Cloud Forensics: Trends and Challenges

Nachiket Vaidya
Ernst and Young

Abstract:- **Cloud is no longer a new word to the computing world and has transformed the IT industry, as services can now be deployed with relative ease. Fifteen minutes and clicking of a button is all it takes for personnel to create or reset the entire infrastructure for a computing resource that is offered in three different cloud computer service models namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These models present three indifferent and unique challenges for conducting cloud forensic investigations. This paper talks about the challenges facing Forensics in Cloud Computing Environment and opportunities associated with it.**

Keywords: Cloud Forensics, Cloud Computing, Cloud Model, Cloud Environments, Enterprise Cloud solutions,

1. INTRODUCTION

The advent of cloud computing provides unique opportunities for optimistic and pessimistic use. Malicious users can exploit the frailties in certain areas of the cloud such as security.Since cloud offerings don't require users to physically own the infrastructure, users can access most features by remote desktoping into the cloud virtual machines, perform their activities and then destroy the virtual machines later. This kind of computing presents a unique challenge to digital forensic investigators.It also raises the importance of developing specialized forensic tools for collecting and studying digital evidence in the digital world, in some situations even before they are lost or structures and various service models, had added more challenge to digital forensic investigators to gain the full access and control to the spread cloud resources.The concept of virtualisation in computing involves operating systems running on another operating system as if they were running on their own hardware. [4]Virtualization provided grounds for the birth of cloud computing. Such developments in computing paradigms present more opportunities for cyber crimes.Research efforts were at an advanced stage in addressing issues of digital forensics for traditional computing paradigms including virtual environments but these solutions may not be directly applicable in the cloud. User data in a cloud environment is distributed and often resides beyond the jurisdiction of forensics investigators.

2. CLOUD COMPUTING

Cloud computing can be defined as highly scalable computing resources provided as an external service via the Internet on a pay-as-you-go basis . This means that service consumers only pay for the services they use in the cloud. The cloud infrastructure can be deployed in three different forms, namely private cloud(which lies within organizations premise), public cloud which lies in the cloud service providers data center) and a hybrid cloud where responsibilities of the infrastructure are shared between Cloud Service Providers data center and organization's premise. Cloud computing is grouped into three layers, cloud application, cloud platform and cloud infrastructure.These layers in a cloud are offered as services .Most cloud provider generally follow a three model approach for delivery cloud offering namely-

Software As a Service(SAAS)

In SAAS offering - applications that are accessed over the web are not managed by your company, but by the software provider. [1]This relieves your organization from the constant pressure of software maintenance, infrastructure management, network security, data availability, and all the other operational issues involved with keeping applications up and running.

Infrastructure as a Service(IAAS)

[1]Infrastructure as a service offers a standardized way of acquiring computing capabilities on demand and over the web. Such resources include storage, networks, processing power, and virtual private servers. These are charged under a "pay as you go" model where you are billed by factors such as how much storage you use or the amount of processing power you consume over a certain timespan.In this service model, customers do not need to manage infrastructure, it is up to the provider to guarantee the contracted amount of resources and availability.

Platform as a Service(PAAS)

Platform as a Service is halfway between Infrastructure as a Service (IaaS) and Software as a Service (SaaS). In this type of model, users generally use the Cloud service providers platform offering to build and deploy applications. Additionally they are given flexible choices to choose between different cloud components and deployment options based on the subscription levels.

Out of many cloud components that are offered in different service models, one is a Hosted Desktop. A Hosted Desktop is a virtual machine hosted in the cloud. In a hosted desktop, applications and data are hosted on a Cloud service providers data center can be easily accessed with ordinary desktops or thin clients. A hosted computer like this can be used in the same way as a physical computer to commit cyber crimes.. It is when such crimes are committed in the cloud tracking the crime can often be a challenge and the services of a forensic expert will be required.

3. FORENSICS IN CLOUD

Digital forensics is a methodology in which the elements of law and computer science are combined to collect and analyse data from computer applications/systems, networks, wireless communications, and storage devices in a way that can be considered as evidence in a court of law. According to [2] digital forensic process can be broken into four distinct phases:

1. Collection of artefacts (both digital evidence and supporting material) that are considered of potential value are collected
2. Preservation of original artefacts in a way that is reliable, complete, accurate, and verifiable
3. Filtering analysis of artefacts for the removal or inclusion of items that are considered of value
4. Presentation phase in which evidence is presented to support investigation.

Traditionally, two categories of digital forensics existed namely -Static forensics which involves analysis of static data such as hard drives obtained using traditional formalized acquisition procedures and Live forensics that involves the analysis of the system memory and any other relevant data while the system being analysed is running.

Cloud Forensics is the application of digital forensics in cloud computing environments.With digital devices advancing rapidly, data generated by these devices require an enormous amount of computational power to analyze them. The concept of 'Forensic Cloud' is proposed and aims to allow an investigator to focus solely on investigation processes.

The cloud service providers are yet to establish forensic capabilities that will support the investigation in case if any crime is committed.

4. CLOUD FORENSIC CHALLENGES

Forensic frameworks for traditional forensics methods such as static forensics and live forensic can help trace the issue relatively easily especially where data centers are within physical reach.

A cloud model poses unique challenges like the ones listed below -

- Storage System is no longer local and can violate the jurisdiction laws.
- Each cloud server contains files from many tenants
- Even if data belonging to a particular suspect is identified, separating it from other tenant data is difficult.
- Reconstruction of deleted Data.
- Other than the cloud service provider, there is usually no evidence that links a given data file to a particular suspect.to digital forensics as information is difficult to locate, acquisition is challenging if it cannot be located, and there can be no analysis without acquisition.

According to[4], there are three sources from which evidence can be extracted in a cloud, i.e., the client side, the network layer and the cloud service provider (CSP). Of the three sources the most difficult to gather evidence from is the cloud service provider side. What makes it difficult on the cloud provider side is that the provider is usually outside the jurisdiction of the investigators. International laws and international collaborations have to be taken into consideration, which may be costly and time consuming.

Forensics as a Service

Cloud Vendors are most likely to offer Forensics as a service which creates unique propositions for resolving the challenges related to digital forensics under one roof which can be a lucrative subscription for the organizations.

In order to analyze the domain of Cloud Forensics more comprehensively, it is necessary to understand that it is not only a technical issue, but a multi-dimensional one which involves Organizational as well as Legal aspects.

While the Technical Dimension consists of tools and frameworks that are required to perform forensic investigations in Cloud Computing environment, Organizational dimension comes into picture when multiple parties are involved where Cloud Service Provider must communicate with third-parties for their expertise in the Investigation.Another aspect which is a Legal Dimension requires development of regulations and agreement to ensure that the forensic activities do not breach laws and regulations in the jurisdictions where the data resides. [3]The confidentiality of other clients using the same infrastructure should also not be compromised.

The existing tools and framework are limited in terms of their ability to resolve cyber crime related issues mainly due to the distributed and elastic characteristics of cloud computing as the existing tools cannot cope with cloud environment.Tools and procedures are yet to be developed for investigations in virtualized environments especially on the hypervisor level.

5. CLOUD FORENSIC OPPORTUNITIES

Cost Efficiency:

As cloud platforms ,services and infrastructure continue to mature and become cost efficient , cloud forensics will also become cost effective over a period of time when implemented at a large scale using more mature frameworks and processes.

Data Recovery:

With Cloud vendors continuing to expand their footprints and investing in creating data centers that are more local, data availability is bound to increase. Data replicated across the data center is less likely to be siloed and recovery will become easier.

Policies and Frameworks:

Cloud Computing is still evolving , which creates opportunities for Digital Forensics to establish uniform policies and develop mature frameworks and standards to aid in cyber crime investigation.

6. CONCLUSION

The continually prevailing cloud and digital economy may be disrupting a lot of industries , but is also creating great opportunities. Cloud Forensics may not be the need of the hour but it will certainly be in future, based on the pace at which cloud computing is growing and conquering everyone. The limitations are but small obstacles which can be worked upon since the cloud is still in early stages. Cloud Forensics is still in its infant stage and Future work in this area will need to focus on analyzing the continuous improving investigation method of Cloud related cybercrime, Cloud forensics model will be proposed, and certain cases encountered till now will be used to demonstrate the method and the model.

7. REFERENCES

[1] The three service models of Cloud Computing | OPEN https://www.openintl.com/the-three-service-models-of-cloud-computing/

[2] Forensics Plan | Computer Forensics | Digital Forensics https://www.scribd.com/document/144828523/Forensics-Plan

[3] Cloud Forensics: What is it And Why is it so important https://www.techstagram.com/2013/03/20/cloud-forensics-importance/ [Online]. Available: https://cloud.google.com/customers/ bnp-paribas-fortis/.

[4] Digital Forensics Environment for Cloud https://www.scribd.com/document/168145892/Sibiya-2012