

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 25 October 2025

Hand-in Date: 15 November 2025

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

Assignment Report: literature Review Common Security Vulnerabilities and Countermeasures in Home-Based IoT Devices

Table of contents:

- Summary research
- Critical Analysis
- Connections
- Conflicts between the findings
- Synthesis Matrix for Literature Review:
- Reference

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 Huiyil, 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 fundamentals, 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 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 .

Critical Analysis:

Connections

1. **Resource Limitations:** similar idea for several papers is that resource limitation (power, computation, storage & budget) in low-end commercial IoT devices are the root cause for absence of strong security structure like advanced encryption & device authentication.
2. **Universal Threat and Attack Surface:** All reviewed papers confirm that widespread use of IoT devices in critical sectors (smart homes, healthcare, and industry) creates a vast attack surface. Common attack types discussed in general IoT (paper 1, paper 3 & paper 6) and specifically in IIoT (paper 5) include unauthorized access, data theft & DoS attacks often utilize well known vulnerabilities.
3. **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

Conflicts between the findings

1. **Mitigation Strategy Focus:** the researchers differ in their primary proposed mitigation strategy. Most paper offer wide range of countermeasures, protocols and solutions while paper 2 narrow the focus on details ML as dedicated modern effective solution.
2. **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.
3. **Attack Layer Focus:** Ramadan's review provide strong focus on hardware security, which is different from primary focus of other papers that tend to focus on security of network, firmware, application & software layers.

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

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.