IoT Security Threat Detection for SMEs:

A Machine Learning Approach Using CIC-IoT Dataset

Research Study Report

April 22, 2025

Dept of Computer Science and Engineering (AI & ML)

Abstract

This research study addresses the critical cybersecurity challenges faced by Small and Medium-sized Enterprises (SMEs) in protecting their Internet of Things (IoT) deployments. As SMEs increasingly adopt IoT technologies to enhance operational efficiency and customer experience, they become vulnerable to a range of security threats while typically lacking the resources for enterprise-grade security solutions.

Using the comprehensive CIC-IoT-2023 dataset, which contains network traffic from various IoT devices under normal conditions and multiple attack scenarios, this study develops and evaluates machine learning approaches specifically optimized for SME environments. The research focuses on balancing detection accuracy with computational efficiency to create practical security solutions that can be implemented within the resource constraints typical of smaller organizations.

The study progresses through seven stages, from preliminary data assessment to final recommendations, with a particular emphasis on identifying critical security metrics, developing lightweight detection models, and creating implementation frameworks tailored to different SME scenarios. Visualizations and analytical tools are extensively employed to extract actionable insights from complex network data patterns.

The expected outcomes include a tiered detection framework that SMEs can implement based on their available resources, a set of optimized machine learning models for different attack types, and practical deployment guidelines that consider the unique operational contexts of smaller businesses. This research aims to bridge the security capability gap for SMEs in the expanding IoT landscape.

1. Introduction

The proliferation of Internet of Things (IoT) devices across business environments has created unprecedented opportunities for operational optimization and innovation. Small and Medium-sized Enterprises (SMEs) have been quick to adopt these technologies, implementing everything from smart environmental controls to inventory tracking systems. However, this rapid adoption has introduced significant security vulnerabilities that many SMEs are ill-equipped to address.

Unlike larger enterprises with dedicated cybersecurity teams and substantial IT budgets, SMEs typically operate with limited technical resources and expertise. This creates a security capability gap where the organizations can afford to deploy IoT solutions but struggle to properly secure them against the increasingly sophisticated threat landscape.

The security challenges are further complicated by the diversity of IoT devices, each with different firmware, communication protocols, and security features. This heterogeneity makes traditional security approaches less effective, while the high volume of network traffic generated by these devices creates substantial noise in which malicious activities can hide.

This research focuses specifically on addressing these challenges through machine learning approaches that can detect security threats in IoT deployments within SME contexts. By analyzing network traffic patterns from the CIC-IoT-2023 dataset, we develop models that can identify various attack types including Distributed Denial of Service (DDoS), reconnaissance activities, and spoofing attacks.

The significance of this work lies in its practical orientation toward SME needs, emphasizing solutions that balance security effectiveness with implementation feasibility. Rather than proposing theoretical approaches that require enterprise-grade resources, we focus on developing detection frameworks that can be incrementally deployed with modest computational requirements.

2. Research Objectives

This study aims to achieve the following research objectives:

1. Identify and characterize the most relevant security threats to IoT deployments in SME environments through analysis of the CIC-IoT-2023 dataset.

2. Determine the critical network traffic metrics that most effectively indicate different types of attacks while minimizing false positives in IoT contexts.

3. Develop machine learning models optimized for SME resource constraints that can detect multiple attack types with high accuracy.

4. Create a tiered implementation framework that allows SMEs to deploy security monitoring based on their available resources and critical assets.

5. Establish practical guidelines for model selection, feature prioritization, and alert handling tailored to the operational realities of smaller organizations.

6. Evaluate the performance of different detection approaches not only in terms of traditional metrics (accuracy, precision, recall) but also in terms of computational efficiency and implementation complexity.

7. Provide recommendations for future enhancements that can adapt to evolving threats without requiring complete system redesigns.

These objectives guide our research methodology and analytical approach throughout all stages of the study, ensuring that the outcomes remain focused on addressing the specific security needs of SMEs rather than proposing general cybersecurity solutions.