Chapter 53
An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms

Ammar Almomani
IT Department, Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan

Firas Albalas
Department of Computer Science, Jordan University of Science and Technology, Irbid, Jordan

Mohammad Alauthman
Department of Computer Science, Faculty of information technology, Zarqa University, Zarqa, Jordan

O. Dorgham
Prince Abdullah Ben Ghazi Faculty of Information Technology, Al-Balqa Applied University, Al Salt, Jordan

Atef Obeidat
IT Department, Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan

ABSTRACT

This article describes how as network traffic grows, attacks on traffic become more complicated and harder to detect. Recently, researchers have begun to explore machine learning techniques with cloud computing technologies to classify network threats. So, new and creative ways are needed to enhance intrusion detection system. This article addresses the source of the above issues through detecting an intrusion in cloud computing before it further disrupts normal network operations, because the complexity of malicious attack techniques have evolved from traditional malicious attack technologies (direct malicious attack), which include different malicious attack classes, such as DoS, Probe, R2L, and U2R malicious attacks, especially the zero-day attack in online mode. The proposed online intrusion detection cloud system (OIDCS) adopts the principles of the new spiking neural network architecture called NeuCube algorithm. It is proposed that this system is the first filtering system approach that utilizes the NeuCube algorithm. The OIDCS inherits the hybrid (supervised/unsupervised) learning feature of the NeuCube algorithm and uses this algorithm in an online system with lifelong learning to classify input while learning the system. The system is accurate, especially when working with a zero-day attack, reaching approximately 97% accuracy based on the to-be-remembered (TBR) encoding algorithm.

DOI: 10.4018/978-1-7998-2460-2.ch053

INTRODUCTION

Since the dawning of the computer networking, IDS have played an essential role in assuring of the network's safety for the users, but this role has changed in recent decades (Keegan et al., 2016). Previous studies have not capable to efficiently detect the attacks instantly. therefore, they have been commonly utilized as forensic means to examine security evidence in ex-post facto. (Keegan et al., 2016). As network traffics are increased and attacks became more and more obvious with the prevalence of using the Internet since the 1990s, the demand for a speedier intrusion detection system to diagnosis and block attacks became essentially. To address this issue, researchers worked on understanding patterns of network traffic, which resulted in the development of behavior-based and signature-based detection approaches. In Signature-based techniques, the network traffic is compared with the pattern of previous known attack signatures. whereas behavior-based techniques detect intrusions by differentiation it from legitimate network traffic behavior (Keegan et al., 2016). Cloud computing is a modern technology that facilitates and allows the dynamic and varied of using computational resources and services. In spite of the advantages of cloud computing, the security and privacy of cloud services are still the critsl issues. The adoption of cloud services have influenced the security situation of organizations infrastructures; so, the emerging threats and risks that carried out via this model should be mitigated and classified (Kandias, Virvilis, & Gritzalis, 2011).

To utilize intrusion detection for cloud computing, new computational models are necessary to be constructed using the paradigm of parallel processing. As an alternative, current computational models require modified for the cloud computing environment. Numerous computational algorithms unable to use used in the cloud computing structure directly (Zhao, Ma, & He, 2009). To address this shortcoming, researchers have begun implement and designing several machine learning applications that have the ability to work in environment of cloud computing. Additionally, many researchers have highlighted the importance of utilizing machine learning algorithms to cloud computing in order to intrusion detection evaluations (Hu & Shen, 2012; Suthaharan, 2014).

Popular attacks form that target cloud computing is distributed denial of service (DDoS) attacks (Badve & Gupta, 2016; Ficco & Rak, 2015; Gupta & Badve, 2017; Osanaiye, Choo, & Dlodlo, 2016). Interested readers may refer to (Gou, Yamaguchi, & Gupta, 2016; A. N. Khan, Kiah, Madani, Ali, & Shamshirband, 2014) for additional cloud-related privacy and security issues. In DDoS attacks, the attacker attempts to infect and take control of enormous numbers vulnerable computers, to carry out and coordinated attacks. Current defence techniques that are able of managing quantities of data, generally suffer from handling data include irrelevant or redundant features, which rise the training and classification time (Peng, Choo, & Ashman, 2016).

The ultimate aim of this proposal is to develop a system for the evolving network traffic stream data which leads to improving the classification performance and accuracy of identifying different malicious attack classes used by intruders, especially the zero-day attack in online mode, we define zero-day attacks as attacks that intruder mount using hosts that do not appear in blacklists and not trained on the old data sample and it is a noise data) (Almomani, Gupta, Wan, Altaher, & Manickam, 2013; Gupta, Yamaguchi, & Agrawal, 2017), which increases the level of difficulty to detect phishing email. The proposed approach addresses the following objectives. Generally, the attack features are studied to build a more accurate system, minimize the threat of attack, and increase the trust of different organizations in performing online transactions and other e-commerce businesses. Specifically, the study aims to enhance the learning rate by using a cost-effective online method and analyze data for improved detec-