DeepScience

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 Cumberlands, 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

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

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

List of Abbreviations

Words	Meaning
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