Detection of Ddos Attacks in Iot Networks Using Machine Learning Algorithms

ICETAS 2024 - 9th IEEE International Conference on Engineering Technologies and Applied Sciences • Conference Paper • 2024 • DOI: 10.1109/ICETAS62372.2024.11120083

Ahmed, Alwan [a] ✉ ; Shah, Asadullah [b] ✉ ; Abdullah, Alwan [c] ✉ ; Laghari, Shams Ul Arfeen [c] ✉ ; Alwan, Abdulrahman [a, c]

[a] Islamic University Malaysia Kuala, Abdulrahman Alwan Kulliyyah Information & Communications Technology, Lumpur, Malaysia

Show all information

0

Citations

View PDF Full text Export Save to list

Document Impact Cited by (0) References (20) Similar documents

Abstract

The rapid proliferation of Internet of Things (IoT) devices has revolutionized various industries by enabling seamless connectivity and data exchange. However, this connectivity also introduces significant security challenges, particularly in the form of Distributed Denial of Service (DDoS) attacks. These attacks can overwhelm IoT networks, leading to service disruptions and substantial financial losses. This paper presents a robust and efficient framework for detecting DDoS attacks in IoT networks using advanced machine learning techniques and effective feature selection methods. The study utilizes the CICIoT2023 dataset and employs Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA) to enhance the performance of machine learning models, including Random Forest, Support Vector Machine (SVM), Näive Bayes, XGBoost, and K-Nearest Neighbors (KNN). The models are trained and validated using k-fold cross-validation to ensure robustness and generalizability. Expected results indicate significant improvements in detection accuracy, precision, recall, and computational efficiency. The findings underscore the importance of feature selection in improving model performance and provide valuable insights into the strengths and weaknesses of different machine learning models. This research contributes to the development of scalable and effective DDoS detection solutions for IoT networks, ensuring their reliability and resilience against evolving cyber threats. Future work will focus on exploring additional feature selection methods, integrating deep learning techniques, and validating the models in real-world IoT environments. © 2024 IEEE.

Author keywords

Distributed Denial of Service (DDoS) attacks; Feature selection; Internet of Things (IoT); Machine learning

Indexed keywords

Engineering controlled terms

Classifiers; Computational efficiency; Deep learning; Electronic data interchange; Internet of things; Learning systems; Losses; Machine components; Nearest neighbor search; Network security; Principal component analysis; Random forests; Support vector machines

Engineering uncontrolled terms

DDoS Attack; Denialof- service attacks; Distributed denial of service; Distributed denial of service attack; Feature selection methods; Features selection; Internet of thing; IOT networks; Machine learning models; Machine-learning

Engineering main heading

Feature extraction

Abstract

Author keywords

Indexed keywords

Language

Customer Service