Abstract

Globally, the Internet of Things (IoT) has grown exponentially in the last few years. The integration of numerous IoT devices enhances connectivity but also exposes them to various cyber-attacks. With the increase of complex and intelligent cyber-attacks, the traditional methods of cyber-attack detection, such as anomaly and misuse intrusion detection systems (IDS), have proven ineffective in combating emerging cyber-attacks. Scholars have suggested that the existing IDS's performance can be enhanced by integrating machine learning methods. This study explored the integration of ELM (Extreme Learning Machine) with NSGA-II (Non-Dominated Sorting Genetic Algorithm II). Our empirical analysis reveals that ELM outperforms other algorithms regarding learning rate, usability, and effectiveness of generalization. NSGA-II provides an equilibrium between exploration and exploitation, successfully managing the trade-offs present in multi-objective optimization problems to identify a range of excellent solutions along the Pareto front. Most of the existing works on ELM optimization focuses on improving one input parameter. This study explored the integration of ELM with NSGA-II for both input weights and hidden neurons. The model was trained and tested using two datasets namely IoT_ToN network and UNSWNB15 datasets. This research used TON_IoT Windows dataset to further test the capacity of the model to identify novel attacks. Using the UNSWNB15 and IoT_ToN network datasets, respectively, the model's accuracy was 0.68 and 0.65. In addition, the model recorded an accuracy 0.768 using TON_IoT Windows dataset, demonstrating the potential of the model in detection of new forms of attacks. This study acknowledges the ongoing evolution of challenges in IoT security and the need for continuous innovation to stay ahead of emerging threats in the future. The contributions of this study can be explored further to develop reliable intrusion detection solutions for the dynamic IoT landscape.