ABSTRACT

Machine Learning (ML)-based Intrusion Detection Systems (IDS), particularly those employing Deep Learning (DL) approaches, in Internet of Things (IoT) environments face major challenges due to severe class imbalance and the presence of redundant features in the Bot-IoT dataset. These conditions may lead to high overall accuracy while limiting the model's ability to effectively recognize both normal and malicious traffic behaviors. This study aims to enhance both the performance and interpretability of an anomaly-based IDS through a feature selection approach based on correlation analysis using the Pearson Correlation Coefficient (PCC) with respect to the target class, combined with standard deviation analysis and absolute standard deviation change to determine the optimal number of features.The selected features are then used as input to a Bidirectional Gated Recurrent Unit (BiGRU) model for binary classification (normal and attack). To achieve optimal performance, hyperparameter tuning is conducted by systematically exploring various model configurations using high computational resources. Evaluation results of the Deep Learning (DL) model without rule integration achieve a macro precision of 99%, macro recall of 97%, and macro F1-score of 98%. Furthermore, the interpretability of the selected features is leveraged to design an initial rule-based filtering layer applied prior to model inference, forming a hybrid approach that combines threshold-based filtering with DL-based classification. Additional evaluation of the hybrid approach demonstrates improved detection sensitivity by reducing false negatives to zero under the evaluated testing scenario, although accompanied by a slight increase in false positives. These findings indicate that integrating interpretable feature selection with deep learning can produce a more balanced, efficient, and practically applicable intrusion detection system for real-world IoT environments.

Keywords : Intrusion Detection System, Bot-IoT, Feature Selection, Pearson Correlation Coefficient, BiGRU, Macro Average, Hybrid IDS