A Review on Deep Ensemble Models to Detect an Classify Intruder Behavior

EL.Thanga Uma,
Assistant Professor,Department of Computer Science and Engineering,
Sri Bharathi Engineering College for Women, Pudukkottai-622 303, Tamilnadu, India.
Email: uma085@gmail.com

Abstract **- Intrusion Detection Systems(IDS) can be used to find intrusions in computer networks, cloud computing, and data systems. It involves challenging to demonstrate that these systems are secure and to maintain their security while they are in use. The Deep Ensemble Model for Intrusion Detection and Classification is a solution to these issues. The application of this approach consists of three primary stages: classification, best feature selection, and feature extraction. Among the tasks performed during the feature extraction step are feature reduction, feature conversion, and data standardization. The data provided is the first standard using an improved data normalization technique. Following the normalization of the data, feature conversion is carried out. For feature reduction, the Principal Component Analysis (PCA) approach is employed. Then, from the smaller pool that is left, the best traits are selected. To do this, we suggest applying the SUSSO (Self-Upgraded Squirrel Search Optimization) method.**

Keywords—PCA, SUSSO, IDBN, RNN

I INTRODUCTION

Cloud computing describes a brand-new Internet-based infrastructure that consumers lower-cost access to a range of computer and information technology (IT) features are OS, data storage services, network architecture, hardware parts, and software application suites. The notion of cloud computing and the advancements in Internet technology provides widespread accessibility of computer resources [1]. through a variety of on-demand service models, these cloud resources are made available to client applications. The services cloud computing provided are referred as "Software- as-a-Service" (SaaS), "Infrastructure-as-a-Service" (IaaS), "Platform-as-a-Service" (PaaS), and "Expert-as-a-Service" (EaaS) [7]. IDS is a vital component of network security in Web-based software, including e-commerce platforms, plays a critical role in identifying cyber attacks. They accomplish this by analyzing a wide range of networked data records. Network security has grown in significance for websites and web-based applications in recent years. An intrusion detection system (IDS) can identify intrusions in two ways: either by using anomaly detection, which focuses on identifying deviations from typical patterns that may signal intrusions, or by using abuse detection[8], which uses system vulnerabilities or known attack patterns to identify intrusions. These two approaches are explained in this article.

Since cloud computing intrusion detection is a challenging task, a significant amount of data security research has been done to find and stop intrusions [9]. When used in tandem with firewalls, effective intrusion detection systems aim to reduce false negatives and increase detection rates, improving overall security.

It is often difficult for traditional intrusion detection systems to react to new incursions, data mining and meta-heuristic algorithms based on information gathered from several sources have been adopted [10]. Fuzzy Clustering Algorithms, Artificial Bee Colony (ABC) algorithm, and Artificial Neural Networks (ANNs) are the three parts of a novel technique that combines these three techniques. While ANNs can function independently in an IDS, their combined use with fuzzy clustering and ABC improves system performance [11]. By dividing the dataset into homogenous groupings, fuzzy clustering speeds up the training process. By creating homogenous subsets of the training data, this is achieved. In order to link loads and preferences more quickly and efficiently, ABC helps the ANN discover the ideal values. It may take some time and work to integrate these two algorithms into the ANN, but [15]. If one wishes to enhance the detection of rogue nodes, they may want to take into account putting adaptive optimization principles into practice [16].

II LITERATURE REVIEW

A new IDS has been developed, according to Hajimirzaei and Navimipour [1] (2018), by combining fuzzy clustering techniques, the Artificial Bee Colony (ABC), and the Multilayer Perception (MLP) network. The MLP was utilized by the authors to distinguish between normal and anomalous traffic packets. Additionally, they adjusted the link weights and intrinsic biases of the MLP using the ABC technique.

In 2018, Seth and Chandra [2] developed a cloud-based DOS attack detection model (CDOSD) using Binary Artificial Bee Colony Optimization (BABCO) and a DT classifier. After extracting characteristics from the gathered dataset using BABCO, the authors classified the elements using the DT Classifiers.

Using distributed denial of service tools, a real- time attack on a cloud server was conducted to assess the efficacy of the concept. The data showed that the CDOSD model was adequate, with a lower false positive rate and improved accuracy.

Based on the Voting Extreme Learning Machine (V-ELM), Kushwah and Ranga [4] presented a novel approach in 2020 for identifying distributed denial of service (DDoS) attacks in cloud computing environments. Two benchmark datasets were utilized in the experiments to assess the effectiveness of the system: The NSL-KDD and ISCX intrusion detection datasets are two that are frequently used in intrusion detection. Additionally, a number of tests were conducted to look into how well the system performed with various parameter values, such as the amount of ELMs in V-ELM and the number of neurons in a single ELM's hidden layer.

Tummalapalli and Chakravarthy [7] developed a clustering and two-level classifier-based cloud-based intrusion detection system in 2020. The nodes were first grouped using Bayesian fuzzy clustering, and the groupings' likelihood of compromise was then predicted using a two-tiered gravitational group search-based support vector neural network (GG-SVNN) classifier. The gravitational search algorithm and the group search optimizer were combined by the GG-SVNN technique. The number of compromised nodes was ascertained by the level 2 classifier using the compacted intrusion data that it had acquired from the level 1 classifier. In 2020, Rabbani et al. [8] introduced a novel technique to enhance the Cloud service's capacity to simulate user behavior. To find and identify bad actors in the cloud, a particle swarm optimization-based probabilistic neural network (PSO-PNN) was employed. After the users' behaviors were interpreted in an intelligible way, a multilayer neural network was utilized to identify dangerous conduct. A detailed examination of the test results validated the method's potential utility for security monitoring and anomaly detection.

Table 1: Characteristics of detecting harmful activity in cloud computing

Adopted Methodology	Features	Challenges
fuzzy clustering technique, artificial bee colony (ABC) network, and multilayer perceptron (MLP) network	Minimize the square root of the error, often known as the mean absolute error (MAE). raises the kappa value	Training efficiency must be increased. There have to be tweaks made to improve the detection's precision.
CDOSD	The accuracy of detection has been enhanced. Low rate of false positives	It is feasible to determine more host characteristics.
FCM-ANN	A high degree of precision in the detection The low percentage of false alarms	It is recommended that the classifier's capacity for learning be improved.
Voting extreme learning machine (V-ELM)	Enhanced precision	The use of resources is significantly higher than average. There needs to be more emphasis placed on maintaining security.
DLMNN	Better overall recall value. The results for F-measure and accuracy are significantly	more excellent. Enhances should be made to achieve better compression times and ratios.

III. METHODOLOGY

Many firms are outsourcing their data and computing needs in order to take advantage of the rapid advancements in computer technology. Upholding security criteria like confidentiality, availability, and integrity is crucial for cloud-based computing, so a highly secure platform should be on focus.

Knowing the entire behavioral space that malware resides in offers a significant advantage over more traditional protection approaches. This proposal includes a novel approach to enhance cloud service providers' ability to simulate the behavior of their clients. Proposed feature extraction, ideal feature selection, and attack categorization are the three main steps that must be completed in order to identify and recognize hazardous conduct.

IV. CONCLUSION

A brand-new intrusion detection system is analysed in order to reduce the dangers connected with recurrent invasions and technical issues in computer networks. The three main phases of this model are categorization, ideal feature selection, and feature extraction. Three steps are involved in the feature extraction phase: feature reduction, feature conversion, and data normalization. An enhanced data normalization method is used to the input data. Following normalization, feature conversion is applied to the data. The PCA method is then applied to the modified features in order to reduce their feature count. The optimal feature selection procedure is then applied to the reduced features, and the most pertinent portions are chosen by using the SUSSO algorithm. The characteristics that were chosen are then sent on to the classification phase, where an ensemble model made up of classifiers from the Improved Deep Belief Network (IDBN), Recurrent Neural Network (RNN), and Deep Maxout Network is used. The Deep Maxout Network receives the classifications produced by the IDBN and RNN classifiers, which use the chosen features as input. By using the suggested SUSSO technique, the Deep Maxout Network's weights are adjusted. Lastly, a variety of intrusions, such as worms, analysis, DoS, backdoors, shellcode, exploits, generic, standard, fuzzes, and reconnaissance will be detected by the system's output.

REFERENCES

[1] Bahram Hajimirzaei1 and Nima Jafari Navimipour," Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm," ICT Express, January 2018

[2] N. Pandeeswari & Ganesh Kumar, "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN," Mobile Network Application, 2016

[3] Gopal Singh Kushwah and Virender Ranga, "Voting extreme learning machine based distributed denial of service attack detection in cloud computing," Journal of Information Security and Applications, vol.53, 2020

[4]. Deevi Radha Rani, G. Geethakumari, "Secure data transmission and detection of anti-forensic attacks in cloud environment using MECC and DLMNN," Computer Communications, November 2019

[5]. Ahmad Shokoohsaljooghi and Hamid Mirvaziri, "Performance improvement of an intrusion detection system using neural networks and particle swarm optimization algorithms," International Journal of information technology, 2019

[6]. Siva Rama Krishna Tummalapalli and A. S. N. Chakravarthy, "Intrusion detection system for cloud forensics using Bayesian fuzzy clustering and optimization based SVNN," Evolutionary Intelligence, April 2020

[7] Mahdi Rabbani, Yong Li Wang, Reza Khoshkangini, Hamed Jelodar, Ruxin Zhao, Peng Hu, "A hybrid machine learning approach for malicious behavior detection and recognition in cloud computing," Journal of Network and Computer Applications, vol.151, 2020

[8] Jagsir Singh, Jaswinder Singh, "Detection of malicious software by analyzing the behavioral artifacts using machine learning algorithms," Information and Software Technology, vol.121, May 2020

[9] Shamsul Huda, Suruz Miah, John Yearwood, Sultan Alyahya, Robin Doss, "A malicious threat detection model for cloud-assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network," Journal of Parallel and Distributed Computing, vol.120, pp. 23-31, October 2018

[10] Amandeep Singh Sohal, Rajinder Sandhu, Sandeep K. Sood, Victor Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," Computers & Security, vol.74, pp.340-354, May 2018

[11] Abdulaziz Aldribi, Issa Traoré, Belaid Moa, Onyekachi Nwamuo, "Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking," Computers & Security, vol.88, January 2020

[12] Sahil Garg, Kuljeet Kaur, Shalini Batra, Gagangeet Singh Aujla, Rajiv Ranjan, "En-ABC: An ensemble artificial bee colony based anomaly detection scheme for cloud environment," Journal of Parallel and Distributed Computing, vol.135, pp. 219-233January 2020

[13] Preeti Mishra, Ishita Verma, Saurabh Gupta," KVM Inspector: KVM Based introspection approach to detect malware in a cloud environment," Journal of Information Security and Applications, vol.51, April 2020

[14] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, "Scale Inside-Out: Rapid Mitigation of Cloud DDoS Attacks," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 6, pp. 959-973, 1 Nov.-Dec. 2018

[15] O. Alkadi, N. Moustafa and B. Turnbull, "A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions," in IEEE Access, vol. 8, pp. 104893-104917, 2020

[16]. A. Sahi, D. Lai, Y. Li, and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," in IEEE Access, vol. 5, pp. 6036-6048, 2017

[17] S. Dong, K. Abbas, and R. Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," in IEEE Access, vol. 7, pp. 80813-80828, 2019