TechXplore 2K25 - Innovate. Exhibit. Inspire

29th August 2025

PREVENTION OF CYBER ATTACKS IN NETWORK INTRUSION DETECTION SYSTEM (NIDS) USING MACHINE LEARNING MODELS

**ABSTRACT**

**Purpose:**  
The growth of the Internet of Things (IoT) and Industrial IoT (IIoT) has increased system interconnectivity while exposing networks to advanced cyber threats. Traditional security mechanisms lack scalability in lightweight IoT environments, creating the need for efficient Network Intrusion Detection Systems (NIDS).

**Methodology:**  
This study utilizes the ToN-IoT dataset, consisting of telemetry data, operating system logs, and IoT network traffic, to design ML-based NIDS. Preprocessing and feature selection are performed using Extremely Randomized Trees to eliminate redundancy and enhance classification. Five machine learning models—Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Naïve Bayes (NB)—are implemented. Models are evaluated based on accuracy, precision, recall, F1-score, and computational efficiency.

**Results:**  
Random Forest demonstrates superior performance, achieving 90% accuracy with efficient training and testing times, while Naïve Bayes yields comparatively lower results. Tree-based algorithms outperform other models, highlighting their robustness in IoT security applications.

**Conclusion:**  
The findings confirm the effectiveness of ML-based NIDS for IoT security. However, dataset imbalance remains a challenge. Future work will explore deep learning methods and balancing techniques to enhance detection accuracy and resilience in dynamic IoT environments.

**Keywords:** Intrusion Detection, IoT Security, Machine Learning, ToN-IoT

|  |
| --- |
| **TEAM MEMBERS**  **1. CHELLA KRISHNAN D** |
| **Name of the Institution:SARANATHAN COLLEGE OF ENGINEERING** |
| **Department:CSE** |