INTELLIGENT INTRUSION DETECTION SYSTEM USING MACHINE LEARNING AND DEEP LEARNING MODEL IN ADVERSE ENVIRONMENT

ABSTRACT

Computer networks play a pivotal role in advancing science and technology. With the proliferation of communication channels and an ever-growing number of network devices, cybersecurity has emerged as a critical concern. Safeguarding valuable data from intruders is imperative due to the heightened vulnerability posed by this expansive network landscape.Attackers continuously evolve their methods, necessitating effective Intrusion Detection Systems (IDSs) capable of identifying and thwarting new infiltration patterns and attacks.

The extensive integration and connectivity of computing systems have become essential for improving our daily operations. As vulnerabilities arise, cybersecurity systems are crucial for ensuring secure communication exchanges. Effective transmission security necessitates measures to combat evolving threats and the development of security protocols capable of addressing emerging risks. Despite the initial purpose of firewalls in network security, they often fail to detect intrusions in real-time. With the emergence of destructive cyber-attacks presenting significant security challenges, there is a need for dependable and adaptable Intrusion Detection Systems (IDS) capable of efficiently monitoring unauthorized access, policy breaches, and malicious activities.

Traditional Machine Learning (ML) methods have been effective in identifying data patterns and detecting cyber-attacks within Intrusion Detection Systems (IDSs). However, Deep Learning (DL) techniques have emerged as a valuable tool for developing highly accurate and efficient IDS approaches. The adoption of deep learning-based cybersecurity methods for intrusion detection has seen a surge in popularity. Intrusion Detection Systems (IDSs) stand as a crucial component in safeguarding ICT infrastructure. Intelligent solutions are imperative for managing the complexities and addressing the growing diversity of attack vectors.

The adoption of intelligent systems, whether based on Deep Learning (DL) or Machine Learning (ML), has become widespread due to their ability to effectively manage complex and high-dimensional data. Intrusion Detection Systems (IDSs) encounter various types of attacks, including known, unknown, and zero-day attacks, which can be effectively identified using unsupervised machine learning techniques A novel approach has been introduced that combines the advantages of the isolation forest (One Class) and Support Vector Machine (OCSVM) with an active learning methodology to detect threats without prior knowledge. The evaluation of different ML/DL methods with active learning has been conducted using the NSL-KDD dataset. The result of OCSVM algorithm without UAI layer is 62.13% and the algorithm with UAI layer is 79.25%.The findings illustrate the

effectiveness of unsupervised anomaly detection, particularly when employing a UAI layer at top of various machine learning or deep learning techniques.

In the next work, the study focuses on optimizing feature selection within the realm of Intrusion Detection Systems (IDS). In this context, the research introduces an intelligent IDS method termed IIDS-EAOADL, which integrates an enhanced arithmetic optimization algorithm with deep learning techniques. The IIDS-EAOADL model initiates with a data standardization phase to normalize input data. Additionally, it incorporates an Equilibrium Optimizer based Feature Selection (EOFS) approach to identify an optimal subset of features. For intrusion detection tasks, a Deep Wavelet Autoencoder (DWAE) classifier is employed. Given the significance of parameter tuning in the DWNN, the EAOA algorithm is utilized for this purpose. To validate the simulation results of the IIDS-EAOADL technique, extensive simulation analysis is conducted using a benchmark dataset. The result shows better accuracy as 99.31% and running time as 0.860 seconds compared to other existing techniques.The experimental findings underscore the advancements achieved by the IIDS-EAOADL model compared to other existing techniques.