



UNDERGRADUATE THESIS

**IMPLEMENTATION OF HYBRID DETECTION
WITH CASCADE MECHANISM FOR DDOS
MITIGATION ON IOT NETWORKS USING
RASPBERRY-PI**

MUCHAMMAD BASROIL BILLAH
NPM 22081010260

THESIS ADVISORS

Dr. Ir. Mohammad Idhom, SP, S. Kom., MT.
Hendra Maulana, S.Kom., M.Kom.

**MINISTRY OF HIGHER EDUCATION, SCIENCE, AND TECHNOLOGY
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FACULTY OF COMPUTER SCIENCE
INFORMATICS STUDY PROGRAM
SURABAYA
2026**

APPROVAL SHEET

IMPLEMENTATION OF HYBRID DETECTION WITH CASCADE MECHANISM FOR DDOS MITIGATION ON IOT NETWORKS USING RASPBERRY-PI

By:
MUCHAMMAD BASROIL BILLAH
NPM. 22081010260


Has been defended before, and accepted by, the Board of Assessors of the Thesis Examination of the Informatics Study Program, Faculty of Computer Science, Universitas Pembangunan Nasional Veteran Jawa Timur, on April 16, 2026:

Approved,


Dr. Ir. Mohammad Idhem, SP, S. Kom., MT.
NIP. 19861008 202121 1 001


..... (Advisor I)


Hendra Maulana, S.Kom., M.Kom.
NIP. 19900412 202406 1 003


..... (Advisor II)

Retno Mumpuni, S.Kom., M.Sc.
NIP. 198707162025212045


..... (Head Assessor)

Henni Endah Wahanani, ST, M.Kom.
NIP. 19780922 202121 2 005


..... (Assessor I)

Acknowledge by,

Dean of the Faculty of Computer Science



Prof. Dr. Ir. Novirina Hendrasarie, M.T.
NIP. 19681126 199403 2 001

APPROVAL SHEET

IMPLEMENTATION OF HYBRID DETECTION WITH CASCADE MECHANISM FOR DDOS MITIGATION ON IOT NETWORKS USING RASPBERRY-PI

By:
MUCHAMMAD BASROIL BILLAH
NPM. 22081010260

Approved to proceed to the Thesis Examination

Approved by,

Coordinator of Informatics Study Program
Faculty of Computer Science



Dr. Intan Yuniar Purbasari, S.Kom. MSc.

NIP. 19800602 202521 2 029

STATEMENT OF ORIGINALITY

I am the undersigned:

Student Name : Muchammad Basroil Billah
NPM : 22081010260
Degree Program : Bachelor (S1)
Study Program : Informatics
Faculty : Faculty of Computer Science

Hereby declares that this undergraduate thesis contains no part of any other scientific work that has been submitted to obtain an academic degree at any higher education institution. Furthermore, it does not contain any work or opinions previously written or published by others, except for those which are explicitly cited in this thesis and listed completely in references.

And I declare that this scientific document is free from elements of plagiarism. If in the future indications of plagiarism are found in this Thesis, I am willing to accept sanctions in accordance with the applicable laws and regulations.

Thus, I made this statement without any coercion from anyone and to be used as it should.



Surabaya, April 10, 2026
Declarant,



MUCHAMMAD BASROIL BILLAH
NPM. 22081010260

ABSTRACT

Student Name / NPM : Muchammad Basroil Billah / 22081010260
Thesis Title : Implementation of Hybrid Detection with Cascade Mechanism for DDoS Mitigation on IoT Networks using Raspberry-Pi
Advisor : 1. Dr. Ir. Mohammad Idhom, S.P., S.Kom., M.T.
2. Hendra Maulana, S.Kom, M.Kom

Internet of Things (IoT) devices typically operate with limited computational resources, leaving them highly vulnerable to Distributed Denial of Service (DDoS) attacks. Existing approaches present a fundamental trade-off: rule-based detection offers low latency but struggles with ambiguous attack patterns, while machine learning achieves higher accuracy at the cost of substantial computational overhead unsuitable for edge devices. This research develops a hybrid DDoS detection system with a cascade mechanism on a Raspberry Pi 4B acting as a security gateway. The architecture consists of three sequential layers: Tier 1 rule-based detection for immediate blocking using three high-precision rules (R1: rate > 456.08 pps; R2: ICMP flag; R3: SYN-only flag), Tier 2 weighted scoring with five rules (R4–R8, maximum score 160, blocking threshold 70%) for ambiguous traffic, and a Random Forest model trained on the CICIoT2023 dataset (46 features, 1,154,684 samples) as the final layer. Threshold values were derived from percentile-based statistical distribution analysis, with mitigation enforced through iptables and real-time alerts delivered via Telegram Bot API. Evaluation results demonstrate 99.84% accuracy, 99.99% recall, and 99.92% F1-score, with 94.76% of traffic resolved directly by the rule-based layer. Stress testing up to 50,000 pps recorded maximum CPU usage of 26.2%, confirming sufficient headroom on the Raspberry Pi 4B. Scenario testing and independent pentester validation confirmed a 100% detection rate across volumetric, protocol, and application-layer attacks with detection latency below one second, while MQTT-based IoT communication remained unaffected with zero false positives. The proposed cascade-based hybrid detection system effectively combines rule-based responsiveness with machine learning accuracy on resource-constrained devices.

Keywords: DDoS, Hybrid Detection, Cascade, Rule-Based, Random Forest, IoT, Raspberry Pi, Security Gateway

ACKNOWLEDGEMENTS

All praise is due to Allah SWT, whose grace, guidance, and countless blessings have accompanied the author throughout every stage of this journey. Through His mercy and strength, the author was able to complete this thesis entitled **Implementation of Hybrid Detection with Cascade Mechanism for DDoS Mitigation on IoT Networks using Raspberry-Pi** as a requirement for obtaining a Bachelor's degree in Informatics at UPN "Veteran" Jawa Timur.

Throughout the process of completing this thesis, the author received invaluable support, guidance, encouragement, and prayers from many individuals. Therefore, with sincere gratitude, the author would like to express heartfelt appreciation to:

1. Prof. Dr. Ir. Novirina Hendrasarie, M.T., as Dean of the Faculty of Computer Science, UPN "Veteran" Jawa Timur.
2. Dr. Intan Yuniar Purbasari, S.Kom. MSc., as Coordinator of the Informatics Study Program, Faculty of Computer Science, UPN "Veteran" Jawa Timur.
3. Budi Mukhamad Mulyo, S.Kom., M.T., as the author's academic advisor, who has provided continuous guidance from the beginning of the author's studies to the very end.
4. Dr. Ir. Mohammad Idhom, S.P., S.Kom., M.T. and Hendra Maulana, S.Kom., M.Kom., as Thesis Supervisors, who have patiently guided and directed the author throughout the completion of this thesis.
5. Retno Mumpuni, S.Kom., M.Sc. and Henni Endah Wahanani, S.T., M.Kom., as Thesis Examiners, whose constructive feedback has helped refine this thesis into its final form.
6. All lecturers of the Informatics Study Program at UPN "Veteran" Jawa Timur, who have imparted knowledge, guidance, and inspiration that have shaped the author's academic development.
7. My beloved mother, Srinarwati, who has always been the safest place for the author to return to in every situation. Thank you for your endless love, prayers, unwavering support, and strength that have accompanied the author throughout this journey.

8. My beloved father, Gatot Wibisono, who taught the author the values of responsibility, perseverance, and hard work. His advice and example have become the foundation that encourages the author to keep striving and never give up.
9. My beloved brothers, Dimas Fatchurrohman Rijali Wicaksono and Adhika Achmad Jalalludin Rummy, who have always provided support, encouragement, and care throughout every stage of this journey.
10. Raihana Sakhi Aswanda, who has always been there through every difficulty and every step of this long journey. Thank you for being a source of strength, comfort, and motivation, and for always being there with patience and support through moments of exhaustion and uncertainty.
11. Bregas, Wahyu, Paskal, Fadika, Amanda, Belia, Kadek, and Deva, for the shared struggles, laughter, and memories that have made this journey meaningful and unforgettable. Thank you for the support and companionship throughout university life.
12. Yasir, Ryan, Nabil, and the rest of the Mamino circle, for the support, the chaos, and the kind of friendship that makes everything else feel easier.
13. Mavel, Pramudya, Al-Fitra, and Nathan, for the support, friendship, and memorable moments shared throughout this journey.
14. All members and administrators of the Informatics Student Association (HIMATIFA) at UPN "Veteran" Jawa Timur, who have taught the author the meaning of camaraderie and shared purpose.
15. The author also sincerely thanks everyone who has provided support, prayers, and encouragement throughout the completion of this thesis

The author humbly welcomes constructive criticism on this thesis, in the hope that it may continue to grow and bring something of value to its readers and to the field.

Surabaya, April 10th 2026

Author

TABLE OF CONTENTS

APPROVAL SHEET	ii
APPROVAL SHEET	iii
STATEMENT OF ORIGINALITY	iv
ABSTRACT	v
ACKNOWLEDGEMENTS.....	vi
TABLE OF CONTENTS.....	viii
LIST OF TABLES	xi
LIST OF FIGURE.....	1
CHAPTER I INTRODUCTION.....	4
1.1. Background	4
1.2. Problem Formulation.....	6
1.3. Research Objectives	6
1.4. Research Benefits	6
1.5. Research Limitations.....	7
CHAPTER II LITERATURE REVIEW	9
2.1. Previous Research	9
2.2. Network Security.....	11
2.3. Distributed Denial of Service (DDoS)	12
2.4. Intrusion Detection System (IDS)	14
2.5. Internet of Things (IoT).....	15
2.6. Rule-Based	15
2.7. Machine Learning	16
2.7.1. Preprocessing.....	17
2.7.2. Classification	19
2.7.3. Random Forest	19
2.8. Raspberry Pi 4B	23
2.9. CVSS (Common Vulnerability Scoring System).....	24
2.10. Supporting Tools	25
2.10.1. Telegram.....	25
2.10.2. Kali Linux.....	25

2.10.3. Iptables	26
2.10.4. Scapy	26
2.10.5. Nmap	27
2.10.6. Hping3	28
2.10.7. SlowHTTPTest.....	28
CHAPTER III METHODOLOGY.....	30
3.1. Research Approaches	30
3.2. Observations.....	31
3.3. Literature Study.....	31
3.4. Analysis.....	32
3.4.1. Problem Analysis.....	32
3.4.2. Solution Analysis.....	33
3.4.3. Requirements Analysis.....	33
3.5. Design.....	34
3.5.1. Raspberry Pi 4B Design	34
3.5.2. System Architecture System Design	35
3.5.3. Rule-Based Detection Design.....	37
3.5.4. Machine Learning Model Design.....	38
3.5.5. Decision Logic Design	39
3.5.6. Network Topology Design	41
3.6. Development	42
3.6.1. Rule-Based Detection Development	42
3.6.2. Machine Learning Development	47
3.7. Implementation.....	60
3.7.1. Set Up Raspberry Pi 4B.....	60
3.7.2. Action Executor & Notification Implementation	61
3.8. Evaluation.....	63
3.8.1. Functionality Testing.....	63
3.8.2. Performance Testing.....	63
3.8.3. Scenario Testing	64
3.8.4. Pentesting	66
3.8.5. Analysis and Results.....	68

CHAPTER IV RESULT AND DISCUSSION.....	69
4.1. General Overview of Testing	69
4.1.1. Results of Raspberry Pi 4B Assembly.....	70
4.1.2. IoT Device (Greenbeans Moisture Content)	71
4.1.3. Results of the Network Topology Assembly.....	72
4.2. Functional Testing Results	73
4.2.1. Results of Rule-Based	73
4.2.2. Results of Machine Learning.....	82
4.2.3. Results of Hybrid Detection	94
4.2.4. Results of System Component Implementation and Testing.....	98
4.3. Result of Performance Test	105
4.3.1. Results of the Latency Test	105
4.3.2. Results of the Stress Test.....	107
4.4. Results of Scenario Testing.....	112
4.4.1. Normal Scenario	113
4.4.2. Attack Scenario	115
4.5. Pentester Validation Results.....	129
4.5.1. Attack Test Results	129
4.5.2. Analysis of Validation Result.....	130
4.6. Analysis of Results.....	130
4.6.1. The Crucial Role of Rule-Based Detection During Attacks.....	130
4.6.2. Trade-off in the Hybrid Cascade Architecture	132
4.6.3. Rate Context in the Dataset vs the Real IoT Environment.....	133
CHAPTER V CONCLUSION	134
5.1. Conclusion.....	134
5.2. Recommendations	135
BIBLIOGRAPHY	137
APPENDIX	141

LIST OF TABLES

Table 2. 1 Previous Research	9
Table 3. 1 Rule-Based Design.....	38
Table 3. 2 Decision Logic Design.....	40
Table 3. 3 Statistical Analysis Results of the CICIoT2023 Dataset.....	43
Table 3. 4 Threshold Determination for the 8 Rules.....	44
Table 3. 5 Implementation of the 8 Rules in the Rule-Based System.....	45
Table 3. 6 Execution of Rule R1 with Various Inputs	46
Table 3. 7 Retained Categories	48
Table 3. 8 Binary Labeling.....	48
Table 3. 9 Results of Data Filled with Mean Values	49
Table 3. 10 Results of Duplicate Data Removal	49
Table 3. 11 Normalized Data Results.....	51
Table 3. 12 Class Weighting	51
Table 3. 13 Sample Data for the Random Forest Process.....	54
Table 3. 14 Bootstrap Sampling Tree 1.....	55
Table 3. 15 Bootstrap Sampling Tree 2.....	55
Table 3. 16 Prediction Results.....	57
Table 3. 17 Predictions from 5 Trees	58
Table 3. 18 Confusion Matrix	59
Table 3. 19 Raspberry Pi 4B Setup Stages.....	60
Table 3. 20 Network Interface Configuration	61
Table 3. 21 iptables Configuration.....	62
Table 3. 22 IP Whitelist.....	63
Table 3. 23 Performance Testing	64
Table 3. 24 Pentester Bioprofile.....	66
Table 3. 25 Pentester Experience	67
Table 4. 1 Hardware Specifications	69
Table 4. 2 Feature Distribution Analysis Results.....	75
Table 4. 3 Threshold Determination Results per Feature.....	77
Table 4. 4 Tier 1 Configuration – Immediate Block.....	78
Table 4. 5 Tier 2 Configuration – Scoring Rules.....	79

Table 4. 6 Rule-Based Performance Metrics	81
Table 4. 7 Analysis of Attack Types That Passed Through	82
Table 4. 8 Training, Validation, and Test Metrics	87
Table 4. 9 Results of Model Validation Analysis	90
Table 4. 10 Analysis of Detection Accuracy - Attack Type	92
Table 4. 11 Machine Learning Benchmark Test	93
Table 4. 12 Comparative Analysis of Hybrid Detection Metric Improvements ...	95
Table 4. 13 Analysis of Hybrid Detection Results.....	97
Table 4. 14 Configuration Results.....	100
Table 4. 15 Network Discovery Results.....	102
Table 4. 16 Service Enumeration Results	103
Table 4. 17 Configuration Results for Each Implemented Component	105
Table 4. 18 Analysis of System Response to Attacks	107
Table 4. 19 Stress Test Parameters.....	107
Table 4. 20 Summary of Stress Test Results.....	112
Table 4. 21 Attack Scenario Configuration.....	116
Table 4. 22 Summary of Attack Scenario Results	127
Table 4. 23 Comparison of Normal vs DDoS Attack Conditions.....	131
Table 4. 24 ML Load Simulation During a 10,000 pps Attack.....	131
Table 4. 25 Hybrid Detection Trade-off Analysis.....	132
Table 4. 26 Rate Context Comparison Across Different Levels.....	133

LIST OF FIGURE

Figure 2. 1 CIA Triad.....	11
Figure 2. 2 DDoS Attack.....	13
Figure 2. 3 Raspberry Pi 4B.....	23
Figure 2. 4 CVSS (Common Vulnerability Scoring System)	24
Figure 2. 5 Telegram.....	25
Figure 2. 6 Kali Linux.....	26
Figure 2. 7 Firewall iptables	26
Figure 2. 8 Scapy	27
Figure 2. 9 Nmap	27
Figure 2. 10 Hping3	28
Figure 2. 11 SlowHTTPTest (Slowloris)	29
Figure 3. 1 R&D ADDIE Flowchart.....	30
Figure 3. 2 Dataset CICIOT2023	34
Figure 3. 3 Raspberry Pi 4B Design.....	35
Figure 3. 4 System Architecture Design	36
Figure 3. 5 Execute Actions	40
Figure 3. 6 Network Topology Design	41
Figure 3. 7 Rule-Based Development Flowchart.....	42
Figure 3. 8 Rule-based Evaluation Flow.....	45
Figure 3. 9 Machine Learning Model Development Flow.....	47
Figure 3. 10 Preprocessing Stage.....	49
Figure 3. 11 Training Model Flowchart.....	52
Figure 3. 12 Random Forest Flowchart	53
Figure 3. 13 Scenario Testing	64
Figure 3. 14 Normal Traffic Test Scenario	65
Figure 3. 15 DDoS Attack Test Scenario.....	65
Figure 4. 1 Raspberry Pi 4B Assembly.....	70
Figure 4. 2 Raspberry Pi Debian OS Display	71
Figure 4. 3 IoT Device (Greenbeans Moisture Content)	71
Figure 4. 4 Network Topology Assembly.....	72
Figure 4. 5 Visualization of Feature Distribution Results: Normal vs Attack.....	74
Figure 4. 6 Percentile Analysis Visualization with Threshold Lines.....	76
Figure 4. 7 Tier 1 Precision & Tier 2 F1-Score & Weight	80

Figure 4. 8 Confusion Matrix Rule-Based	81
Figure 4. 9 Dataset Loading	83
Figure 4. 10 Label Filtering Results.....	84
Figure 4. 11 Hybrid Balancing Results	84
Figure 4. 12 Hybrid Balancing Results	85
Figure 4. 13 Feature Scaling Results Using Standard Scaler.....	85
Figure 4. 14 Model Parameter Initialization	86
Figure 4. 15 Machine Learning Confusion Matrix	87
Figure 4. 16 Model Validation Test	89
Figure 4. 17 Data Leakage Check	89
Figure 4. 18 Feature Dependency Test	90
Figure 4. 19 Top 10 Feature Importance of Random Forest.....	91
Figure 4. 20 Detection Rate Results - Attack Type	92
Figure 4. 21 Comparison of Rule-Based Standalone vs Hybrid Detection.....	95
Figure 4. 22 Hybrid Detection Results.....	96
Figure 4. 23 Hybrid Detection Comparison Confusion Matrix	97
Figure 4. 24 IP Configuration on eth0 and wlan0.....	98
Figure 4. 25 Access Point Configuration (hostapd).....	99
Figure 4. 26 DHCP Server Configuration (dnsmasq)	99
Figure 4. 27 iptables Rules and NAT.....	100
Figure 4. 28 IP Forwarding Status	100
Figure 4. 29 Network Discovery Using Nmap	102
Figure 4. 30 Service Enumeration.....	103
Figure 4. 31 System Integration & Configuration Results.....	104
Figure 4. 32 Telegram Alert Notification	104
Figure 4. 33 Latency Test Results – Audit Trail.....	106
Figure 4. 34 First Stress Test Using Nmap	108
Figure 4. 35 System Response to the First Stress Test.	109
Figure 4. 36 Second Stress Test Using Nmap.....	109
Figure 4. 37 System Response to the Second Stress Test	110
Figure 4. 38 Third Stress Test Using Nmap.....	110
Figure 4. 39 System Response to the Third Stress Test.....	111
Figure 4. 40 Fourth Stress Test Using Nmap.....	111
Figure 4. 41 System Response to the Fourth Stress Test.....	112

Figure 4. 42 IoT Connection Configuration.....	113
Figure 4. 43 IP of Connected IoT Device	114
Figure 4. 44 Detection System Initialization on RPI	114
Figure 4. 45 IoT Dashboard & MQTT Status	115
Figure 4. 46 SYN Flood Attack Parameters.....	116
Figure 4. 47 System Blocking of SYN Flood Attack	117
Figure 4. 48 Telegram Notification for SYN Flood Attack.....	118
Figure 4. 49 ICMP Flood Attack Parameters.....	119
Figure 4. 50 System Blocking of ICMP Flood Attack.....	119
Figure 4. 51 Telegram Notification for ICMP Flood Attack	120
Figure 4. 52 UDP Flood Attack Parameters.....	121
Figure 4. 53 System Blocking of UDP Flood Attack	121
Figure 4. 54 Telegram Notification for UDP Flood Attack.....	122
Figure 4. 55 Low-Rate Attack Parameters	123
Figure 4. 56 System Blocking of Low-Rate Attack.....	123
Figure 4. 57 Telegram Notification for Low-Rate Attack	124
Figure 4. 58 Very Low-Rate Attack Parameters.....	125
Figure 4. 59 System Blocking of Very Low-Rate Attack.....	125
Figure 4. 60 Telegram Notification for Very Low-Rate Attack	126
Figure 4. 61 IoT Workflow Dashboard Uninterrupted	128
Figure 4. 62 Network Audit Trail After the Attack	128
Figure 4. 63 Summary of Pentester Test Results	129