Computers and Electrical Engineering 000 (2017) 1–13

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Forensics framework for cloud computing[☆]

M. Edington Alex[a,*], R. Kishore[b]

[a] Department of Information Technology, Rajalakshmi Engineering College, Chennai, India
[b] Department of Electronics & Communication Engineering, SSN college of Engineering, Chennai, India

ARTICLE INFO

Article history:
Received 14 June 2016
Revised 6 February 2017
Accepted 6 February 2017
Available online xxx

Keywords:
Cloud computing
Cloud forensics
Digital forensics
Cloud forensics model
Cloud forensics challenges
Forensic solutions

ABSTRACT

The popularity of cloud computing has been on the rise in recent years, as cloud resources are not only shared by many users but can be allocated on demand. A recent survey reports success of the cyber criminals in using cloud computing technology for fraudulent activities, due to its essential characteristics and the lack of suitable digital forensic techniques for the cloud environment. While mitigating cloud crime, investigators face several challenges and issues dealing with cloud forensics. In this paper, the challenges faced by forensic investigators are highlighted. Most of the research work deals with the identification of challenges in cloud forensics and the proposed solutions reported in literature depends on Cloud Service Provider (CSP) for forensic investigation. The dependence on CSP includes the collection of data for the forensics process and there may be a chance of altering data that affects the entire investigation process. For mitigating the dependency on CSP, a new model for collecting forensic evidence outside the cloud environment is developed.

1. Introduction

1.1. Cloud forensics

National Institute of Standards and Technology (NIST) [1] defines cloud computing as “Cloud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events. This is done through identification, collection, preservation, examination, and interpretation and reporting of digital evidence”. Ruan et al. [2] have defined cloud forensics as “the application of digital forensic science in cloud environments as a subset of network forensics”, as shown in Fig. 1. Here, the authors highlight the significance of cloud forensics in three different aspects, namely, technical, organizational and legal. Technical aspects are engaged in forensic tools, mechanisms, and procedures. Organizational aspects incorporate the interaction between cloud actors for forensic investigation. Legal aspects deal with multi-jurisdictional and multi-tenant situations. The authors also identify cloud forensics as an associate of cloud computing and digital forensics.

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. M. D. Selvaraj.
[*] Corresponding author.
E-mail addresses: edingtonalexm@ssn.edu.in (M.E. Alex), kishorer@ssn.edu.in (R. Kishore).

http://dx.doi.org/10.1016/j.compeleceng.2017.02.006
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

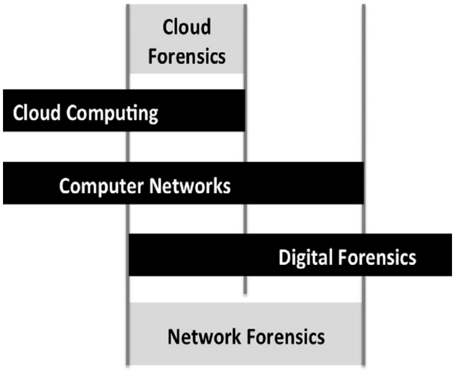

Fig. 1. Cloud forensics [2].

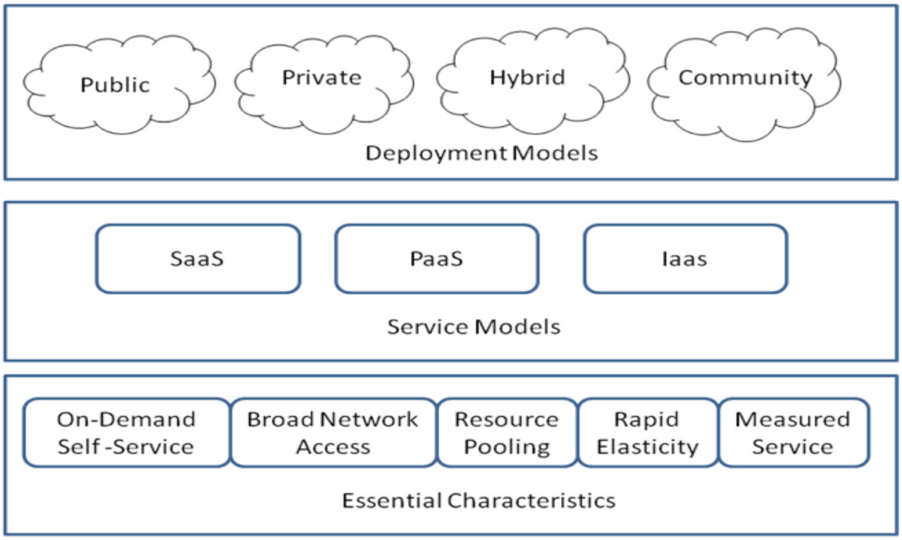

Fig. 2. NIST cloud model [3].

1.2. Cloud computing

The term cloud computing means sharing of computer resources among different users. As per NIST [3] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The cloud model consists of five essential characters, namely**,** on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, and three service models, namely: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and four deployment models such as Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud [3] as depicted in Fig. 2.

1.3. Digital forensics

Digital Forensics refers to "an applied science to identify an incident, collection, examination, and analysis of evidence data" [1]. The different phases of digital forensics are**:**

- Identification: Two major steps are involved in this phase, (i.e.) identification of malicious activity and isolating the evidence towards malicious activity.
- Collection: Evidences related to the malicious activity from different digital media are collected and the integrity of the evidence is maintained.
- Organization: In this phase, the examiner investigates the collected evidence which forms the examination phase and all identified evidence are correlated in the context of the malicious activity.
- Presentation: The investigator produces an organized report to the jury in the context of his investigation towards the case.

Please cite this article as: M.E. Alex, R. Kishore, Forensics framework for cloud computing, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.02.006