IoT Security Threat Detection for SMEs:

A Machine Learning Approach Using CIC-IoT Dataset

STAGE 1, STEP 2: SME CONTEXT DEFINITION

This report defines hypothetical Small and Medium Enterprise (SME) scenarios,
outlines typical IoT device deployments, maps dataset devices to SME-relevant equivalents,
and establishes relevant security metrics for these environments.

Hypothetical SME Scenarios for IoT Security Analysis

Retail SME

Small to medium retail business with physical storefront and online presence

- 10-50 employees
- 1-5 store locations
- Inventory tracking and management
- Point-of-sale systems
- Customer analytics
- Environmental controls
- Security systems
- Digital signage

Smart Office SME

Small to medium professional services business with smart office setup

- 20-100 employees
- Office automation systems
- Meeting room booking systems
- Access control systems
- HVAC and lighting controls
- Employee presence tracking
- Asset tracking
- Security cameras

This figure outlines two hypothetical Small and Medium Enterprise (SME) scenarios for our IoT security threat analysis.
The first scenario is a Retail SME, which represents businesses like specialty shops, boutiques, or small retail chains
with both physical and online presences. These businesses typically deploy IoT devices for inventory tracking, point-of-sale
systems, environmental monitoring, and security. The second scenario is a Smart Office SME, representing professional
services businesses like law firms, marketing agencies, or small tech companies that utilize IoT for office automation,
meeting room management, access control, and environmental systems. These scenarios were selected to represent common
SME environments where IoT devices play increasingly important roles in day-to-day operations, but where cybersecurity
expertise may be limited compared to larger enterprises.

IoT Device Deployment in Retail SME

Device Type	Typical Quantity	Connectivity	Data Sensitivity
Smart POS Terminals	2-10	Wi-Fi, Ethernet	High
Inventory Scanners	5-20	Wi-Fi, Bluetooth	Medium
Smart Cameras	5-15	Wi-Fi, Ethernet	High
Digital Signage	3-12	Wi-Fi, Ethernet	Low
Environmental Sensors	10-30	Wi-Fi, Zigbee	Low
Smart Lighting	20-50	Wi-Fi, Zigbee	Low
Customer Counters	2-8	Wi-Fi	Medium
RFID Readers	2-8	Wi-Fi, Ethernet	Medium

This table illustrates the typical IoT device deployment in a retail sme environment. The devices are categorized by type, showing their typical quantity in such environments, connectivity methods, and data sensitivity levels. Data sensitivity is classified as High (containing personal, financial, or access control data), Medium (operational or business data), or Low (environmental or non-critical data). This deployment model represents common IoT infrastructure that small and medium businesses implement to enhance operational efficiency. The diversity of devices, connectivity methods, and varying sensitivity levels creates a complex security landscape that requires careful consideration. Understanding this deployment model is crucial for mapping appropriate security controls and threat detection mechanisms relevant to SME operations.

IoT Device Deployment in Smart Office SME

Device Type	Typical Quantity	Connectivity	Data Sensitivity
Smart Access Controls	5-15	Wi-Fi, Ethernet	High
Room Occupancy Sensors	10-50	Wi-Fi, Zigbee	Medium
Smart Cameras	5-20	Wi-Fi, Ethernet	High
Smart Thermostats	5-15	Wi-Fi, Zigbee	Low
Smart Lighting	30-100	Wi-Fi, Zigbee	Low
Meeting Room Displays	5-20	Wi-Fi, Ethernet	Medium
Asset Trackers	20-100	Bluetooth, Wi-Fi	Medium
Smart Printers/Scanners	3-10	Wi-Fi, Ethernet	Medium

This table illustrates the typical IoT device deployment in a smart office sme environment. The devices are categorized by type, showing their typical quantity in such environments, connectivity methods, and data sensitivity levels. Data sensitivity is classified as High (containing personal, financial, or access control data), Medium (operational or business data), or Low (environmental or non-critical data). This deployment model represents common IoT infrastructure that small and medium businesses implement to enhance operational efficiency. The diversity of devices, connectivity methods, and varying sensitivity levels creates a complex security landscape that requires careful consideration. Understanding this deployment model is crucial for mapping appropriate security controls and threat detection mechanisms relevant to SME operations.

Mapping CIC-IoT Dataset Devices to SME-Relevant Equivalents

CIC Dataset Device	SME Equivalent	Attack Relevance	Notes
IP Camera	Security Cameras	High	Vulnerable to DDoS, credential attacks, firmware exp
Smart Refrigerator	Smart Environmental Controls	Medium	Can be leveraged for DDoS, less critical data
Motion Sensor	Room Occupancy Sensors	Medium	Privacy concerns, tampering can affect security syste
Smart Thermostat	Smart Thermostats (HVAC Control)	Medium	Environmental control disruption, lateral movement ve
Smart Light Bulb	Smart Lighting Systems	Low	Potential for DDoS participation, low data sensitivit
Smart Door Lock	Access Control Systems	Very High	Critical security impact, unauthorized access risk
Generic IoT Gateway	IoT Network Infrastructure	Very High	Compromise affects all connected devices, central contr
Weather Station	Environmental Sensors	Low	Limited security impact, primarily DDoS risk

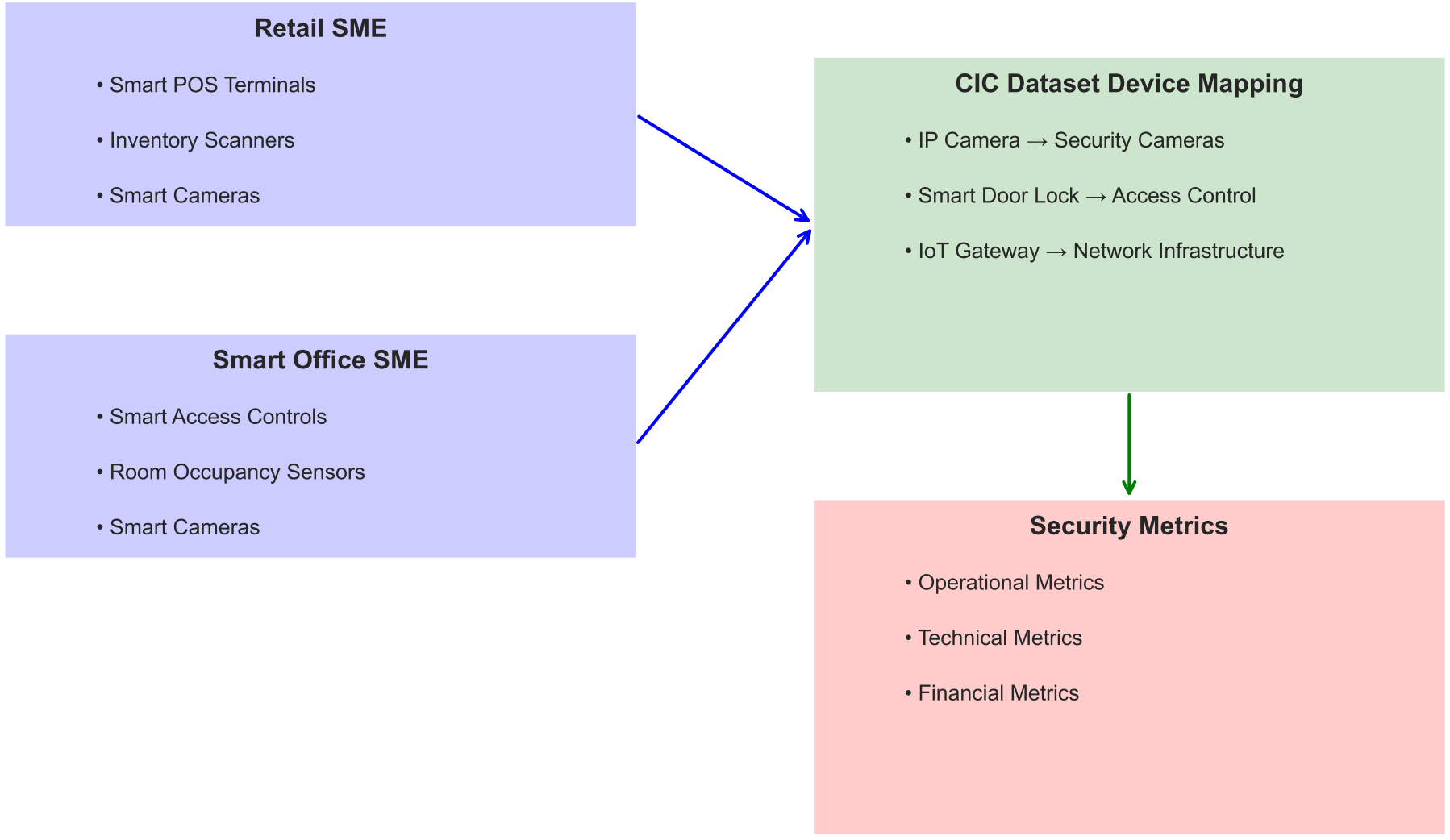
This mapping table shows how devices in the CIC-IoT dataset correspond to equivalent devices typically found in SME environments. The "Attack Relevance" column indicates the potential security impact if these devices are compromised, with corresponding color-coding (darker red indicating higher risk). For example, IP cameras in the dataset are equivalent to security cameras in SMEs, with high attack relevance due to their potential for privacy breaches and use as entry points into the network. Similarly, smart door locks correspond to access control systems with very high relevance due to their direct impact on physical security. This mapping helps translate the dataset's attack patterns to real-world SME scenarios, enabling more targeted and relevant security controls. Understanding which devices carry the highest security risks allows SMEs to prioritize their security investments and monitoring efforts accordingly.

Security Metrics Relevant to SME IoT Deployments

Category	Metric	Description	SME Relevance
Operational			
	Device Availability	Percentage of time IoT devices are operational and responsive	Critical for business continuity, especially for POS and security system
	Incident Response Time	Time taken to detect and respond to security incidents	Directly impacts potential damage from attacks; critical for SMEs with
	Service Degradation	Reduction in performance or functionality due to attacks	Affects customer experience in retail and employee productivity in offi
Technical			
	Anomalous Traffic Rate	Percentage of network traffic flagged as anomalous	Early indicator of potential attacks; helps prioritize investigation efforts
	Authentication Failures	Rate of failed login attempts to IoT devices/systems	Potential indicator of brute force attacks; critical for access control sys
	Network Segmentation Effectivene	Degree to which compromised devices can access critical systems	Limits lateral movement and attack scope; essential for SMEs with mi
Financial			
	Security Cost per Device	Security expenditure normalized by number of devices	Helps SMEs optimize security investments with limited budgets.
	Potential Revenue Impact	Estimated financial impact of IoT security incidents	Translates technical metrics to business impact; critical for security inv

This table defines key security metrics relevant to IoT deployments in SME environments, organized into three categories: Operational, Technical, and Financial. Operational metrics focus on business continuity and service delivery, such as device availability and incident response time, which directly impact customer and employee experience. Technical metrics provide specific indicators for security monitoring and threat detection, such as anomalous traffic rates and authentication failures, which are particularly relevant given the limited security expertise in most SMEs. Financial metrics translate security concerns into business terms, helping SME decision-makers understand the return on security investments and potential
risks. These metrics provide a comprehensive framework for SMEs to assess their IoT security posture in business-relevant terms, rather than purely technical indicators that may be difficult for non-specialists to interpret and act upon.

Integrated Framework for SME IoT Security Analysis



This diagram presents an integrated framework for IoT security analysis in SME environments, illustrating the relationships between our defined SME scenarios (retail and smart office), the IoT device mappings from the CIC dataset, and the security metrics established for monitoring and assessment. The framework shows how
our analysis flows from understanding the specific SME deployment scenarios to mapping the relevant devices
from our dataset, and finally to establishing appropriate security metrics for those environments. This integrated approach ensures that our security analysis remains relevant to real-world SME contexts, focusing on the devices and metrics that matter most in these environments. For security practitioners in SMEs, this framework provides a structured way to think about IoT security, connecting technical details from the dataset

to business-relevant contexts and metrics that can guide security investments and monitoring efforts.