

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 30%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 2 November 2025

Hand-in Date: 25 November 2025

Hand-in Method: Online Submission via E-Learning.

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

Table of contents:

- Problem Statement
- Research Objectives

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 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 of 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 create 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.

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.

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.