Cloud Intrution Detection System Using Antlion Optimization Algorithm and Support Vector Machine (SVM) Techniques

Haruna Atabo Christopher
Department of Computer Science
Federal University of Technology
Minna, Nigeria
christatabo@yahoo.com

Joseph Adebayo Ojeniyi
Department of Cyber Security
Federal University of Technology
Minna, Nigeria
ojeniyija@futminna.edu.ng

Solomon Adelowo Adepoju
Department of Computer Science
Federal University of Technology
Minna, Nigeria
solo.adepoju@futminna.edu.ng

Opeyemi Aderike Abisoye
Department of Computer Science
Federal University of Technology
Minna, Nigeria
O.abisoye@futminna.edu.ng

***Abstract*— Cloud computing is an emerging technology that provides services and computing resources on demand to users with less management effort through the internet. Because of the increase in the number of internet user and the distributed nature of cloud, it has become a platform for criminal activities from within and outside of cloud environment. It is on this note that Cloud Intrusion Detection System (CIDS) is mostly deployed into cloud environment to identify and also prevent attacks in some instance. In this research work, a cloud intrusion detection system that identifies malicious activities inside cloud, utilizing Antlion Optimization (ALO) algorithm for feature selection and Support Vector Machine Classifier was developed. Experimental result shows 98.56% accuracy, 2.29% FPR, 96.32% (Recall, Precision and F-Measure), and 92.52% Kappa Statistics.**

***Keywords*—** Ant Lion Optimization, Support Vector Machine (SVM), CIDS, Feature Selection, Cloud Computing.

I. INTRODUCTION

Cloud computing is an emerging technology that provides services and computing resources on demand to users with less management effort through the internet. Because of its many benefits, it has gained more popularity amongst users. These benefits include: scalability, flexibility and cost effectiveness. Cloud computing provides services like software, platform, and infrastructure as a service to users by service providers [1][2].

Because of the increase in the number of internet user and the distributed nature of cloud, it has become a platform for criminal activities from within and outside of cloud environment. Some malicious activities of external attackers include Denial of Service (DOS)/Distributed Denial of Service (DDOS) attacks, phishing attacks and internet Protocol (IP) Spoofing. The level of insecurity is growing rapidly and cloud users are concerned about the safety of cloud resources. Hence the need for a robust security architecture to ensure a trusted and efficient security of tenants' resources in cloud. It is a software or hardware component that monitors the system or network for policy violation or malicious activities [2].

We propose in this paper a Cloud Intrusion Detection System (CIDS) based on Antlion Optimization (ALO) feature selection and Support Vector Machine (SVM) Classifier for classification.

Our major contributions in this paper are to:

- Design an Antlion Optimization (ALO) algorithm-based feature selection system for detecting cloud intrusions.
- Classify cloud intrusion dataset using Support Vector Machine (SVM) Classifier.
- Evaluate the technique's performance using standard metrics such as Accuracy, False Positive (FP), and Precision.

The remaining part of this work is organised as follows: section II explain the related works while section III discuss the proposed CIDS. Section IV presents the experimental result and finally conclusion at section V.

II. RELATED WORK

[3]Suggested a cloud intrusion detection system based on data mining approach. The authors in their paper proposed a Modified-Firefly Algorithm (MFA) to reduce the dimension of the dataset. This is achieved by blending the idea of three different data mining methods namely: Particle Swarm Optimization (PSO), Firefly Algorithm and Fuzzy Logics. Three different classifiers: AdaBoost, Neural Network and Random Forest ware used on the optimized dataset to obtain an efficient result. Experimental result shows the classification results obtained by the classifier is uncompromised. However, the proposed model is only for private cloud where we have limited number of cloud users. While, [4] presented an Integrated Cloud-based Intrusion Detection System that fight against intrusion in cloud environment. The proposed CIDS consists of five main modules which performs the following actions: monitoring the network, capturing the traffic flows, extracting features, analyzing the flows, detecting intrusions, taking a reaction, and logging all activities. An enhanced bagging ensemble system of three deep learning models is utilized to predict intrusions effectively. Experimental result shows that the proposed system can detect intrusion accurately, minimizing false alarm. However, the signature-based