Analyzing IoT Vulnerabilities

A Longitudinal Study of CVE Disclosures and Exploitability Trends

Stephen Mujeye, SHSU

Introduction

- IoT devices have expanded across sectors, increasing security risks (Kumar & Fung, 2024)
- Common issues: weak authentication, poor encryption, delayed patches (Bonaventura et al., 2025)
- Focus: CVE trends, exploitability, and machine learning classification (Khanmohammadi & Khoury, 2022)

Overview

The proliferation of IoT devices has introduced major cybersecurity challenges due to weak authentication, poor encryption, and delayed patching.

This study analyzes IoT vulnerability trends, time-to-exploitation, and develops a framework for automated vulnerability classification using statistical and machine learning approaches.

The Role of CVE in IoT Security

The Common Vulnerabilities and Exposures (CVE) framework plays a critical role in documenting security weaknesses across IoT ecosystems.

CVE assigns unique identifiers to vulnerabilities.

- These IDs standardize tracking, communication, and remediation.

- Organizations use CVEs to prioritize and coordinate security responses.

What the Literature Reveals About CVEs

- CVE records often lack critical metadata.

- This gap leads to delays in security assessments and patch deployment.

- Metadata deficiencies impact vulnerability prioritization.

(Khanmohammadi & Khoury, 2022)

Manual Processes and CNA Variability

Manual vulnerability disclosure and remediation introduce inconsistencies.

CVE Numbering Authorities (CNAs) differ in response times and coordination.

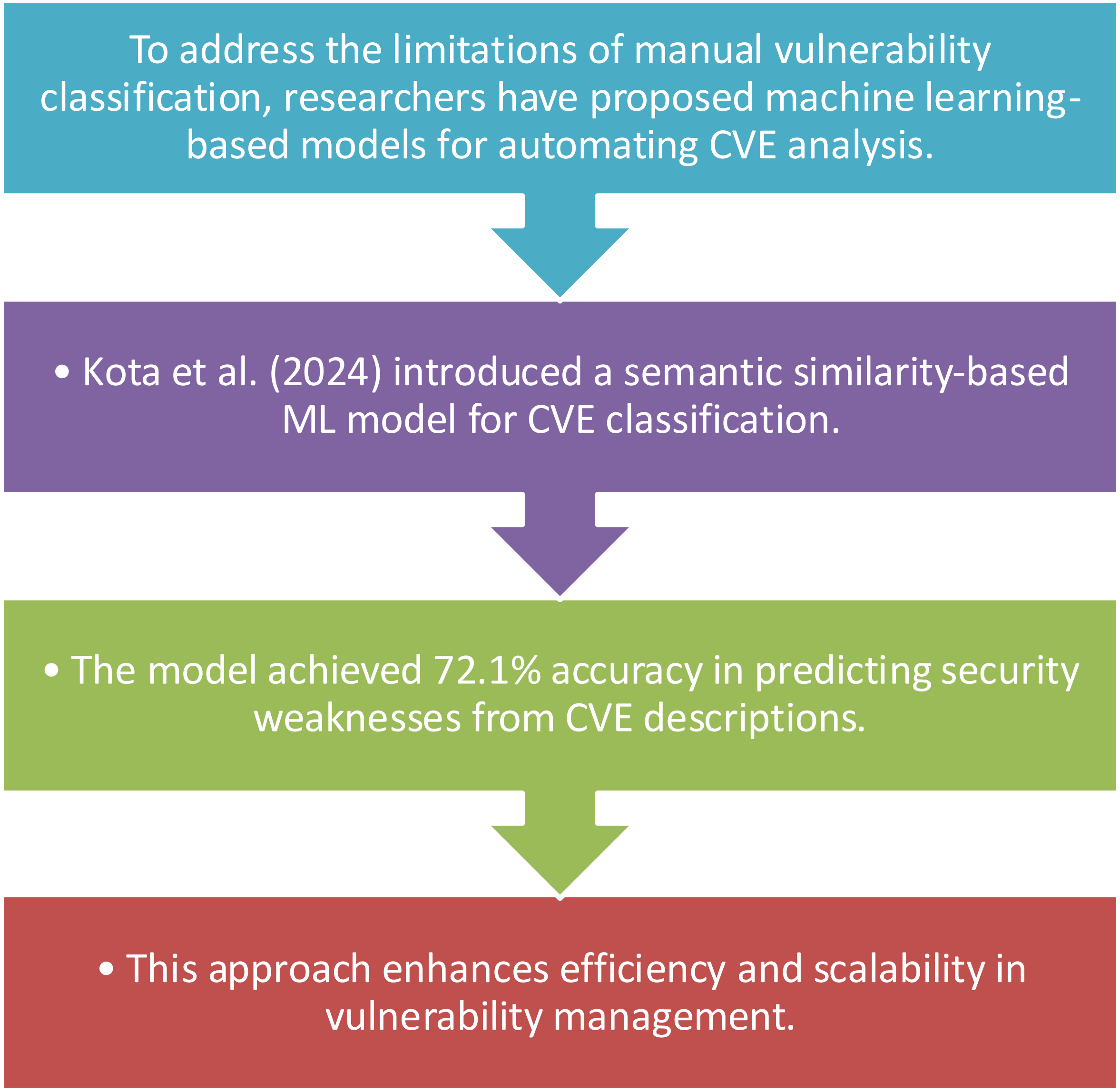
This variability complicates global vulnerability management.

(Lin et al., 2023)

Rapid Exploitation and Need for CVD

- Attackers often exploit newly disclosed vulnerabilities within days.
- Speed of exploitation highlights the need for timely response.
- Strengthening Coordinated Vulnerability Disclosure (CVD) frameworks is essential.
- (Pauley et al., 2023)

ML for CVE Classification



To address the limitations of manual vulnerability classification, researchers have proposed machine learning-based models for automating CVE analysis.

- Kota et al. (2024) introduced a semantic similarity-based ML model for CVE classification.

- The model achieved 72.1% accuracy in predicting security weaknesses from CVE descriptions.

- This approach enhances efficiency and scalability in vulnerability management.

Aim of the Study

Analyze the evolution of IoT vulnerabilities, with a focus on:

Tracking and classification of vulnerabilities.

Identifying effective mitigation strategies.

Investigating the time gap between CVE disclosure and real-world exploitation.

Assessing trends in vulnerability severity and exploitability.

Classifying IoT security risks by device category: Consumer, Industrial, and Healthcare IoT.

Research Questions

RQ1: How have IoT-related vulnerability disclosures, severity ratings, and exploitability patterns evolved over the past decade based on National Vulnerability Database (NVD) data?

RQ2: How accurately can supervised learning models (e.g., SVM and BERT-based NLP models) predict the likelihood of exploitability and automate the categorization of IoT vulnerabilities?

RQ3: How do threat intelligence feeds (e.g., CISA KEV, VirusTotal, IBM X-Force Exchange) contribute to tracking the progression of IoT vulnerabilities from disclosure to real-world exploitation?

RQ4: What is the average time between IoT vulnerability disclosure and the first recorded exploitation attempt, and how do different vulnerability repositories (e.g., Exploit-DB, Metasploit, Shodan, AttackerKB) contribute to monitoring this timeline?

Research Objectives

- Analyze IoT vulnerability trends (2015–2025)
- Assess disclosure-to-exploitation time gaps
- Identify high-risk IoT categories
- Develop ML-based framework for exploitability prediction

Data Sources

- National Vulnerability Database (NVD)
- CISA KEV Catalog
- CVSS, CWE, CPE datasets
- Future: VirusTotal, IBM X-Force Exchange

Methodology Overview

- Automated NVD pipeline (`nvd_iot_pipeline.py`)
- IoT identification via keyword/vendor heuristics
- Statistical analysis using GLM and MLM
- Cross-referenced with KEV exploit data

IoT Vulnerability Share (2015–2025)

IoT CVEs account for ~18% of all CVEs (≈44,569 of 247,189).

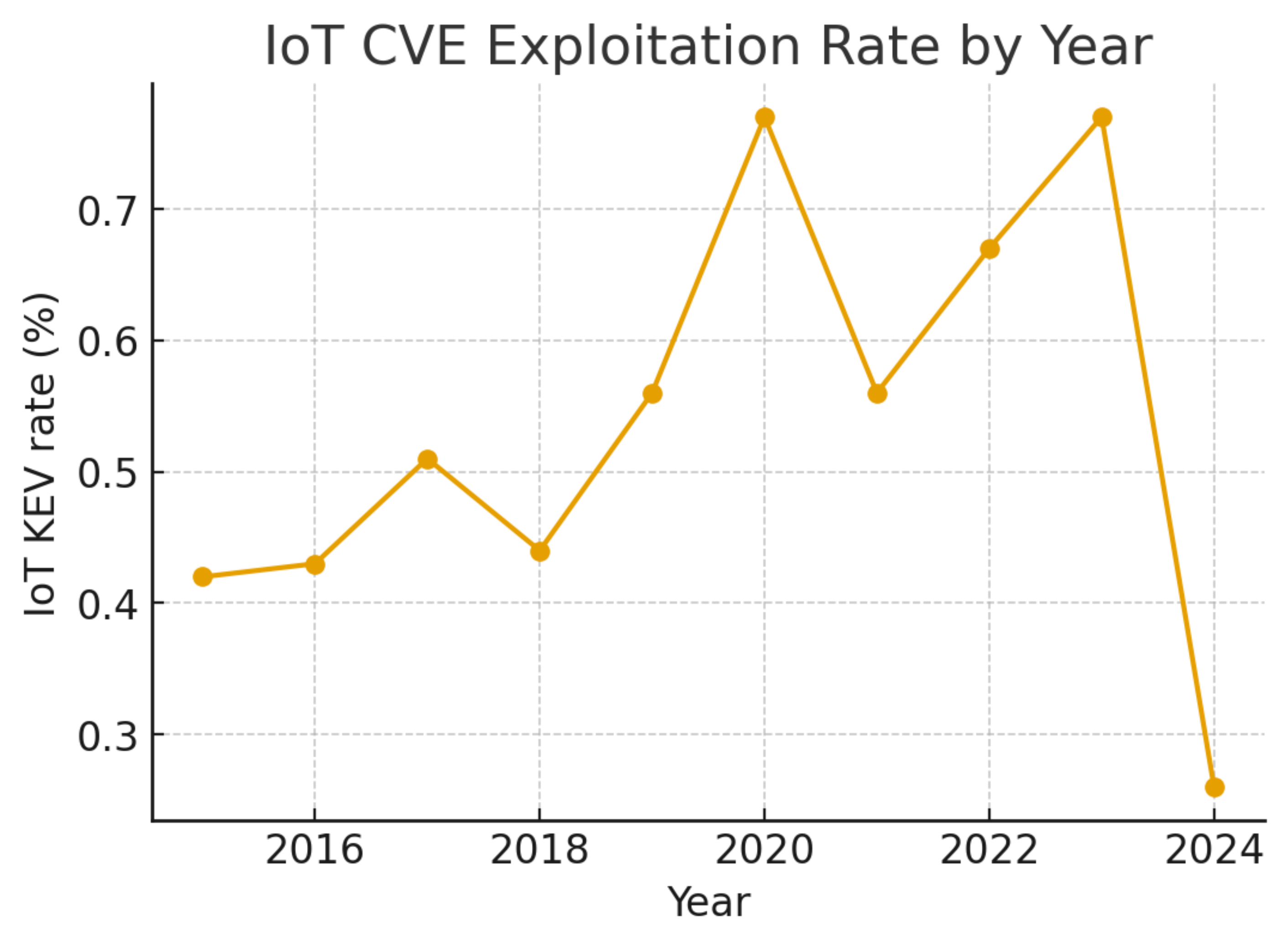
Exploitation Rates by Year (All CVEs)

- Exploitation rates remain below 0.2% overall but show spikes in 2020–2023.

IoT Exploitation by Year

- IoT exploitation 5–10× higher than general CVEs, peaking at 0.77% in 2020 and 2023.

Year	Total IoT CVEs	Exploited (KEV)	Exploitation Rate (%)
2015.0	713.0	3.0	0.42
2016.0	706.0	3.0	0.43
2017.0	5143.0	26.0	0.51
2018.0	3639.0	16.0	0.44
2019.0	3714.0	21.0	0.56
2020.0	3643.0	28.0	0.77
2021.0	4444.0	25.0	0.56
2022.0	3713.0	25.0	0.67
2023.0	4011.0	31.0	0.77
2024.0	7042.0	18.0	0.26


IoT CVE Exploitation Rate by Year
IoT KEV rate (%)
0.7
0.6
0.5
0.4
0.3
2016
2018
2020
2022
2024
Year

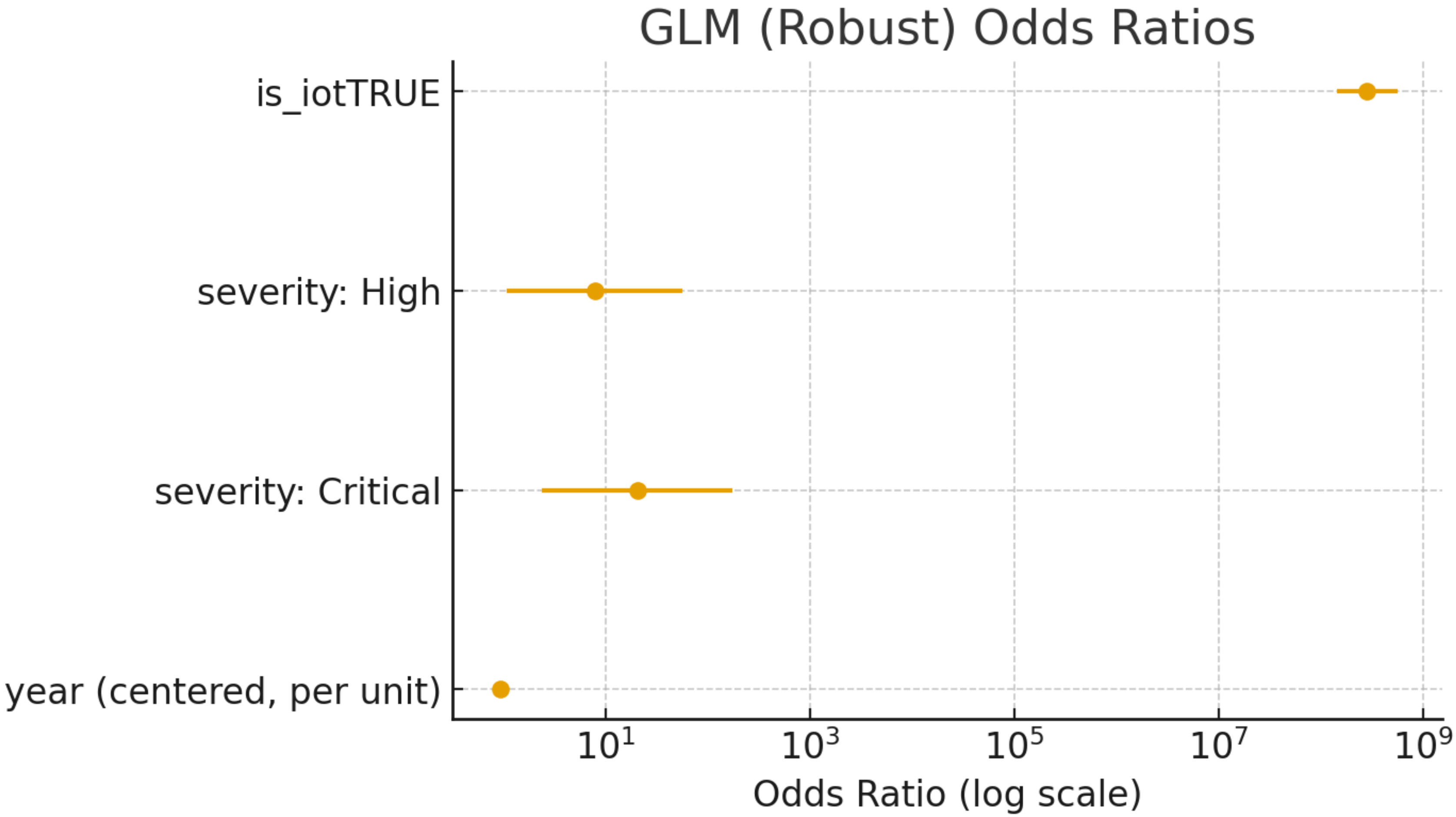
GLM Statistical Results

IoT (TRUE): OR ≈ 2.8×10^{8} (p<0.001)

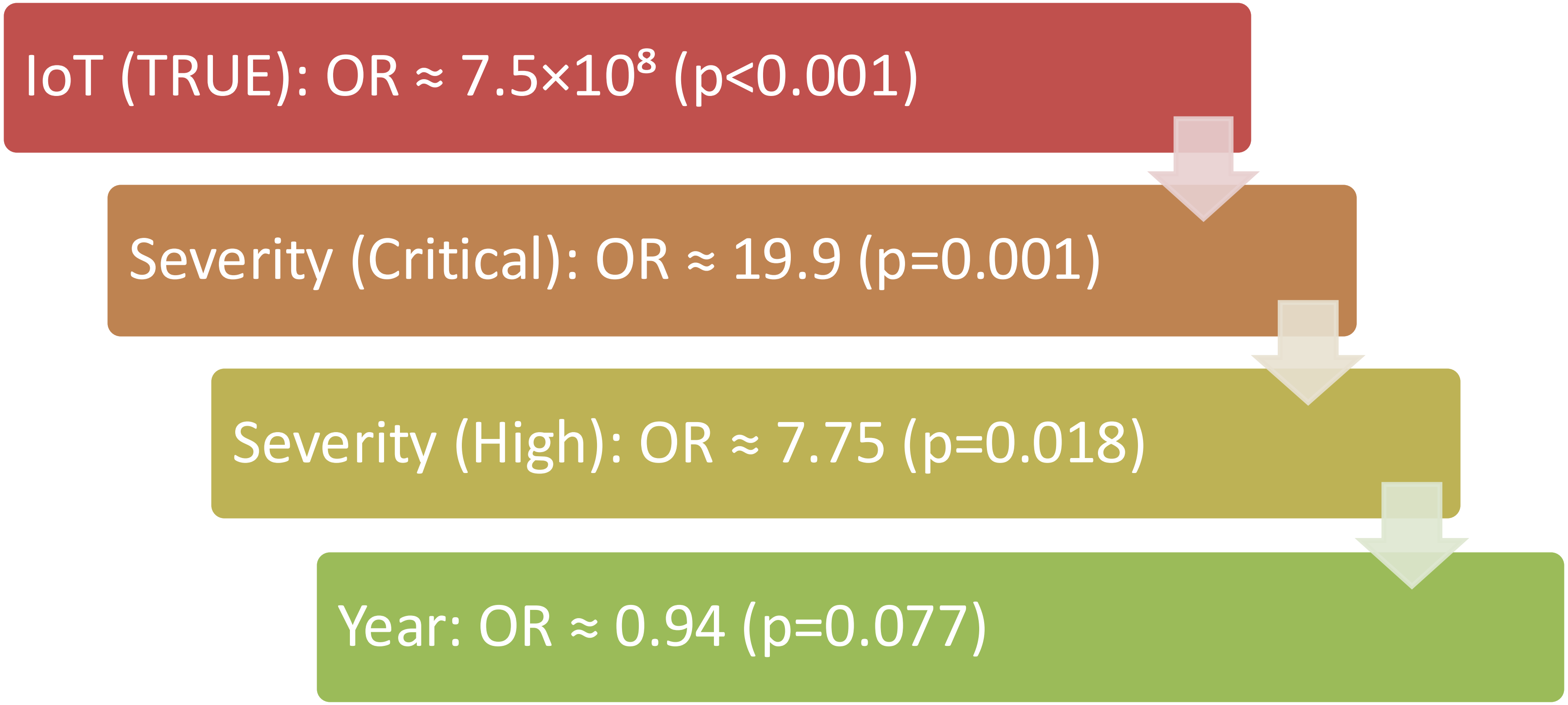
Severity (Critical): OR ≈ 20.3 (p=0.006)

Severity (High): OR ≈ 7.75 (p=0.042)

Year: OR ≈ 0.93 (p≈0.05)


GLM (Robust) Odds Ratios
is_iotTRUE
severity: High
severity: Critical
year (centered, per unit)
10^1
10^3
10^5
10^7
10^9
Odds Ratio (log scale)

Mixed-Effects (MLM) Results

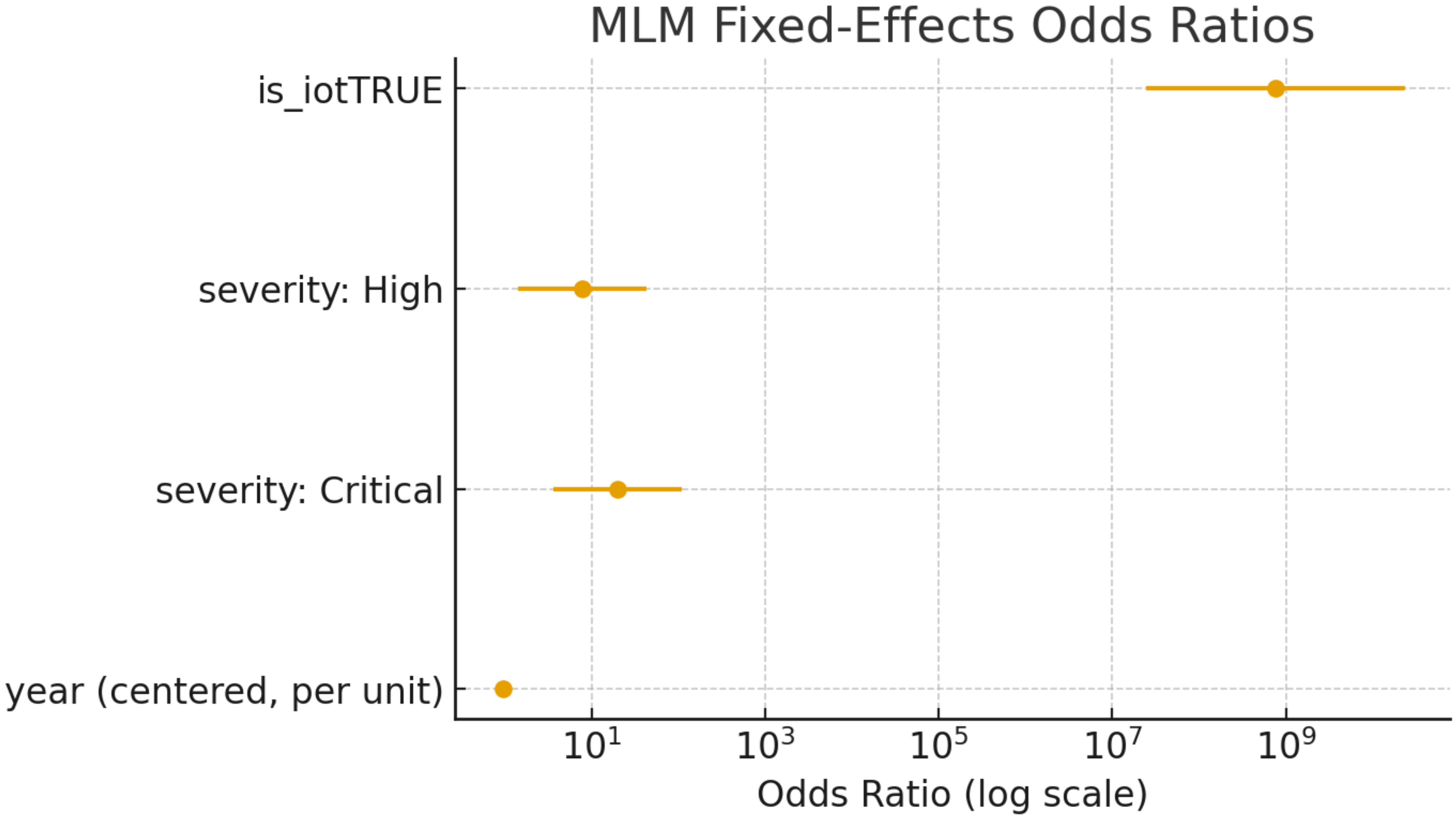


IoT (TRUE): OR ≈ 7.5×10^8 ($p<0.001$)

Severity (Critical): OR ≈ 19.9 ($p=0.001$)

Severity (High): OR ≈ 7.75 ($p=0.018$)

Year: OR ≈ 0.94 ($p=0.077$)


MLM Fixed-Effects Odds Ratios
is_iotTRUE
severity: High
severity: Critical
year (centered, per unit)
10^1
10^3
10^5
10^7
10^9
Odds Ratio (log scale)

Key Statistical Findings

IoT CVEs ≈ 18% of total

IoT exploitation risk ≈ 10^8× higher

Severity and IoT both predict exploitability

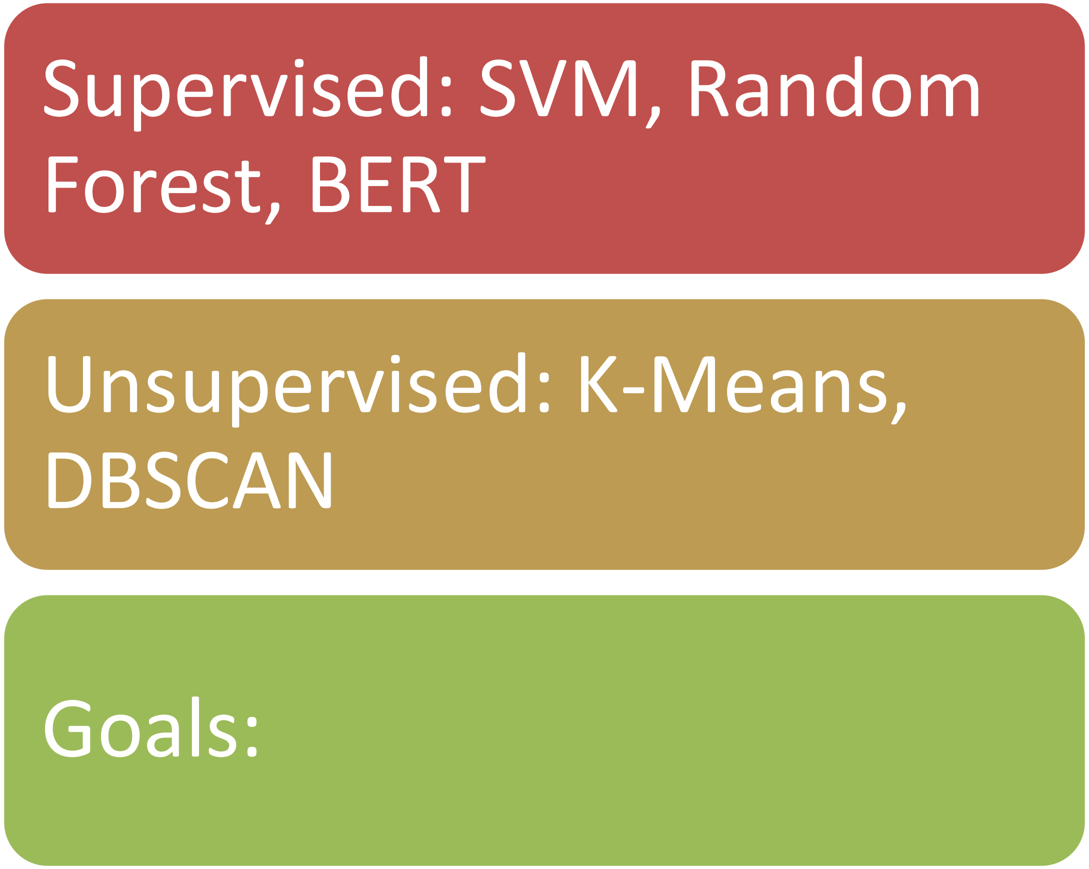
Slight decline post-2023

Transition: Machine Learning Phase (Work in Progress)

Next stage will apply ML models to predict exploitability.

Currently in progress — model training phase.

Planned Machine Learning Framework



Supervised: SVM, Random Forest, BERT

Unsupervised: K-Means, DBSCAN

Goals:

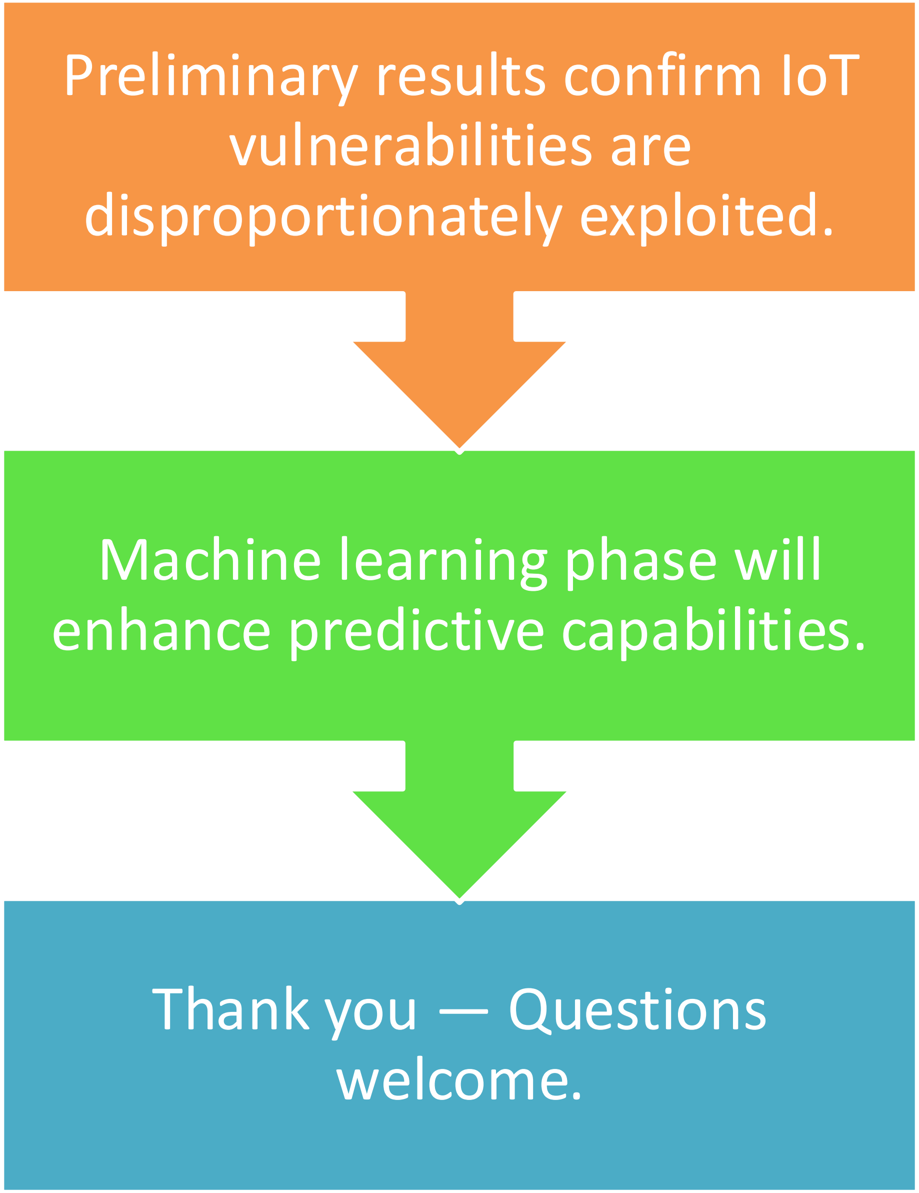
- Predict exploitability
- Cluster vulnerabilities
- Automate prioritization

Expected ML Outcomes

- Predict exploitability likelihoods
- Identify emerging zero-day clusters
- Prioritize high-risk IoT CVEs
- Improve patch response times

Research Impact and Implications

- Enhances IoT risk awareness
- Strengthens vulnerability disclosure practices
- Provides foundation for predictive threat intelligence



Preliminary results confirm IoT vulnerabilities are disproportionately exploited.

Machine learning phase will enhance predictive capabilities.

Thank you — Questions welcome.