iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IV Month of publication: April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69632

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue IV Apr 2025- Available at www.ijraset.com*

# Distributed Denial of Service (DDoS) Attack Mitigation using AI

Aman Kumar[1], Aman Roy[2], Ankur Babu[3], Himesh Chaudhary[4], Dr. Saumya Chaturvedi[5], Ms. Poonam Verma[6], Dr. Sureshwati[7]
*Department of Computer Applications Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India*

***Abstract: Distributed Denial of Service(DDoS) attacks have been the major threats for the Internet and can bring great loss to companies and governments. With the development of emergingtechnologies, suchascloudcomputing, InternetofThings(IoT), artificialintelligence techniques, attackers can launch a huge volume of DDoS attacks with a lower cost, and it is much harder to detect and prevent DDoS attacks, because DDoS traffic is similar to normal traffic. Naive Bayes and Random Forest trees are two examples of artificial intelligence techniques that have been used to detect and categorize DDoS attacks using machine learning algorithms. The paper provides advice on artificial intelligence techniques to be employed in DDoS attack detection and prevention, as well as a summary of the most recent developments in DDoS attack detection utilizing AI techniques.***

***Keywords: Active Attacks, Passive Attacks, Cloud Computing, Internet of Things, AI, Security.***

## I. INTRODUCTION

Distributed Denial of Service (DDoS) attack is an attack using multiple distributed resources against targets, which will deprive authorized client from services. Attack targets include system resources, networkbandwidthandotherresources.DDoSattackshavebeen themostcommonandfatalattacksto the Internet. However, DDoS attack is hard to be detected, because attack traffic is similar to normal traffic in most case. Due to its attempt to obstruct legitimate traffic between clients and servers, DDoS attacks pose a serious danger to availability. DDoS assaults can involve massive traffic levels in a short period of time, low traffic volumes in a long period of time, or large traffic volumes in a long period of time [4], the latter of which is challenging to identify and stop. The evolution of cloud computing, the Internet of Things (IoT), and artificial intelligence approaches has led to a change in DDoS attacks, making detection and prevention more challenging. DDoS attacks can be launched against IoT devices, including light bulbs.

## II. DDOS DETECTION AND PREVENTION

### *A. DDOS classifications and features*

DDoS attacks can significantly affect the victims and increase the attack's power. Two specific DDoS assaults include IP spoofing and flooding. Attackers pose as reliable sources in IP spoofing. Attackers use flooding attacks to interfere with service availability by sending an excessive number of packets. Three types of flooding dos attacks exist: flood attack via TCP. Attackers will send the intended victim server an excessive number of TCP connection requests without acknowledging the SYN-ACK response server. Due to the excessive use of system resources by these half connections, the server will be unavailable. One of the most popular DDoS techniques is the TCP flood attack. Smurf assault, or ICMP flood attack. Sending ICMP packets with a fake IP source address is known as an ICMP flood attack. The person who owns the fake IP address will be the possible victim since it will receive a large number of ICMP responses and be overloaded. UDP flood assault. Sending an excessive number of UDP packets to a target's various ports at random is known as a UDP flood attack. assault using DNS amplification. An assault known as a DNS amplification attack occurs when the attackers fabricate the victim's source address. The DNS server receives a modest request from the attacker and responds with a huge response.

### *B. DDoSdetectionandprevention:*

Attack prevention, attack detection, and attack reaction are the most widely used methods for identifying and stopping DDoS. Because it is difficult to distinguish between attack and legitimate traffic, DDoS attacks are difficult to detect. Finding the anomaly in the traffic is the first step in identifying DDoS assaults. Additionally, the good and bad packets can be distinguished using machine learning classification techniques. We will drop packets that are categorized as attack traffic.

The number of packets, average packet size, time interval variance, packet size variance, number of bytes, packet rate, and bit rate are some characteristics that can be used to identify DDoS attacks.

### *C. Artificial Intelligence techniques*

Natural language processing, speech recognition, and machine learning are examples of common artificial intelligence approaches. Machine learning methods, specifically anomaly detection, have been used in DDoS defence and detection. The methods that are most commonly employed are support vector machines, neural networks, and Naive Bayes.

#### *1) Bayesclassification*

Based on the application of the Bayes theorem, Bayes classifiers are widely used machine learning classification techniques. Simple Bayes and independence Bayes are examples of naive Bayes models.

#### *2) Artificialneuronnetwork*

Artificial neurons with the ability to communicate with one another make up artificial neuron networks. Artificial neural networks have been applied in a variety of fields and are intended to solve issues similar to those encountered in the brain.

#### *3) Supportvectormachine*

Support vector machines are supervised learning models that examine data for regression and classification using related learning methods. Both linear and nonlinear classification can be effectively carried out using support vector machines.

### *D. Trend of DDoS attacks*

WecansummarizetheDDoStrendsas follows:

1) Highest intensity flood and largest volumetric attack: Attacks are declining, but volume, peak attack size, and speed are all increasing; 36% of attack sizes peaked at more over 5 Gbps;
2) The majority of DDoS attacks are multi-vector; in 2017, 30% of attacks used more than three attack types, while 6% used more than five. Detection will become more challenging if more attack types are employed. TCP SYN and TCP RST floods are two examples of the two primary attack types that are based on TCP and UDP. It will become more difficult to identify and stop DDoS attacks as their number, peak attack size, and speed grow.

## III. APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN DDOS ATTACK AND PREVENTION

Litrature survey

Yuan proposes Deep Defense, a deep learning-based DDoS detection approach, to improve the performance of DDoS attack detection. He formulates the DDoS detection problem as a sequence classification problem and transform the packet-based detection to window-based detection. The Deep Defense is composed of CNN, RNN (recurrent neural network) and fully connected layers. RNN can learn features better than other machine learning methods, especially longer historical features. LSTM and GRU are used to eliminate scaling issues when RNN is used to trace the history from previous packets. RNN also has a better performance in generalization than random forest does.

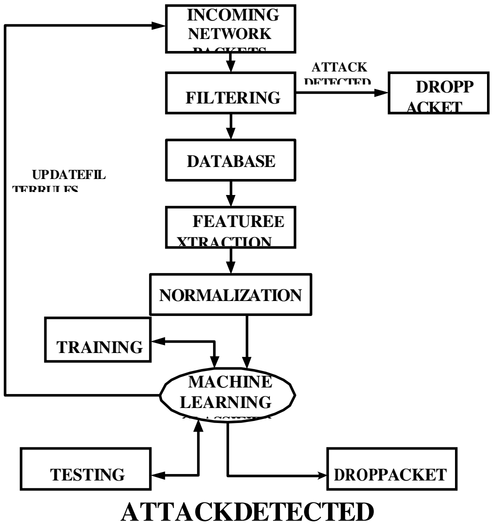


Figure1ArchitectureofDDoSAttackDetectionBasedonMachineLearning

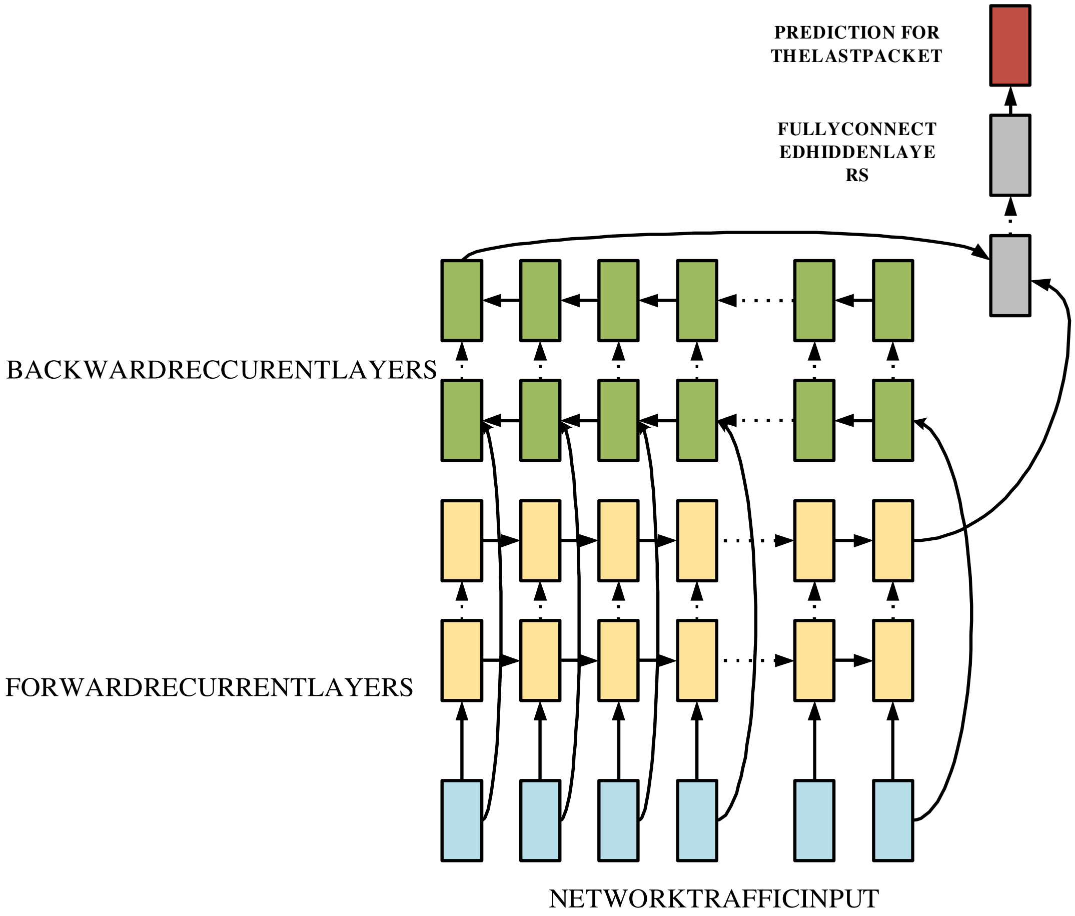


Figure2OverallNetworkArchitectureforDeep Defense

Heesh proposes a DDoS detection systembased on Neural-Networkthat is composed of five phase, packetcollector, HadoopHDFS, formatconverter,dataprocessorandneuralnetworkdetectionmodule. They choose Hadoop distributed file system to store traffic data, use big data platform integrated the neural network to detect DDoS attacks by seven parameters.

The detection system can analyze high velocity and volume network traffic and neural network can identify packet features efficiently.

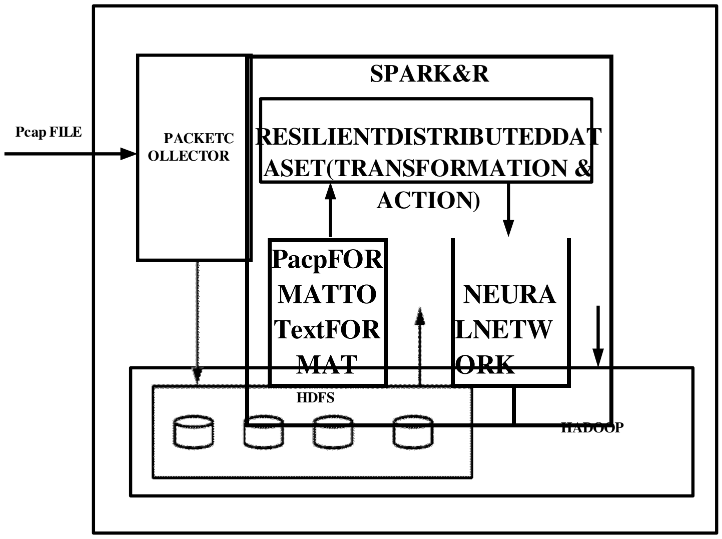

Pcap FILE
PACKETC OLLECTOR
SPARK&R
RESILIENTDISTRIBUTEDDAT ASET(TRANSFORMATION & ACTION)
PacpFOR MATTO TextFOR MAT
NEURA LNETW ORK
HDFS
HADOOP

Figure3Detectionsystemarchitecture

Barral extends a framework proposed by Zhang in 2006 to detect and prevent DDoS flood attacks based on machine learning. All nodes in the framework have the ability of learning independently and can react according to different situations. The well-known cumulated sum algorithm is used to detect huge traffic volume. Classifiers and detectors are used to distinguish pattern of normal traffic, such as Naive Bayes. Each node has the algorithmthat compares the accumulated sumof means for each time unitwithacharacteristicthresholdtoclassifymessage.ThemechanismcanstopandavoidDDoSflood attacks or abuse at early time.

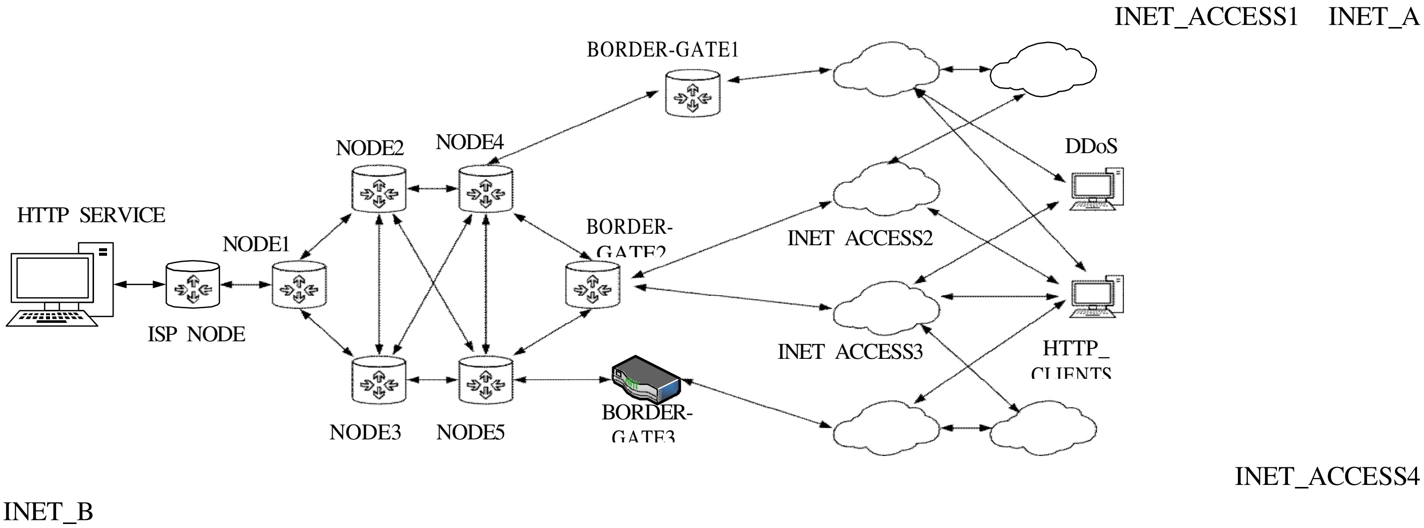


Figure4TheNetworkStructure,withthevictimservice,intermediatenetwork,exteriornetwork,and clients and attackers

KiruthikaproposesaDDoSattackdetectionandmitigationmodelusingmachinelearningalgorithm. The model is composed of online monitoring system (OMS), spoofed traffic detection module and interface-based rate limiting algorithm. OMS uses automated tools and scripts to monitor the degradation and provide DDoS impact measurements. The spoofed traffic detection module incorporateshopcountinspectionalgorithmtochecktheauthenticityofincomingpacket.Heconstructs legitimate records with IP and hop count to detect potential attacks. Hop count inspection algorithm is tochecktheauthenticityofpacket.HCF-SVMistrainedandupdatedwithsourceIPandrespectivehop count. The performance of the model is better than random forest and decision tree when classifying instance.

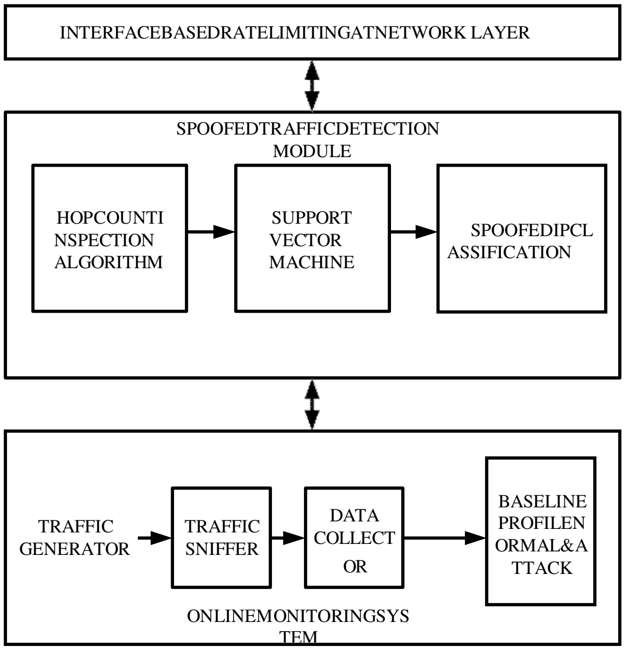

INTERFACEBASEDRATELIMITINGATNETWORK LAYER
SPOOFEDTRAFFICDETECTION MODULE
HOPCOUNTI NSPECTION ALGORITHM
SUPPORT VECTOR MACHINE
SPOOFEDIPCL ASSIFICATION
TRAFFIC GENERATOR
TRAFFIC SNIFFER
DATA COLLECT OR
BASELINE PROFILEN ORMAL&A TTACK
ONLINEMONITORINGSYS TEM

Figure5ProposedModel

ZhaodevelopsaDDoSdetectionsystembasedonneuralnetworkandimplementsinApacheHadoopclusterandHBasesystem.Thesystemhasa neuralnetworkarchitecturethathastheabilityofadapting to new types of DDoS attacks. A Hadoop and HBase cluster are setup to process huge traffic, then a neural networkmodel is designed to detect DDoS attacks. The neural networkselects parameters from Hadoop and HBase cluster module, such as CPU usage, packet size and total number of TCP connections.Hechoosesthemulti-factordetectionapproachinsteadofsinglefactordetectionapproach to detect DDoS attack, which can improve the performance of detection.MeiteidesignamodelofsystembasedonANNandthepacketheaderstatisticalinformationtodetect DDoS DNS amplification attack. They classify the DNS traffic using machine learning classification algorithms, including decision tree, multi-layer perception (MLP), Naive Bayes and support vector machine (SVM). Then choose decision tree as machine learning classification models for its best performance. The selection approach is attributed based, optimal features are extracted fromattributed selection algorithms like information gain, gain ratio and chi square. The feature parameters selected are inter packet arrival time, probability of occurrence of one IP address, answer, additional and authority of resource record, minimum packet size, average packet size and maximum packet size.

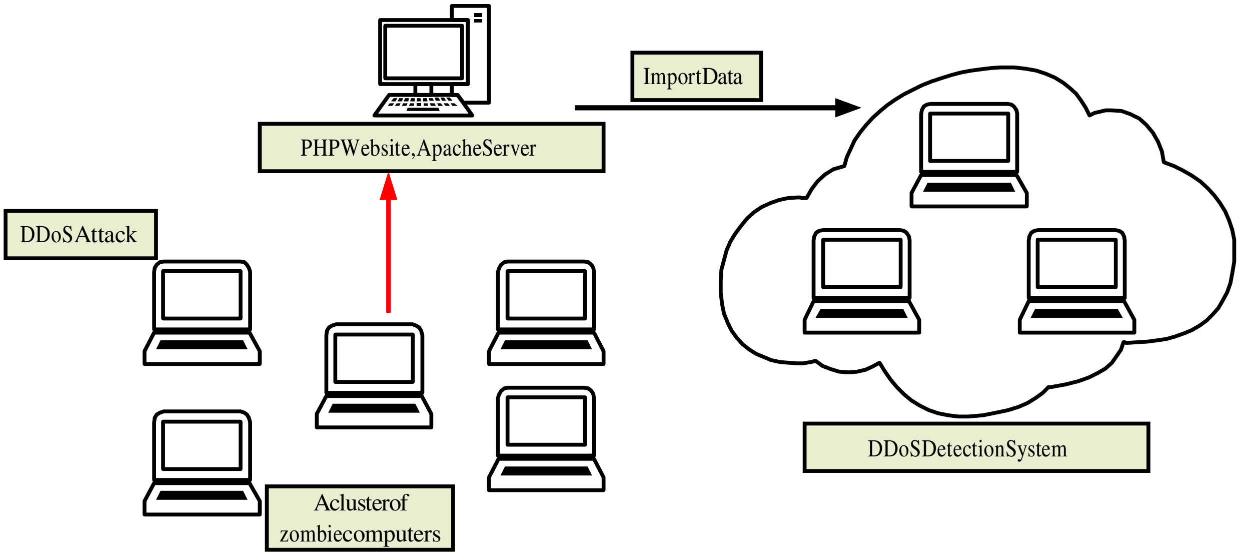


Figure6Theoverallprocessforthedesigned scenario

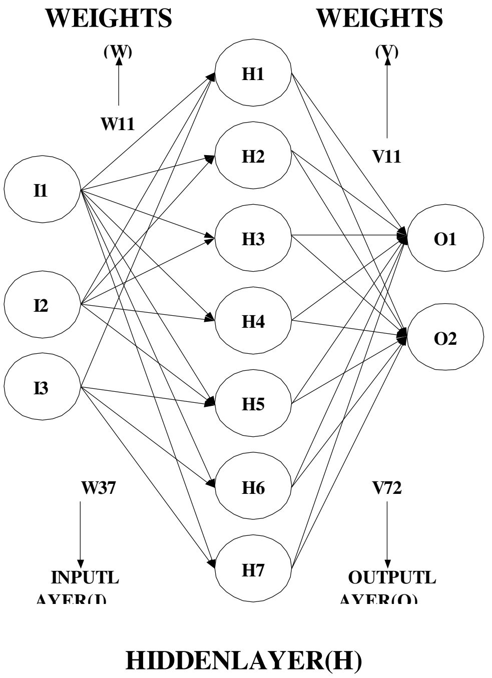


Figure7TheneuralnetworkarchitectureforDDoSdetectionsystem

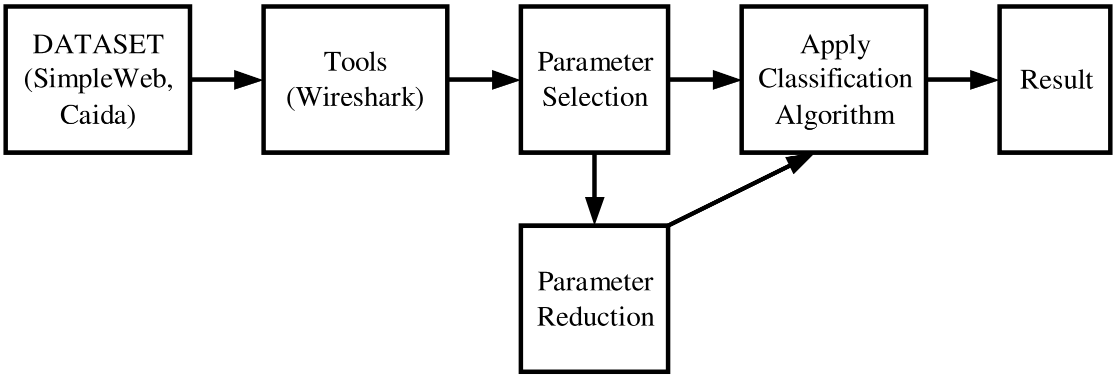


Figure8ModelofProposed system

Ndi wileproposesasimplenetworkarchitecturethatmakesuseofrealwebserver,Baitserver,and Decoy web servers to distinguish DDoS traffic from normal traffic. The architecture uses a customized Intrusion Prevention System (IPS) at the network gateway that use rules generated by random tree machine learning algorithm through supervised learning. Decision tree is chosen to classify malicious traffic from normal traffic. Random tree machine learning algorithm using labeled datasets is used to avoid false positive traffic.

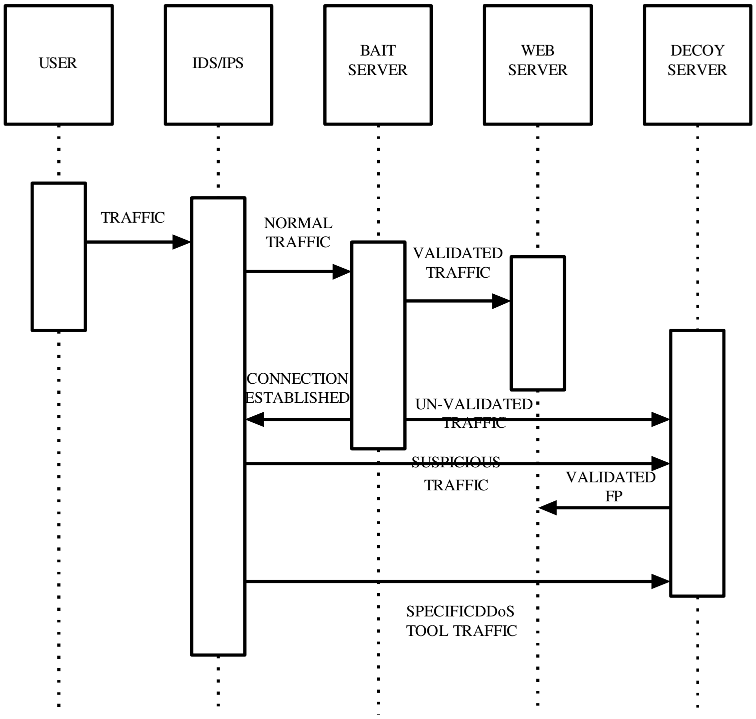


Figure9MitigationofDDoSattacktrafficsequence

Ramadhan[7]designsaTCPfloodDDoSdetectionsystemwhichusesArtificialImmuneSystem(AIS). Thesystemiscomposedoftwomaincomponent,collectiondataandanalysisdata.IntheAIS,thereare many algorithms based on human immune functions, principles and models can be applied to detect attacks, such as Dendritic Cell Algorithm (DCA). The four phase of DCA are preprocessing and initialization phase, detection phase, context assessment phase, and classification phase. The system presents DDoS attack by danger signals. Danger signals have been predefined as danger, safe, PAMA and inflammation. PAMA is a confident indicator of an abnormality and different signals indicate different kinds of attacks.

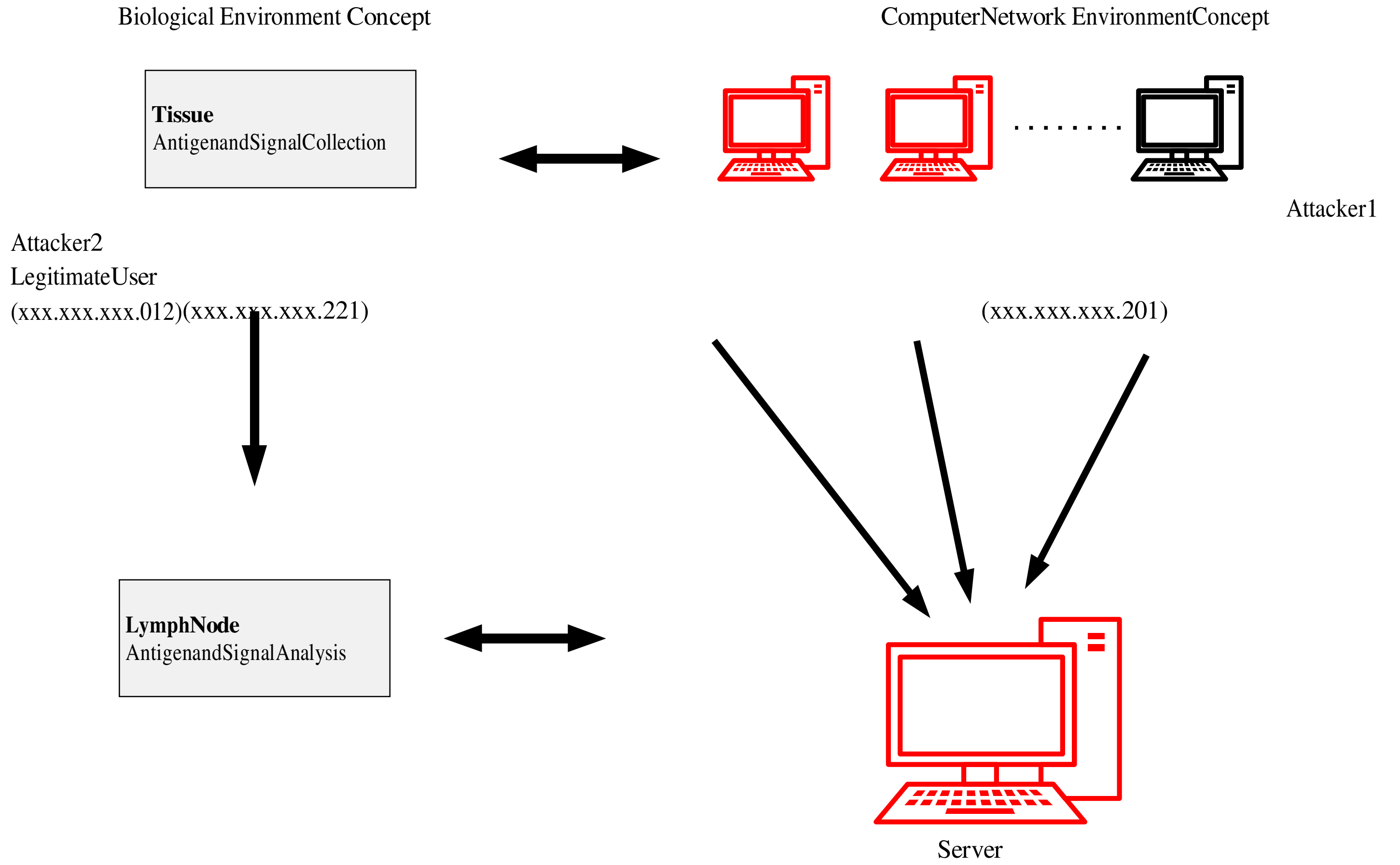

Biological Environment Concept
ComputerNetwork EnvironmentConcept
Tissue
AntigenandSignalCollection
Attacker1
Attacker2
LegitimateUser
(xxx.xxx.xxx.012)(xxx.xxx.xxx.221)
(xxx.xxx.xxx.201)
LymphNode
AntigenandSignalAnalysis
Server

Figure10Dendriticcellalgorithmdata structure

Perkovich develops a detection and classification model system based on artificial neural network (ANN) architecture to detect DDoS attack. In the developed ANN model, traffic is classified as four kinds, class-DNS DDoS attack traffic, charge DDoS attack traffic, UDP DDoS attack traffic and normal traffic.

Parameters used in detection of DDoS are source IP address, destination IP address, protocol and packet length. Because of the correspondence of the features of UDP DDoS attack and those of normal traffic, the accuracy in detection and classification of UDP DDoS attacks is a little lower.

While signature-based detection compares a data instance with a signature that is already stored in the database using pattern matching, anomaly-based detection analyses the behaviour of regular traffic to differentiate attack traffic from normal. Using features to characterize the data, machine learning-based classifiers are skilled in identifying patterns in the dataset.

In addition to automatically generating rules for use in network intrusion detection systems, machine learning approaches can help analysts make decisions.Classifiers are instruments that categorize data according to certain characteristics or trends found in the data. Gil and Poletto's work, which assumes that packet rates between two hosts are proportionate during normal operation, is among the noteworthy studies in the subject of DDoS detection.

To track packet rates for every IP address, the study uses a dynamic tree structure called Multi Level Tree for Online Packet Statistics.

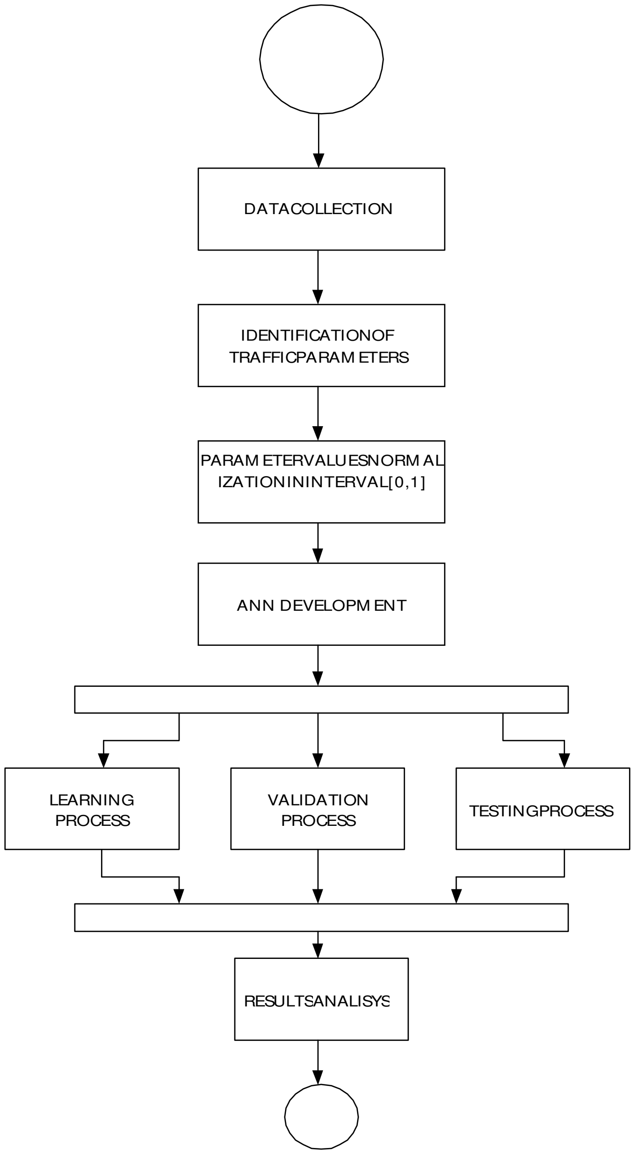


Figure11UMLActivitydiagramofproposedmodeldevelopment

## IV. Conclusion

DDoS assaults are one of the biggest risks to the Internet and can cause significant financial losses for both governments and businesses. Emerging technologies like cloud computing, the Internet of things, and artificial intelligence approaches have made it more difficult to identify and mitigate DDoS assaults and allowed attackers to launch them at a low cost. Naive Bayes and Random Forest trees are two examples of artificial intelligence techniques that have been used to detect and categorize DDoS attacks using machine learning algorithms. In the paper, we provide an overview of the most recent developments in artificial intelligence-based DDoS attack detection. Features including the number of packets, average packet size, time interval variance, packet size variance, number of bytes, packet rate, and bit rate can all be utilized to identify DDoS attacks. For their superior performance, we suggest using Naive Bayes and random forest trees among those artificial intelligence algorithms to distinguish between malicious and legitimate communications. DDoS assaults can be detected more accurately and efficiently by combining multiple machine algorithms.

## REFERENCES

[1] X. Yuan, C. Li and X. Li, Deep Defense: Identifying DDoS Attack via Deep Learning, IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, 2017

[2] M. Guri, Y. Mirsky and Y. Elo vici, DDoS: Attacks, Analysis and Mitigation, 2017 IEEE European Symposium on Security and Privacy (Europe), Paris, France, 2017;

[3] R. F. Fouladi, C. E. Kayatta's and E. Ana rim, Frequency based DDoS attack detection approach using naive Bayes classification, 39th International Conference on Telecommunications and Signal Processing (TSP), Vienna, 2016;

[4] C. J. Hsieh and T. Y. Chan, Detection DDoS attacks based on neural-network using Apache Spark, International Conference on Applied System Innovation (ICASI), Okinawa, 2016;

[5] Zijin Ren, Xiangyang Liu, Runge Ye, Tao Zhang, Security and Privacy on Internet of Things, IEEE 7th International Conference on Electronics Information and Emergency Communication (ICEIEC 2017), Shenzhen, 2017;

[6] B. S. Kiruthika Devi, G. Preetha, G. Selvaraj and S. Mercy Shalinie, an impact analysis: Real time DDoS attack detection and mitigation using machine learning, International Conference on Recent Trends in Information Technology, Chennai, 2014.

[7] G. Ramadhan, Y. Kurniawan and Chang-Soo Kim, Design of TCP SYN Flood DDoS attack detection using artificial immune systems, 6th International Conference on System Engineering and Technology (ICSET), Bandung, 2016;

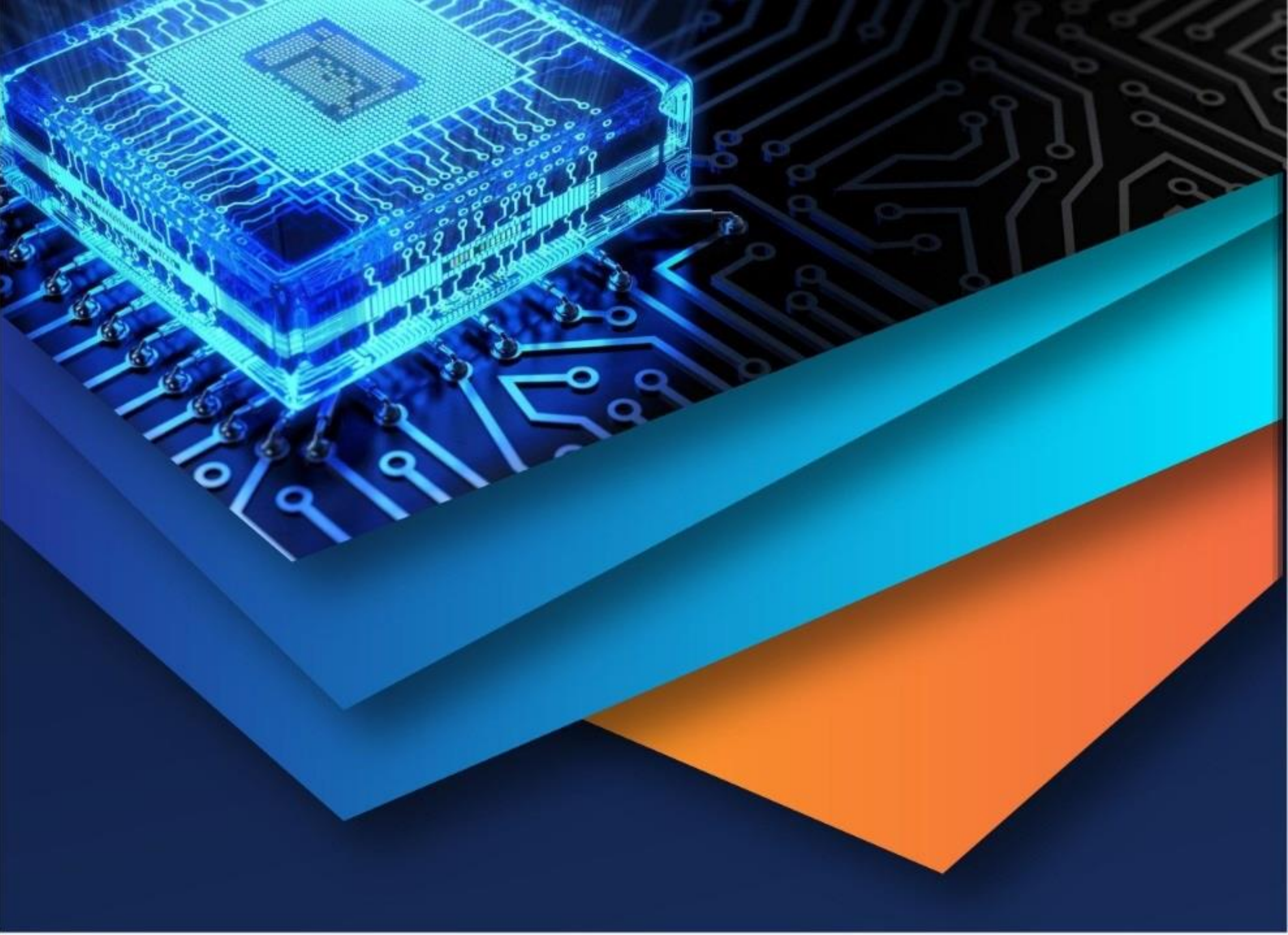
[8] Josep L. Barral, Nicolas Poggi, Adaptive distributed mechanism against flooding network attacks based on machine learning, New York;

[9] T. Zhao, A Neural-Network Based DDoS Detection System Using Hadoop and HBase, IEEE 17th International Conference on High Performance Computing and Communications, New York, 2015;

[10] Lalit Meitei, Chandrika Johnson Singh, Detection of DDoS DNS Amplification Attack Using Classification Algorithm, International Conference on Informatics and Analytics, New York;

[11] J. D. Ndi wile, A. Govardhan, Web Server Protection against Application Layer DDoS Attacks Using Machine Learning and Traffic Authentication, IEEE 39th Annual Computer Software and Applications Conference, Taichung, 2015;

[12] D. Perkovich, M. Periša, Artificial neuron network implementation in detection and classification of DDoS traffic, 24th Telecommunications Forum (TELFOR), Belgrade, 2016.



10.22214/IJRASET

INDEX COPERNICUS
45.98

ISRA JIF
IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY