

Enhancing Botnet Detection in IoT Networks Using Hybrid Deep Learning and Ensemble Models

Mohammad Wajeeh Bader
Advisor: Dr. Mohammed Anber

Contents

1	Abstract	3
2	Chapter 1: Introduction	3
2.1	Background	3
2.2	Problem Statement	3
2.3	Research Objectives	4
2.4	Research Scope	4
3	Chapter 2: Literature Review	5
4	Chapter 3: Research Methodology	6
4.1	Data Collection	6
4.2	Model Development	6
4.3	Validation	6
4.4	Expected Outcomes	6
4.5	Gantt Chart	7
	References	8

1 Abstract

This study seeks to build an advanced hybrid model that effectively detects and counters botnet attacks within IoT networks by combining deep learning with ensemble learning techniques. The proposed model is designed to tackle key challenges such as real-time performance, computational efficiency, and scalability. By thoroughly analyzing existing methods and incorporating recent technological advances, the research introduces a resilient and adaptable detection framework. The goal is to deliver a high accuracy, lightweight solution that can be practically deployed on IoT devices with limited resources.

2 Chapter 1: Introduction

The rapid expansion of the Internet of Things (IoT) has resulted in increased security vulnerabilities, particularly with botnet attacks. Botnets pose severe threats to IoT ecosystems, leading to data breaches, privacy invasion, and disruption of critical infrastructure. To counteract these threats, effective detection techniques leveraging advanced machine learning (ML) and deep learning (DL) approaches have become indispensable.

2.1 Background

Botnets are networks of compromised devices controlled remotely by malicious entities, often employed in cyberattacks such as Distributed Denial of Service (DDoS). IoT devices, characterized by limited computational resources and decentralized architectures, are particularly susceptible. Recent approaches in ML and DL, including Convolutional Neural Networks (CNN), ensemble learning (e.g., AdaBoost, RUSBoost), and transfer learning, have shown potential but face significant practical challenges in real world scenarios.

2.2 Problem Statement

In the ever-expanding domain of Internet of Things (IoT) security, botnet detection has become an increasingly critical challenge. This is largely due to the decentralized architecture and limited computational capabilities of IoT devices, which make them attractive targets for attackers and simultaneously difficult to protect.

While machine learning (ML) and deep learning (DL) techniques have shown considerable success in detecting malicious activities, most of these solutions are designed and tested in controlled environments. As a result, they often struggle to perform effectively in real time and real world IoT settings, where networks are dynamic, devices are resource constrained, and threats constantly evolve.

The importance of protecting IoT ecosystems from botnet attacks cannot be overstated. These attacks not only compromise user privacy but also threaten the reliability of critical infrastructure, from smart homes to healthcare systems. Although various solutions have been proposed ranging from CNN based intrusion detection systems [2] to ensemble learning models such as AdaBoost, RUSBoost [1], and transfer learning approaches [4], most fall short when it comes to scalability, adaptability, and lightweight deployment.

Therefore, there is a clear and pressing need for a hybrid, lightweight, and adaptive detection framework that balances high detection accuracy with real time performance and minimal computational overhead. Closing this gap could pave the way for practical, deployable security solutions that align with the diverse and evolving nature of modern IoT environments.

2.3 Research Objectives

The overarching goal of this research is to develop an efficient and lightweight hybrid detection model that leverages both ensemble learning and deep learning to identify botnet attacks in real time IoT environments. The specific objectives are:

1. To review and benchmark current ML and DL-based approaches for IoT botnet detection with respect to their accuracy, scalability, and computational efficiency.
2. To design a hybrid detection framework that integrates ensemble learning with deep transfer learning for improved detection performance.
3. To optimize the model for deployment on low resource IoT devices, enabling practical real time use.
4. To validate the model’s effectiveness using both benchmark datasets (e.g., CSE-CIC-IDS2018, N-BaIoT) and live IoT network traffic.
5. To test the model’s generalizability, particularly its ability to detect emerging and previously unseen botnet attack types.

2.4 Research Scope

This research will focus on IoT networks with an emphasis on real time detection performance and adaptability. Evaluation and validation will involve both standard benchmark datasets (e.g., CSE-CIC-IDS2018, N-BaIoT) and practical real-world scenarios.

3 Chapter 2: Literature Review

Recent research has demonstrated significant progress in applying machine learning (ML) and deep learning (DL) techniques for botnet detection in IoT networks. Idrissi et al. [2] proposed a CNN-based intrusion detection system trained on the CSE-CIC-IDS2018 dataset, which achieved high detection accuracy but required substantial computational resources.

In a similar effort to enhance detection performance, Kadhim et al. [4] implemented an ensemble deep transfer learning approach that leveraged pre-trained models such as ResNet101 and VGG16. Their method involved transforming binary network traffic data into grayscale images, which improved classification accuracy.

Building on ensemble techniques, Abu Al-Haija and Al-Dala'ien [1] introduced ELBA-IoT, a comprehensive framework combining AdaBoost, RUSBoost, and Bagging. This model, validated on the N-BaIoT dataset, achieved an impressive 99.6% detection accuracy while maintaining relatively low computational overhead.

Meanwhile, Srinivasan and Deepalakshmi [9] developed ECASP, an ensemble-based classifier with a focus on optimal feature selection; however, the model faces limitations in terms of scalability.

Rezaei [8] proposed a method combining supervised, unsupervised, and regression learning, reaching 100% accuracy, but its lack of real-world testing raises questions about practical applicability.

Khoa et al. [5] explored a novel collaborative learning framework integrating federated learning and transfer learning, reporting a 40% improvement in detection performance over baseline models, albeit with considerable computational cost.

Wang et al. [10] introduced Def-IDS, an ensemble-based defense mechanism incorporating multi-class GANs and adversarial retraining. Their framework significantly improved detection accuracy against adversarial attacks. However, its high computational complexity presents a challenge for practical deployment.

Nguyen et al. [6] proposed a collaborative early detection model for botnet activity, achieving an impressive 99.37% accuracy. The approach emphasizes proactive threat identification to mitigate potential damage, though it still requires broader validation in real-world environments.

Popoola et al. [7] developed the SMOTE-DRNN algorithm, a hybrid technique combining SMOTE for class balancing and a deep recurrent neural network for classification. The model attained a notable 99.62% F1-score, demonstrating strong performance in detecting minority classes, despite concerns over computational demands.

Jithu et al. [3] designed a DNN-based intrusion detection system tailored for IoT environments. Their deep learning model achieved strong results in mitigating DDoS attacks under realistic conditions. Nonetheless, its implementation is hindered by intensive computational requirements.

4 Chapter 3: Research Methodology

This research employs a mixed-methods approach involving both qualitative and quantitative analyses:

4.1 Data Collection

- Utilize established benchmark datasets (e.g., CSE-CIC-IDS2018, N-BaIoT).
- Capture live IoT traffic data for realistic evaluation.

4.2 Model Development

- Design a hybrid architecture combining deep transfer learning and ensemble classifiers (AdaBoost, RUSBoost).
- Optimize model parameters to minimize computational resource consumption.

4.3 Validation

- Evaluate model performance on accuracy, precision, recall, and F1-score.
- Conduct cross-validation using multiple datasets and real time IoT network scenarios.

4.4 Expected Outcomes

The expected outcomes include:

- A robust, adaptive, lightweight detection model.
- Enhanced real time performance for deployment in IoT devices.
- Comprehensive validation demonstrating high detection accuracy.

4.5 Gantt Chart

The following Gantt chart presents the project timeline with milestones.

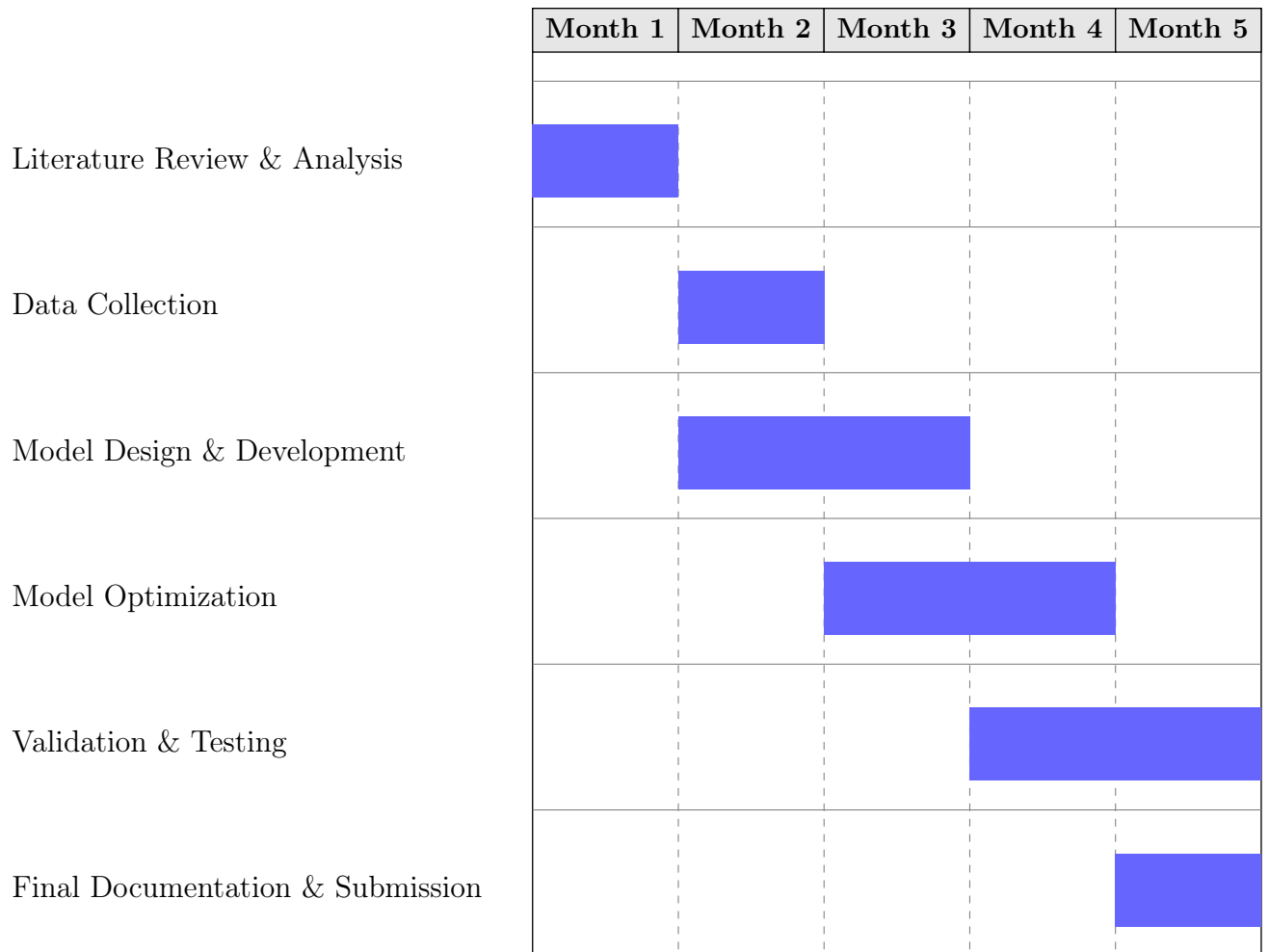


Figure 1: Project Gantt Chart showing the timeline and milestones.

References

- [1] 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.
- [2] 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 (IJ-AI)*, 10(1), 110–120.
- [3] 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.
- [4] Kadhim, Q. Kh., Al-Sudani, A. Q. A. S., Almani, I. A., Alghazali, T., Dabis, H. Kh., Mohammed, A. T., Talib, S. G., Mahmood, R. A., Sahi, Z. T., & Mezaal, Y. S. (2022). IOT-MDEDTL: IoT malware detection based on ensemble deep transfer learning. *Majlesi Journal of Electrical Engineering*, 16(3), 47–54.
- [5] Khoa, T. V., Hoang, D. T., Trung, N. L., Nguyen, C. T., Quynh, T. T. T., Nguyen, D. N., Ha, N. V., & Dutkiewicz, E. (2022). Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks. *IEEE Internet of Things Journal*. Advance online publication.
- [6] 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 and Electrical Engineering*, 97, 107525.
- [7] 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.
- [8] Rezaei, A. (2021). Using ensemble learning technique for detecting botnet on IoT. *SN Computer Science*, 2(3), 148.
- [9] Srinivasan, S., & Deepalakshmi, P. (2023). Enhancing the security in cyber-world by detecting the botnets using ensemble classification-based machine learning. *Measurement: Sensors*, 25, 100624.
- [10] Wang, J., Pan, J., AlQerm, I., & Liu, Y. (2021). Def-IDS: An ensemble defense mechanism against adversarial attacks for deep learning-based network intrusion detection. In *2021 International Conference on Computer Communications and Networks (ICCCN)* (pp. 1–9). IEEE.