Bio Core
Exploring Scientific Community

World Congress & Expo on
Biotechnology and Bioengineering
March 27-29, 2017, Crowne Plaza Dubai – Deira, Dubai, UAE

Proactive model for locating and collecting cybercrime evidences on cloud computing

Abdulghani Ali Ahmed*, Chua Xue Li

Universiti Malaysia Pahang, Malaysia

The high scalability of cloud computing provides more opportunities to business and IT organization to develop high end computing services with low cost. Businesses has been given many choices in selecting cloud service providers as this process requires careful thinking to weight the advantages against the possible drawbacks of losing control on resources, applications and data storage. Despite the advancement of cloud storage and the advantageous it brings to all computer users, cloud storage is still subjected to misuse of malicious users and criminals. This includes the use of cloud storage for storing and exchanging illegal material and for committing botnet attacks. In fact, increasing number of crimes against cloud storage makes the investigation process of extracting and collecting cybercrime evidences in cloud forensics more challenging. Although a number of researches and solutions are proposed to address cloud computing security, several studies and surveys reported that security in cloud computing still posing several challenges to the researchers. Loss of control over the data stored in cloud computing is one of the security challenge in that clouds. Location of data storage in the cloud and the multi tenancy of customers on cloud servers are all representing security concerns. At the same time, cloud technology nowadays is also creating challenges for forensic practitioners. This paper reviews the current challenges in cloud forensic and propose a proactive model to improve the process of locating and collecting cybercrime evidences in cloud computing. The objective of this paper is two pronged. Former is to study the existing digital evidence collection methodology, the location and the data fragments left on user's computer prior to the usage of cloud storage application. Last is find the location and the data fragments left on user's computer prior to the usage of cloud storage application for new cloud storage.

-