0251IEEE | DOI: 10.1109/ICMLANT68509.2025.11394850

# Robust and Transparent IoT Anomaly Detection via Feature Selection and Explainable Machine Learning

Sanzida Sultana Rupai
Dept. of ICE
East West University
Dhaka, Bangladesh
sanzidasultanarupail850@gmail.com

Tamim Hasan Saykat*
Dept. of CSE
East West University
Dhaka, Bangladesh
muhammadtamim9083@gmail.com

Seendid Saleh Kabir
Dept. of CSE
East West University
Dhaka, Bangladesh
seendidsalehs@gmail.com

Md Abu Rafe Ruman
Dept. of ICE
East West University
Dhaka, Bangladesh
ruman2029bd@gmail.com

Apurbo Roy Chowdhury
Dept. of MPS
East West University
Dhaka, Bangladesh
apurbo.roy@ewubd.edu

**2025 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)**

**11-12 Dec. 2025, DOI: 10.1109/ICMLANT68509.2025**

**Abstract:**

Growing popularity of Internet of Things (IoT) and Internet of Medical Things (IoMT) devices has brought to the rise of major security issues as these systems that are interconnected are at risk. Anomaly detection plays an important role in safeguarding IoT networks against the diverse cyber threats, such as spoofing and data alteration attack. The proposed study introduces a complete model of machine learning of multi-class anomaly detection on the dataset WUSTL-EHMS-2020. This is done using a methodology that involves intensive preprocessing and feature selection of the data along Synthetic Minority Over-sampling Technique (SMOTE) to overcome the imbalance in the classes. Several different classifiers have been tested, and XGBoost has performed the best as it reached an accuracy of 99.96%, F1-score 0.9998 and Cohen Kappa 0.9997. The model also has good computational performance, it took 3.7-second training and 0.068 seconds to infer a single sample. In order to improve transparency and trust in the selective decisions made by the model, explainable AI approaches like SHAP and permutation importance were used. The suggested idea has a very good trade-off between accuracy, interpretability and computational cost, which makes it highly applicable to implement in the drastically constrained IoT systems.

**Index Terms**—IoT Intrusion, IoT Anomaly, IoT in Healthcare, IDS, Explainable AI.