

Research Methodology in Computer Science

Course Code: AI800

ASSIGNMENT 2

Toward Early and Lightweight Machine Learning-Based Detection of IoT Botnet Attacks

Student Name: Ibrahim Mohammed Alsidrani

Student ID: 262000987

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 27 June 2026

Hand-in Date: 11 July 2026

Assignment Weight: 30%

Table of Contents

1. Research Title	1
2. Problem Statement	1
3. Research Aim	2
4. Research Objectives	2
5. Literature Review	2
6. Research Questions	4
7. Scope of the Study	4
8. Significance of the Study	4
9. Expected Contribution	4
10. Key Concepts	5
11. Conclusion	5
References.....	6

1. Research Title

Toward Early and Lightweight Machine Learning-Based Detection of IoT Botnet Attacks

2. Problem Statement

The problem domain of this research is IoT cybersecurity, specifically the detection of botnet attacks targeting Internet of Things (IoT) environments. IoT devices are increasingly used in smart homes, universities, healthcare environments, industrial systems, and public services. These devices provide important benefits by enabling automation, monitoring, and remote access. However, many IoT devices have limited computing power, weak default configurations, and irregular security updates. These weaknesses make them attractive targets for botnet attacks, where compromised devices can be remotely controlled and used to perform malicious activities such as distributed denial-of-service attacks, network scanning, credential theft, and data exfiltration.

Existing solutions show that machine learning and deep learning can detect IoT botnet traffic with high performance in controlled experiments. For example, DNN-based intrusion detection, CNN-based botnet detection, SMOTE-DRNN, ensemble learning, and collaborative early-detection approaches have all been proposed for IoT botnet detection (Jithu et al., 2021; Idrissi et al., 2021; Popoola et al., 2021; Rezaei, 2021; Nguyen et al., 2022; Abu Al-Haija & Al-Dala'ien, 2022). These studies demonstrate that data-driven detection can be effective when models are trained and tested on selected datasets.

Despite these promising results, high detection accuracy alone does not fully solve the practical security problem. Many existing approaches are evaluated using known datasets and random train-test splits, which makes it difficult to determine whether the same models can detect unseen botnet families or perform reliably under changing network conditions. In addition, some deep learning models may require more computational resources than IoT gateways or edge devices can provide. Other approaches may detect attacks only after enough malicious traffic has already appeared, reducing the opportunity for early response (Popoola et al., 2021; Nguyen et al., 2022).

The significance of this problem is that IoT environments often operate in resource-constrained and security-sensitive settings. If detection is late, heavy, or unreliable against new botnet behavior, compromised IoT devices may already be used to disrupt services, steal data, or participate in wider cyberattacks. Therefore, there is a clear need for research that moves beyond laboratory accuracy and investigates how IoT botnet detection can be made early, lightweight, and more reliable in realistic deployment conditions.

Therefore, the research problem addressed in this study is the lack of a practical IoT botnet detection approach that can combine three requirements at the same time: early detection, lightweight operation, and reliable performance against unseen or changing botnet behavior. This research is needed because IoT security solutions should not only perform well on existing datasets but should also support timely response and practical deployment on resource-constrained devices.

3. Research Aim

The primary goal of this research is to investigate how machine learning can be used to support early and lightweight detection of IoT botnet attacks while maintaining reliable performance against unseen or changing attack behavior.

4. Research Objectives

1. To identify the main limitations of current machine learning-based IoT botnet detection methods in relation to early detection, computational cost, and generalization.
2. To examine the suitability of lightweight models and deep learning models for deployment in IoT gateways or resource-constrained environments.
3. To analyze the effect of class imbalance and unseen botnet behavior on the reliability of reported detection results.
4. To propose a conceptual layered detection approach that combines fast gateway-level screening with deeper analysis for suspicious or uncertain cases.
5. To define practical evaluation criteria for IoT botnet detection models, including accuracy, inference time, resource consumption, early detection capability, and robustness to unseen attacks.

5. Literature Review

The literature reviewed in Assignment 1 shows that IoT botnet detection has received significant attention because compromised IoT devices can be used to launch large-scale cyberattacks. Several studies have investigated machine learning and deep learning models to improve detection accuracy, but their methods differ in terms of datasets, model complexity, feature use, class imbalance handling, and deployment readiness.

Jithu et al. (2021) proposed a deep neural network-based intrusion detection system for detecting IoT botnet attacks using the Bot-IoT dataset. Their work showed that deep learning can learn useful traffic patterns and achieve strong detection performance. The main strength of this study is its ability to capture complex relationships in network traffic. However, the study mainly focused on detection performance in a controlled dataset, which leaves questions about generalization to unseen botnet families and deployment in resource-limited IoT environments.

Popoola et al. (2021) introduced SMOTE-DRNN, which combines Synthetic Minority Oversampling Technique (SMOTE) with a deep recurrent neural network. This study is important because it directly addresses the class imbalance problem, which is common in cybersecurity datasets. Its results show that balancing minority attack classes can improve the reliability of detection. However, the use of oversampling and recurrent deep learning may increase training complexity and computational cost, which can limit direct deployment on lightweight IoT gateways.

Idrissi et al. (2021) proposed BotIDS, a CNN-based intrusion detection approach for IoT botnet attacks. Their results showed very high validation accuracy and fast prediction time. This study supports the idea that deep learning models can be effective in identifying botnet traffic. Nevertheless, CNN-based approaches may still require careful evaluation under cross-dataset or unseen-attack

conditions because high performance on one dataset does not necessarily guarantee robustness in realistic IoT environments.

Nguyen et al. (2022) focused on a collaborative approach for early detection of IoT botnets. Their study is especially relevant to this assignment because it highlights the importance of detecting botnet activity before the full attack impact occurs. The strength of this approach is its use of behavioral information for early security response. However, collecting behavioral and system-level data may introduce additional processing overhead and deployment complexity.

Abu Al-Haija and Al-Dala'ien (2022) proposed ELBA-IoT, an ensemble learning model for botnet attack detection in IoT networks. Their work demonstrated that ensemble methods can provide high accuracy and efficient inference. Ensemble-based approaches are useful because they can improve stability by combining multiple learners. However, their effectiveness still depends on the quality and representativeness of the training data, and they require further validation against unseen or evolving botnet behaviors.

Rezaei (2021) investigated ensemble learning for detecting botnets on IoT. The study reported strong performance using selected features and a sequential ensemble strategy. This paper contributes to the literature by showing that feature selection and ensemble design can reduce unnecessary complexity. However, like several other studies, the results are mainly based on experimental evaluation using a specific dataset, which limits certainty about performance in different real-world IoT networks.

Overall, the reviewed studies agree that machine learning can improve IoT botnet detection, but they also reveal important gaps. Some studies prioritize high accuracy, while others address class imbalance, early detection, or efficient inference. However, few approaches combine early detection, lightweight deployment, and robust generalization in one practical direction. This literature gap directly supports the problem statement and research objectives of the current assignment.

Summary of Reviewed Literature

Authors / Year	Focus	Method	Key Strength	Limitation
Jithu et al. (2021)	IoT botnet IDS	DNN	Learns complex traffic patterns	Limited real-world generalization evidence
Popoola et al. (2021)	Class imbalance	SMOTE-DRNN	Improves minority attack detection	Higher complexity and resource cost
Idrissi et al. (2021)	Botnet traffic detection	CNN-based BotIDS	High validation accuracy and fast prediction	Needs stronger unseen-attack validation
Nguyen et al. (2022)	Early detection	Collaborative behavioral analysis	Supports early response	May require richer data collection
Abu Al-Haija & Al-Dala'ien (2022)	Efficient detection	Ensemble learning	High accuracy and efficient inference	Depends on dataset representativeness
Rezaei (2021)	Feature-efficient detection	Ensemble learning	Uses selected features	Dataset-specific evaluation

6. Research Questions

1. What are the main practical limitations of existing machine learning-based IoT botnet detection methods?
2. How can early detection and lightweight operation be combined in an IoT botnet detection approach?
3. How does class imbalance affect the reliability of detection results in IoT botnet datasets?
4. What evaluation criteria are needed to determine whether an IoT botnet detection model is suitable for real deployment?
5. How can a layered detection approach improve the balance between accuracy, speed, and practical usability?

7. Scope of the Study

This study focuses on machine learning-based detection of IoT botnet attacks. The scope includes approaches that rely on network traffic features, behavioral features, or a combination of both. The study pays particular attention to four main aspects: early detection, lightweight operation, class imbalance, and generalization to unseen botnet behavior.

The study does not aim to develop a complete commercial intrusion detection system. Instead, it focuses on formulating the research problem and objectives that can guide future development of a practical detection framework. The proposed direction is mainly suitable for IoT gateways, edge devices, or monitoring systems that need to identify suspicious botnet activity before major damage occurs.

8. Significance of the Study

The significance of this study comes from the growing use of IoT devices in daily life and organizational environments. As the number of connected devices increases, the number of potential attack points also increases. If these devices are compromised, they can become part of botnets and contribute to large-scale cyberattacks.

This study is significant because it shifts the focus from simply achieving high accuracy to developing detection methods that are useful in real operational settings. A model should not be judged only by its accuracy score. It should also be assessed based on how fast it can respond, how much processing power it requires, whether it can detect attacks early, and whether it can remain reliable when new attack patterns appear.

9. Expected Contribution

This research is expected to contribute to the field of IoT security by clarifying the gap between machine learning detection accuracy and real deployment readiness. It highlights that successful IoT botnet detection should consider not only predictive performance, but also operational constraints such as inference time, resource consumption, early response, and robustness.

The study is also expected to provide a structured set of objectives and evaluation criteria that can guide future research. These criteria can help researchers compare IoT botnet detection methods more fairly and practically. Instead of focusing only on accuracy, future evaluations can include

additional factors such as performance against unseen botnet families, class imbalance handling, and suitability for IoT gateways.

In addition, the proposed direction of a layered detection approach may help balance speed and depth of analysis. A lightweight model can be used for fast initial screening, while more complex models can be applied to suspicious or uncertain cases. This can improve practical usability without overloading resource-constrained IoT environments.

10. Key Concepts

IoT Botnet Detection: The process of identifying compromised IoT devices or malicious network behavior associated with botnet activity.

Early Detection: The ability to detect suspicious activity before the attack is fully completed or before serious damage occurs.

Lightweight Operation: The ability of a detection model to operate with limited computational resources, especially on IoT gateways or edge devices.

Generalization: The ability of a model to maintain good performance when tested on new data, unseen botnet families, or changing network conditions.

Class Imbalance: A common issue in cybersecurity datasets where some attack types have many examples while others have very few. This can make accuracy misleading if minority attack classes are not detected properly.

Layered Detection: A detection strategy that uses more than one stage, such as fast initial screening followed by deeper analysis for suspicious cases.

11. Conclusion

This assignment formulated a research problem related to early, lightweight machine-learning-based detection of IoT botnet attacks. The problem is important because many existing approaches achieve high performance in controlled experiments but may not be ready for real IoT deployment. Practical detection systems must operate under resource constraints, detect attacks early, and remain reliable in the face of unseen or evolving botnet behavior.

The proposed research aim, objectives, and questions provide a clear direction for future investigation. The study emphasizes that accuracy should not be the only evaluation measure. Instead, IoT botnet detection methods should also be assessed using practical criteria such as inference time, resource use, class imbalance handling, early detection capability, and robustness. This direction can support the development of more realistic and deployable IoT security solutions.

References

- Abu Al-Haija, Q., & Al-Dala'ien, M. (2022). ELBA-IoT: An ensemble learning model for botnet attack detection in IoT networks. *Journal of Sensor and Actuator Networks*, 11(1), 18. <https://doi.org/10.3390/jsan11010018>
- Idrissi, I., Boukabous, M., Azizi, M., Moussaoui, O., & El Fadili, H. (2021). Toward a deep learning-based intrusion detection system for IoT against botnet attacks. *IAES International Journal of Artificial Intelligence*, 10(1), 110-120. <https://doi.org/10.11591/ijai.v10.i1.pp110-120>
- Jithu, P., Shareena, J., Ramdas, A., & Haripriya, A. P. (2021). Intrusion detection system for IoT botnet attacks using deep learning. *SN Computer Science*, 2, 205. <https://doi.org/10.1007/s42979-021-00516-9>
- Nguyen, G. L., Dumba, B., Ngo, Q.-D., Le, H.-V., & Nguyen, T. N. (2022). A collaborative approach to early detection of IoT botnet. *Computers & Electrical Engineering*, 97, 107525. <https://doi.org/10.1016/j.compeleceng.2021.107525>
- Popoola, S. I., Adebisi, B., Ande, R., Hammoudeh, M., Anoh, K., & Atayero, A. A. (2021). SMOTE-DRNN: A deep learning algorithm for botnet detection in the Internet-of-Things networks. *Sensors*, 21(9), 2985. <https://doi.org/10.3390/s21092985>
- Rezaei, A. (2021). Using ensemble learning technique for detecting botnet on IoT. *SN Computer Science*, 2, 148. <https://doi.org/10.1007/s42979-021-00585-w>