on the new techniques to collect this data. They are tasked with being an expert in forensic techniques and procedures, standards of practice, and legal and ethical principles that will assure the accuracy, completeness and reliability of the digital evidence

2. DIGITAL FORENSICS

Digital Forensics is a branch of forensics science pertaining to legal evidence found in computers and digital storage mediums. The goal of digital forensics is to explain the current state of a digital artifact. The term digital artifact can include a computer system, storage medium an electronic document or even a sequence of packets moving over a computer network.

2.1 DIGITAL FORENSIC PREPARATION

There are basically five steps of Digital Forensics processes:

1. Preparation and Identification
2. Collection
3. Preservation
4. Examination and Analysis
5. Presentation

Forensics Examiner or Investigator must have done all their Preparation before conducting the forensics case. This includes preparation of the tools and equipments necessary for conduction the job.

Forensics Examiner of Investigation must be able to identify the suspect - a person or a group of people such as obtaining the suspect personal information which includes accommodation, job, travelling records etc. or the target.

Once the suspect or target is identified, the next stage of digital forensics process is to collect the essential data and information which will be useful for examination and analysis. This collection of required information can be from a physical device, such as a PC hard drive, USB drive etc. It can be an ongoing data transfer session such as data captured of collected from a LAN or WLAN networks.

There is a need to preserve, image or duplicate the collected data or information to protect the collection in

case of any damage and also for further analysis or reference. When preserving of imaging this collected data of information, forensics investigator needs to ensure that there is no alteration of data duplicated. Therefore write block and hashing is normally required.

Forensics examiner and investigator will have to examine and analyze the obtained data or information. This important information retrieve or obtained will be useful to be presented as evidence in court or to be use for further intelligence operation.

The last stage of the digital forensic process is to report and present the findings and evidence in readable and recognizable format which may be useful in term of law and in court.

3. FORENSIC LAW

In simple terms forensic science can be put across as a study and application of science to matters of law. Forensic law also includes the business of providing accurate, timely, and thorough information to all levels of decision makers in our criminal justice system. Forensic science is a multidisciplinary subject used for probing crime scenes and gathering evidence to be used in prosecution of offenders in a court of law. Forensic science techniques are also used to examine compliance with international agreements regarding weapons of mass destruction.

4. CLOUD FORENSICS CHALLENGES

Both live forensic and static forensic approaches face challenges in the cloud. The static forensic process involves, for example shutting down the system so that the hard disk can be cloned. This cannot be carried out in the cloud as a number of virtual machines share the same physical infrastructure. Shutting down the host machines disrupts all the hosted virtual machines wherein some of them may be running mission critical systems. Live forensics, on the other hand, only involves taking snapshots of running virtual machines and crime scenes cannot be recreated as in the case of static forensics. Digital forensic procedures could be performed easily in traditional settings where data storage centres are within physical reach.

Digital forensics has to catch up with the continuous changes in computing paradigms. A cloud model poses challenges to digital forensics as information is difficult to locate, acquisition is impossible if it cannot be located, and there would be no analysis without acquisition. Challenges relating to digital forensics that hinder data acquisition in the cloud include distributed storage, protected data, identity, etc

In a cloud environment, data is likely to be partitioned and stored in distributed systems usually spanning different jurisdictions; hence, it would be extremely difficult to locate. Cloud users may also store their data in the cloud in an encrypted format such that even if data is located and acquisitions are performed successfully, it cannot be useful to the digital investigator. This is still a challenge in traditional settings but it is worse in the cloud as data is encrypted further by the storage service provider over another encryption layer. Obtaining decryption keys from the data owner will not be sufficient. Other further decryption keys need to be obtained from the cloud storage service provider. In the cloud, there is also an issue of identity, wherein it is difficult to associate a cloud user with data stored in the cloud. In traditional settings, a physical machine owner is by default assumed to be the owner of all data stored in that machine. In a cloud environment, data is stored in remote locations and accessed using thin clients. It is a challenge in a cloud environment to single out a user from a large number of cloud users distributed globally and assume them to be the owner of the data. Cloud users may also use aliases as owners of data and not their real names.

CHALLENGE	DESCRIPTION
Identity	It is hard to link data stored in the cloud to an individual cloud user
Encryption	Data encrypted by the client before sending it for storage and further by the cloud service provider before storing it
Jurisdiction	Accessing data stored in computers beyond local borders may violate laws in other countries
Distribution	A cloud user may distribute data in several countries hence collaborating with each of these countries may be costly

Table 1: Digital Forensic Challenges in the cloud

5. FORENSIC INVESTIGATIONS IN CLOUD COMPUTING ENVIRONMENT

The main purpose of digital forensic investigation to step into the cloud computing environments is to find evidence against the criminals throughout the web. Because of overflow technologies in cloud computing, the digital forensic analysis have to deal with some difficulties such as the security issues, the limited access and other issues that we had discussed before. As we know, digital forensics is a structured investigation that is done in the past or ongoing of the data transmission and processing occurrences while still maintaining the chain of the document as the evidence where it can be used and validated in cases. Moreover in applying digital forensic toward the cloud computing environment, the investigators will have to involve a lot of people whether

inside of the country or even outside of the country where the processes of retrieving the evidence in cloud storage is not a simple as copying file from one folder to another folder. It may cost a lot of time which will cost us a lot of money in parallel to the time spend in doing the investigations.

5.1. DIGITAL EVIDENCE IN CLOUD COMPUTING ENVIRONMENT

Everything that an individual did in his life is kept somewhere as a record of what he's been doing and sometimes it is good and sometimes it is bad. The evidences are everywhere even if we want to deny it. In scientific angle, the evidence can be our fingerprint, DNA, human witnesses, CCTV, the residue of gun explosion, tools used, alibis, and also cloud computing environment. As in the law, the enforcers have a warrant to be used to enter and search premises, this also applies if the constable required information stored in the electronic form where it includes that the electronic devices are with the suspect such as a laptop, mobile phone, compact disc or external hard disk and the devices is on the property as amended by the Criminal Justice. Other than that is the evidence from other jurisdictions such as answering questions or producing articles and information where it also include evidence in digital format. In seizing evidence, for example enforcers enter a premise to inspect and search the premises, if they found that the computers inside the premises are connected and on-line to a cloud storage server, that server is considered as a part of the computer hardware even if the server is out of the country. Thus, the enforcer or investigator may copy the data and information on to the computer of the suspects or they can have the remote access to the server thus they can download the data.

6. ANALYSIS

Cloud computing environment actually makes the process of investigation easier and faster because without using the cloud computing, the investigators may have trouble with cross platform software, multiple operating system in a different computers or mobile phone and there is also a lot of devices to be examined and that may cost time and also money. This paper will further discuss on the analysis on forensic investigations and the implication of digital investigation, both in a cloud computing environment.

6.1. ANALYSIS ON FORENSIC INVESTIGATIONS IN CLOUD COMPUTING ENVIRONMENTS

The authors of [1] from Electronics and Telecommunications Research Institute, South Korea proposed a forensic service concept named as Forensic Cloud to enable the investigators focus more on the investigation process while does not have to think much about the technology used which means that they do not have to learn much about the latest technology but they still can continue with the process of investigation. In order to achieve this, they need a high speed processing of basic investigation which includes hacking, cracking, analyzing and many more and the needs of intuitive presentation and lastly to support user mobility while data access is secured.

Another analysis is proposed by [2], where he embedded the analysis software in the cloud to monitor the dynamic data network stream in real time. Thus, all of the incoming connections, outgoing packet, logging, time and date and others is recorded and monitored just like what have been done by Google in Google Doc storage or it is like antivirus software that monitors any malicious data connection to the user's computer. The software also recorded the temporary files, deleted files, exchanging files, system log files, backup medium, system buffer, registered information software, boot sector, allocated and unallocated space and slack space which also considered as a type of concealed evidence. Most of this can be recorded and traced even if the system is shut down. Figure 1 shows the framework of the engine is placed.

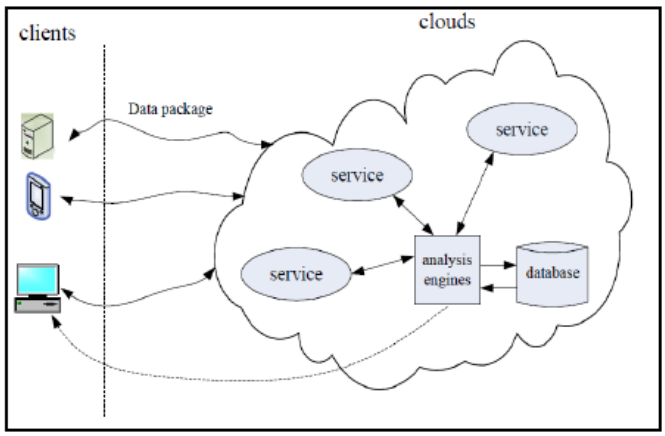

Figure 1: Framework of Analysis Engine

7. CONCLUSION

The main use of forensic science is for purposes of law enforcement to investigate crimes such as murder, theft, or fraud. Forensic scientists are also involved in investigating accidents such as train or plane crashes to establish if they were accidental or a result of foul play.

REFERENCES

[1] S. D. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments," Fifth International Conference on IT Security