Locating and Collecting Cybercrime Evidences on Cloud Storage: Review

Abdulghani Ali Ahmed, Chua Xue Li
Faculty of Computer Systems & Software Engineering
University Malaysia Pahang
Gambang, Pahang, Malaysia
abdulghani@ump.edu.my, xueli93@live.com

Abstract: Despite the advancement of cloud storage and the benefits it brings to computer users, it cannot be denied that cloud storage is still subject to misuse by malicious users and cyber criminals. This includes the cases where criminals use cloud storage for storing and exchanging illegal material and for committing botnet attacks. In addition, the increase in the number of cybercrimes against cloud services challenges the forensic process of locating and collecting cybercrime evidence in cloud storage. Although a number of researches are proposed to address cloud storage security, several studies and surveys reported that security in cloud computing still pose several concerns and challenges to the researchers. Loss of control over the data stored in cloud storage is one of the security challenges in that cloud. Moreover, location of stored data in the cloud and the multi tenancy of customers on cloud servers are all representing security concerns. At the same time, current cloud storage technology creates challenges for digital forensic practitioners in presenting and interpreting meaning to the obtained evidence to investigators, lawyers, and, ultimately, to the jury. This paper reviews the existing works in locating and collecting cybercrime evidence in cloud storage and provides an in-depth discussion of their limitations.

Keywords: Cybercrimes, Cloud Storage, Forensic Investigation, Cloud Services.

978-1-5090-5493-0/16/$31.00 ©2016 IEEE