International Journal of Distributed Artificial Intelligence
Volume 11 • Issue 1 • January-June 2019

WLI Fuzzy Clustering and Adaptive Lion Neural Network (ALNN) for Cloud Intrusion Detection

Pinki Sharma, Punjabi University Patiala, Patiala, India
Jyotsna Sengupta, Punjabi University Patiala, Patiala, India
P. K. Suri, Kurukshetra University, Kurukshetra, India

ABSTRACT

Cloud computing is the internet-based technique where the users utilize the online resources for computing services. The attacks or intrusion into the cloud service is the major issue in the cloud environment since it degrades performance. In this article, we propose an adaptive lion-based neural network (ALNN) to detect the intrusion behaviour. Initially, the cloud network has generated the clusters using a WLI fuzzy clustering mechanism. This mechanism obtains the different numbers of clusters in which the data objects are grouped together. Then, the clustered data is fed into the newly designed adaptive lion-based neural network. The proposed method is developed by the combination of Levenberg-Marquardt algorithm of neural network and adaptive lion algorithm where female lions are used to update the weight adaptively using lion optimization algorithm. Then, the proposed method is used to detect the malicious activity through training process. Thus, the different clustered data is given to the proposed ALNN model. Once the data is trained, then it needs to be aggregated. Subsequently, the aggregated data is fed into the proposed ALNN method where the intrusion behaviour is detected. Finally, the simulation results of the proposed method and performance is analysed through accuracy, false positive rate, and true positive rate. Thus, the proposed ALNN algorithm attains 96.46% accuracy which ensures better detection performance.

KEYWORDS

Cloud Computing, Intrusion Detection, Lion Algorithm, LM Algorithm, WLI Fuzzy Clustering

INTRODUCTION

Recently, the cloud computing is defined as the novel paradigm where the services are either to be hosted or delivered over the Internet world, hence, it is also termed as the Internet computing. In other words, the term cloud computing is the process of computing service over the Internet world. In cloud computing, it poses the resource provider where the user utilizes the resources anywhere, anytime and also anything (Rajendran, Muthukumar, & Nagarajan, 2015). The rapid development of cloud computing is caused by the location independent of information processing. Furthermore, the trust or security is considered as the main aspect among the cloud users in the cloud computing services. Hence, Cloud security becomes the challenging task for the users utilize the cloud resources and also successfully exploitation of its respective services (Deshpande, Sharma, Peddoju, & Junaid, 2014). There are three services provided in the cloud computing, which are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The intrusion or malicious activity

DOI: 10.4018/IJDAI.2019010101

or attacks are the major drawbacks of the cloud services. Thus, require to enhancing the security and trusting management through intrusion detection system. Some of the common available attacks in the cloud computing are DNS poisoning, port scanning, man-in-the-middle attack, IP spoofing, etc. (Modi, Dhiren R. Patel, Avi Patel, and Rajarajan 2012). The attacks in the cloud computing are categorized into two ways, insider attack and outsider attack.

The attacker's attacks the network from the external source of origin is termed as external attack. On the contrary in insider attacks, unauthorized internal users are involved in the cloud services to abuse the access privileges. In order to detect the attack or malicious node in the network, an intrusion detection system (IDS) is employed. This system is used to detect the intrusions assist by computerizing the intrusion detection scheme. In other words, the intrusion detection is the process of monitoring computers or networks to detect an unauthorized entry, file and activity modification (Patel, Taghavi, Bakhtiyari, & Junior, 2013). The basic concept of intrusion detection system is to collect the network traffic, analyzes the traffic, and makes response or alerts the network when an intrusion detects in the network. Therefore, the aim of the IDS is to alert or notify the system if some malicious activities take place by such intruders (Krishnan & Chatterjee, 2012). Some of the key factors of intrusion detection systems are fast, critical to fraudulent users, ease of configuration, self-monitored, available without interruption, fault tolerant and free from false errors leads to possibility of minimum overhead. Then, the information system is evaluated which has the tendency to detect the activities of malicious node or any intruder in the network. Thus, the security level should be enhanced by performing the intrusion detection system (Raja & Ramaiah, 2016).

Signature based detection and anomaly-based detection are the two main detection method in the intrusion detection system. The signature-based method is employed to detect known attack. Also, it can be used either in front-end or back-end of the cloud environment where we can mitigate the external and internal attacks. On the other hand, unknown attacks are detected by anomaly-based detection techniques in Cloud network at different levels (Patel, Borisaniya, Patel, Patel, & Rajarajan, 2013). The IDS can be classified in two types depends on the location of deployment: i) In HIDS (Host-based intrusion detection system), as the name provides, the user (host) and application performs the action assist by the operating system used to evaluate the collected information and ii) Whereas, the information is collected from network packets are analyzed by the network-based intrusion detection system (NIDS) (Mishra, Vijay, & Tazi, 2016). Furthermore, the machine learning method plays a vital role to detect the intrusions in the cloud environment. Among them, an artificial neural network (ANN) is used to guide the system to detect the malicious activities of the cloud network. Then, the single controller is utilized to manage the occurrence of intruder with the aid of knowledge based and ANN pattern matching techniques (Raja & Ramaiah, 2016).

In this paper, the core intent is to detect the intrusion behaviour of the cloud environment. The cloud intrusion detection is performed by the WLI fuzzy clustering mechanism and proposed adaptive lion based neural network. The WLI fuzzy clustering mechanism is applied into the cloud network where the objects are grouped for the subsequent steps. The clustered output data is then undergone for the training algorithm. In addition to, the intruder is detected by the newly proposed adaptive lion based neural network (ALNN). The novel method is designed by the Levenberg-Marquardt algorithm of neural network and lion algorithm. In the proposed method, firstly, the LM algorithm is used to determine the weight function. Secondly, the lion algorithm exploits the LM weight function to update the weights adaptively by the female lion, termed as adaptive lion based neural network (ALNN). Finally, the proposed ALNN model is used to train the clustered data which is then aggregated into new data format. Thus, the proposed method efficiently detects or classifies the normal and abnormal node.

Main contributions of this paper are:

- To generate the multiple numbers of clusters the WLI fuzzy clustering mechanism is utilized for intrusion detection system.