

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 30%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 1 March 2025

Hand-in Date: 15 March 2025

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

**PROBLEM STATEMENT AND RESEARCH OBJECTIVE FOR
INTERNET OF THINGS (IOT) SECURITY AND ROUTING
PROTOCOLS**

Student ID: 251002398

Student Name: Abdel Hafez Alassar

PROBLEM STATEMENT AND RESEARCH OBJECTIVE FOR INTERNET OF THINGS (IOT) SECURITY AND ROUTING PROTOCOLS

Problem Statement:

Particularly in routing protocols and intrusion detection systems, the fast growth of the Internet of Things (IoT) has notably raised security risks. Highly sensitive to several cyber risks, including version number attacks, botnets, and distributed denial_of_service (DDoS) attacks; are IoT networks which are often limited by power efficiency needs and little computational power. An immediate need for sophisticated, artificial intelligence driven security measures arises from the inability of conventional Intrusion Detection Systems (IDS) and routing security protocols to provide strong, scalable, and energy-efficient protection against changing cyber dangers.

The literature shows that machine learning-based Intrusion Detection Systems (IDS) have been highly accurate in catching IoT network attacks, with methods like ensemble learning, deep learning, and anomaly detection showing great results. Nonetheless, these artificial intelligence-powered security features have several drawbacks, including great computational overhead, scalability issues, high false positives, and absence of real-world validation. Moreover, more advanced routing attacks compromise routing security techniques such as

RPLbased ones, so hybrid security models are needed that combine anomaly detection with small cryptographic methods.

Although artificial intelligence and machine learning for IoT security solutions have improved, there remains a need to create balanced detection accuracy, computational efficiency, and scalability in practical IoT installations dynamic, efficient, and cost-effective security frameworks that balance detection accuracy, computational efficiency, and scalability in real world IoT deployments. Research is needed to maximize Intrusion Detection Systems and routing security protocols so as to guarantee strong cybersecurity solutions that can run effectively in a resource-constrained Internet of Things setting while adjusting to changing online threats.

Research Objectives:

The main aim of this study is to improve IoT security by means of an AI powered, energy-efficient intrusion recognition and routing security system hence effectively reducing cyber threats. The particular objectives are:

- To investigate current IoT security issues, especially in routing security protocols and intrusion detection.
- To judge how well machine learning-based Intrusion Detection Systems (IDS) detect and stop IoT cyber threats.

- To create in resource-constrained IoT settings an integrated AI-driven security system that maximizes intrusion prevention but keeps energy use down.
- To examine how artificial intelligence-driven security systems are affected by computational restrictions and suggest ideas for maximizing performance in Internet of Things networks.
- To create hybrid security systems that combine anomaly detection and low-weight cryptographic techniques, improve IoT routing security.
- To confirm the suggested security framework is suitable for real-world implementation by means of actual deployment and checks.

References

- Zagrouba, R., &Alhajri, R. (2021). Machine learning based attacks detection and countermeasures in IoT. *International Journal of Communication Networks and Information Security*, 13(2), 158-167. <https://core.ac.uk/download/pdf/539893726.pdf>
- Alfriehtat, N., Anbar, M., Karuppayah, S., Rihan, S. D. A., Alabsi, B. A., & Momani, A. M. (2024). Detecting version number attacks in low power and lossy networks for internet of things routing: review and taxonomy. *IEEE Access*. <https://ieeexplore.ieee.org/abstract/document/10443394/>
- Ejeofobiri, C. K., Victor-Igun, O. O., & Okoye, C. (2024). AI-Driven Secure Intrusion Detection for Internet of Things (IOT) Networks. *Asian Journal of Mathematics and Computer Research*, 31(4), 40-55. <https://hal.science/hal-04826235/>
- Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., &Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, 61(12), 9395-9409. <https://www.sciencedirect.com/science/article/pii/S1110016822001570>
- Alghamdi, R., &Bellaiche, M. (2022). Evaluation and selection models for ensemble intrusion detection systems in IoT. *IoT*, 3(2), 285-314. <https://www.mdpi.com/2624-831X/3/2/17>
- Arshad, J., Azad, M. A., Amad, R., Salah, K., Alazab, M., & Iqbal, R. (2020). A review of performance, energy and privacy of intrusion detection systems for IoT. *Electronics*, 9(4), 629. <https://www.mdpi.com/2079-9292/9/4/629>