Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 149 – 154

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment

Sheik Khadar Ahmad Manoj*, D.Lalitha Bhaskari

Department of Computer Science and Systems Engineering,Andhra University College of Engineering, Visakhapatnam-53003, India

Abstract

With the rapid growth of cloud adoption in both private and public sectors globally, cloud computing environment has become one of the prospective battle field for cyber attackers where one of the major challenges of cloud computing is the protection of data from various attacks. Mostly, Cloud services are provided by the service providers where data security is a major concern for the client. In this paper an attempt to provide a possible solution for such threats is proposed along with an exposure to various issues related to data security in cloud and the various challenges faced by forensic experts in cloud. A model based on trusted third party (TTP) along with a cloud forensics investigation team (CFIT) proves to be a better solution to enhance the trustworthiness of the service provider and thereby facilitate the cloud providers to trap cyber attackers with strong collection of evidences which might help in further legal process.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Cloud computing;Trusted Third party (TTP); Cloud forensics;Digital investigation;Cyber attacks.

1. Introduction

Cloud computing is a new IT phenomenon which is being widely adapted by many people around the globe. This adaption generated a security concern for the stored data in cloud environment. When security attacks or

* Corresponding author. Tel.: +91-8886854522;
*E-mail address:*skamanoj@gmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.202

policy violations occur, it makes necessary to conduct a digital forensic investigation. But, existing digital forensic principles, frameworks, practices and tools are largely intended for off-line investigation and in particular, these approaches assume that the storage media under investigation is completely within the control of the investigator[1]. Conducting investigations in a cloud computing environment presents new challenges which are to be addressed.

This paper proposes a frame to make the cloud environment reliable and preserve the trustworthiness of cloud service providers. This paper is organized into 5 sections where in section II overview of cloud computing is given. Section III deals with the introduction to cloud forensics and the challenges of forensics in cloud environment. In section IV a detailed explanation of the proposed frame work model is presented followed by conclusions in section V.

2. Cloud Computing

Cloud computing is continuously growing and emerging technology. The hardware and software resources that provide diverse services over the network or the internet to address the user requirements are called "Cloud". Here, resources refer to computing applications, network resources, platforms, soft ware services, virtual servers and computing infrastructure. The cloud computing can be conceived as pay-go-use model wherein the clients pay for the requested resources. Cloud computing eliminates the costs and complexity of buying, configuring and managing the hardware and software.

The cloud architecture mainly provides three categories of services [2] Iaas(Infrastructure as a Service), Paas(Platform as a Service) and Saas(Software as a Service)

The four well-known deployment models used in cloud computing are[2] Public Cloud, Private Cloud ,Hybrid Cloud and Community Cloud.

3. Cloud Forensics

A cyber criminal can be described as a person who legitimately involves in destruction of privacy or security of data and utilizing unauthorized resources causing loss to the digital users. Cloud computing environment is becoming a new battle field of cybercrime where new challenges are being posed to defend the cyber attacks. To meet the challenges of digital data threat, digital forensics methods[6] are applied over the remote servers of cloud giving way to a new term called "Cloud Forensics".

Basing on NIST Cloud Computing Reference Architecture[6], the researchers revisited the definition proposed in Ruan et al. 2011A, and proposed a working definition of cloud forensics as "Cloud forensics is the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multijurisdictional and multi-tenant situations"

According to National Institute of Standards and Technology[4], the major challenges of Cloud Forensics are categorized into the following nine major groups which are summarised as

- Architecture (e.g., diversity, complexity, provenance, multi-tenancy, data segregation, etc.)
- Data collection (e.g., data integrity, data recovery, data location, imaging, etc.)
- Analysis (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines, etc.)
- Anti-forensics (e.g., obfuscation, data hiding, malware, etc.)
- Incident first responders (e.g., trustworthiness of cloud providers, response time, reconstruction, etc)
- Role management (e.g., data owners, identity management, users, access control, etc.)
- Legal (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc.)