

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 20 June 2026

Hand-in Date: 4 July 2026

Hand-in Method: Online Submission via E-Learning (Moodle)

Assignment Report: Literature Review to early detection Botnet in Smart home IoT

Student ID: 262001048

Student Name: Ahmed Hasan Salem Alhamdi

Table of contents:

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

Summary research paper's:

Paper1: A collaborative approach for early detection of IoT Botnet

This paper proposes a collaborative machine learning model for early detection of IoT botnets through Machine learning and deep learning algorithms, this approach needs time to collect data before executions. This duration of collecting data and executing gives time to the malware from the attacker to deploy botnet such as DDoS , the objective of this research is to minimize the focus on capturing the abnormality on the first initial attempt of attack before the malware complete and take control of the devices.

Paper2: Toward a deep learning-based intrusion detection system for IoT against botnet attacks.

This paper proposes a new IDS solution baptized BotIDS based on deep learning convolutional neural networks (CNN), it designs, implement and tests the IDS against some well-known Botnet attacks using specific Bot-IoT dataset. The study uses the latest Bot-IoT dataset that was created specifically for IoT systems. The environment processes a combination of usual normal and bad traffic, with sis types of attacks and 10 subcategories. The objective of this study is to move from traditional binary classification to multilabel classification network model.

Critical Analysis:

In paper 1 the preprocessing dataset uses early detection approach from the beginning first seconds it executes once receives the attack before the program finish installing and taking control of the device. Its uses V-sandbox methodology but has a limitation on 3 minutes collecting data at some process.

In paper 2 the preprocessing dataset uses full network traffic mentoring through multilabel classification model CNN architecture that have limitations with The network security, it does not execute security controls locally on resource-constrained end-devices.

Connections:

Both papers focus on securing IoT environments against botnet attacks. Both papers uses their defensive models to secure consumer electronics. Both Papers tests their models using real firmware binaries extracted from IoT smart home Devices IP cameras, routers, Smart TVs, and home smart devices.

Conflicts between the findings:

Paper 1 propose Early detecting on first seconds before waiting for the attacker (like a DDoS attack) has to execute and deploy and taking control (like a DDoS attack) has already executed.

Paper 2 proposes that a detecting model needs the data to achieve maximum accuracy. the cutting off data collection too early leads to missing hidden malware.

• **Synthesis Matrix for Literature Review**

Study	Authors	Year	Research Design	Key Findings/Result	Methodology	Limitations
A collaborative approach for early detection of IoT Botnet	• Giang L. Nguyen. • Braulio Dumba • Quoc-Dung Ngo • Hai-Viet Le • Tu N. Nguyen	2022	Experimental Quantitative	The paper proposed collaborative approach early detection IoT Botnet achieves high classification accuracy of 99.37% with a very low False Positive rate 0.0194. This approach needs 6 seconds to identify and detect an attack.	A fusion function machine learning multi stage distribution of dataset V-Sandbox Execution : (ARM,MIPS, Intel 80386, PowerPC, X86-64) Collaborative Learning: (KNN, RF, Soft Voting)	Starting up the virtual machines and launching V-Sandbox to collect data including a loop to collect more data after each run leads to an increase in total time processing a sample up to approximate 3 min. This is a limitation of Botnet IoT detection framework.
Toward a deep learning-based intrusion detection system for IoT against botnet attacks	• Idriss Idrissi • Mohammed Boukabous • Mostafa Azizi • Omar Moussaoui • Hakim El Fadili	2021	Experimental Quantitative	The paper proposed multi-class classification model. The CNN approach IoT Botnet achieves high classification accuracy of 99.94% and low loss of 0.58%. The solution needs only 0.34 milliseconds to execute.	Data preprocessing: Attack distribution in training and testing set and subsets using the benchmark Bot-IoT dataset (from UNSW Canberra Cyber Range Lab). Building model: The CNN uses Convolution2D layer, MaxPooling2D layer, Flatten layer, layer and an output layer	In some smart home types such as DoS (HTTP), DDoS (HTTP), key logging, and data exfiltration attacks on dataset have very small data which prevents the model from learning & identifying these threats. The network security, does not execute security controls locally on resource-constrained end-devices.

- **Reference:**

IAES International Journal of Artificial Intelligence (IJ-AI) 110 Vol. 10, No. 1, March 2021, pp. 110~120
ISSN: 2252-8938, DOI: 10.11591/ijai.v10.i1.pp110-120

Computers and Electrical Engineering 97 (2022) 107525 Contents lists available at ScienceDirect
ComputersandElectricalEngineering

journal homepage: www.elsevier.com/locate/compeleceng