Chapter 5
Optimized Deep Learning-Based Intrusion Detection Using WOA With LightGBM

R. Jayashree
SRM Institute of Science and Technology, India

J. Venkata Subramanian
https://orcid.org/0000-0003-2343-6790
SRM Institute of Science and Technology, India

ABSTRACT

Machine learning is a powerful tool in both cryptosystem and cryptanalysis. Intrusion detection is a significant part of cyber defence plans where improvements are needed to deal with the challenges such as detection of false alarms, everyday new threats, and enhancing performance and accuracy. In this chapter, an optimized deep learning model is proposed to detect intrusion using whale optimization algorithm (WOA) with light gradient boosting machine (LightGBM) algorithm. To increase the performance of the model, the collected network data from the KDD dataset are pre-processed with feature selection and dimensionality reduction methods. The WOA-LightGBM algorithm processes the pre-processed data for training. The outcomes of these experiments are compared with the performance of benchmarking algorithms to prove that this intrusion detection model provides better performance and accuracy. The proposed model detects the intrusion with high accuracy in short period of time.

1. INTRODUCTION

Cryptography is the art of generating secure systems for secret data through encryption and decryption techniques (Yan et al., 2022). Machine learning (ML) Techniques are used to automates the analytical model facilitating continuous learning even for big data inputs. This is the major reason for the application of ML in cryptosystems (CS). Moreover, ML and CS both process a huge amount of data with large search spaces. Private Key generation in cryptography is supported through reinforcement learning ML techniques (Yan et al., 2022). From the steganography perspective, ML classification methods, Bayesian

DOI: 10.4018/979-8-3693-1642-9.ch005

classification, AdaBoost and Support Vector Machine (SVM) are popularly used to perform classification of encrypted traffic and conversion of objects to steganography (Yan et al., 2022). The intrusion is an effort for influence upon the security mechanism and its regulations. This intrusion detection structure is in the direction to watch the network traffic and discover unfamiliar behaviour that may causes a harm (Ahmad and Mirvaziri, 2019). The techniques of detection are used to spot the attributes of data sets that they appear to be homogeneous and typical but these are rare (Sahil et al., 2020). These unusual cases are also referred as outliers, variations, exceptions, divergences, peculiarities, etc. (Sahil et al., 2020).

A Swarm Intelligence based approach detects the intrusion effectively for dynamic system (Hanieh et al., 2019). Here, a cryptosystem is viewed as a communication network in which individual node's dynamic behaviour is fully or partially observed by another node. Changes in system behaviour might be directly change the system's domestic communication structure by including or removing or altering i.e., strengthening or weakening of existing communication channels. Thus, the changes in the communication structure may replicate changes in the operating conditions of the system, and the detection of these modifications is a key component for intrusion detection (Hanieh et al., 2019). The familiar Whale Optimization Algorithm (WOA) is a novel meta-heuristic population-based optimization algorithms used for clustering which cohorts the hunting behaviour of humpback whales. In WOA, each whale represents a potential solution to the optimization problem, and the whales move through the search space to find the optimal solution.

The ML model such as XGBoost has been utilized in the networks or IoT (Internet of Things) intrusion detection. Zhang and Hamori (Zhang and Hamori, 2020) and Deng et al. (Deng et al., 2021) utilized intense gradient boosting (XGBoost) as an investigational model for prediction, and the outputs shown that the XGBoost model was capable to attain the exactness value of 86%. In (Cheng and Shi, 2021) Yan Song et al. proposed an intrusion detection model that is mostly based on the XGBoost, and uses the WOA to discover the suitable constraints for this. Though if accuracy rate is not bad, the drawback of the XGBoost model is found to traverse the dataset even during the node dividing process which tremendously increases the computational load (Xiang et al., 2022) and has particular boundaries in selecting or optimizing model parameters (Huang et al., 2021 and Chaofei et al., 2020). Light Gradient Boosting Machine (LightGBM) is an enhanced version of the gradient boosting decision tree model using an exclusive leaf-wise developing idea based on the huge depth limit, which may decrease many issues and obtain the improved accuracy while using the equivalent amount of splits (Xiang et al., 2022). Therefore, the detection methods become more efficient and more precise when WOA optimized parameters are combined with LightGBM model, which is planned in this article to enhance the correctness of intrusion detection. The architectural diagram of the proposed model is shown in the Figure 1.

2. LITERATURE REVIEW

In (Yan et al., 2022), Amir Anees et al. made a review on a number of latest works on proceed in various features of ML applications in cryptosystems and cryptanalysis. Developing anomaly detection models directly on data has a huge fault rate with respect to exactness and detection (Sahil et al., 2020). The dimensionality of datasets can be considerably condensed using feature selection methods. Deep learning approach, Restricted Boltzmann Machine is highly effective in extracting high-level features and creating clusters at various scale levels (Sahil et al., 2020).