On Cloud Data Transaction Security Using Encryption and Intrusion Detection

Mahmoud Jazzar, Department of IT, Royal University for Women, Riffa, Bahrain

ABSTRACT

The rapid increase of cybercrimes and wide-ranging security measures has created an obvious need for deep understanding of security vulnerabilities for Cloud Computing environments, and for best practices addressing such vulnerabilities. Cybercrime activities have affected many regional and international organizational functions and operations. Finding clear and direct evidence of cybercrimes is critical, because huge amounts of data are on networks, and the analysis of such data is complex. This paper propose and discuss a security-enhanced cloud data transaction model for simplifying and filtering cybercrime evidence. The model consumes a number of intrusion-detection sensor inputs that contribute to collecting and fine-tuning large items of evidence at a lower level. A relevant evidence-processing criteria are defined for further reduction and fine-tuning of cybercrime evidence. Initial results of the up-to-date testbed show that it is possible to reduce substantial levels of irrelevant patterns from randomly collected datasets.

KEYWORDS

Cloud Computing, Cybercrimes, Digital Evidence, Intrusion Detection, Network Forensic

INTRODUCTION

Dramatic threats of cybercrimes and network-based security concerns of various organizations are drawing attention to develop specific and dedicated intrusion detection sensors (IDS) as a first line of defense. The security strength for various information systems tools is associated with the development of specific and dedicated IDS tools and technologies. However, the strength of the security for information systems can be measured based on different means and factors. As such, in order to develop secure information system tools, the dedicated IDS tools must be reliable enough to detect all new and up to date events, provide detailed reports and classification of events in term of relevance and related factors (Jazzar, 2013).

Secure network communication is an essential component of overall security policy. As such, secure network communication against unauthorized disclosure of information sharing, denial-of-service (DoS) or destruction of data have to be protected. In other words, the availability, confidentiality, and integrity of information and computing system resources must be provided (Depen, Topallar, Anarim, & Ciliz, 2005).

As a solution, IDS technologies are designed to monitor network traffic, operating systems logs, and/or application programs for signs of intrusions. Thus, developing more sophisticated and specialized sensors to be deployed at sensitive locations as supplemental systems is recommended. In general, variety of means and mediums of delivering and receiving data and information, using the Internet, will enable gathering forensic evidence. However, finding clear and direct evidence for

DOI: 10.4018/JCIT.2017100102

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
1 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/article/on-cloud-data-transaction-security-using-encryption-and-intrusion-detection/189202?camid=4v1