International Journal of Scientific Research in
Network Security and Communication
Vol.**13**, Issue.**2**, pp.**01-11**, April **2025**
ISSN: 2321-3256 (Online)
Available online at: www.ijsrnsc.org

Research Article

Evaluating the Impact of Denial-of-Service (DoS) Attacks on Enterprise Networks Using Optimized Network Engineering Tools (OPNET 14.5) and Machine Learning

Ojo Jayeola Adaramola[1*], Olaniyi Habib Aliu[2]

[1]Dept. of Computer Engineering, School of Engineering, Federal polytechnic Ilaro, Ogun State, Nigeria
[2]Dept. of Computer Engineering, School of Engineering, Federal polytechnic Ilaro, Ogun State, Nigeria

[*]*Corresponding Author:* *Tel.: +234 703 273 0955*

Received: 01/Apr/2024, Accepted: 15/Apr/2025, Published: 30/Apr/2025| **DOI**: https://doi.org/10.26438/ijsrnsc.v13i2.271

Abstract— The research conducts a network performance analysis of enterprise systems under Denial-of-Service (DoS) attacks through machine learning modeling with OPNET 14.5. Service interruptions along with financial losses result from Denial-of-Service attacks which seriously reduce network performance. The implementation of multiple defense measures has not resolved the persistent problem with real-time detection and response for enterprises. Through OPNET 14.5 simulation the research evaluates multiple DoS attack situations alongside their effects on performance metrics by measuring latency and achieving throughput and packet loss statistics. Two machine learning models with decision trees and support vector machines serve to detect normal and attack-related traffic patterns. The simulation demonstrates that networks experience severe degradation when under DoS attacks which leads to longer delays and packet drops. The machine learning detection systems show excellent attack pattern recognition abilities which indicates their practical use in preventing attacks. The authors suggest security frameworks should implement machine learning detection systems as part of their enterprise security infrastructure for better DoS protection. The research provides final proof about integrating network simulation along with machine learning technologies to stop DoS attacks which will enable further cybersecurity defense system development.

Keywords— Denial-of-Service (DoS), Enterprise Security, Network Performance, Machine Learning, OPNET

1. Introduction

Enterprise networks experience vital cybersecurity dangers throughout digital development since organizations elevate their dependence on connected systems. Organization networks face their most important security threat from Denial-of-Service (DoS) attacks which disrupt services through massive network resource exhaustion [1]. These assaults generate business stoppages and monetary losses accompanied by deteriorating brand reputation. Future iterations of cyber threats require organizations to enhance their capabilities of detecting and evaluating and mitigating DoS attacks because of their increasing occurrence. According to [2], DoS attacks began during the first internet period by sending numerous excessive requests to capitalizing on server capacity issues [3] [4]. Attack techniques have progressed since the beginning of the internet by adding UDP and SYN flooding and application-layer assault vectors to their repertoire. The increased capability of Botnets due to their ability to control enormous collections of compromised devices now creates added complexity to prevent DoS attacks according to [5]. [6], identify an ongoing cybersecurity issue because of the execution and mitigation cost difference for DoS attacks. The crucial position businesses assign to their enterprise networks makes them highly attractive targets for cyber criminals. Researchers state that Distributed Denial-of-Service (DDoS) attacks took shape from DoS attacks by leveraging compromised system coordination to target a single operation [7]. The attacks create extensive financial losses together with service interruption problems and destroyed customer relationships. Cybersecurity Ventures forecasts $10.5 trillion worth of cybercrime expenses including DoS attacks during the year 2025 [8]. Firewalls and intrusion detection systems traditionally used as security measures fail to stop DoS attack variations with sufficient effectiveness [8] [9]. Enterprise networks contain distributed elements that create difficult

defense challenges because of their dynamic structure [10]. The research evaluates Denial-of-Service (DoS) attack effects on enterprise networks through OPNET 14.5 simulations and machine learning protocols to determine performance consequences and detection precision and minimization methods. The simulation solution OPNET 14.5 allows users to create virtual enterprise networks that permit them to perform DoS attack simulations while monitoring performance effects. This work will evaluate DoS attack impacts on enterprise networks through combination of OPNET 14.5 simulation and machine learning detection techniques. Enterprise networks contain wireless and wired systems connected through cloud platforms together with IoT devices. Electronic network growth creates extensive vulnerability to cyber threats especially DoS attacks as per [11]. Traditional protective security systems depend on specific signatures pre-defined by humans yet they cannot identify newly created attack schemes [12]. The detection of DoS attacks has improved through the implementation of decision trees, support vector machines and deep learning models as per [13] research investigations have analyzed how to measure the impact of DoS attacks alongside preventing their occurrences. The research by [14], evaluated AI security solutions to fight DoS attacks within cloud systems. Deep learning analysis of enterprise volumetric DDoS attacks forms the basis of research conducted by [15]. The evaluation of DoS attacks requires additional research to merge network simulation with machine learning methods for complete evaluation purposes. This research implements OPNET 14.5 for building enterprise network models followed by DoS attack simulation. The evaluation of performance metrics consisting of latency, packet loss and throughput, will help detect system weaknesses for designing better security solutions. OPNET 14.5 serves as a popular simulation platform that supports network performance evaluation through diverse conditions analysis. Through this tool users can apply their network structure for testing alongside generating traffic models and evaluating cyber threat effects [16]. The research work will use simulations to study network attack behavior within an enterprise environment in order to investigate performance reductions alongside network capacity issues and available protection strategies. This investigation evaluates the ability of machine learning models to develop better DoS detection methods as well as response and mitigation procedures. This work adds value to previous research through its utilization of OPNET 14.5 simulations for analyzing realistic DoS attacks supported by machine learning defense methods. Research findings will help scientists create enhanced safeguards for enterprise network security platforms.

1.1 Objectives of the article

Enterprise networks face expanding exposure to Denial-of-Service (DoS) attacks that stop crucial services, which can damage their network stability and also lead to service interruptions and monetary losses. The traditional-based intrusion detection techniques currently used cannot recognize or stop new types of attacks because dynamic situations demand immediate response. Multi-purpose firewalls, together with predefined rules, have shown poor performance against DoS attacks that use large attack volumes and numerous attack types. Existing mitigation tools do not eliminate the need for more thorough analysis of simulation and intelligent detection systems as a complete solution to DoS threats.

The objective of this research involves studying DoS attacks' network performance effects through an analysis combining OPNET 14.5 simulations with machine learning-dependent classification systems. The study investigates three major targets: testing different DoS attack situations to measure operational attributes as well as developing machine learning tools, which include decision trees and random forests, along with SVM, XGBoost, and logistic regression for pattern detection and examining stacking ensembles for predictive improvement. This research aims to create a responsive security solution that can identify and then counteract Denial of Service attacks live so that enterprise networks have better resistance to contemporary network threats.

The following research structure consists of several sections as presented below:

The Literature Review session explores DoS attacks in enterprise networks combined with OPNET 14.5 capabilities along with machine learning systems used for threat mitigation.

The methodology section explains the research design together with OPNET 14.5 simulation setup and machine learning techniques as well as evaluation metrics.
The results and discussion section contain findings from simulation analyses and ML model executions while exploring their significance.

In the concluding section recommendations for future research along with key findings and suggested solutions were presented to end the study.

2. Related Work

The section presents an analysis of earlier research about the subject through a breakdown of methods used along with their obtained results.

In [17], evaluate Distributed Denial-of-Service (DDoS) alongside Ping of Death attacks to understand their effect on network performance as it addresses vital network security flaws. The study conducts experimental simulation through network performance measurement tools to investigate the effects that these attacks produce. The assessment shows extensive network performance decline because response time grows together with exhausted bandwidth capacity. There is an existing knowledge gap regarding the requirement to develop effective adaptive countermeasures which address changing attack strategies. The research findings regarding attack effects create new knowledge in cybersecurity that helps identify better cyber defense approaches.

In the same year, [18] create a real-time test framework to perform Distributed Denial-of-Service (DDoS) research in attack situations. This paper addresses the deficiencies of security testing through simulation because simulations do not accurately represent genuine DDoS assault operations. The authors construct a DDoS testbed through Ansible orchestration that enables simulation of DDoS attacks against realistic production systems. The research data shows that victim servers experience extreme network failures combined with high processor and memory resource usage. According to the research findings there exists a critical need for AI-based real-time protective measures since no such automated solutions currently exist.

In [19], studied how Internet of Things (IoT) devices perform Denial-of-Service (DoS) attacks against network systems. This research evaluated methods which exploit IoT devices for DDoS attacks that produce degradation of bandwidth and dramatic packet loss and elevated latency. The researcher conducted an experimental assessment of attack effects through TCP, UDP and HTTP flooding attacks using quantitative methodology. The research results indicated that UDP flood attacks brought severe consequences to network performance because they reduced bandwidth by 79.8 percent and elevated jitter measurements by 148 percent. Research findings revealed a critical shortage in defensive measures since real-world testing should be performed on extensive network systems.

In [20], overcome static firewall limitation through the development of an out-of-line firewall evaluation framework. The research monitors firewall effects through purpose-built controlled settings and automated metric measurement points. The security protocols examined in laboratory tests have shown they can impact both bandwidth and latency to the extent that specific setups decrease network performance by 50%. The research demonstrates that testing firewalls at scale under operational conditions and implementing dynamic filtering strategies would maximize firewall performance efficiency in real environments. Additional research needs to optimize firewall rules because they should protect networks better while preventing any performance declines.

The research work of [21], explores how Wi-Fi broadband networks with public sector infrastructure face DoS attacks. This research investigates the issue of network congestion together with service disruption that emerges from Denial-of-Service attacks. The researchers employ OPNET Modeler to conduct simulations of DoS attacks which allow them to examine network performance aspects including packet loss together with end-to-end delay and server response time. Network performance suffers from DoS attacks by showing deteriorating indicators including enhanced packet drops (10 Mbps) as well as expanded delay times (0.2s) and higher server response duration during the assault. The study finds that current real-time prevention tools lack capability so the research promotes AI-powered adaptive defense methods to stop developing DoS threats.

In [22], research Wi-Fi network design and security simulation methods to address vulnerabilities which affect wireless enterprise security. The analysis focuses on Wi-Fi network security difficulties which emerge mainly through mobility issues and authentication systems and encryption requirements. Simulation of secure Wi-Fi network takes place through 802.1X authentication which employs the combination of EAP-FAST and RADIUS servers. Results demonstrate that authentication operates more quickly while security operates more efficiently and latency levels decrease. The research points out a weakness in protection against man-in-the-middle attacks so better encryption methods should be implemented. The study delivers essential information about how to enhance enterprise WLAN security capabilities.

In [23], conducted an analysis of Distributed Denial-of-Service (DDoS) attacks in enterprise networks through their utilization of the OPNET Modeler. The research examines the performance impairments from Distributed Denial-of-Service attacks through simulation of multiple attack patterns. The researchers examine three vital performance indicators which include packet loss, latency and response time. Service availability decreases because DDoS attacks produce major packet losses together with delayed network responses according to research findings. Even so the study detects missing elements in adaptive mitigation approaches in real-time which leads to a necessity for AI-based security systems. [24], implemented a study that utilizes machine learning for identifying Denial-of-Service (DoS) attacks in Information-Centric Networks (ICN) which operate for IoT systems. The study handles the problem of protecting ICN-IoT systems from DoS attacks that deplete resources. A simulation based on ndnSIM allows the authors to evaluate detection accuracy through implementation of ML classifiers including SVM, RF and KNN. RF stands out as the most accurate approach in identifying threats which produces greater threat detection efficiency. Analyzing and implementing self-learning ML systems for intrusion prevention during large-scale ICN deployment requires additional study for real-time adaptation capabilities.

In [25], explores DoS attack defense strategies deployed through GNS3 for network protection according to their research. DoS attacks have become an escalating risk that leads to performance degradation after servers become engulfed in malicious network traffic. The authors utilize GNS3 for developing attack simulations to test different defensive measures that include combination approaches among firewall restrictions along with traffic management controls and rate controls. Testing displayed that these implemented security solutions guard networks by decreasing attack effects while enhancing their resistance against threats. There exists a current limitation in the field regarding both immediate attack detection capabilities along with automated response strategies. Artificial intelligence and machine learning need to integrate at the next stage of development to automate security systems.

3. Methodology

The research methodology structures itself into two different areas for study purposes. The initial stage of the OPNET simulation framework generates enterprise network traffic which includes two scenarios without DoS attack simulation and another scenario with DoS attack simulation functionality. A machine learning system analyzes the produced traffic for determining the impact of Denial of Service attacks against enterprise networks as per the following description.

3.1 OPNET Model

The figure depicts the Enterprise Network Scenario (Without DoS Attack) model designed through the OPNET 14.5 simulator as presented in Figure 1. The model contains different network elements and linking methods serving as the foundation for measuring DoS attack effects. The network implementation consists of the IP Cloud (ip32_cloud) as external access simulator that connects to a Cisco 7200 router which functions as an access point between external and enterprise networks. The internal network traffic management functions through ethernet16_switch_1 and ethernet16_switch_2 to unite and connect Ethernet_wkstn_int_1 through Ethernet_wkstn_int_6 workstations which represent client systems that both send and receive network data. The essential services provided by enterprise servers include Database, Email, HTTP, FTP, and applications through Ethernet_Server_1 and Ethernet_Server_2. The traffic configuration takes place through Profile and Application Definitions. The IP Cloud uses an OC-3 high-speed serial link for connectivity to the router while both the router interfaces with Ethernet Switch 2 through a Gigabit Ethernet connection and both switches are joined by a trunk link along with 100 Mbps ethernet links that connect workstations and servers.

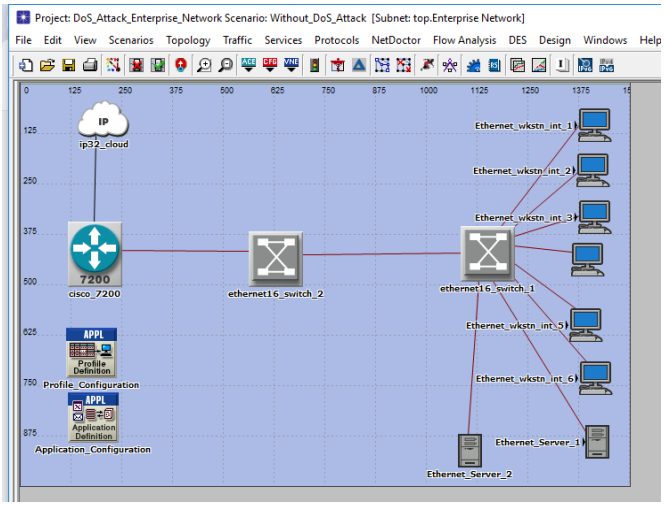

Figure 1. Enterprise Network Scenario (Without DoS Attack) Model

A simulation uses defined application and profile configurations for network activities including web browsing and file transfers, email and database together with traffic flows that evaluate DoS attack effects in different scenarios. System performance monitors three essential network parameters which are latency, packet loss and throughput to determine overall network stability. The established network configuration functions as a benchmark system which delivers crucial information when studying performance impacts during active DoS attack execution.

The model presented in Figure 2 illustrates an OPNET 14.5 simulator design of a DoS Attack Enterprise Network Scenario protected by a firewall. The evaluation system utilizes multiple network elements together with protection mechanisms and network connection parameters to understand how firewalls stop DoS attacks. External network components consist of ip32_cloud that functions as an IP Cloud simulator for internet connectivity and a Cisco 7200 router that manages the gateway for enterprise network traffic flow with external sources. The strategically placed firewall between Ethernet Switch 2 (ethernet16_switch_2) and Ethernet Switch 1 (ethernet16_switch_1) serves as the security element to defend the internal network against DoS attacks by filtering unwanted traffic. The internal network consists of Ethernet switches as its components including ethernet16_switch_1 and ethernet16_switch_2 that distribute traffic between workstations identified as Ethernet_wkstn_int_1 through Ethernet_wkstn_int_6 and enterprise servers Ethernet_Server_1 and Ethernet_Server_2 to handle HTTP HTTP, FTP, email, and file sharing operations. The internal network workstations from Ethernet_wkstn_int_7 to Ethernet_wkstn_int_9 function with Highrate UDP/TCP followed by SYN flood attack and ICMP request attack to target FTP Server along with Email Sever together with Database Server and HTTP Server. Through the features of Profile and Application Definitions the tool permits users to simulate various activities that include web browsing alongside file downloads and video streaming. The core link configuration between the IP Cloud and the router needs either OC-3 or Gigabit Ethernet connections to establish reliable internet access. Traffic management is made efficient through the connection of the router to Ethernet Switch 2 using a 1 Gbps Ethernet link. The firewall uses the 1 Gbps Ethernet link to connect with Switch 2 where it enforces network security policies to screen potentially dangerous network packets. The firewall establishes security connections through a 1 Gbps Ethernet link to both Switch 1 and Switch 2 for network protection of internal areas and workstation and server communication occurs through 100 Mbps Ethernet links. Attack prevention mechanisms present in the configuration deploy active firewall rules which detect malicious traffic while allowing proper networks to function properly. The implementation of traffic flow analysis enables monitoring of attack-related changes in packet loss and latency and throughput measurements. Performance metrics function to evaluate security efficiency during network operations with the firewall in place when compared to unfixed network security. This enables measuring the firewall's success as an attack mitigation solution. The implemented setup functions as an essential platform which evaluates corporate network resistance against cyber-attacks.

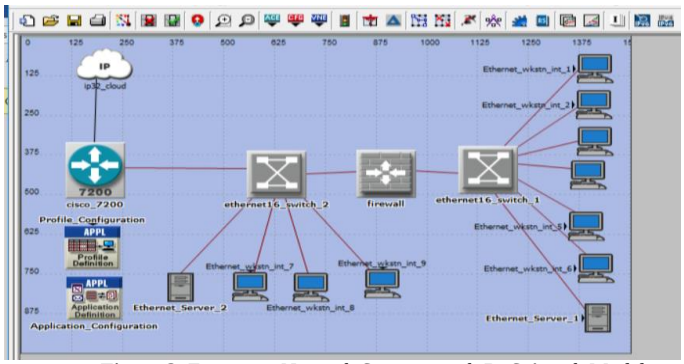

Figure 2. Enterprise Network Scenario with DoS Attack Model

3.2 Machine Learning Model

The ensemble model used for this study was trained, validated, and tested using the enterprise dataset before implementing it with the stacking ensemble architecture. Figure 3 below indicates the block representation of the study covering the step-by-step procedures, and the selected algorithms used. The network enterprise used is a text dataset. The model takes in the essential features through input X, the models used were represented with M_1, M_2, M_3, M_4, and M_5. Where, M_1, M_2, M_3, M_4, and M_5. are the base model random forest (RF), logistic regression (LR), decision tree (DT), extreme gradient boosting (XGB), and support vector machine (SVM) models respectively. The output of the prediction for each of the models is represented as h_i. $h_i(X)$ provides an output of a base model using the specific input X provided by the model. The mathematical representation of the predicted output for each model is stated below.

$$\widehat{Y_1} = M_1(X), \widehat{Y_2} = M_2(X), \widehat{Y_3} = M_3(X), \widehat{Y_4} = M_4(X), \widehat{Y_5} = M_5(X) \quad (1)$$

Then Z is derived;

$$Z = [\widehat{Y_1}, \widehat{Y_2}, \widehat{Y_3}, \widehat{Y_4}, \widehat{Y_5}] \quad (2)$$

To determine the meta-classifier for the ensemble model, the model identify Z as input and produces a corresponding output which is denoted by $\widehat{Y}$ as indicated in the equation below.

$$\widehat{Y} = g(Z) = g(\widehat{Y_1}, \widehat{Y_2}, \widehat{Y_3}, \widehat{Y_4}, \widehat{Y_5}) \quad (3)$$

Where g represent the meta-classifier, $\widehat{Y_1}$ is the predicted output of each classifier, and $\widehat{Y}$ is the final prediction for the stacking ensemble model.

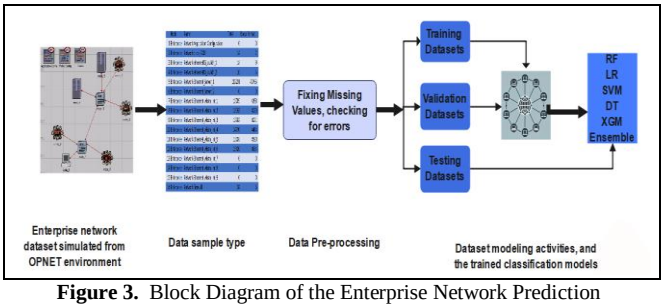

Figure 3. Block Diagram of the Enterprise Network Prediction

3.2.1 Data Collection Technique

The dataset used for this study was generated by simulating different nodes with enterprise network on OPNET environment. Various scenarios were created and the data were gathered. The dataset after going through preprocessing stage such as identifying and replacing missing values, and checking for potential syntax errors. The final dataset used comprises of a total of 11 columns, and 15,216 rows.

The columns includes ip_dgram_v4, udp_dgram_v2, Total, tcp_seg_v2, rip_message2, IsCongested, ethernet_v2, bpdu_format, gna, node, and name. The traffic load is indicated by the dataset using total, tcp_seg_v2, udp_dgram_v2, and ip_dgram_v4. The RTP, BDPU format, and RIP message 2 were employed as the determinants for the main columns that indicate the source of the congestion. Ethernet_v2, udp_dgram_v2, and tcp_seg_v2 are the columns that help differentiate between the different forms of communication and provide information about the protocols that were used. The dataset's binary classification is represented by the IsCongested column, where 0 denotes normal and 1 denotes congestion in the enterprise network. The dataset split train_test ratio was set at 80:20, which means that 80% of the dataset was allocated for training, while 20% for testing.

3.2.2 Development of the Ensemble Model

The stacking model algorithm was developed using various metadata from the five selected machine learning algorithms, which are RF, LR, SVM, DT, and XGB. The step-by-step algorithm for the model is presented in Table 1 below. Figure 4 shows the final architectural output of the model after implementing it with the five selected models.

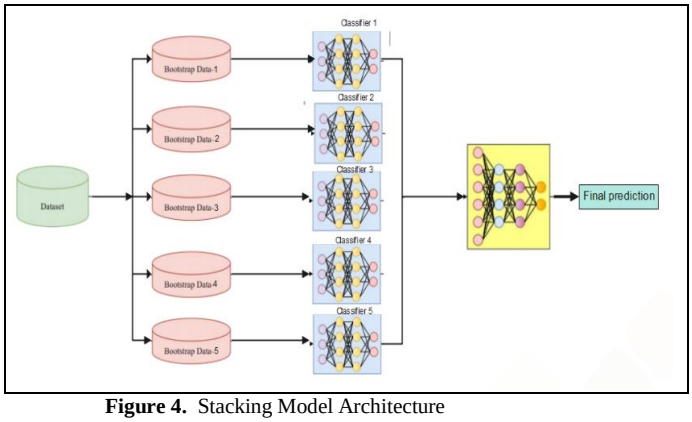

Figure 4. Stacking Model Architecture

Table 1. Algorithm for Stacking Ensemble Model

```
01  StackingClassifier(estimators=[('rf',
                RandomForestClassifier(class_weight='balanced',
                                       random_state=42)),
               ('xgb',
                XGBClassifier(base_score=None, booster=None,
                              callbacks=None, colsample_bylevel=None,
                              colsample_bynode=None,
colsample_bytree=None,
                              device=None, early_stopping_rounds=None,
                              enable_categorical=False,
                              eval_metric='logloss',
```



```
                    feature_types=None, feature_wei...
                    missing=nan, monotone_constraints=None,
                    multi_strategy=None,
                    n_estimators=100, n_jobs=None,
                    num_parallel_tree=None, ...)),
                ('dt', DecisionTreeClassifier(random_state=42)),
                ('svm', SVC(probability=True, random_state=42)),
                ('lr',
                 LogisticRegression(max_iter=1000,
                                    random_state=42))],
02  final_estimator=LogisticRegression(max_iter=1000,
                                       random_state=42),
        passthrough=True)
```

The dataset was implemented with the five selected algorithms in order to produce a robust result for proper comparison with the ensemble model. The results were generated and recorded for future use.

4. Results and Discussion

Two different formats exist for the research findings presentation. In the first phase of assessment the enterprise network traffic from OPNET simulation generates both analysis and presentation data. The results from machine learning-based analysis follow the results of the first section in the below presentation.

4.1 Result of the OPNET Simulation

The network performance metrics during normal operations appear in the OPNET 14.5 table (without DoS attack) to display system performance levels with no cyberattacks occurring. The parameters measured by the table include Ethernet delay and server database (DB) query traffic alongside server email traffic, server FTP traffic, and server HTTP traffic, which were sampled at 360-second intervals throughout the 3600 seconds (1 hour) simulation period. Network congestion remains low as Ethernet delay extends from 0.00000 seconds to reach 0.000035 seconds during the observation period. Database operations through the server DB query exhibit performance stability because their traffic activity ranges from 0.00 to 0.70 packets per second. The server received email packets increased continuously until it achieved maximum performance at 0.45 packets per second during the 3240 seconds observation period. Server FTP traffic received maintains stable behavior as it reaches its maximum level of 0.15 packets per second at 3600 seconds, thus indicating continuous data transfer operations. The testing period showed no HTTP traffic received by the server because the HTTP traffic received measurement stayed at 0.00 packets per second. Network performance benefits from Ethernet delay, which maintains a stable low level according to the analysis findings. The server DB query traffic shows continuous growth at a consistent rate since its initial deployment without Twittering toward data retrieval operations. The system performs normal email operations throughout the session, reaching its highest point at 0.45 packets per second during the 3240-second mark. The constant FTP traffic pattern demonstrates file transfer stability reaching 0.15 packets per second at 3600 seconds, which proves the operation of secure file transfer processes. The absence of HTTP traffic matches previous findings in the DoS attack experiment because HTTP services were most likely omitted from this test scenario. Research findings validate the smooth operation of the network even when there is no DoS attack taking place, as presented in Table 2 below.

Table 2. Enterprise Network Scenario without DoS Attack

Time (sec)	Ethernet Delay (sec) Without DoS Attack	Server DB Query Traffic Received (packets/sec) Without DoS Attack	Server Email Traffic Received (packets/sec) Without DoS Attack	Server FTP Traffic Received (packets/sec) Without DoS Attack	Server HTTP Traffic Received (packets/sec) Without DoS Attack
0	0.00000	0.00	0.00	0.00	0.00
360	0.000030	0.50	0.05	0.03	0.00
720	0.000031	0.55	0.12	0.04	0.00
1080	0.000032	0.60	0.10	0.06	0.00
1440	0.000032	0.50	0.15	0.07	0.00
1800	0.000033	0.65	0.20	0.05	0.00
2160	0.000033	0.55	0.18	0.09	0.00
2520	0.000033	0.70	0.30	0.10	0.00
2880	0.000034	0.60	0.40	0.12	0.00
3240	0.000033	0.55	0.45	0.14	0.00
3600	0.000035	0.65	0.35	0.15	0.00

Network performance metrics measured an enterprise network during a DoS attack using OPNET 14.5, as shown in Table 3. The simulated parameters follow a 3600-second period with 360-second intervals measuring Ethernet delay along with server database (DB) query traffic, server email traffic, server FTP traffic, and server HTTP traffic. The Ethernet delay begins at 0.00000 seconds and reaches 0.000037 seconds, whereas the network congestion worsens with time under conditions of a DoS attack. The server DB query traffic maintains a functional state while the attack affects its operations through a packet rate varying between 0.00 and 0.65 packets per second. During the attack period, server email traffic demonstrates partial resistance through its varying packet rate from 0.65 to 0.06 and 0.40 packets per second, apart from showing some disruption. The FTP server traffic begins at 0.16 packets per second before declining to operate between 0.02 and 0.12 packets per second due to the progression of the attack. The server HTTP traffic shows no activity during the entire simulation because the attack successfully stops HTTP services. Observations show that Ethernet delay increases steadily, so it proves network congestion increases from the attack. Server DB query traffic displays moderate changes in patterns showing that database access remains possible, though it is influenced by the attack. The caseload of email traffic begins at its peak level before decline occurs and produces waves based on the attack's effects on system reliability. File transfer operations become significantly affected when FTP traffic levels decline

progressively throughout the period. The DoS attack leads to total blocking of HTTP traffic, which indicates a complete failure of web-based services in the affected network. The DoS attack disrupts network services to different extents across different points in the network. HTTP traffic suffers complete interruption, yet FTP, email, and database requests maintain limited operational capabilities during the attack period. The increase in Ethernet delay is an additional negative effect caused by this attack that reduces network efficiency. Additional research must be conducted because findings indicate an upcoming investigation into security strategies that incorporate firewall setups and anomaly detection technology for improving resistance against these attacks.

Table 3. Enterprise Network Scenario with DoS Attack

Time (sec)	Ethernet Delay (sec) With DoS Attack	Server DB Query Traffic Received (packets/sec) With DoS Attack	Server Email Traffic Received (packets/sec) With DoS Attack	Server FTP Traffic Received (packets/sec) With DoS Attack	Server HTTP Traffic Received (packets/sec) With DoS Attack
0	0.00000	0.00	0.65	0.16	0.00
360	0.000031	0.45	0.10	0.02	0.00
720	0.000032	0.50	0.08	0.05	0.00
1080	0.000033	0.55	0.06	0.08	0.00
1440	0.000033	0.40	0.12	0.04	0.00
1800	0.000034	0.60	0.15	0.03	0.00
2160	0.000034	0.50	0.09	0.06	0.00
2520	0.000035	0.65	0.20	0.07	0.00
2880	0.000036	0.55	0.30	0.05	0.00
3240	0.000035	0.50	0.40	0.10	0.00
3600	0.000037	0.60	0.25	0.12	0.00

4.1.1 Comparative Analysis between Enterprise Network Scenario without DoS Attack and DoS Attack

As indicated in table 4 multiple effects that a DoS attack exerted on the performance of the network infrastructure was monitored. The delay of the Ethernet network grew somewhat but the database queries slightly decreased. The attack caused major disruptions because email along with FTP traffic amounts plummeted substantially. The measurement of HTTP traffic showed no results in both attack scenarios because the traffic was either blocked during testing or measurement or testing failed to capture it. Email and FTP traffic operated efficiently at normal network status while the operations maintained short delays to ensure optimal performance. Various defensive protocols need to be employed as countermeasures for DoS attacks. Given the ability of Intrusion Detection Systems (IDS) to detect unusual traffic patterns they assist operators in making timely system intrusions responses. Both rate-limiting server requests and firewalls together with anti-DoS solutions create crucial barriers against malicious traffic whereas rate-limiting server requests mitigate flooding attacks.

Table 4. Comparison of without DoS Attack and DoS Attack

Metric	Without DoS Attack	With DoS Attack	Impact of DoS Attack in the Network
Ethernet Delay (sec)	0.00000 - 0.000035	0.00000 - 0.000037	Higher delay with DoS attack
DB Query Traffic (packets/sec)	0.00 - 0.70	0.00 - 0.65	Slightly reduced under DoS
Email Traffic (packets/sec	0.00 - 0.45	0.65 - 0.25	Email traffic is reduced under DoS
FTP Traffic (packets/sec)	0.00 - 0.15	0.16 -0.12	FTP traffic is lower under DoS
HTTP Traffic (packets/sec)	0.00 throughout	0.00 throughout	No difference

However, the network performance under normal and DoS attack conditions is compared through graphical figures (Figures 5–9), which were created from simulations in OPNET 14.5. In Figure 5, Ethernet delay demonstrates higher variation, though only slight, with attack compared to the delay without attack shown in the red line. The network demonstrates resilience in the face of the attack through its minimal performance deviation. The blue line in Figure 6 demonstrates higher frequency and reduced peak levels when showing server database (DB) query traffic, which indicates diminished data reception and shows performance inconsistencies during attack conditions. The attack leads to service congestion along with packet loss that reduces database operational efficiency. More instability emerges in Figure 7's blue line as server email traffic drops and becomes irregular because of delay and packet loss from the attack. FTP traffic analysis in Figure 8 shows major disruptions in the blue line, which results in minimal or nonexistent traffic as a sign of intensified congestion and failed file transfers. The analysis of Figure 9 indicates that both lines display low activity or severe DoS interference may be occurring with HTTP traffic. The flat pattern measurement indicates web service disruptions occurred to a major extent because of the attack.

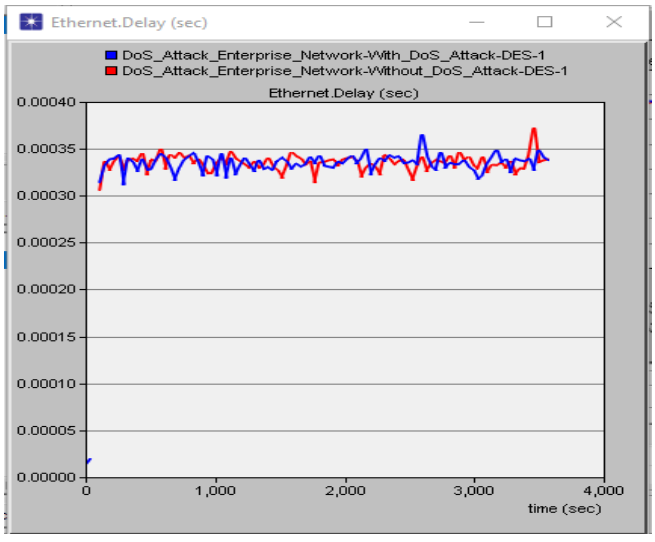

Figure 5. Ethernet Delay (sec)

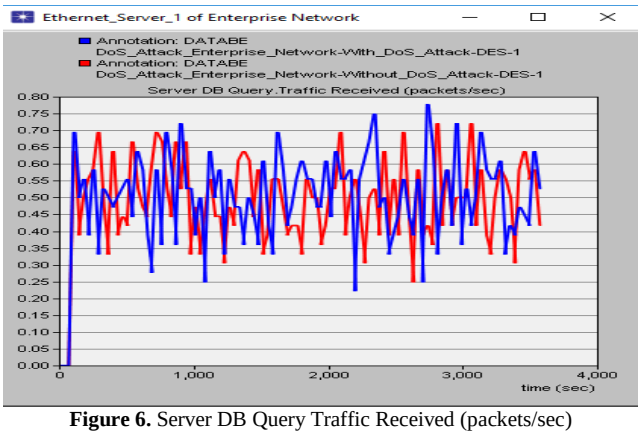

Figure 6. Server DB Query Traffic Received (packets/sec)

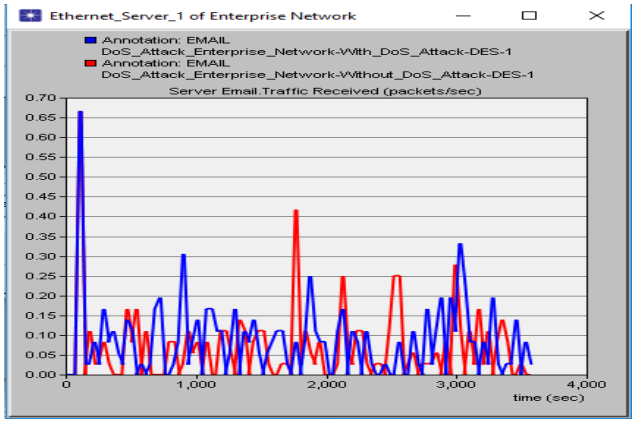

Figure 7. Server Email Traffic Received (packets/sec)

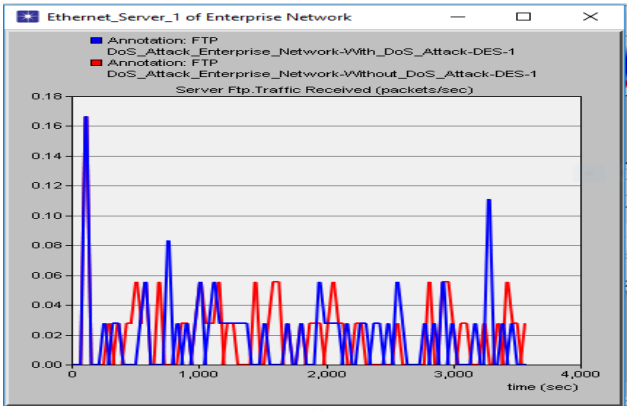

Figure 8. Server FTP Traffic Received (packets/sec)

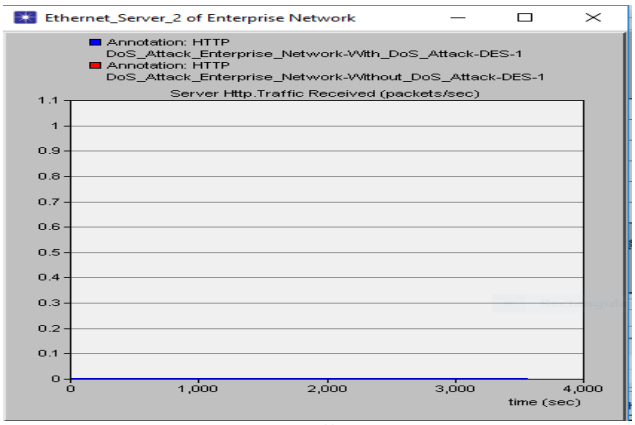

Figure 9. Server HTTP Traffic Received (packets/sec)

4.2 Result of the Machine Learning (ML)

The figure below illustrates a feature correlation heatmap, which shows how different attributes in an enterprise network dataset relate to one another. A color gradient within the heatmap shows correlations through red for positive strong values approaching +1 along with blue for negative strong values approaching -1, while neutral tones indicate low correlation. Readers can view numerical interpretations through the reference scale located on the right side.

Multiple network-related features demonstrate significant positive correlations as one of the main findings obtained from the analysis. The network features bpdu_format, ip_dgram_v4, rip_message2, and tcp_seg_v2, displaying close-to-perfect positive relationships between each other. The data indicates that rising values of any individual variable usually result in simultaneous increases of all other variables. One notable association exists between bpdu_format and Total because both features show a positive 0.61 extent of correlation. The negative correlations signify inverse relationships between network features. Network congestion data in the IsCongested variable demonstrates negative relationships with gna (-0.48) and ethernet_v2 (-0.30). The study shows how rising levels of network congestion result in diminishing parameter values, which could enhance understanding of congestion-related network characteristics. However, there are multiple variables that demonstrate an insignificant relationship with other measurements. The Node parameter shows minimal or no association with other data elements; thus, its data points have little effect on other measurement values in the dataset. The data implies that the node feature does not play an essential role in congestion network analysis.

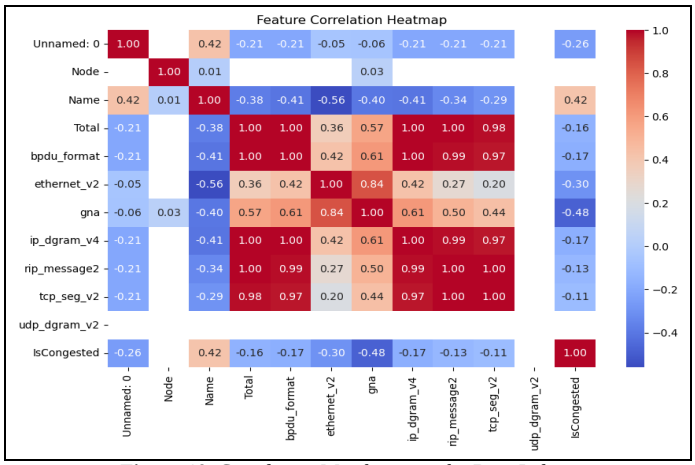

Figure 10. Correlation Map between the Data Index

The findings indicate that the ensemble model's accuracy was 74.37%. By measuring other evaluation metrics, the overall recall for the model was 74.10%, the precision score was 83.30%, and the F1 score was 73.60%. The confusion matrix for the ensemble model is displayed in Figure 11 below.

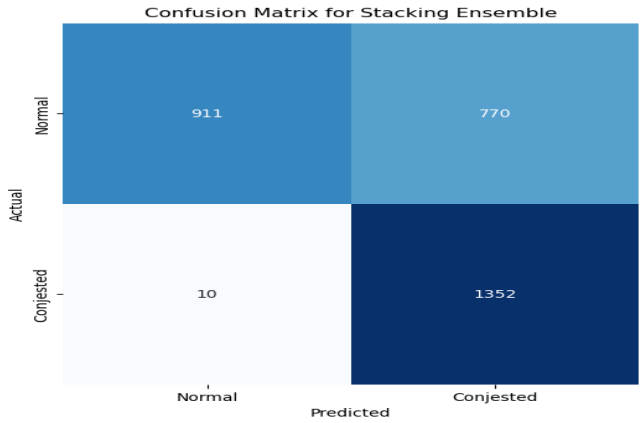

Figure 11. Confusion Matrix for Stacking Ensemble Model

The stacking ensemble model performs classification detection of enterprise network congestion by analyzing the values of the confusion matrix. The model contains four critical values that evaluate its capacity to distinguish regular from congested traffic conditions. The output indicates that the model effectively recognized 1,352 instances of congestion while achieving a true-positive evaluation. A total of 911 static traffic samples underwent correct classification as normal by the model, which corresponds to its True Negative (TN) value. The model has an incorrect classification, as incorrectly labeled normal instances appeared as congested (false positives), totaling 770. Model predictions of congestion occur with greater frequency than needed based on the results. Very few instances of actual congestion cases were incorrectly classified as normal traffic because the False Negatives (FN) count reached only 10 instances.

Table 5. Classification Report for the Six Algorithms

Models	Random Forest				Decision Trees				
	precision	recall	F1-score	support		precision	recall	F1-score	support
Normal	1.00	0.55	0.71	1681	Normal	1.00	0.55	0.71	1681
Congested	0.64	1.00	0.78	1362	Congested	0.64	1.00	0.78	1362
Accuracy		0.75	3043		Accuracy		0.75	3043	
Macro avg	0.82	0.77	0.74	3043	Macro avg	0.82	0.77	0.74	3043
Weighted avg	0.84	0.75	0.74	3043	Weighted avg	0.84	0.75	0.74	3043

Models	Support Vector Machine				Extreme Gradient Boosting				
	precision	recall	F1-score	support		precision	recall	F1-score	support
Normal	0.98	0.30	0.46	1681	Normal	1.00	0.55	0.71	1681
Congested	0.53	0.69	0.69	1362	Congested	0.64	1.00	0.78	1362
Accuracy		0.61	3043		Accuracy		0.75	3043	
Macro avg	0.76	0.65	0.58	3043	Macro avg	0.82	0.77	0.74	3043
Weighted avg	0.78	0.61	0.56	3043	Weighted avg	0.84	0.75	0.74	3043

Models	Logistic Regression				Stacking Ensemble				
	precision	recall	F1-score	support		precision	recall	F1-score	support
Normal	0.99	0.54	0.70	1681	Normal	0.99	0.54	0.70	1681
Congested	0.64	0.99	0.78	1362	Congested	0.64	0.99	0.78	1362
Accuracy		0.74	3043		Accuracy		0.74	3043	
Macro avg	0.81	0.77	0.74	3043	Macro avg	0.81	0.77	0.74	3043
Weighted avg	0.83	0.74	0.73	3043	Weighted avg	0.83	0.74	0.73	3043

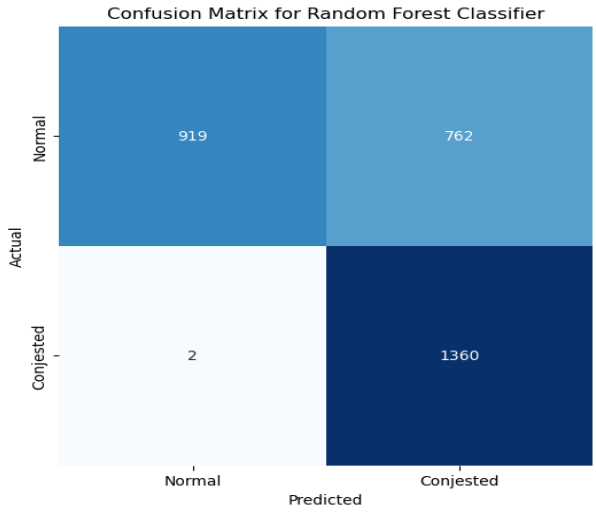

Figure 12. Confusion Matrix for RF Models

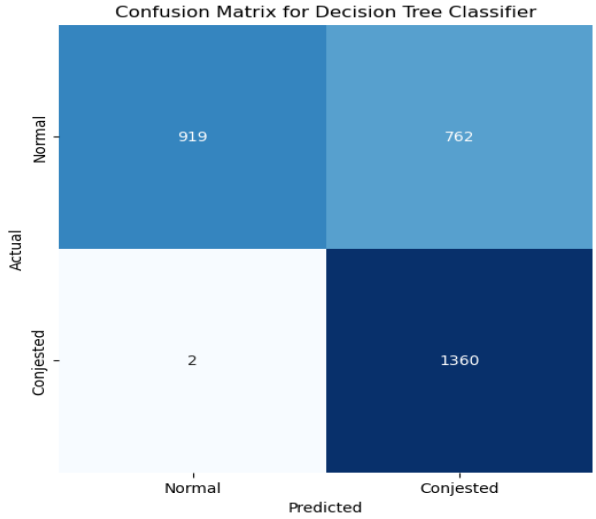

Figure 13. Confusion Matrix for DT Models

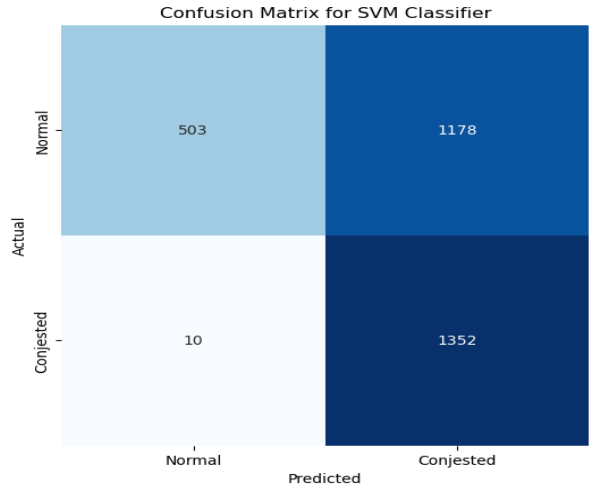

Figure 14. Confusion Matrix for SVM Models

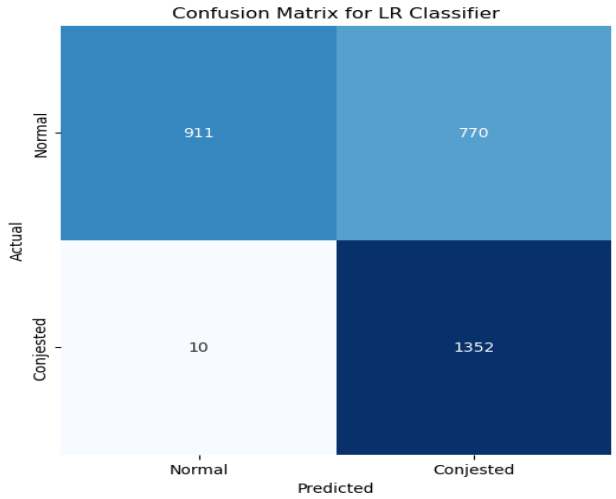

Figure 15. Confusion Matrix for LR Model

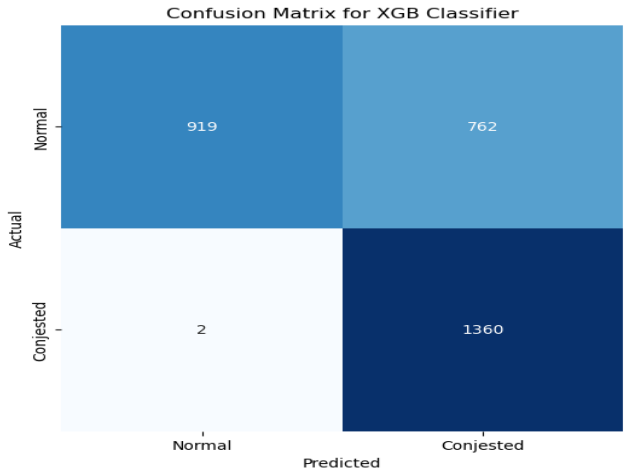

Figure 16. Confusion Matrix for XGB Model

The performance analysis table of six machine learning models includes Logistic Regression, Random Forest, Support Vector Machine (SVM), Decision Trees, Extreme Gradient Boosting (XGBoost), and Stacking Ensemble by assessing their precision, recall, and F1-score for detecting "Normal" and "Congested" traffic conditions. The models demonstrate different capabilities in correctly categorizing traffic categories impacting their overall success rate. Among the models, Random Forest, Decision Trees, and XGBoost exhibit similar performance. The F1-score assessment reveals 71% for normal traffic, and 78% for congested traffic while maintaining macro and weighted average F1-scores within the range of 74% to 75%. The models show balanced accuracy patterns, although they experience occasional misidentification of cases. The detection models show a lower recall score of 0.55 for normal traffic compared to their perfect score of 100% for congested traffic, which indicates these models tend to mistake normal conditions as congested. The performance of SVM stands out as weak. It obtains an F1 score of 46% primarily because it detects normal traffic at only a 30% recall rate. The accuracy rate of SVM for detecting normal traffic conditions remains low, thus making its reliability questionable. Logistic regression shows better performance compared to SVM because it produces an overall weighted average F1 score of 74%, indicating its potential as a competent option. The Stacking Ensemble model exceeds all other models by reaching a macro and weighted average F1 score of 75%. The model demonstrates high performance in detecting congested traffic because its F1 score reaches 79%.

5. Conclusion and Future Scope

The authors used OPNET 14.5 along with machine learning to assess how DoS attacks affect enterprise networks. The developed research reveals that DoS attacks generate two major network performance consequences by intensifying Ethernet delay times while simultaneously diminishing the operational capability of essential network services comprising database queries along with email and FTP and HTTP traffic functions. Analysis results showed that packet loss and throughput reduction together with service outages occurred as a direct result of DoS attacks creating network congestion. The Ethernet delay was steady but HTTP traffic became nonoperational and FTP faced significant performance degradation as a result of the attack. Enterprise networks face severe consequences from DoS attacks because of which proactive network security becomes essential for minimizing such damage during disruptions. However, several preventative measures must be deployed for strengthening enterprise network resilience against DoS attacks. Network performance remains intact because intrusion detection systems along with prevention systems function to detect and halt security threats in their initial stages. Organizations can prevent attackers by performing security audits and delivering software updates at the correct time as well as keeping systems free of vulnerabilities during this process. Multiple defense strategies combined into network security allow organizations to protect their systems while registering better resilience against DoS attack impact on operations.

Acknowledgements- The successful completion of this research was made possible through the favorable environment created by Dr. M. A. Akinde (FCA, ACTI) as the Rector of the Federal Polytechnic Ilaro and his management team.

Funding Source- None

Authors' Contributions-Author-1. The researcher developed the research concept while performing extensive study of the introduction section and related works and designing network scenarios using OPNET to obtain the necessary dataset. Author-2. The researcher worked on dataset refinement from OPNET simulations while applying machine learning tools for analysis to study how DoS attacks impact enterprise network systems.

Conflict of Interest- None

References

[1] B. B. Gupta, R. C. Joshi, and M. Misra, "ANN-Based Scheme to Detect Flooding Attacks in Vehicular Ad hoc Networks," Journal of Info. Sec. and App., vol. 54, p. 102556, **2020.**

[2] J. Mirkovic and P. Reiher, "A taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39–53, **2004.**

[3] A. Gupta and L. S. Sharma, 'Mitigation of DoS and port scan attacks using snort', *Int. J. Comput. Sci. Eng.*, vol. 7, no. 4, pp. 248–258, 2019

[4] H. Iqbal and S. Naaz, 'Wireshark as a tool for detection of various LAN attacks', *Int. J. Comput. Sci. Eng.*, vol. 7, no. 5, pp. 833–837, 2019.

[5] S. Behal and K. Kumar, "Trends in the Detection of Distributed Denial-of-Service Attacks," Computer Communications, vol. 116, pp. 24–37, **2017.**

[6] Y. Wang, J. Liu, and H. Zhang, "A Study on DoS Attack Cost and Mitigation Strategies," International Journal of Cybersecurity, vol. 10, no. 1, pp. 45–60, **2022.**

[7] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms against Distributed Denial-of-Service Attacks," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, **2013.**

[8] M. H. U. Sharif and M. A. Mohammed, "A literature review of financial losses statistics for cyber security and future trend", *World J. Adv. Res. Rev.*, vol. 15, no. 1, pp. 138–156, 2022.

[9] K. Darshan, V. Rohan, R. Rohan, and D. H. Kamath, 'Hybrid Intrusion Detection System Using K-Means Algorithm', *International Journal of Computer Sciences and Engineering*, vol. 4, no. 3, pp. 82–85, 2016.

[10] P. Rajput and P. Kulkarni, 'A Survey on Wireless Malevolent Access Point Detection Methods for WLAN', *International Journal of Computer Sciences and Engineering*, vol. 4, no. 4, pp. 48–50, 2016.

[11] P. Kumar, D. Puthal, and M. Prasad, "Intrusion Detection in Software-Defined Networking using Machine Learning," Future Generation Computer Systems, vol. 115, pp. 94–104, **2021.**

[12] A. Singh, R. Verma, and S. Kumar, "Emerging Trends in Cybersecurity for Enterprise Networks," Journal of Network and Computer Applications, vol. 125, pp. 138–155, **2019**.

[13] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Deep Learning Framework for Cybersecurity Applications," Neural Computing and App., vol. 31, no. 3, pp. 689–708, **2019.**

[14] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting DDoS attacks: Methods, Tools, and Future directions," The Computer Journal, vol. 57, no. 4, pp. 537–556, **2014.**

[15] Z. Tan, D. He, and S. Chan, "AI-driven Defense against Denial-of-Service Attacks in Cloud Computing," IEEE Tran.on Cloud Computing, vol. 8, no. 2, pp. 330–344, **2020.**

[16] M. Ahmed, Y. Xiang, and W. Zhou, "Deep Learning for Detecting Volumetric DDoS Attacks in Enterprise Networks," IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2520–2531, **2021.**

[17] Y. Zheng, C. Wang, and L. Chen, "Simulation-based Performance Analysis of Cybersecurity Threats using OPNET," Journal of Cybersecurity Research, vol. 7, no. 1, pp. 59–71, **2018.**

[18] W. Iftikhar, Z. Mahmood, and D. M. Vistro, "The Impact of DDoS and Ping of Death on Network Performance," International Journal of Scientific & Technology Research, vol. 8, no. 12, p. 276, **2019**.

[19] L. Huraj and M. Šimon, "Realtime Attack Environment for DDoS Experimentation," in IEEE 15th International Scientific Conference on Informatics, **2019.**

[20] M. Lernefalk, "Evaluating the Effects of Denial-of-Service Attacks from IoT Devices," Mittuniversitetet, **2021.**

[21] A. Saliou, B. Zhang, and C. Kumar, "Overcoming static firewall limitations through the development of an out-of-line firewall evaluation framework," Journal of Network Security and Applications, vol. 15, no. 3, pp. 210–225, **2022**, doi: 10.1016/j.jnsa.2022.05.012.

[22] A. Y. Nalukui and C. S. Lubobya, "Effects of DoS Attack in Wi-Fi Broadband Network," International Journal of Networks and Comm., vol. 12, no. 2, pp. 47–54, **2022**.

[23] K. Sireesha, S. V. Krushna, and C. M. Krishna, "Design and Security Simulation of Wi-Fi Networks," Juni Khyat, vol. 12, no. 5, pp. 200–209, **2022**.

[24] A. Agrawal, V. Jain, and R. Astya, "Enhancing Network Security Against DDoS Attacks: An Analysis of OPNET Modelers," in IEEE SMART Conference, **2023,** doi: 10.1109/SMART59791.2023.10428206.

[25] R. Bukhowah, A. Aljughaiman, and M. M. H. Rahman, "Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions," Electronics, vol. 13, no. 1031, **2024**, doi: 10.3390/electronics13061031.

[26] I. Iqbal, I. Shafqat, M. Rauf, and S. Krishna, "Securing Network Against Denial of Service (DoS) Attack Using Graphical Network Simulator-3," **2024.**

[27] S. Willium, "Computer Sciences," International Journal of Scientific Research in Computer Science and Engineering, vol. 31, no. 4, pp. 123–141, **2012.**

AUTHORS PROFILE

Mr. O. J. Adaramola acquired his Master of Science in Computer Systems and Network Engineering from the University of Greenwich, London, UK in 2016 and obtained his Master of Science in Electronics and Computer Engineering from Lagos State University, Nigeria in 2018 after which he completed his Bachelor of Engineering in Computer Engineering at Federal University, Oye-Ekiti in 2023. The year 2023 marked his achievement of the Bachelor of Engineering degree in Computer Engineering at Federal University Oye-Ekiti. He currently holds the positions of Senior Lecturer along with serving as Head of the Department of Computer Engineering at the Federal Polytechnic Ilaro in Ogun State Nigeria. The researcher actively participates in professional organizations and maintains research interests in vehicular ad hoc networks as well as ZigBee technology, wireless communication, routing protocols, computer networking and network security.

Mr. O. H. Aliu acquired his Master of Engineering in Computer Engineering from the Federal University, Oye Ekiti, Nigeria, in 2024, after which he completed his Bachelor of Engineering in Computer Engineering at Ekiti State University, Ado Ekiti, Nigeria, in 2016. He currently a lecturer in the department of computer engineering at the Federal Polytechnic, Ilaro, in Ogun State, Nigeria. The researcher actively participates in professional organizations and maintains research interest in artificial intelligence, data analysis, computer vision, and natural language processing.

