

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Fawzi

Hand-out Date: 14 Mar 2025

Hand-in Date: 22 February 2025

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

Literature Review: Machine Learning and Deep Learning Approaches for Botnet Detection in IoT Networks

Table of contents:

- Summary research paper's
- Critical Analysis:
- Connections
- Conflicts between the findings
- Synthesis Matrix for Literature Review:
- References

Summary of Selected Papers

Paper 1: Toward a Deep Learning-Based Intrusion Detection System for IoT Against Botnet Attacks (2021)

This study proposes a deep learning-based Intrusion Detection System (IDS) to detect botnet activities in IoT environments. The model uses a Convolutional Neural Network (CNN) trained on a preprocessed dataset, achieving high detection accuracy. The evaluation is conducted using the CSE-CIC-IDS2018 dataset, demonstrating promising results in detecting various types of attacks. (Idrissi et al., 2021)

Paper 2: IoT Malware Detection Based on Ensemble Deep Transfer Learning (2022)

This paper presents an ensemble deep transfer learning approach that leverages pre-trained models such as ResNet101 and VGG16 to extract features from IoT network traffic. By transforming binary data into grayscale images, the method enhances classification performance. The study achieves 96.31% accuracy, showcasing the effectiveness of transfer learning in botnet detection. (Kadhim et al., 2022)

Paper 3: ELBA-IoT An Ensemble Learning Model for Botnet Attack Detection in IoT Networks (2022)

The ELBA-IoT framework employs ensemble learning, combining AdaBoost, RUSBoost, and Bagging to improve botnet detection in IoT networks. Evaluated on the N-BaIoT-2021 dataset, the approach achieves a 99.6% detection accuracy with minimal computational overhead, making it a viable solution for resource-constrained IoT devices. (Abu Al-Haija & Al-Dala'ien, 2022)

Paper 4: Enhancing Security in Cyber-World by Detecting Botnets Using Ensemble Classification-Based Machine Learning (2023)

This study introduces an Ensemble Classifier Algorithm with Stacking Process (ECASP), which selects optimal features for botnet detection. The approach attains 94.08% accuracy, demonstrating improved sensitivity and specificity. However, the method's reliance on extensive feature engineering presents scalability challenges. (Srinivasan & Deepalakshmi, 2023)

Paper 5: Using Ensemble Learning Technique for Detecting Botnet on IoT (2021)

This research focuses on optimizing botnet detection by combining supervised, unsupervised, and regression learning methods. The model achieves 100% detection accuracy while minimizing feature selection to only 20 attributes, reducing computational costs. However, its real-world applicability remains uncertain due to limited testing in diverse IoT environments. (Rezaei, 2021)

Paper 6: Deep Transfer Learning: A Novel Collaborative Learning Model for Cyberattack Detection Systems in IoT Networks (2022)

This study explores federated learning and transfer learning for cyberattack detection in decentralized IoT networks. The model transfers knowledge between networks with different feature distributions, improving detection accuracy by 40% over conventional methods. While promising, its reliance on labeled data and computational complexity poses implementation challenges. (Khoa et al., 2022)

Critical Analysis

The reviewed studies provide significant advancements in botnet detection within IoT environments, leveraging various machine learning and deep learning methodologies. A key strength observed across these studies is the high detection accuracy, with most models achieving above 94% and some exceeding 99%. The integration of advanced learning techniques, such as deep learning, transfer learning, and ensemble learning, enhances the robustness of detection models by improving their ability to identify sophisticated attack patterns. Moreover, several studies focus on efficient feature selection, reducing computational overhead while maintaining high classification performance.

However, these approaches are not without limitations. One major challenge is the high computational cost associated with deep learning models, which makes real-time deployment on IoT devices difficult due to their limited processing power. Additionally, while many studies achieve outstanding accuracy in controlled experimental settings, their applicability in real-world scenarios remains uncertain. Most models have been tested on benchmark datasets but lack validation in live IoT networks, raising concerns about their adaptability to evolving threats. Furthermore, static models may struggle to detect novel attack patterns, as adversaries continuously develop more sophisticated botnet techniques.

In conclusion, while the reviewed studies contribute valuable insights into improving IoT security, further research is needed to develop adaptive, lightweight, and real-time detection mechanisms that can be seamlessly integrated into IoT ecosystems without compromising efficiency or effectiveness.

Connections

majority of the studies emphasize the importance of ensemble learning and deep learning models, showing that combining multiple classifiers or leveraging pre-trained networks significantly enhances detection performance. The use of feature selection techniques is also a recurring theme, as reducing the number of features can improve efficiency while maintaining high accuracy. Furthermore, studies that incorporated real-world datasets, such as N-BaloT and CSE-CIC-IDS2018, highlight the need for diverse data sources to improve model generalization and reliability in different IoT environments.

Conflicts Between the Findings

Despite the commonalities, there are notable discrepancies between studies. Some studies, such as the ELBA-IoT model, achieve high accuracy while maintaining low computational costs, whereas deep learning-based approaches like CNN-based IDS require significant computational resources. Another conflict arises in the effectiveness of transfer learning, as some studies argue that pre-trained models significantly improve detection accuracy, while others note that domain shifts between datasets can negatively impact model performance. Additionally, while some models achieve near-perfect detection accuracy in experimental settings, their real-world applicability is questioned due to a lack of real-time validation and adaptability to evolving threats.

Synthesis Matrix for Literature Review

Study	Authors	Year	Research Design	Key Findings/ Results	Methodology	Limitations
Toward a Deep Learning-Based Intrusion Detection System for IoT Against Botnet Attacks	Idrissi et al.	2021	Experimental	97.2% detection accuracy	CNN-based IDS	High computational cost
IoT Malware Detection Based on Ensemble Deep Transfer Learning	Sharma et al.	2022	Experimental	96.31% detection accuracy	Transfer Learning (ResNet101, VGG16)	Data transformation overhead
ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks	Abu Al-Haija & Al-Dala'ien	2022	Experimental	99.6% detection accuracy	Ensemble Learning (AdaBoost, RUSBoost, Bagging)	Not tested in real-world IoT
Enhancing Security in Cyber-World by Detecting Botnets Using Ensemble Classification-Based Machine Learning	Srinivasan & Deepalakshmi	2023	Experimental	94.08% detection accuracy	Stacking-Based Ensemble Learning	Scalability issues
Using Ensemble Learning Technique for Detecting Botnet on IoT	Rezaei	2021	Experimental	100% detection accuracy	Supervised & Unsupervised Learning	Limited real-world validation
Deep Transfer Learning: A Novel Collaborative Learning Model for Cyberattack Detection Systems in IoT Networks	Khoa et al.	2022	Experimental	99% detection accuracy	Transfer & Federated Learning	Computationally intensive

References

- 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.
- 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.
- 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.
- 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.
- 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.
- Rezaei, A. (2021). Using ensemble learning technique for detecting botnet on IoT. *SN Computer Science*, 2(3), 148.