

**A Machine Learning-Based Framework for Detecting
and Mitigating Security Vulnerabilities in Resource-
Limited Home IoT**

Dr. Mohammed Taleb Barajjash

☐ **Abstract**

☐ **Chapter1: Introduction**

- 1.1 Introduction
- 1.2 Background
- 1.3 Problem Statement
- 1.4 Research Objectives
- 1.5 Research Scope

☐ **Chapter 2: Literature Review**

- 2.1 Summary Research Papers
- 2.2 Critical Analysis
- 2.3 Synthesis Matrix

☐ **Chapter 3: Research Methodology**

- 3.1 Research Methodology
- 3.2 Expected Outcomes
- 3.3 Gantt Chart

☐ **References**

Abstract

Resource-constrained home IoT devices are highly vulnerable due to limited processing power and memory, which prevent the implementation of robust security. This research propose ML based framework for detecting and mitigating security vulnerabilities in resource-limited home IoT. The work will:

1. Categorize critical vulnerabilities
2. Design lightweight machine learning model
3. Validate the model in simulated testbed using security datasets
4. Compare its performance against exisiting systems.

The framework is expected to deliver a practical, highly accurate and low overhead solution to enhance customer IoT security.

Chapter 1: Introduction

1.1 Introduction

The proliferation of IoT devices in smart homes has introduced substantial security vulnerabilities. Traditional security measures are often inadequate for this ecosystem due to device diversity and the lack of standardized defense mechanisms. Securing the IoT is a critical contemporary challenge. This research proposes an innovative framework utilizing ML to provide robust, low-overhead vulnerability detection, directly addressing the core security deficits inherent in resource-limited home IoT devices.

1.2 Background

The security weakness of consumer IoT is primarily caused by resource constraints. These limitations prevent manufacturers from installing robust security features, often resulting in devices with default credentials and insecure communications. This lack of built-in security creates a vast, exploitable attack surface in home networks, highlighting the urgent need for an automated ML-based detection solution.

1.3 Problem Statement:

The Internet of Things (IoT) contains a vast network of interconnected, smart devices embedded in everyday objects, from home appliances to industrial sensors. The security of this domain, particularly for low-end consumer products, is a critical area of study (Meneghello, F. et al., 2019) & (Ramadan, R. A., 2022). The core problem within this domain is that a great number of these commercial IoT devices are shipped with weak or non-existent security measures (Meneghello, F. et al., 2019). This lack of built-in security is primarily a consequence of fundamental resource restrictions, which include severely limited computation power, storage, and battery life (Yu, M. et al., 2020).

This widespread insecurity poses a threat to user privacy and safety (Ramadan, R. A., 2022). The deployment of these vulnerable devices in critical areas like smart homes creates a vast attack surface, enabling severe attacks such as (DoS) and unauthorized access (Ghazal, T. M. et al., 2020).

Current papers provides board of surveys of IoT security risks and proposes various countermeasures (Yu, M. et al., 2020) & (Ramadan, R. A., 2022). However, researchers note that these traditional security approaches are often insufficient for the current threat landscape (Bin Hulayyil, S. et al., 2023). Furthermore, the focus on existing research is fragmented; some studies concentrate specifically on industrial environment (IIoT) (Jiang, X. et al., 2020), while others analyze physical hardware risks (Meneghello, F. et al., 2019). This leaves the security needs of common home-based devices insufficiently addressed.

There is urgent need to develop and validate comprehensive, modern and resource-efficient framework that utilize Machine Learning (ML) for automated vulnerability detection and classification (Bin Hulayyil, S. et al., 2023). Such framework is justified as it would specifically tailored to overcome the constraints of general consumer IoT devices, directly addressing weakness in current ecosystem.

1.4 Research Objective:

This research aim to design, build and evaluate machine learning –based framework that can automatically detect and classify security vulnerabilities in common home-based IoT devices, thereby providing solution to mitigate security risks.

Objectives

- 1- **To identify and categorize** the most critical security vulnerabilities that target the communication protocols and firmware of low-end, home-based IoT devices, creating a clear classification of threats.
- 2- **To design** a robust, resource efficient machine learning model specifically tailored to run in constrained IoT environment, capable of detecting both known and unknown vulnerabilities.
- 3- **To validate** this proposed framework by implementing it within simulated smart home environment, testing against existing security datasets and using standard performance metrics to ensure real world applicability.
- 4- **To conduct** a thorough comparison of the framework, track its accuracy, execution speed and resource consumption against existing security tools.

These research objectives align with the urgent need identified in the literature for comprehensive, modern and resource efficient frameworks that utilize machine learning (ML) for automated vulnerability and classification in consumer IoT.

1.5 Research Scope:

This research is strictly focused on consumer grade, resource-constrained IoT devices in smart home environment.

It will focus on security vulnerabilities related to network protocol anomalies and software weaknesses caused by resource constraints. Industrial IoT, enterprise systems and hardware level attacks are excluded. The ML framework will be implemented and validated in a controlled, simulated testbed using available IoT security datasets like Ton-IoT. real-world commercial deployment is excluded.

Chapter 2: Literature Review

2.1 Summary Research Papers:

Paper 1: IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices (Meneghello, F. et al., 2019)

This article summarizes the security risk in the IoT field in general. The researchers comment that most low-end commercial IoT products are available with little to no robust security measures, which lead to different kinds of potential security attacks such as DoF and unauthorized access, all due to weak security features. Specifically, the paper investigates widely used IoT communication protocols by selecting security mechanisms and explores real-world attacks on such protocols.

Paper 2: Machine-Learning-based vulnerability detection and classification for the Internet of Things Device Security (Bin Hulayyil, S. et al., 2023)

This paper summarizes the current literature on using machine learning to identify vulnerabilities in IoT, it analyzes classifying and detection strategies that are applied in different levels of IoT structure. The study describes ML methods for detecting the issue and suggests ML-based vulnerability detection and mitigation frameworks, with recent research developments in the field.

Paper 3: An overview into security weaknesses of IoT devices (Yu, M. et al., 2020)

This study provides an overview of research on how to analyze, discover, detect & fix security weaknesses on IoT devices. The paper highlights that as the number of IoT devices grows, so does the risk of security failures, which jeopardizes users' privacy and property. The paper is structured by describing the fundamental architecture and typical attack points of IoT before moving to describe the challenges.

Paper 4: An Experimental Study of Security Weaknesses in Industrial IoT Systems (Jiang, X. et al., 2020)

Covering the industrial Internet of Things (IIoT) environment, the paper looks at the attack surface of the commonly used network embedded systems for IIoT. It demonstrates collection of attack vectors for these systems followed by creating of attack scenarios. It focuses on simulation of Mirai attacks of interest for industrial devices.

Paper 5: Internet of Things (IoT) Security Vulnerabilities: A Review (Ramadan, R. A., 2022)

The paper aims to look into certain kind of attacks which compromise the devices physical components, like software or hardware. Also investigation ways to overcome these attacks.

Paper 6: Security Vulnerabilities, Attacks, Threats and the Proposed Countermeasures for the Internet of Things Applications (Ghazal, T. M. et al., 2020)

Paper emphasize the importance of IoT in organizational operations and need to facilitate the integration and assessment of security models in defending their organization from attackers who mainly target activities to boost cost or gain access to sensitive data & materials .

Paper 7 : Securing constrained IoT system: A lightweight machine learning approach anomaly detection and prevention (Alwaisi et a., 2024)

This study establishes that decision tree algorithm are the most effiecent for memory-constrained sensors, achieving over 96% accuracy while minimizing power consumption. It highlights that using quantization and pruning allow complex models to be converted into “TinyML” versions that run locally on small hardware without needing the cloud

Paper 8: Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models (Almotairi et al., 2024)

The researcher found that using the K-Best algorithm to select only top 15 network features significantly reduces computational overhead. Their stacking ensemble models proved more robust than single models at detecting threats in the ToN_IoT dataset, providing more reliable defense.

Paper 9: A Smart Framework to Detect Threats and Protect Data of IoT Based on Machine Learning (Almasabi et al., 2024)

The study demonstrate that a fog-based framewok can achieve over 98% detection accuracy for advanced attacks like injection and backdoor threats. A critical findings was that adding two specialized features calculated at the fog layer dramatically imporved the model ability to distinguish between normal traffic and malicious audits.

Paper 10: Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes (Javed et al., 2024)

The study successfully implemented a dual-layered IDS where an XGBoost model runs directly on an ESP32 microcontroller. Found that while cloud-level detection is very accurate (99.50%), the local device layer can detect MITM and DoS attacks in just 3.51 ms, which is essential for preventing damage before it spreads through a smart home.

2.2 Critical Analysis:

Connections:

Resource Limitations : There is general agreement that the limited processing power, memory and energy of IoT devices are the fundamental reasons manufacturers fail to implement advanced security measures (Meneghello et al., 2019; Bin Hulayyil et al., 2023; Alwaisi et al., 2024).

Universal Threat and Attack Surface: All reviewed papers confirm that widespread use of IoT devices in critical sectors (smart homes, healthcare, industry) creates a vast attack surface. Common attack types discussed in general IoT (Meneghello et al., 2019; Bin Hulayyil et al., 2023; Almotairi et al., 2024) and specifically in IIoT (Jiang et al., 2020) include unauthorized access, data theft & DoS attacks often utilize well known vulnerabilities.

Need for Advanced Detection: most papers emphasize that traditional security approaches are insufficient given the threat level. This necessitates the development of complete security models or the adoption of modern, sophisticated techniques like Machine Learning for automated vulnerability detection and classification (Ghazal et al., 2021; Almotairi et al., 2024; Almasabi et al., 2024).

2.3 Conflict Between the Findings:

Mitigation Strategy Focus: the researchers differ in their primary proposed mitigation strategy. Most papers offer a wide range of countermeasures, protocols and solutions while paper 2 narrows the focus on details of ML as a dedicated modern effective solution.

Domain Focus: Jiang et al. stand out by concentrating on IIoT. Contrasting with the other papers that focus on the general IoT, where risks are privacy, data theft, and network-level (e.g. DoS) attacks (Almasabi et al., 2024; Javed et al., 2024).

Attack Layer Focus: Ramadan's review provides strong focus on hardware security, which is different from the primary focus of other papers that tend to focus on security of network, firmware, application & software layers (Alwaisi et al., 2024; Almotairi et al., 2024).

Deployment Architecture: A conflict exist regarding where the detection logic should reside. Some framework suggest using the Fog or Cloud layer to handle the computational load (Almasabi et al., 2024), while others argue for local execution (TinyML) directly on the devices to ensure real-time response and data privacy (Alwaisi et al., 2024; Javed et al., 2024).

Model Complexity vs Efficiency: there is agreement between the use of complex models to improve accuracy in diverse networks (Almotairi et al., 2024) and the use of simple decision trees to stay within the strict memory limits (Alwaisi et al., 2024).

Simulated vs Real-World Performance: while most paper report high accuracy in simulated environments, recent findings show that performance specifically for MITM attacks can drop significantly when tested on physical hardware like an ESP32 (Javed et al., 2024)

2.4 Synthesis Matrix for Literature Review:

Study	Authors	Year	Research Design	Key Findings/Results	Methodology/Focus
Paper 1	Meneghello, F. et al.	2019	Survey	Many low-end commercial products lack strong security mechanisms. Leading to potential attack like DoF & unauthorized access due to weak security features	Investigate widely used IoT protocols by selecting security mechanism & explore real world attacks on these protocols.
Paper 2	Bin Hulayyil, S. et al.	2023	Comprehensive Survey	Describes the ML method for detecting the threats and suggest ML based model	Summarize the current literature on using ML to identify classifying and detection strategy applied on different level of IoT structure
Paper 3	Yu, M. et al.	2020	Survey	The number of IoT growing which increase the risk of security failure.	Provide an overview of research on how to analyze, discover, detect and fix security weakness on IoT devices
Paper 4	Jiang, X. et al.	2020	Experimental Analysis	Demonstrated collection of attacks in IIoT, followed by creating scenarios of these attacks. Focus on simulation of Mirai attack	Looks at the attack surface of commonly used embedded systems for IIoT
Paper 5	Ramadan, R. A.	2022	Review Article	Aim to look into attacks that comprise the physical components like software or hardware	Looks into certain type of physical attack investigate ways to overcome them
Paper 6	Ghazal, T. M. et al.	2020	Survey/Proposed Solutions	High level of threats necessitates the integration and assessment of security model in defending organization from attackers.	Focus the importance IoT in organizational operations and need to facilitate the integration and assessment of complete security models
Paper 7	Alwaisi, Z. et al.	2024	Research Article	Identified Decision Trees as highly efficient for memory-constrained sensors, achieving 96.9% accuracy via TinyML.	Evaluates Cloud, Edge, and TinyML models using quantization and pruning for resource-constrained IoT.
Paper 8	Almotairi, A. et al.	2024	Experimental Analysis	The K-Best algorithm successfully reduced overhead by selecting 15 features; Stacking ensemble models provided the most robust defense.	Focuses on enhancing IDS using ML-based feature selection and ensemble stacking validated on the ToN_IoT dataset.

Paper 9	Almasabi, A. M. et al.	2024	Framework Proposal	Achieving over 98% accuracy by adding specialized security features calculated at the Fog layer to improve classification.	Proposes a smart framework using ML and Fog computing to offload heavy processing from end devices.
Paper 10	Javed, A. et al.	2024	Experimental Implementation	Successfully detected MITM and DoS attacks in 3.51 ms. Noted performance drops when moving from simulation to real hardware.	Implements a lightweight IDS using XGBoost directly on an ESP32 microcontroller for real-time smart home protection.

Chapter 3: Research Methodology

3.1 Research Methodology

This project uses an experimental approach to develop and test the proposed framework. The goal is to move beyond theory and build a practical system that can actually run on low-power hardware. The work is organized into the following four phases:

Phase1: Data Preparation and Feature Selection: The ToN_IoT dataset serves as the primary source for identifying attacks. To reduce computational strain on home IoT devices, the K-Best algorithm is used to filter out redundant data. This ensure that only the most significant network features are processed, which is essential for maintaining performance on low-power CPUs.

Phase 2: Designing the Lightweight Model: ML model is constructed using either Decision Tree or XGBoost architectures. To ensure the model can actually run on local hardware without cloud support, TinyML techniques like quantization and pruning are applied. These steps are taken to shrink the model size and lower its memory usage while keeping detection accuracy high

Phase 3: Simulation & Testing: The framework will be tested in a simulated smart home environment. This setup will allows for the execution of common attcaks, such as DoS and MITM, to see how the model react in real-life.

Phase 4: Evaluation & Comparison: The final stage focuses on measuring the effectiveness of the framework. Performance is judged based on accuracy and more importantly, latency. The goal is to verify that the system can detect threats within a few milliseconds while operating tight RAM and CPU limits of standard consumer IoT devices.

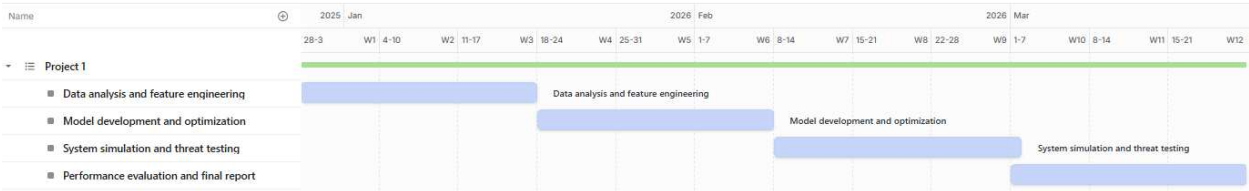
3.2 Expected Outcomes:

The following results are anticipated upon the completion of this research:

- A functional, lightweight ML model that maintains high detection accuracy (targeted above 96%) on resource-constrained microcontrollers.
- Verification that security tasks can be offloaded from the cloud to the local device level, reducing the time it takes to respond to abreach.
- A clear assessment of how different communication protocols in the home react to various attack types.
- Data demonstrating significant reduction in power and memory overhead compared to exisiting, non-optimized security solutions.

3.3 Gantt Chart

Project estimated to complete in 12 weeks



References:

1. **Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019).** IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, 6(5), 8186-8203.
2. **Bin Hulayyil, S., Li, S., & Xu, L. (2023).** Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security. *Electronics*, 12(18), 3927.
3. **Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020).** A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. *Future Internet*, 12(2), 27.
4. **Jiang, X., Lora, M., & Chattopadhyay, S. (2020).** An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. *ACM Transactions on Embedded Computing Systems (TECS)*, 19(3), 1-27.
5. **Ramadan, R. A. (2022).** Internet of Things (IoT) Security Vulnerabilities: A Review. *PLOMS Journal of Artificial Intelligence (PLOMS AI)*, 1(1), 1-13.
6. **Ghazal, T. M., Hasan, M. K., Hassan, R., Islam, S., Abdullah, S. N. H. S., Afifi, M. A. M., & Kalra, D. (2020).** Security Vulnerabilities, Attacks, Threats and the Proposed Countermeasures for the Internet of Things Applications. *Solid State Technology*, 63(1s), 1-14.
7. **Alwaisi, Z., Kumar, T., Harjula, E., & Soderi, S. (2024).** Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention. *Internet of Things*, 28, 101398.
8. **Almotairi, A., Atawneh, S., Khashan, O. A., & Khafajah, N. M. (2024).** Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models. *Systems Science & Control Engineering*, 12(1), 2321381.
9. **Almasabi, A. M., Khemakhem, M., Eassa, F. E., Abi Sen, A. A., Alkhodre, A. B., & Harbaoui, A. (2024).** A Smart Framework to Detect Threats and Protect Data of IoT Based on Machine Learning. *IEEE Access*, 12, 176831-176844.
10. **Javed, A., Ehtsham, A., Jawad, M., Awais, M. N., Qureshi, A. U. H., & Larijani, H. (2024).** Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes. *Future Internet*, 16(6), 200.