**Enhancing DDoS Attack Detection through Hybrid Deep Learning and Explainable AI: A Comprehensive Approach Utilizing Random Forest, Logistic Regression, and Neural Networks**

ANIK SENa, & RIADUL ISLAM RABBIa

aMultimedia University, 75450, Melaka, Malaysia

[aniksen360@gmail.com](mailto:aniksen360@gmail.com), [riadul.rabbi72@gmail.com](mailto:riadul.rabbi72@gmail.com)

ABSTRACT

In the rapidly evolving landscape of cybersecurity, the detection of Distributed Denial of Service (DDoS) attacks remains a critical challenge. This paper presents a novel hybrid deep learning framework for the detection of Distributed Denial of Service (DDoS) attacks, integrating multiple machine learning models with explainable AI techniques to enhance both accuracy and interpretability. Our approach utilizes Random Forest, Logistic Regression, and Neural Networks in conjunction with SHapley Additive exPlanations (SHAP) to identify the most influential features contributing to DDoS attack detection.The dataset was meticulously preprocessed, involving the removal of missing values, encoding of categorical variables, and normalization of numerical features. We employed a rigorous training and testing protocol, splitting the data into 70% training and 30% testing subsets. Our Random Forest classifier demonstrated exceptional performance with an accuracy of 99.96%, an F1 score of 99.96%, a precision of 100%, and a recall of 99.92%. The Logistic Regression and Neural Network models also achieved substantial results, with accuracies of 92.95% and 96.91% respectively. To further enhance detection capabilities, we implemented a hybrid model approach combining Stacking, Boosting, and Voting classifiers. The Stacking model, which integrates Logistic Regression, Random Forest, and Gradient Boosting as base learners with Logistic Regression as the meta-learner, achieved a superior accuracy of 99.96%. The application of SHAP provided valuable insights into feature importance, identifying key features such as 'Flow Duration', 'Total Fwd Packets', and 'Fwd Packet Length Mean' as critical determinants in DDoS attack detection. Our comprehensive analysis demonstrates the efficacy of hybrid models in achieving high detection accuracy while maintaining interpretability through explainable AI. This research significantly contributes to the cybersecurity domain by providing a robust, interpretable framework for DDoS attack detection, potentially informing future developments in threat detection systems and enhancing the security infrastructure.

*Keywords* DDoS attack detection, explainable AI, Neural Networks, Stacking classifier, Boosting classifier