ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 3 (July - Sept. 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

A Review of Cloud Forensics Issues & Challenges

[I]Sonam Jain, [II]Tejbir Rana
[I]M.Tech CSE, [II]Assistant Professor (CSE)
[I,II]Shivalik Institute of Engineering & Technology

Abstract
Cloud Computing is becoming most sought after and desired service among organizations as it can share entities such as, process units, storage and software and promises simplicity and delivering services based on virtualization technologies. Convenience, availability, elasticity, speed, large storage capacity, scalability, and on-demand network access are some of the key features of cloud computing. The surge in adoption of cloud computing solutions makes it inevitable for digital forensics not to follow since considerable & extensive potential security risks girdle this new technology. This paper provides a review of cloud forensics including the issues and existing challenges in order to give better future prospects and also offers some steps to be taken to overcome these challenges.

Keywords
Cloud computing; Cloud forensics, security; virtualization, forensic challenges

I. Introduction

The abrupt increase of online and offline users with multiple devices the storage of user data is moving towards cloud computing. With the advancement in technology there come potential threats to the information of user And if any attack is made on the cloud it becomes extremely strenuous to investigate the cloud because of huge size . The most offend challenges are difficulties to deal with different current liability on variety of data secured at different locations, access to obtain evidences from cloud and even the issue of capturing the physical evidence for the sake of collaboration of the validation or evidence present the role of digital forensics in cloud computing starts there. The cloud forensic is a phenomenon to explore the non ethical activities on a cloud. It comes with all types if analysis and assessment on all types of information's on cloud computing. carried out in this field.

II. Cloud Forensics

Cloud forensics can be defined as the application of advance forensics in cloud computing exploring the criminal activities. The cloud computing is so beneficial that is making forensic community so concerned about user information . The scalability of the cloud means at one point, data from different sources can occupy the same sectors within the storage media which creates an ambiguity during e-discovery, while a company is being explored; the investigator unknowingly acquires residual data from another company the growth of storage capacity in cloud computing is a disadvantage for digital forensics since there would be more forensic data and more time consumption to analyze the data, of course, if nothing goes wrong. There are other insufficiencies and incompetence's of the traditional digital forensics methods (e.g. encoding) in cloud computing therefore it is necessary to know more about digital forensics knowledge and specified tools in cloud computing in order to establish a forensically capable environment producing successful way towards reducing cloud security risks. Cloud computing is a new model and digital forensics community is still exploring what touble this new era technology is carrying for it. so many authors stating the potential encountered difficulties in the process of maintaining the chain of continuity . Even leading organizations have not yet presented a set of suggestions or practices to be made to follow certain set of instructions when there is a security accident inside of the cloud or guidelines on how to implementing cloud in organizations. In some cases, cloud computing able us to assist network investigation in their online investigations for cyber securities and crimes. Criminals may abuse professional independent communications systems such as Tor and Anonymizer which were originally modeled for protecting network users form identity thieves andportraying. Therefore, law enforcement may purchase tens of Amazon EC2 VMs, using the Tor network as sentinels which can act as entry & exit nodes for Tor circuits and that can check the attack sources within appropriate trace back techniques [11]. Amazon web services (AWS) is another good example which can self based provide a MD5 of every file that is on the system so when a bit by bit copy is being processed, everything is carried over with that including the Metadata files in Microsoft Office, email stores and exact backupsEase of Use

III. Technical Challenges and Impact of Cloud Forensics

The Conventional forensics is not capable of mapping complete events within the cloud computing environment where some are listed below:

- Loss of user information during mapping process for different reasons, such as shut down of the server, can cause parallel or unrelated services to get interrupted
- Not ease of access to network routers, load balancers and other networking equipments.
- Lack of access to large firewall
- Challenges in imaging hops from one to other which will remain static across the cloud routing schemes
- Problem faced in log analysis of cloud applications
- Reinforcement and bendability of logs
- Access of logs
- Velocity of attacking
- Malicious nodes
- Information deletion
- Hypervisor-level exploration

In order to address the challenges in the cloud computing , a variety of studies were carried out by researchers such as Lu et al. who proposed the need of a secure origin that records processing and manipulations history of data objects in cloud computing. They stated that the secure origin must satisfy two conditions of unworkability and privacy concerns and then proposed a formal definition based on the bilinear pairings followed by using security technique to ensure its private security in the standard model. It was claimed that the proposed secure origin scheme provides trusted evidence for data disputation in cloud computing however,

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

the study was carried out theoretically and there is no evidence whether it works in practicality with different services and deployed models. In 2011, Ruan et al. published a paper proposing a new definitions for cloud investigation after conducting a survey among digital forensic experts and practitioners from around the world in United Arab Emirates, hosted by Zayed University. The survey was aiming to indicate a better understanding of some concepts such as the cloud forensics definitions, the challenging issues, most crucial research directions, and the critical measures for cloud investigation capability. Based on Ruan et al. definition, cloud forensics is a crosslayer between digital cloud computing and digital cyber crime investigation .Also, it is a subset of network crime investigators which deals with forensic investigations in any kind of networks with extended existing techniques made for for cloud computing environment. Cloud forensics can be expanded in three dimensions of technical, organizational, and legal dimensions .

IV. Digital Forensics Tools and Procedures

This phenomenon includes a set of tools and procedure to carry out the digital investigation of crimes process in cloud computing environments and its main key aspects are defined in following:

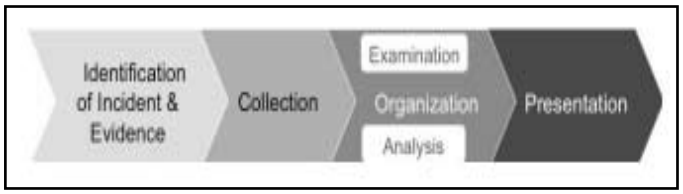

Fig.1 : Flow Diagram of procedure of cyber crime crime diagnosis

A. Idenification

The distributed nature of cloud make identification of possible sources of evidences a comparatively difficult task. In this section we are making a deeper look on issues that investigators could face in this stage. Access to evidences in logs, is the first issue in evidence identification stage. Checking system status and log files are a part of
collecting evidences, which is not feasible in SaaS and PaaS because the client access is completely limited to the API or the pre-designed interface. It is just applicable to IaaS cloud model as it provides the Virtual Machine which behave as an Actual Machine.

B. Forensic Data Collection

It is the process of recognising , classifying , storing , and retrieving data from other possible sources of data in the cloud either from the source -side or destination -side artifacts. Due to the different cloud services and deployed models, duties varies from one service or deployed model to another in the cloud therefore, different tools and procedures are to be required .

C. Preservation

The evidence, in forensic investigation is the proof to a crime and any offence to the relation of the evidence can make it of no use. Usefulness of evidences in cases that the client is involved with the non ethical activities , it is possible for the client to claim that his/her authentication credentials were taken and embezzled by other . As the client can also connect to the cloud automatically and independently , there is no way to prove that the claim is wrong.

D. Analysis

Data analysis is another crucial stage of the forensic investigation; especially in computer forensic investigation it demands for a more delicate examination as the quantity of objects to be inspected isincreased on large scale . In cloud computing, this can be even called a disaster as the nature of the cloud computing involves utilization of large amount of resources with a good chance of containing proof. This is an another view of cloud forensic investigation mainly due the limitations in processing and identifying the vast data.

E. Reconstruction

Data reconstruction stage of the forensic investigation produces different types of analyze results . The digital forensic practices demands for generation of temporary analysis to logically recreate the non ethical act , as part of data collection steps. In cloud computing, each piece of crime might have happened in different place due to different the nature of cloud computing which involves using and sharing resources; this brings an issue which interrupt the generation of the temporary analysis.

F. Reporting /Presentation

The last stage or the last challenge of forensic investigators involves in choosing the right court for reporting the case. In usual computer forensic investigation it is not difficult to decide about the court and the case would be brought to the
court in the country in which the crime has been committed; but in distributed networks and particularly in cloud computing it is absolutely complicated due to the characteristic of the cloud computing. It is not clear that where the crime has committed and where evidences are physically located since usually the cloud resources are shared between multiple clients in multiple countries. This
obviously confuses the investigator in deciding where and what legal system the suit should be used.

V. Conclusion

The cloud computing with the pleasant offer of computer as service and lots of hopes to companies and businesses with limited computing resources problems.
As the prevalence of Cloud computing continues to rising, cyber crimes related to Cloud or directly target to Cloud also increases. In this paper we discussed and analyzed the troubles and challenges faced by digital forensics investigators when they encountering Cloud related non ethical activities and introduced our suggestion about Cloud forensics, which including the main objects of the investigation, investigating process and its needs, and finally propose 3 basic forensics skills that investigators should process.
Future work will focus on analyzing the continuous improving investigation method of Cloud related cyber
crime, Cloud forensics model will be proposed, and certain cases we've encountered will be used to demonstrate the method and the model.

References

[1] Angus McKenzie Marshall. Digital Forensics: Digital Evidence in Criminal Investigations. John Wiley, 2009.
[2] M Reith, C Carr, G Gunsch. An Examination ofDigital

Forensic Models. International Journal of Digital Evidence, 2002.

[3] Brian Carrier. Defining Digital Forensic Examination and Analysis Tools. DigitalResearch Workshop II, 2002.

[4] Wikipedia. DigitaL Forensics.http://en.wikipedia.org/wiki/Digital_forensics.

[5] Eoghan Casey. Digital Evidence and Computer Crime:Forensic Science, Computers and the Internet. AcademicPress,2011.