CIC-IIoT-2025 Security Analysis

Machine Learning for Intrusion Detection in Industrial IoT

Alexis Le Trung, Yahya Ahachim, Rayan Drissi, Aniss Outaleb

ML Security – EPITA SCIA 2026

January 2026

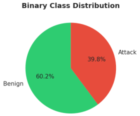
Agenda

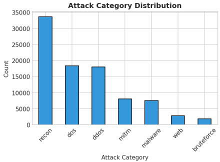
1. Dataset Overview and Exploration
2. Anomaly Detection (Unsupervised)
3. Classification (Supervised)
4. Adversarial Machine Learning
5. Recommendations

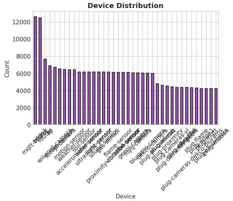
Objective: Evaluate ML methods for IIoT intrusion detection and assess adversarial robustness

CIC-IIoT-2025 Dataset

Attribute	Value
Total Samples	227,191
Features	94
Attack Samples	90,391 (39.8%)
Benign Samples	136,800 (60.2%)
Attack Categories	7







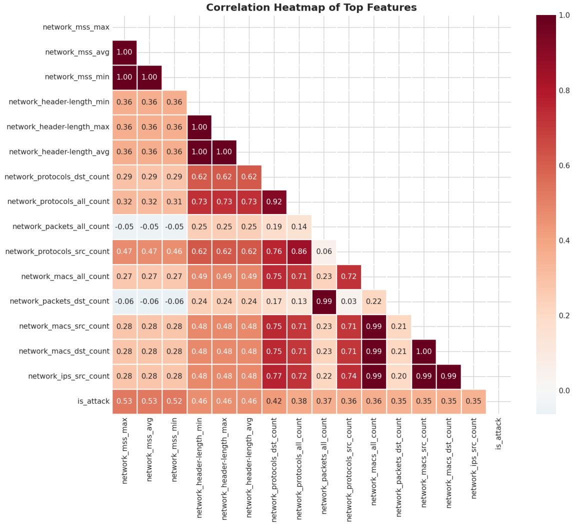
Categories: Reconnaissance, DoS, DDoS, MitM, Malware, Web, Brute Force

Key Discriminative Features

Top Correlated Features:

Feature	Corr.
network_mss_max	0.526
network_mss_avg	0.525
network_header-length_min	0.464
network_protocols_dst_count	0.423
network_packets_all_count	0.367

TCP MSS and protocol diversity are strong attack indicators



Anomaly Detection (Unsupervised)

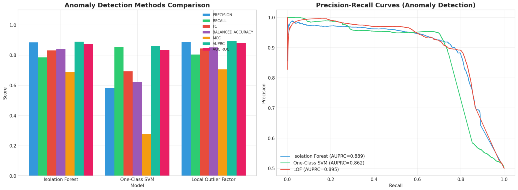
Trained on benign traffic only – Detects zero-day attacks

Method	Approach
Isolation Forest	Tree-based isolation via random partitioning
One-Class SVM	Kernel-based boundary in feature space
Local Outlier Factor	Local density deviation detection

Evaluation Metric: AUPRC (Area Under Precision-Recall Curve) – robust for imbalanced detection

Anomaly Detection Results

Model	F1	AUPRC	MCC
Isolation Forest	0.832	0.889	0.688
One-Class SVM	0.693	0.862	0.276
LOF	**0.844**	**0.895**	**0.705**



Winner: Local Outlier Factor

Density-based methods excel on this dataset

Classification (Supervised)

Using labeled attack and benign samples

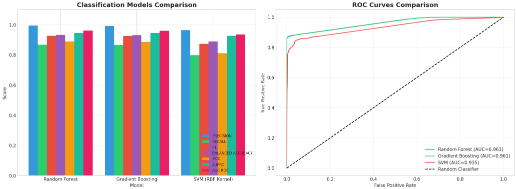
Method	Approach
Random Forest	Ensemble of decision trees with majority voting
Gradient Boosting	Sequential boosting with error correction
SVM (RBF Kernel)	Kernel-based non-linear separation

Terminology:

- **Astute Accuracy:** Performance on clean (non-adversarial) data
- **Robust Accuracy:** Performance under adversarial attack

Classification Results

Model	F1	MCC	AUC
Random Forest	**0.927**	**0.890**	**0.961**
Gradient Boosting	0.925	0.886	0.961
SVM (RBF)	0.874	0.811	0.935



Winner: Random Forest

All classifiers achieve >87% F1-score

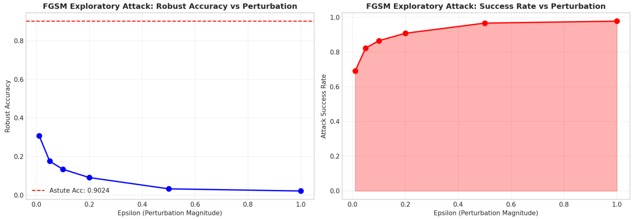
Adversarial ML: Exploratory Attack (FGSM)

Fast Gradient Sign Method – Perturbs test samples

$$x_{adv} = x + \epsilon \cdot \mathrm{sign}(\nabla_x J(\theta, x, y))$$

ϵ	**Robust Acc.**
0.01	86.7%
0.05	26.0%
0.10	16.0%
0.50	3.5%

Linear SVM (Astute: 89.8%)



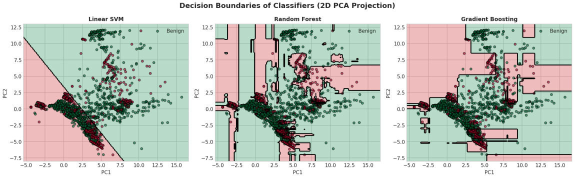
Adversarial ML: Causative Attack (Data Poisoning)

Label Flipping – Poisons training data to shift decision boundary

Attack Mechanism:

- Attacker corrupts training labels
- Model learns incorrect boundaries
- Attacks evade detection at inference

Poison Rate	Accuracy
0%	94.3%
10%	85.2%
20%	72.1%



Model Robustness Comparison ($\epsilon = 0.5$)

Model	**Astute Acc.**	**Robust Acc.**	**Robustness Ratio**
Linear SVM	90.2%	3.2%	3.6%
Random Forest	94.6%	3.8%	4.0%
Gradient Boosting	**94.4%**	**34.0%**	**36.0%**

Finding: Gradient Boosting retains 36% accuracy under FGSM attack
Linear models collapse to near-random performance

Summary: Best Models by Task

Task	**Best Model**	**Key Metric**
Zero-day Detection	Local Outlier Factor	$\text{F1} = 0.844$, $\text{AUPRC} = 0.895$
Attack Classification	Random Forest	$\text{F1} = 0.927$, $\text{AUPRC} = 0.946$
Adversarial Robustness	Gradient Boosting	36.0% robust acc.

Key Insight: No single model excels at all tasks – defense-in-depth required

Recommendations

Multi-Layer Defense Architecture:

1. **Layer 1 (LOF):** Zero-day attack early warning
2. **Layer 2 (Random Forest + Gradient Boosting):** Classification ensemble for accuracy and robustness
3. **Layer 3:** Input validation and adversarial training

Production Hardening:

- Implement adversarial training with augmented samples
- Regular model retraining with new threat intelligence
- Feature monitoring for distribution drift

Questions?

CIC-IIoT-2025 Security Analysis
Machine Learning for Intrusion Detection

ML Security – EPITA SCIA 2026