ROAST-IoT: A Novel Range-Optimized Attention Convolutional Scattered Technique for Intrusion Detection in IoT Networks

Authors Anandaraj Mahalingam, Ganeshkumar Perumal, Gopalakrishnan Subburayalu, Mubarak Albathan, Abdullah Altameem, Riyad Saleh Almakki, Ayyaz Hussain and Qaisar Abbas .

Publication Year	2023
Grant Number	IMSIU-RP23079
DOI link	https://doi.org/10.3390/s23198044

Abstract: The Internet of Things (IoT) has significantly benefited several businesses, but because of the volume and complexity of IoT systems, there are also new security issues. Intrusion detection systems (IDSs) guarantee both the security posture and defense against intrusions of IoT devices. IoT systems have recently utilized machine learning (ML) techniques widely for IDSs. The primary deficiencies in existing IoT security frameworks are their inadequate intrusion detection capabilities, significant latency, and prolonged processing time, leading to undesirable delays. To address these issues, this work proposes a novel range-optimized attention convolutional scattered technique (ROAST-IoT) to protect IoT networks from modern threats and intrusions. This system uses the scattered range feature selection (SRFS) model to choose the most crucial and trustworthy properties from the supplied intrusion data. After that, the attention-based convolutional feed-forward network (ACFN) technique is used to recognize the intrusion class. In addition, the loss function is estimated using the modified dingo optimization (MDO) algorithm to ensure the maximum accuracy of classifier. To evaluate and compare the performance of the proposed ROAST-IoT system, we have utilized popular intrusion datasets such as ToN-IoT, IoT-23, UNSW-NB 15, and Edge-IIoT. The analysis of the results shows that the proposed ROAST technique did better than all existing cutting-edge intrusion detection systems, with an accuracy of 99.15% on the IoT-23 dataset, 99.78% on the ToN-IoT dataset, 99.88% on the UNSW-NB 15 dataset, and 99.45% on the Edge-IIoT dataset. On average, the ROAST-IoT system achieved a high AUC-ROC of 0.998, demonstrating its capacity to distinguish between legitimate data and attack traffic. These results indicate that the ROAST-IoT algorithm effectively and reliably detects intrusion attacks mechanism against cyberattacks on IoT systems