

# Analysing Cloud DDoS Attacks Using Supervised Machine Learning

Chisom Elizabeth Alozie

# Analysing Cloud DDoS Attacks Using Supervised Machine Learning

**Chisom Elizabeth Alozie**

University of the Cumberland, United States



**DeepScience**

*Published, marketed, and distributed by:*

Deep Science Publishing  
USA | UK | India | Turkey  
Reg. No. MH-33-0523625  
www.deepscienceresearch.com  
editor@deepscienceresearch.com  
WhatsApp: +91 7977171947

ISBN: 978-93-49307-68-1

E-ISBN: 978-93-49307-78-0

<https://doi.org/10.70593/978-93-49307-78-0>

Copyright © Chisom Elizabeth Alozie

**Citation:** Alozie, C. E. (2025). *Analysing Cloud DDoS Attacks Using Supervised Machine Learning*. Deep Science Publishing. <https://doi.org/10.70593/978-93-49307-78-0>

This book is published online under a fully open access program and is licensed under the Creative Commons "Attribution-Non-commercial" (CC BY-NC) license. This open access license allows third parties to copy and redistribute the material in any medium or format, provided that proper attribution is given to the author(s) and the published source. The publishers, authors, and editors are not responsible for errors or omissions, or for any consequences arising from the application of the information presented in this book, and make no warranty, express or implied, regarding the content of this publication. Although the publisher, authors, and editors have made every effort to ensure that the content is not misleading or false, they do not represent or warrant that the information-particularly regarding verification by third parties-has been verified. The publisher is neutral with regard to jurisdictional claims in published maps and institutional affiliations. The authors and publishers have made every effort to contact all copyright holders of the material reproduced in this publication and apologize to anyone we may have been unable to reach. If any copyright material has not been acknowledged, please write to us so we can correct it in a future reprint.

# Preface

Cloud computing in its simplest form refers to the provision of hardware and software to deliver a service over an internet network. However, Cloud Computing has numerous issues, such as security attacks and distributed denial of service (DDoS). A DDoS attack is defined as a method of attack in which numerous computer systems are allowed to attack a target, such as a server, any resource, or website, resulting in a denial of service for the resource's intended users.

This research analysed the normal traffic and DDoS attack traffic from cloud environments using machine learning technology to detect DDoS attacks. This work's main contribution is the extraction of dataset features and the discovery of new flow features for DDoS attack detection. To create the dataset, novel features are stored in a CSV file using the CICFlowMeter tool. Features were selected using a correlation coefficient to get better model accuracy. Machine learning algorithms were trained on the resulting cloud dataset. The existing work reviews for detection of DDoS attacks either used a cloud dataset or another network data set, or the research findings were kept confidential. The methodology used to solve this problem is the CRISP-DM methodology.

The proposed solution deployed a brand-new dataset with five machine-learning models for classification. The findings of this study help to improve knowledge of the ability of DDoS datasets to detect intrusions. Five performance metrics—accuracy, precision, recall, F1-score, and computation time were used to analyse the datasets. Based on the results achieved with the new dataset, the Random Forest, Support Vector Machine, Decision Tree, and K-NN achieved a 100% rate of 100% on the accuracy, precision, recall, and F1 score in a shorter computation time. With the open-source dataset, Random Forest, Decision Tree, and K-Nearest Neighbor achieved 100% accuracy.

Chisom Elizabeth Alozie

# Contents

<b>1 Cloud security vulnerabilities: Analysing DDoS attack methods and mitigation strategies.....</b>	<b>1</b>
1.1 Introduction.....	1
1.2 Motivation.....	2
1.3 Problem Overview.....	3
1.4 Research Questions.....	3
1.5 Aims and objectives.....	4
1.6 Project Scope.....	4
1.7 Report Organisation.....	5
<b>2 Background study of DDoS attacks.....</b>	<b>6</b>
2.1 Theoretical background.....	6
2.1.1 Overview of DDoS Attacks.....	6
2.1.2 Classification of DDoS Attacks.....	7
2.1.3 DDoS attack operations technique.....	7
2.1.4 Cloud Computing System.....	9
2.1.5 OwnCloud Platform.....	10
2.1.6 DDoS Threats on Cloud System.....	11
2.1.7 Methods of DDoS attacks.....	12
2.1.7.1 Slow request/response attack.....	12
2.1.7.2 Malformed packet attack.....	13
2.1.7.3 Protocol exploited attack.....	13
2.1.7.4 Amplification.....	13
2.1.8 DDoS Attack Tools.....	13

2.1.8.1	Slowloris.....	14
2.1.8.2	Strengths and Weaknesses of Slowloris Tool.....	14
2.1.9	Programming tools.....	15
2.1.10	Machine Learning.....	16
2.1.10.1	Supervised Machine Learning.....	16
2.1.10.2	Models employed in this research.....	17
2.1.10.3	Confusion Matrix.....	18
2.2	Experimental Background.....	19
2.2.1	Method.....	19
2.2.2	Research Gaps.....	21
2.2.3	Investigation Report Summary.....	22
<b>3</b>	<b>Feature selection and machine learning model optimization for DDoS detection.....</b>	<b>24</b>
3.1	Introduction.....	24
3.2	System Setup.....	25
3.2.1	Network Type.....	26
3.2.2	Kali Linux VM.....	26
3.2.3	Oracle VirtualBox.....	26
3.2.4	Host PC.....	26
3.2.5	Performing of DDoS attack in Owncloud VM.....	26
3.2.6	Performing of Benign Traffic.....	27
3.2.7	Collection of Pcap Files.....	27
3.3	Machine Learning Flow Process Design.....	30
3.3.1	Raw Data Collection.....	30
3.3.2	Feature Extraction.....	31
3.3.2.1	Extracted Dataset Description.....	33
3.3.3	Feature Selection.....	37

3.3.3.1	Correlation Coefficient.....	37
3.3.3.2	Feature Selection for The New Dataset.....	38
3.3.3.3	Feature Selection for the CSE-CICIDS2018 Dataset.....	39
3.3.4	Data Pre-processing.....	41
3.3.4.1	Data Cleaning and Transformation.....	41
3.3.5	Dataset Splitting.....	39
3.3.6	Modelling.....	42
3.3.6.1	Selection of Models.....	42
3.3.7	Training.....	42
3.3.8	Validation.....	44
3.3.9	Testing.....	45
3.3.10	Evaluation.....	46
<b>4</b>	<b>Performance metrics analysis: Evaluating machine learning models in the detection of cloud-based DDoS.....</b>	<b>49</b>
4.1	Overview of Performance Analysis Results.....	49
4.2	New Dataset Performance metrics.....	50
4.3	Open-Source Dataset Performance Metrics.....	52
4.4	Confusion matrix for the datasets.....	53
4.5	Validation Results.....	55
4.6	Reflections.....	58
4.6.1	Research Questions Reflections.....	58
4.6.2	Objective Comparison Reflections.....	60
4.6.3	Requirement Achievement Reflection.....	61
4.6.4	Reflection on Legal, Ethical, Social and professional, Risk and safety.....	62
4.6.5	Reflection on observation in this work.....	63

<b>5 Strategic recommendations for enhancing DDoS defense mechanisms in cloud environments .....</b>	<b>64</b>
5.1 Conclusion and Future work.....	64
5.2 Recommendation for Future Work.....	65
<b>References.....</b>	<b>66</b>
<b>Appendix.....</b>	<b>77</b>



## List of Abbreviations

---

<b>Words</b>	<b>Meaning</b>
API	Application Programming Interface
ARP	Address Resolution Protocol
AWS	Amazon Web Service
C&C	Command and controls
CC	Cloud Computing
CICDDoS2019	Canada Institute of Cybersecurity Distributed Denial of Service 2019
CICIDS2017	Canada Institute of Cybersecurity Intrusion Detection System 2017
CSE-CIC-IDS2018	Computer Science and Engineering-Canada Institute of Cybersecurity- Intrusion Detection System 2018
CNN	Cable News Network
CPU	Central Processing Unit
CRISP	Cross Industry Standard Process for Data Mining
CSV	Command Separated Values
DDoS	Distributed Denial of Service
DL	Deep Learning
DNS	Domain Name Service
DoS	Denial of Service
DT	Decision Tree
GPU	Graphics Processing Unit
GRU	Gated Recurrent Unit
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IRC	Internet relay chat

---

---

IRC	Internet Relay Chat
IT	Information Technology
K-NN	K-Nearest Neighbors
LDAP	Lightweight Directory Access Protocol
LR	Linear Regression
ML	Machine Learning
NB	Naïve Bayes
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating system
PC	Personal Computer
PCA	Principal Component Analysis
PCap	Packet Capture
RAM	Random Access Memory
RF	Random Forest
RFR	Random Forest Regression
RIP	Routing Information Protocol
RNN	Recurrent Neutral Network
SDN	Software Defined Network
SQL	Structured Queried Language
SVM	Support Vector Machine
TCP	Transmission Control Protocols
UDP	User Datagram Protocol
VM	Virtual Machine

---