Journal of Cases on Information Technology
Volume 19 • Issue 4 • October-December 2017

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 (Depren, 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

cybercrimes is critical, because of the huge amount of data on the network and the complexity of analyzing such data. In fact, due to the extreme increase in volume of network data packets and the volume of data and information captured, large amount of storage will be wasted, regardless of the accuracy of the possible evidence (Saari & Jantan, 2011; Saari & Jantan, 2013a).

In light of such complexity, the intrusion detection processes for finding forensic evidence require employing comprehensive and sophisticated techniques for proper intrusion detection and response. Therefore, this study emphasizes the proposal of an enhanced cloud security model for simplifying and filtering cybercrime evidence collection. The model consumes a number of intrusion detection sensor inputs that contribute to collecting and fine-tuning large amount of lower-level evidence. Relevant evidence-processing criteria are defined to further reduce and fine-tune cybercrime evidence.

The proposed model consists of three primary phases: evidence collection, evidence mapping, and evidence identification as well as the documentation of the reduced number of evidences. The details of this model are described.

BACKGROUND

According to The CERT Division of SEI (n. d.) and Jazzar (2013) "The best way for administrators to protect their networks is to monitor and analyze their network traffic. Understanding the traffic can help them characterize threats and attacks, and it can also help them identify vulnerabilities in their networks. However, processing traffic on large networks can be time-consuming and expensive, and it may be impossible without effective automation tools…" (p. 4). IDS is an effective network traffic analyzer and defense tool that can analyze and identify vulnerabilities, as well as detect intrusion, exploits, and hostile activities on the system network. This study attempts to support the current IDS by supplementing with an inference monitor system that works in unsupervised learning mode, which can provide adoption, integrity, and an information-sharing platform among the IDS components.

The ICT security process is an ongoing process cycle that includes four processes: assessment, protection, detection, and response process (Bejtlich, 2010). IDS technologies are designed to automate the monitoring and analysis process, so that they provide deeper analysis, detection, and response to any malicious activity occurring in the computer system or network. Conversely, firewalls are widely deployed as a first line of defense for overall network security (Home PC Firewall Guide, n. d.). Firewalls usually make traffic-flow decisions by inspecting data-packet headers, but not the entire contents. Therefore, they cannot detect whether a malicious intrusion is embedded within the normal traffic, making them insufficient on their own. As a result, IDS technologies are being deployed outside and inside firewalls, quickly becoming a mainstay in best practice and secure network implementations (Next Generation Intrusion Detection Systems, n. d.).

This study focuses on the anomaly detection process (i.e., anomaly intrusion detection). At this point, the challenge is to define if and how unauthorized or unapproved network activity can be an intrusion. Several network forensic models that focus on monitoring and analysis of network traffic have been proposed (Khan, Gani, Abdul Wahab, Shiraz, & Ahmad, 2016). As such, a framework to illustrate and gather network based evidence by utilizing mechanisms available in the structure of the general IDS called forensic intrusion detection sensors has been implemented (Saari & Jantan, 2011; Ibrahim & Jantan, 2011; Rasmi, Jantan, & Hani, 2013). The framework uses a distributed mobile agent implemented for the relevant security and reliability of the collected data and information. Such deployments contribute to reducing storage space and hardware costs. Similarly, IDS and firewall integration (Saari & Jantan, 2013b) for getting highest possible items of evidence, and studies on analyzing attack intention (Rasmi & Jantan, 2013), which increases the possible value of evidence, have been proposed.

According to Sobh (2006), intrusion detection elements can be characterized based on primary assumptions and components. Primary assumptions are defined according to the system events observable, normal, and intrusive events that show distinct evidence. As such, the detection engine's