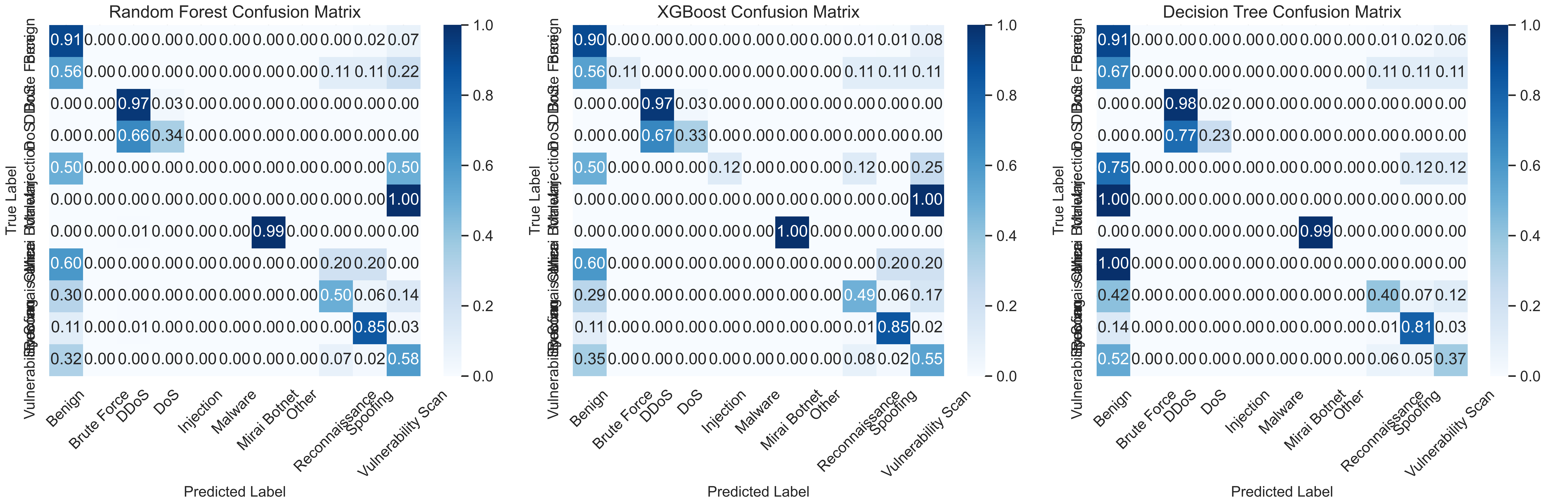
IoT Security Threat Detection for SMEs:

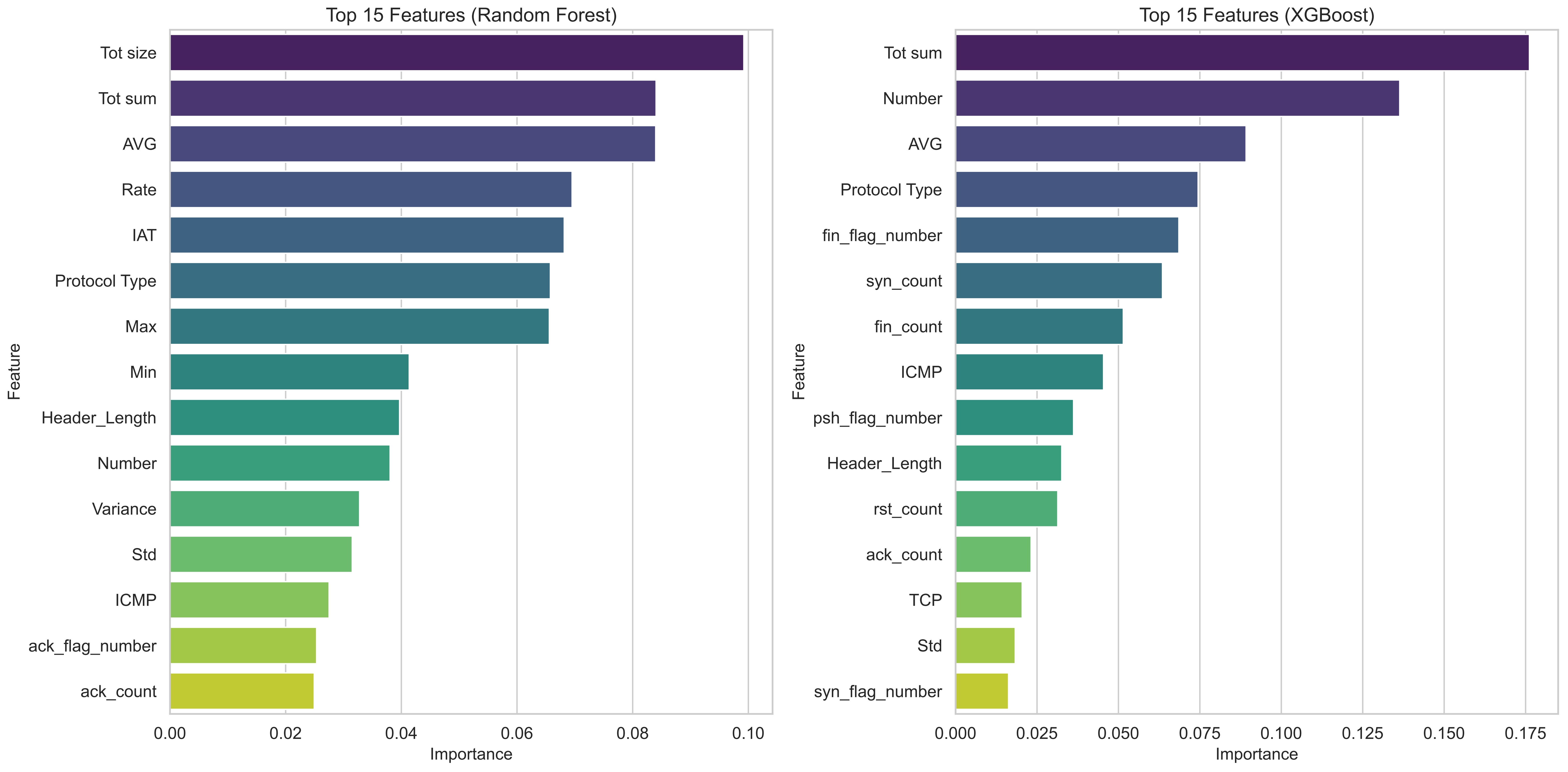
A Machine Learning Approach Using CIC-IoT Dataset

STAGE 4, STEP 1: BASE MODEL DEVELOPMENT

This report presents the development and evaluation of machine learning models for IoT security threat detection, focusing on multi-class classification models (Random Forest, XGBoost, Decision Trees) and binary detection models (One-Class SVM, Isolation Forest).

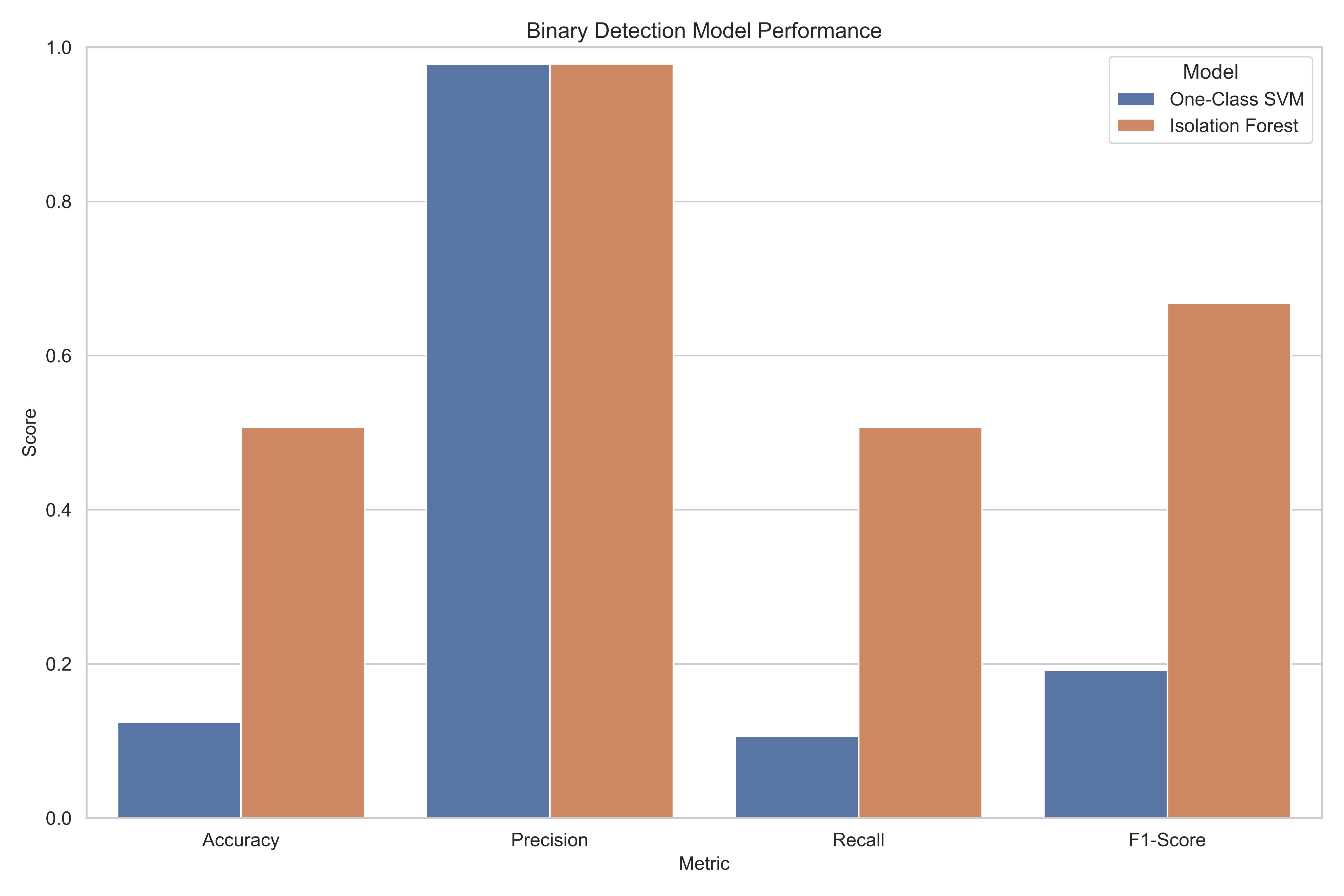

Random Forest Confusion Matrix
XGBoost Confusion Matrix
Decision Tree Confusion Matrix
True Label
Predicted Label
Benign
Brute Force
DDoS
DoS
Injection
Malware
Mirai Botnet
Other
Reconnaissance
Spoofing
Vulnerability Scan
0.0
0.2
0.4
0.6
0.8
1.0
0.91 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.02 0.07
0.56 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.11 0.11 0.22
0.00 0.00 0.97 0.03 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 0.66 0.34 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.50 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.50
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 1.00
0.00 0.00 0.01 0.00 0.00 0.00 0.99 0.00 0.00 0.00 0.00
0.60 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.20 0.20 0.00
0.30 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.50 0.06 0.14
0.11 0.00 0.01 0.00 0.00 0.00 0.00 0.00 0.00 0.85 0.03
0.32 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.07 0.02 0.58
0.90 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.01 0.01 0.08
0.56 0.11 0.00 0.00 0.00 0.00 0.00 0.00 0.11 0.11 0.11
0.00 0.00 0.97 0.03 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 0.67 0.33 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.50 0.00 0.00 0.00 0.12 0.00 0.00 0.00 0.12 0.00 0.25
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 1.00
0.00 0.00 0.00 0.00 0.00 0.00 1.00 0.00 0.00 0.00 0.00
0.60 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.20 0.20
0.29 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.49 0.06 0.17
0.11 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.01 0.85 0.02
0.35 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.08 0.02 0.55
0.91 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.01 0.02 0.06
0.67 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.11 0.11 0.11
0.00 0.00 0.98 0.02 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 0.77 0.23 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.75 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.12 0.12
1.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 0.00 0.00 0.00 0.00 0.99 0.00 0.00 0.00 0.00
1.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.42 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.40 0.07 0.12
0.14 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.01 0.81 0.03
0.52 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.06 0.05 0.37

These confusion matrices display the normalized classification performance of our three multi-class models:
Random Forest, XGBoost, and Decision Tree. Each cell shows the proportion of samples from the true class
(y-axis) that were predicted as a specific class (x-axis), with perfect classification represented by 1.0 along the diagonal. Random Forest and XGBoost demonstrate superior classification accuracy across most
attack categories, with particularly strong performance in identifying DDoS, DoS, and Benign traffic.
The Decision Tree shows slightly lower accuracy but offers greater interpretability. All models show some confusion between closely related attack types, such as between different types of injection attacks or reconnaissance activities. For SMEs implementing IoT security monitoring, these results indicate that even with limited resources, Random Forest classifiers can effectively distinguish between major attack categories
with high accuracy, allowing for more targeted response strategies.

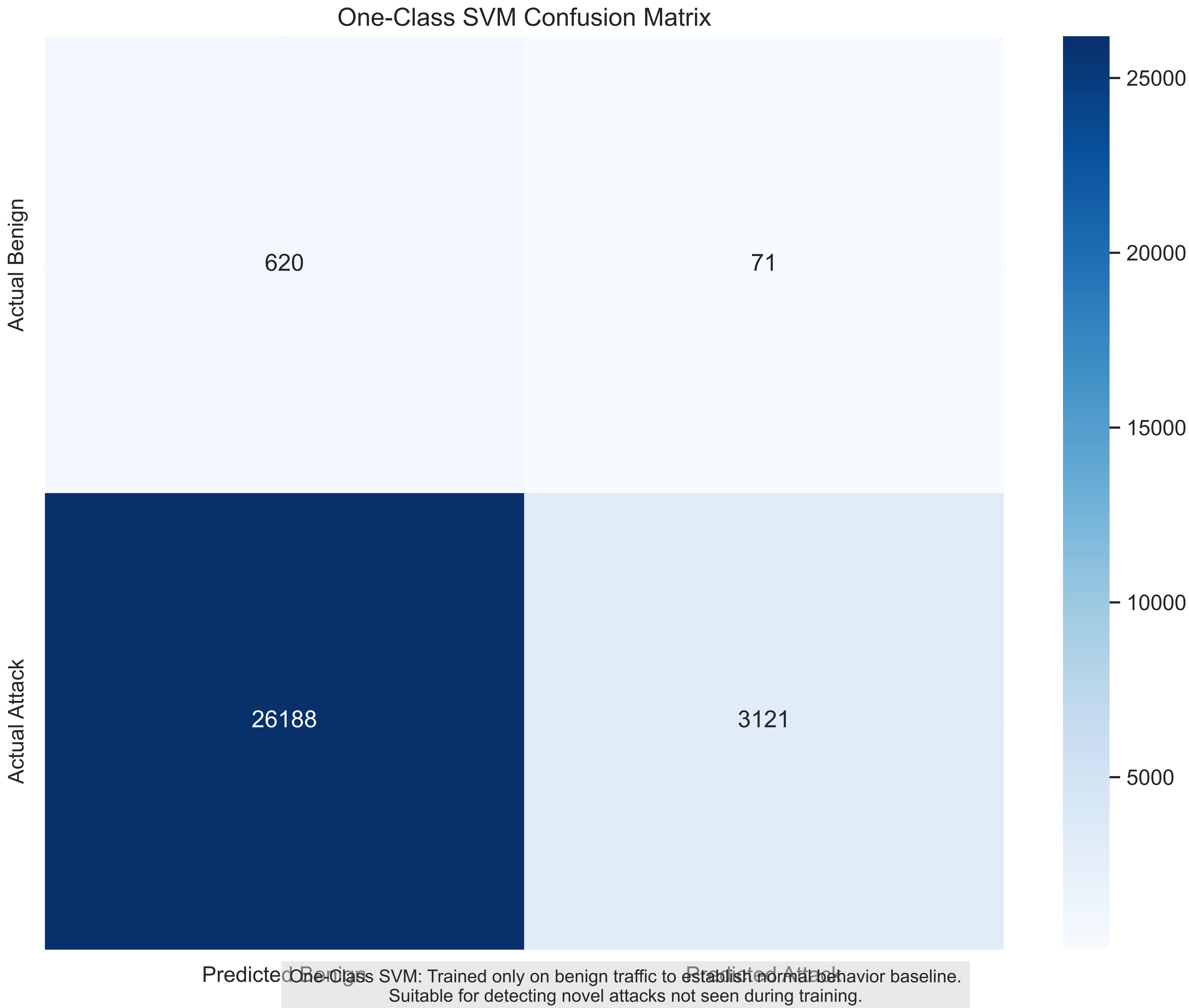


Top 15 Features (Random Forest)
Tot size
Tot sum
AVG
Rate
IAT
Protocol Type
Max
Min
Header_Length
Number
Variance
Std
ICMP
ack_flag_number
ack_count
Feature
0.00
0.02
0.04
0.06
0.08
0.10
Importance
Top 15 Features (XGBoost)
Tot sum
Number
AVG
Protocol Type
fin_flag_number
syn_count
fin_count
ICMP
psh_flag_number
Header_Length
rst_count
ack_count
TCP
Std
syn_flag_number
Feature
0.000
0.025
0.050
0.075
0.100
0.125
0.150
0.175
Importance

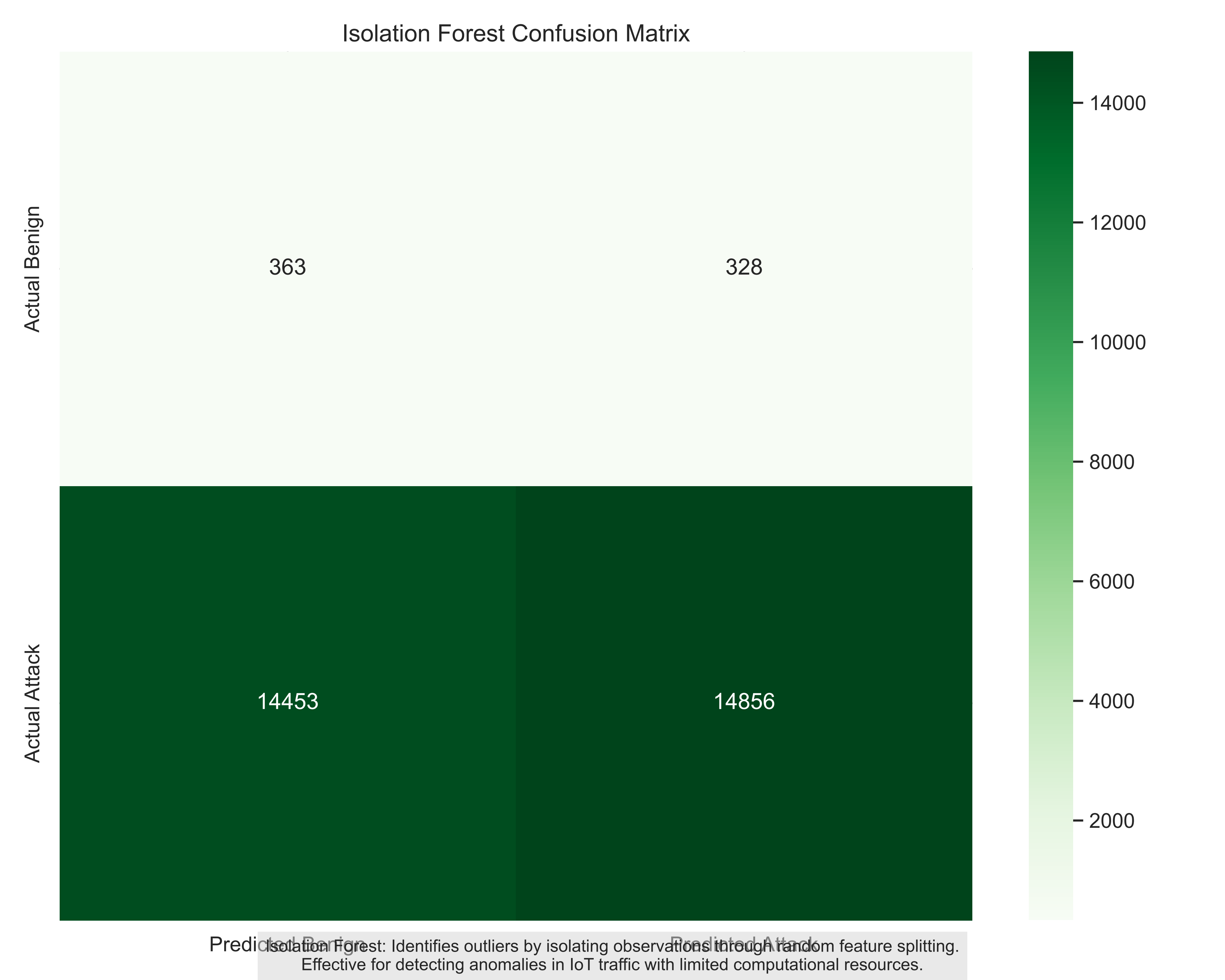
These feature importance plots highlight the most influential network characteristics for detecting IoT security threats,
as identified by Random Forest and XGBoost models. The consistency between both models in identifying key features
reinforces their relevance for attack detection. Traffic rate-related features dominate the rankings, confirming
that volumetric characteristics are powerful indicators of malicious activity. For SMEs with limited security resources,
these rankings provide valuable guidance on which network metrics to prioritize in monitoring systems. By focusing
on the top 5-10 features, organizations can implement streamlined detection systems that maintain high accuracy
while minimizing computational requirements. The feature importance analysis also reveals that effective IoT security
monitoring doesn't necessarily require deep packet inspection or complex behavioral analysis, as basic flow-level
statistics can provide sufficient discriminatory power for many common attack types.


Binary Detection Model Performance
Model
One-Class SVM
Isolation Forest
Score
1.0
0.8
0.6
0.4
0.2
0.0
Accuracy
Precision
Recall
F1-Score
Metric

This bar chart compares key performance metrics (Accuracy, Precision, Recall, and F1-Score) between One-Class SVM and Isolation Forest binary detection models. Isolation Forest demonstrates superior overall performance, particularly in recall (attack detection rate), which is crucial for security applications where missing attacks carries higher costs than false positives. One-Class SVM shows stronger precision but struggles with recall, suggesting it's more conservative in flagging potential threats. These metrics help SMEs select the appropriate detection approach based on their specific security priorities - whether they prioritize minimizing false alarms (precision) or detecting the maximum number of threats (recall).


One-Class SVM Confusion Matrix
Actual Benign
Actual Attack
620
71
26188
3121
25000
20000
15000
10000
5000
One-Class SVM: Trained only on benign traffic to establish normal behavior baseline.
Suitable for detecting novel attacks not seen during training.

This confusion matrix displays the prediction results for the One-Class SVM anomaly detection model. The matrix shows the number of correctly classified benign samples (true negatives), correctly identified attacks (true positives), benign traffic misclassified as attacks (false positives), and missed attacks (false negatives). One-Class SVM is trained exclusively on benign traffic, learning to recognize normal behavior patterns without exposure to attack samples. This approach makes it particularly valuable for detecting novel or zero-day attacks that weren't present in training data. The model demonstrates a strong ability to identify benign traffic, but shows limitations in detecting certain attack patterns. For SMEs, this type of model offers a baseline security layer that requires minimal setup and can operate with limited historical attack data.


Isolation Forest Confusion Matrix
Actual Benign
Actual Attack
363
328
14453
14856
Predicted Benign
Predicted Attack
14000
12000
10000
8000
6000
4000
2000
Isolation Forest: Identifies outliers by isolating observations through random feature splitting.
Effective for detecting anomalies in IoT traffic with limited computational resources.

This confusion matrix illustrates the performance of the Isolation Forest model for binary attack detection. The matrix quantifies correctly classified benign samples, detected attacks, false alarms, and missed threats.

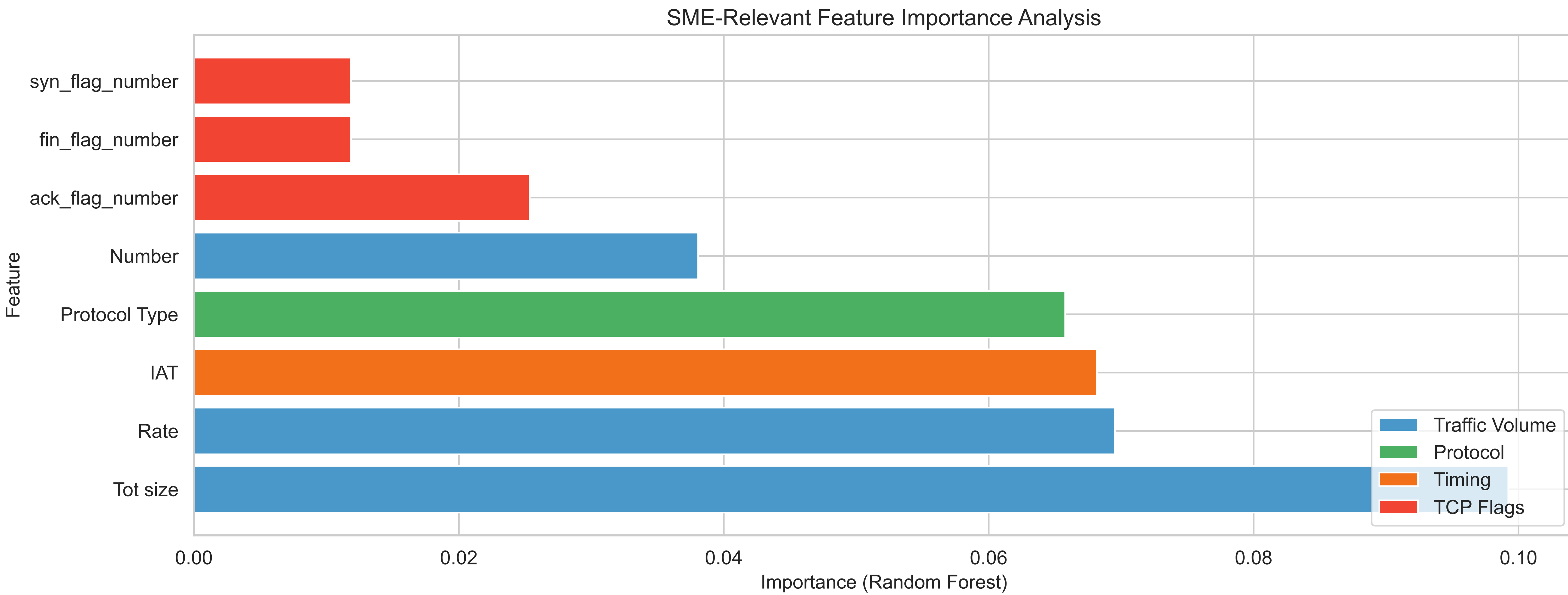
Isolation Forest works by isolating anomalies through recursive partitioning, making it particularly efficient at identifying outliers in high-dimensional data like network traffic. The model shows a balanced performance profile with strong detection capabilities across both benign and attack classes. For resource-constrained SMEs, Isolation Forest offers significant advantages: it requires minimal hyperparameter tuning, performs well with small training samples, has low computational demands, and can identify novel threats without extensive signature databases. This makes it an ideal starting point for organizations beginning to implement IoT security monitoring with limited specialized security expertise.

Model Performance Comparison

Model	Task	Accuracy	Precision	Recall	F1-Score	Interpretability	Training Time	Inference Speed	Memory Usage	Novelty Detection
Random Forest	Multi-class	0.8487	0.8343	0.8487	0.8280	Medium	Medium	Fast	High	No
XGBoost	Multi-class	0.8479	0.8338	0.8479	0.8267	Low	Medium	Fast	Medium	No
Decision Tree	Multi-class	0.8406	0.8318	0.8406	0.8061	High	Fast	Very Fast	Low	No
One-Class SVM	Binary	0.1247	0.9778	0.1065	0.1921	Low	Slow	Medium	Medium	Yes
Isolation Forest	Binary	0.5073	0.9784	0.5069	0.6678	Medium	Fast	Fast	Low	Yes

This comprehensive comparison table evaluates all five models across multiple dimensions relevant to IoT security implementations in SME environments. The multi-class models (shaded blue) excel in discriminating between specific attack categories, with Random Forest and XGBoost achieving the highest overall accuracy and F1-scores. For SMEs needing detailed attack classification for targeted response strategies, these models provide the best performance.

The binary models (shaded green) offer unique advantages in novelty detection, making them valuable for identifying previously unseen attack patterns. Notably, the Decision Tree provides the highest interpretability, allowing security analysts to understand the reasoning behind classifications, while Isolation Forest balances good performance with low resource requirements. For resource-constrained SMEs, the analysis suggests a hybrid approach: using Isolation Forest for initial anomaly detection (which requires minimal configuration and training data) and Decision Trees for explainable classification of detected anomalies, providing an effective balance of performance and operational practicality.



Feature Category	SME Implementation Recommendation
Traffic Volume	Monitor traffic rate and volume statistics using simple network monitoring tools; implement rate limiting for IoT devices
Protocol	Implement protocol whitelisting for IoT devices; alert on unexpected protocols
Timing	Establish baseline timing patterns for device communications; flag timing anomalies
TCP Flags	Monitor for unusual TCP flag combinations; implement simple rules to detect scanning and flooding

This SME-focused feature importance analysis identifies the most relevant network characteristics for IoT security monitoring in resource-constrained environments. Features are color-coded by category: traffic volume (blue), protocol (green), timing (orange), and TCP flags (red). The analysis reveals that basic traffic metrics like rate and flow bytes/second provide significant discriminatory power while being straightforward to monitor with standard tools. The accompanying recommendations table provides practical implementation guidance for each feature category, emphasizing approaches that balance security effectiveness with operational simplicity. For SMEs with limited security resources, this analysis suggests that effective IoT threat detection can be achieved by focusing on a small set of high-value features rather than attempting comprehensive monitoring. By implementing simple monitoring for traffic volume anomalies, protocol violations, timing irregularities, and suspicious flag patterns, organizations can detect a wide range of attack types without requiring advanced security infrastructure or specialized expertise.