BENIN JOURNAL OF PHYSICAL SCIENCES
BJPS Vol. 2(2), December, pg. 144-161 (2025)
ISSN 3043-6931(Print)
3043-694X(Online)
www.bjps.org.ng

DDoS Intrusion Detection in SIP-VoIP Networks Using Genetic Algorithm–Optimized Modular Neural Networks

E. C. IGODAN*[,1], S. D. MADAKI[2], O. UKPEBOR[3], T. JESSA[4], O. SOKOYA[5], and E. MINTAH[6]

[1]*Department of Data Science, University of Benin, Benin-City, Nigeria.*

[2]*Department of Computer Education, Federal College of Education (Technical), Asaba.*

[3]*Department of Computer Information Science, University of the Cumberlands, Williamsburg, U.S.A.*

[4,6]*College of Business, Westcliff University, Irvine, USA*

[5]*College of Business, Engineering and Technology, National University, San Diego, USA*

Received: 24/10/2025 ***Accepted:*** 15/12/2025

Abstract

In order to identify distributed denial-of-service (DDoS) attacks on SIP-VoIP infrastructures in real time, this paper proposes a genetic algorithm-trained modular neural network (MNN) with SMOTETomek balancing. In contrast to traditional firewalls and static filters, our framework leverages modular deep learning and evolutionary optimisation to accurately and adaptively identify malicious traffic. The model incorporates noise reduction and synthetic oversampling using a large-scale SDN-DDoS dataset (1,048,575 records) to mitigate the class imbalance problem prior to modular learning. The experimental results from the study demonstrates that the ensemble outperforms similar machine learning and ensemble baselines, achieving 99.5% accuracy with an F1-score of 0.978. Beyond sheer performance, the modular architecture offers parallelized training and robust generalisation, guaranteeing resistance to diverse DDoS vectors. This study demonstrates how well genetic algorithms combined with modular neural networks can be leveraged for intrusion detection, providing a workable and scalable solution to protect next-generation SIP-VoIP communication systems against evolving hostile threats.

*Corresponding author e-mail: charles.igodan@uniben.edu

Keywords: *Genetic Algorithm, Modular Neural Network, Optimization, Intrusion Detection, Distributed Denial of Service*

1. INTRODUCTION

Advancements in informatics, driven by Moore's Law, have consistently generated novel technologies that improve communication and productivity in contemporary society (Priyanka and Kumar, 2021). The most revolutionary of these is the Internet, enabling worldwide communication and rapid data transmission. Its cost-effectiveness, ubiquity, ease of use, and continued increases in user trust across communication platforms have all contributed to its rapid adoption (Yoro et al., 2023). These characteristics played a major role the Internet's extensive integration into social and commercial contexts, but it has also turned into a platform for malicious behaviour. Cybercriminals target naive consumers with the intention of stealing information, interrupting with services, or compromising infrastructure resources by taking advantage of its accessibility to execute technically complex and socially orchestrated assaults (Nasir et al., 2021). In order prevent discovery and compromise data availability, confidentiality, and integrity, adversarial threats often pose as trustworthy users (Dawodu et al., 2023). The widespread availability of back-end technologies has made techniques like data manipulation, malware injection, and denial-of-service (DoS) attacks a commonplace (Malik et al., 2021). Distributed denial-of-service (DDoS) attacks, in instance, employ a large number of compromised machines to overload targeted servers, causing considerable downtime, resource depletion, and financial losses (Darabian and Javidan, 2022; Kannan et al., 2023). Users' vulnerability to deception, which is frequently impacted by behavioural or psychological variables, further increases their efficacy (Aggarwal et al., 2022; Sahmoud and Mikki, 2022). Despite the implementation of traditional security measures, such as intrusion detection systems, firewalls, and secure gateways, these mechanisms have had little or no effect against the extent and increasing sophistication of DDoS operations (Alsaeedi et al., 2020; Alqahtani et al., 2022). The continuing rise in these threats highlights the necessity of intelligent and adaptable detection methods that can instantly identify malicious traffic at or close to its source. Significant countermeasures are required due to this widespread issue, which results in losses of billions of dollars every year (Darabian and Javidan, 2022). Researchers are increasingly investigating machine learning (ML) as a potential paradigm since it can identify abnormalities, learn intricate traffic patterns, and adapt to new approaches to attack (Mirlekar and Kanojia, 2022). Furthermore, phishing and related attack vectors continue to spread due to the increased reliance on social networking and online platforms for communication and business, underscoring the necessity of intelligent, proactive, and scalable

intrusion detection systems (Khan et al., 2023; Olusola et al., 2024). In order to improve the detection of DDoS attacks in SIP-VoIP infrastructures, this study proposes a novel intrusion detection framework that combines SMOTE-Tomek resampling with a genetic algorithm (GA)-trained modular neural network (MNN). In order to find the most relevant predictors while reducing dimensionality and redundancy, the genetic algorithm is used for feature optimisation, harnessing its evolutionary search capabilities (Goldberg, 1989; Clevert et al., 2016; LeCun et al., 2015; Mirjalili, 2019).

The use of supervised machine learning techniques and associated ensemble approaches to automate intrusion detection in network connections has been the subject of much recent research. Hosseinpour et al., (2018) design an effective effective mechanism for detecting and mitigating denial-of-service (DoS) attacks in session initiation protocol (SIP) networks achieving 98% accuracy overall. However, the study is dependent on accurately modeled normal traffic for baseline generations, limited on potential degradation in performance under highly dynamic or large-scale SIP deployments, and limited validation against real-world traffic heterogeneity and adaptive attackers that closely mimic legitimate behaviour. Zhou et al., (2019) propose an efficient intrusion detection system by integrating optimal feature selection with ensemble classifier using correlation-based feature selection with Bat Algorithm (CFS-BA) to eliminate redundant attributes and then employed an ensemble of C4.5, random forest, and Forest by penalizing Attributes (Forest PA) based on majority-voting scheme. The study achieved 99.81% accuracy, 99.80% detection rate, and a 0.17% false alarm rate connected on NSL-KDD, AWID, and CIC-IDS2017 datasets. The study was characterized by the lack of evaluation under live network conditions, and the need for further optimization to handle concept drift and scalability on real-time applications. Zhou et al., (2019) propose an efficient intrusion detection system by integrating optimal feature selection with ensemble classifier using correlation-based feature selection with Bat Algorithm (CFS-BA) to eliminate redundant attributes and achieved 99.81% accuracy, 99.80% detection rate, and a 0.17% false alarm rate connected on NSL-KDD, AWID, and CIC-IDS2017 datasets. However, the work lacked the evaluation under live network conditions, and has scalability problem on real-time applications. Tama and Lim, (2021) comprehensively analyze existing ensemble learning approaches used in intrusion detection systems (IDS), propose and evaluate a robust ensemble framework that enhances detection accuracy across multiple benchmark datasets. Their results demonstrated that the stack of ensemble (SoE) model, and achieves exceptionally high detection accuracy up to 100%, strong Matthews Correlation Coefficient scores, low false positive rates, and high AUC values across benchmark datasets - NSL-KDD and UNSW-NB15. The work presented by Mirlekar and Kanojia, (2022)

evaluate and compare the performance of various ML algorithms for improving the detection and classification of networks intrusions based on NSL-KDD dataset. However, the study lacks empirical validation, variations in data availability and regulatory maturity across regions and the difficulty of applying complex quantitative models in resource-constrained banking environments limited the study. Dawodu et al., (2023) analyze and identify effective approaches for assessing and managing cybersecurity risks within the banking sector, particularly in developing countries. However, the lack of empirical validation or real-time performance measures, regional differences in data availability and regulatory maturity, and the challenge of implementing sophisticated quantitative models in underdeveloped or resource-constrained banking contexts limit the effort. In order to address the shortcomings of individual models, Lalduhsaka et al. (2022) present an anomaly-based detection method that achieves an accuracy of 98.3% by utilising an ensemble machine-learning strategy that combines numerous classifiers. The study's limitations include its reliance on carefully selected benchmark datasets, possible over-fitting, and an insufficient evaluation of the method's performance in an active operating network context. Kannan et al., (2023) develop an intelligent and efficient detection framework capable of identifying and mitigating denial-of-service (DoS) and distributed-DoS attacks within software-defined networks (SDN). Experimental results showed that random forest achieved the highest accuracy of 99.82%, 99.8% precision, 99.7% recall, and a 0.18% false alarm rate, outperforming others both in speed and reliability. Ali et al., (2024) survey is centered on the unveiling machine learning strategies and considerations in intrusion detection systems. However, the study is limited by the lack of interpretability of deep learning models, lack of real-time validation in dynamic network environments and the absence of standardized evaluation frameworks. Salama et al., (2025) survey and synthesize recent ensemble-based approaches for network intrusion detection systems (NIDS). Whilst, Genuario et al., (2024) survey and synthesize contemporary machine-learning approaches for detecting and monitoring cyberattacks across network traffic, identifying effective algorithms, common feature engineering practices, datasets, and evaluation strategies. Lamin et al. (2024) examine how artificial intelligence techniques improve phishing detection and prevention by breaking over the weaknesses of conventional signature-based methods. However, the generalization of the models to new attack types is uncertain and the lack of interpretability of the AI-models limited their study. Bibers and Abdallah, (2025) design a flexible, practical ensemble-based anomaly detection framework tailored to IoT environments. The study shows greater robustness to heterogeneous IoT, better generalization across dataset using ensemble methods. However, the study advocates AutoML ensemble tuning, integration of explainable AI to improve operational trust, and federated ensemble learning for privacy as future studies.

Nazat et al., (2025) build and evaluate a robust ensemble-based machine-learning framework tailored to detecting anomalies within autonomous vehicle (AV)/vehiclar ad hoc network (VANET) environments. There are four main considerations that motivate this investigation. First, because poorly managed datasets raise the risk of false positives and false negatives, the scarcity of high-quality datasets continues to impede the accurate training and assessment of intrusion detection algorithms (Alsaeedi et al., 2020). Second, in order to guarantee more dependable classification results, the ongoing disparity between attack and genuine traffic calls for the use of extensive sampling methods and ensemble learning strategies, as SMOTE-Tomek (Alqahtani et al., 2022). Third, cross-channel detection systems that can integrate many data streams to improve accuracy and adaptability are necessary due to the increasing reliance on heterogeneous communication channels (Khan et al., 2023). Lastly, adaptive, machine learning-driven detection techniques embedded at network gateways are necessary to provide proactive defence measures because existing VoIP-based detection frameworks frequently fail against undetected, low-rate, and flash-crowd attacks (Aggarwal, 2022). In order to provide a reliable and scalable framework for real-time DDoS detection in SIP-VoIP infrastructures, this study investigates the integration of genetic optimisation, modular neural networks, and hybrid resampling approaches.

2. MATERIALS AND METHOD

Our proposed approach as depicted in Figure 1 employs a stacked learning framework integrating a Cultural Genetic Algorithm (CGA) with a Modular Neural Network. The method proceeds as follows:

2.1 Data Collection

The Software-Defined Networking (SDN)-DDoS Traffic Dataset (Ver 1) used in this study was created in a software-defined networking environment using a Ryu controller and is accessible on Mendeley Data (https://data.mendeley.com/datasets/b7vw628825/1) (Khan et al., 2023). There are 328,765 attack instances and 719,810 instances among the 1,048,575 records and 26 network-centric attributes in the dataset. The initial class disparity is depicted in Figure 2 (Hirsi et al., 2024).

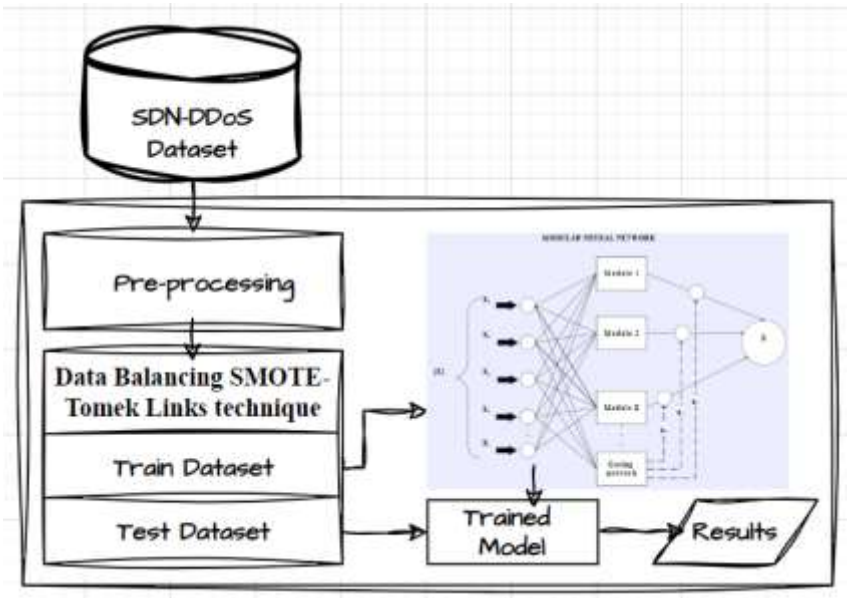

Figure 1: *Workflow Architecture for GA-based MNN DDoS Detection in SIP-MNN Infrastructure*

2.2 Preprocessing

This involves One-hot encoding of categorical features, handling of missing values, and duplicate removal. Categorical values were converted into binary representations appropriate for machine learning models through encoding (Pedregosa et al., 2011; Zheng and Casari, 2018).

2.3 Feature Selection and Fitness Evaluation

By keeping only, the most important predictors for classification, a fitness function was utilised to minimise dimensionality. The Rosenbrock function, which is commonly used as a benchmark test function for comparing optimisation algorithms, was employed as the optimisation objective in order to thoroughly assess the search efficiency and convergence behaviour of the suggested optimisation approach (Sahmoud and Mikki, 2022). Nine of the original 26 attributes depicted in Table 1 were chosen as the most important contributors with a minimum X^2 value of 8.00.

Table 1: *Ranking of Attributes score using the Chi-Square*

S/N	Features	X^2-Value	Selected (Yes/No)
1	Host	13.36	No
2	Source IP	10.041	Yes
3	Destination IP	10.001	Yes
4	Source Port	9.956	Yes
5	Label_attack	9.372	Yes
6	Duration	9.258	Yes
7	Destination Port	9.248	Yes
8	Protocol	8.492	Yes
9	Jitters	8.492	No

2.4 Dataset Splitting, Balancing, and Normalization

The dataset was divided into 209,715 test sets (20%) and 838,860 training sets (80%). We used the SMOTE-Tomek Links technique (Batista et al., 2004; Fernández et al., 2018), that generates synthetic minority instances and eliminates overlapping examples to create a balanced distribution, to resolve class imbalance. The original and balanced distributions are seen in Figures 2 and 3 respectively. In order to reduce skewness and improve convergence, normalisation was then carried out using a conventional scaler to convert feature distributions to zero mean and unit variance (Pedregosa et al., 2011). The normalised dataset is displayed in Figure 4.

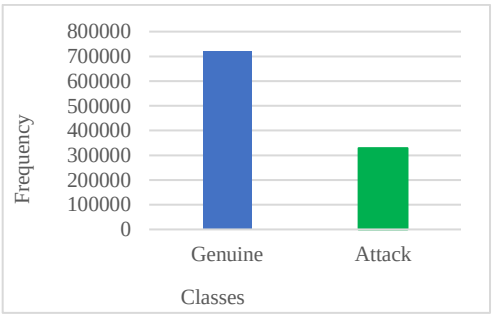

Figure 2: *Original Dataset plot*

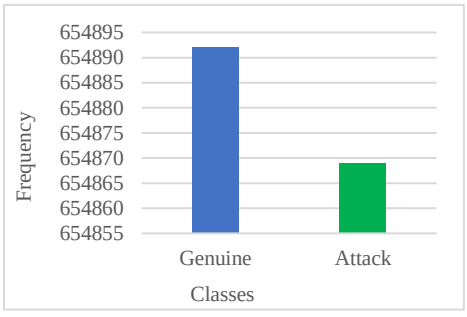

Figure 3: *Dataset with SMOTE applied*

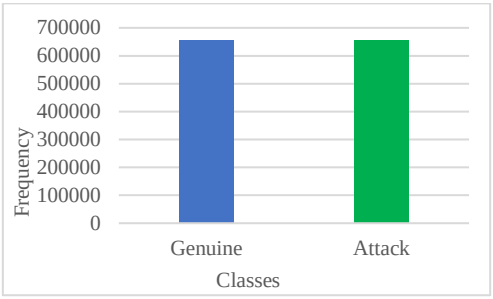

Figure 4: *Normalized Dataset after prior SMOTE-Tomek Links*

2.5 Stacked Ensemble Learning

Two base learners make up the ensemble. The Cultural Genetic Algorithm (CGA) uses initialisation, selection, crossover, and mutation to evolve potential solutions. The high feature dimensionality, class imbalance, and temporal variability of SIP-VoIP DDoS traffic were addressed by optimizing the evolutionary algorithm's hyperparameters. To preserve diversity, larger populations and adaptive mutation were employed, and the reliability of attack detection was enhanced via a weighted fitness function that prioritized false-negative reduction. By introducing normative, domain, temporal, and spatial belief spaces into the evolutionary process, the CGA variant outperforms GA. This speed up convergence and keeps solutions from violating domain limitations (Reynolds, 1994).

2.6 Modular Neural Network (MNN)

A set of separate neural networks that are mediated by an intermediate is what defines a modular neural network. In order to complete a subtask of the task the network is intended to complete, each autonomous neural network functions as a module and operates on distinct inputs (Volna, 2009; Xu et al., 2015; Clevert et al., 2016). Modularization improves scalability, reduces convergence time, and enhances adaptability by training sub-networks independently and recombining their outputs (Mehrotra et al., 1992). A three-layer feed-forward neural network is adopted in this study. Table 2 summarizes the configurations for Genetic Algorithm (GA) feature selection and Modular Neural Network (MNN).

Table 2: *The Cultural Genetic Algorithm Parameter Design and Configuration*

Features	Values	Description
Activation Function	Leaky ReLU	(α = 0.01) for hidden layers, Softmax for final classification.
Learning Rate (η)	0.001 – 0.01	Adam optimizer works best
Hidden Layers	2	Modularized blocks (e.g., 3–7 modules, each with 2 dense layers).
Neurons per Layer	64 - 128	64 per module (tunable via GA)
Batch Size	64	balance between training speed and generalization.
Dropout Rate	0.3 - 0.5	to prevent overfitting.
Epochs	300 - 1000	with early stopping to avoid wasted computation
Weight Initialization	-	Initialization for Leaky ReLU
Normalization	-	Batch Normalization between modular blocks

2.7 Training and Deployment

The ensemble was trained from scratch on the balanced dataset using stratified 10-fold cross-validation to prevent overfitting and ensure generalization. Training combined both original and synthetic samples to enhance robustness. Deployment was conducted via Flask API and Streamlit, enabling integration as an embedded intrusion detection system (Grinberg, 2018). The configuration for the proposed SIP-VoIP DDoS detection modular neural network (MNN) involves an input layer followed by batch normalization, then a dense layer with 128 units using the LeakyReLU activation, a subsequent dense layer with 64 units and LeakyReLU activation combined with a 0.4 dropout rate, modular sub-networks fused into a dense layer of 128 units with LeakyReLU activation, and finally an output layer with a Softmax function for multiclass attack classification. Table 3 depicts the computed fitness function with sample rule explained as: *if* (*duration*="-1,0,-1"&*protocol*= "-1"&*src-port*="1023"&*dest-port*="-1"&*srcIP*="192.168.1.30"&*dest-IP*="192.168.0.-1") *then* {log_network connection = Intrusion}.

Table 3: *Sample Fitness Function Ranking of Attributes with Top 12-Generated Rules*

Time	Protocol	Source Port	Destination Port	Source IP	Destination IP	Attack	Fitness
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	PG	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.168.0.20	PS	0.8063
-1,0,23	telnet	-1	23	192.-1.1.30	192.168.0.20	PC	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.168.0.20	ARS	0.8063
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	ICMP	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.168.0.20	NP	0.8063
0,0,23	telnet	-1	-1	192.168.1.30	192.168.0.20	PA	0.8063
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	FA	0.8063
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	ARS	0.8063
0,0,-1	-1	1023	1021	192.-1.1.30	-1.168.0.20	PODA	0.8031
-1,0,-1	**-1**	**1023**	**-1**	**192.168.1.30**	**192.168.0.-1**	**PODA**	**0.8031**
0,0,14	-1	-1	513	192.168.1.30	192.168.0.20	SR	0.8031

3. RESULT AND DISCUSSION

The analysis of the third hidden layer configuration in Table 4 revealed our model performance varied substantially with the number of neurons employed. Configurations with four and six neurons - 9, 11, 4 and 9, 11, 6 – obtained the highest results with an accuracy of 0.995, recall of 0.996, precision of 0.987, and an F1-score of 0.978 respectively. Additionally, these setups showed moderate iteration counts and low training losses of between 0.216–0.272, demonstrating both efficiency and stability. In contrast, however retaining a high recall, models with very few neurones, such as 9, 11, and 1, experienced underfitting, with a reduced accuracy of 0.832 and a comparatively weak F1-score of 0.847. Larger configurations (e.g., 17 neurones) on the other hand showed instability and overfitting, with accuracy dropping to 0.870, recall to 0.545, and an F1-score of 0.634, respectively. Although they did not outperform the four- and six-neuron

structures, mid-range designs, especially those with seven to sixteen neurones, yielded satisfactory outcomes with accuracies in the range of 0.91-0.94 and F1-scores around 0.90-0.93.

These results are in line with earlier research (Tan and Le, 2019), which highlights the need to carefully balance network breadth and depth to prevent underfitting and overfitting. Research on deep residual networks (He et al., 2016) and neural network optimisation (Goodfellow et al., 2016) both show that while compact structures frequently offer better stability on moderate-sized datasets, overly complicated topologies might degrade generalisation. The current findings support this idea by indicating that the bias-variance trade-off is evident in hidden layer tuning, where the ideal balance between model complexity and generalisation is provided by four to six neurones in the third hidden layer.

Table 4: *Third hidden layer configuration analysis*

Hidden Layer	Accuracy	Recall	Precision	F1-Score	Iteration	Training Loss	Epoch
9, 11,1	0.832	0.961	0.920	0.847	32	0.287	500
9, 11,2	0.914	0.952	0.903	0.859	6	1.592	500
9, 11, 3	0.834	0.914	0.914	0.867	29	0.280	500
9, 11, 4	**0.995**	0.996	**0.987**	**0.978**	**16**	**0.216**	**500**
9, 11, 5	0.921	0.952	0.922	0.930	18	0.741	500
9, 11, 6	0.995	0.961	0.975	0.973	18	0.272	500
9, 11, 7	0.923	0.973	0.923	0.950	6	1.322	500
9, 11, 8	0.912	0.876	0.911	0.868	6	1.239	500
9, 11, 9	0.905	0.961	0.903	0.907	7	1.886	500
9, 11, 10	0.898	0.961	0.889	0.889	8	0.623	500
9, 11, 11	0.922	0.963	0.912	0.961	5	2.000	500
9, 11, 12	0.836	0.853	0.834	0.865	11	2.370	500
9, 11, 13	0.876	0.853	0.873	0.874	8	2.350	500
9, 11, 14	0.934	0.924	0.910	0.924	15	0.560	500
9, 11, 15	0.939	0.933	0.893	0.912	8	1.204	500
9, 11, 16	0.945	0.947	0.899	0.923	8	1.730	500
9, 11, 17	0.87	0.545	0.872	0.634	12	1.730	500
9, 11, 18	0.93	0.943	0.940	0.932	6	1.850	500
9, 11, 19	0.93	0.933	0.920	0.904	9	0.660	500
9, 11, 20	0.92	0.927	0.919	0.905	28	1.180	500

The proposed stacking ensemble outperformed traditional machine learning models, which usually range between 95 and 98% on comparable datasets, as shown in Figures 5 and 6, achieving 99.5% accuracy with balanced sensitivity and specificity (Zhang et al., 2019). Its applicability for real-time deployment is underscored by the low rates of false positives (2,097) and false negatives (2,098), which directly address the trade-off between detection sensitivity and false alarm control noted in other studies (Shen et al., 2021).

While performance on less common classes, including session attacks, was less, class-level analysis consistently showed robust DoS attack detection. This is consistent with previous research showing that dominant classes are easier to capture than minority ones (Aldhyani et al., 2023; Zhou et al., 2024). Unlike residual deep learning approaches that rely primarily on oversampling (Zhou et al., 2024) or GA-SMOTE frameworks developed for other domains (Gupta et al., 2024), our model combines genetic algorithm optimization, SMOTE-Tomek balancing, and modular neural architectures. This integration yields superior scalability, robust generalization, and practical adaptability to SIP-VoIP environments. The results therefore extend state-of-the-art intrusion detection by providing a holistic, scalable, and evolutionarily optimized ensemble capable of countering diverse and evolving adversarial threats.

Figure 5: *Confusion Matrix for the Stacking Ensemble*

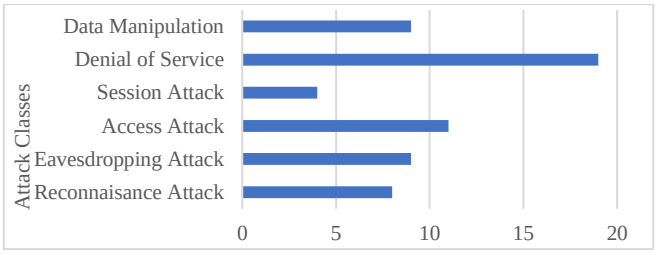

Figure 6: *Comparative DDoS attack detection by proposed ensemble*

While prior studies have combined genetic algorithms with neural networks for intrusion and DDoS detection, and others have utilized SMOTE-Tomek balancing or modular neural nets, however, none to date to the best of our knowledge have combined these three strategies in a modular, scalable, real-time SIP-VoIP context as depicted in Table 5. In the Table, (Anusooya et al., 2024) employed a genetic algorithm for feature selection followed by neural network classification for DDoS detection, but without modularity or imbalance handling (Rahman et al., 2025). Another study developed a modular memetic neural network for anomaly-based DDoS detection, achieving high accuracy, yet did not include genetic optimization or synthetic balancing (Gupta et al., 2024). Balancing approaches such as SMOTE-

Tomek have shown effectiveness in network intrusion detection and other domains, but without concurrent evolutionary learning or modular architectures (Aldhyani et al., 2023). Finally, while residual DL architectures with SMOTE have achieved near-perfect accuracy in DDoS detection, they lack GA-driven feature selection and modular scalability (Zhou et al., 2024). Hence, our framework fills this gap by complementarily combining all three methodologies in a high-performance, real-time SIP-VoIP detection model.

Table 5: *Summary Comparisons*

Article	Techniques	Metrics / Domain
Anusooya et al., (2024)	GA feature selection + Neural Network	DDoS/malware detection, unspecified metrics
Rahman et al., (2025)	Modular NN + evolutionary training	F1 = 0.9945, Accuracy = 0.9984
Gupta et al., (2024)	SMOTE-Tomek balancing + GA model	Software fault prediction, various metrics
Aldhyani et al., (2023)	Data balancing via SMOTE-Tomek	Ensemble model on CICIDS, metric unspecified PMC
Zhou et al., (2024)	SMOTE oversampling + Deep ResNet	99.98% accuracy on DDoS detection
Our Study	SMOTE-Tomek balancing + GA feature selection + Modular Neural Network	F1 = 97.8, Spec=99.10%, Recall=99.62%, 99.50% accuracy on real-time SIP-VoIP detection model

4. CONCLUSION

This study introduced a genetic algorithm–optimized modular neural network (MNN) with SMOTE-Tomek resampling for real-time detection of DDoS attacks in SIP-VoIP infrastructures. The proposed ensemble framework outperformed similar baselines with an F1-score of 0.978 and 99.5% accuracy, proving that the combination of modular deep learning, balanced resampling, and evolutionary feature selection significantly enhances adaptability, scalability, and generalisation. However, implementation in edge environments is difficult due to high computing costs, and real-world applicability is limited by the reliance on a single simulated dataset. Additionally, the model does not incorporate new paradigms like explainable AI and reinforcement learning, and the use of synthetic

oversampling raises the possibility of bias. In order to close these gaps, future research will optimise lightweight deployment for edge devices, incorporate federated and reinforcement learning for adaptability and privacy protection, and validate performance on heterogeneous real-world traffic. Transparency for crucial applications will be further improved by including explainable AI. All things considered, the proposed framework offers a solid basis for developing workable, industry-ready defences against changing DDoS attacks in next-generation SIP-VoIP systems. The SDN-DDoS dataset does not specifically simulate RTP media flows or SIP signaling, which is a drawback of this work. As a result, this work does not cover application-layer VoIP metrics like call quality and signaling consistency.

CONFLICT OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Aggarwal, V., Kumar, P., and Gupta, R. (2022). Ensemble learning for anomaly-based intrusion detection systems: A systematic literature review. IEEE Access, 10, 98215–98236.

https://doi.org/10.1109/ACCESS.2022.3198765

[2] Aldhyani, T. H. H., Alrasheed, H., Alghamdi, A., and Alshamrani, S. S. (2023). Ensemble-based intrusion detection systems with SMOTE-Tomek preprocessing on imbalanced network traffic. Sensors, 23(7), 3511. https://doi.org/10.3390/s23073511

[3] Ali, A. H., Charfeddine, M., Ammar, B., Hamed, B. B., Albalwy, F., Alqarafi, A., and Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. Frontiers in Computer Science, 6, Article 1387354. https://doi.org/10.3389/fcomp.2024.1387354 (frontiersin.org)

[4] Alqahtani, M., Alsaadi, F., and Alghamdi, T. (2022). Intelligent intrusion detection for VoIP networks using deep learning and feature selection. Computers & Security, 118, 102739. https://doi.org/10.1016/j.cose.2022.102739

[5] Alsaeedi, M., Alhaidari, F., and Alsaeedi, A. (2020). Machine learning for detection of DDoS attacks in cloud computing: A survey. IEEE Access, 8, 132526–132544. https://doi.org/10.1109/ACCESS.2020.3009273

[6] Anusooya, P., Ramesh, S., and Anusha, P. (2024). A hybrid genetic algorithm and neural network-based cyber security approach for enhanced detection

of DDoS and malware attacks in wide area networks. American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), 93(1), 34–50. Retrieved from

[7] Batista, G. E., Prati, R. C., & Monard, M. C. (2004). A study of the behavior of several methods for balancing machine learning training data. ACM SIGKDD Explorations Newsletter, 6(1), 20–29. https://doi.org/10.1145/1007730.1007735

[8] Bibers, I., and Abdallah, M. (2025).An ensemble learning framework for enhanced anomaly and failure detection in IoT systems, Cyber Security and Applications,Volume 3, 100105. pp.1-23. https://doi.org/10.1016/j.csa.2025.100105.

[9] Clevert, D.-A., Unterthiner, T., and Hochreiter, S. (2016). Fast and accurate deep network learning by exponential linear units (ELUs). arXiv. https://doi.org/10.48550/arXiv.1511.07289

[10] Darabian, M., and Javidan, R. (2022). Cost analysis of DDoS attacks: Global financial impacts and countermeasures. Journal of Cybersecurity, 8(1), 1–15. https://doi.org/10.1093/cybsec/tyab019

[11] Dawodu, S. O., Omotosho, A., Odunayo, J. A., Abimbola, O. A., and Ewuga, S. K. (2023). Cybersecurity risk assessment in banking: Methodologies and best practices. Computer Science and Information Technology Research Journal, 4(3), 220–243. https://doi.org/10.51594/csitrj.v4i3.659

[12] Fernández, A., García, S., Herrera, F., and Chawla, N. V. (2018). SMOTE for learning from imbalanced data: Progress and challenges, marking the 15-year anniversary. Journal of Artificial Intelligence Research, 61, 863–905. https://doi.org/10.1613/jair.1.11192

[13] Genuario, F., Santoro, G., Giliberti, M., Bello, S., Zazzera, E., & Impedovo, D. (2024). Machine Learning-Based Methodologies for Cyber-Attacks and Network Traffic Monitoring: A Review and Insights. Information, 15(11), 741. https://doi.org/10.3390/info15110741

[14] Grinberg, M. (2018). Flask web development: Developing web applications with Python. O'Reilly Media.

[15] Goldberg, D. E. (1989). Genetic algorithms in search, optimization and machine learning. Addison-Wesley.

[16] Goodfellow, I., Bengio, Y., and Courville, A. (2016). Deep learning. MIT Press. http://www.deeplearningbook.org

[17] Gupta, R., Rajnish, and Bhattacharjee, A. K. (2024). A hybrid SMOTE-Tomek link and genetic algorithm model for software fault prediction. Sensors, 25(5), 1578. https://doi.org/10.3390/s25051578

[18] Hosseinpour, M., Yaghmaee, M-H., Seno, S.A.H., Khosravi, H. and Asadi, M. (2018). Anomaly-based DoS detection and prevention in SIP networks by modeling SIP normal traffic. International Journal of Communication Systems 31(1-4):e3825. DOI:10.1002/dac.3825

[19] He, K., Zhang, X., Ren, S., and Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 770–778). https://doi.org/10.1109/CVPR.2016.90

[20] Hirsi, A., Audah, L., and Salh, A. (2024). SDN-DDoS Traffic Dataset (Version 1). Mendeley Data.

[21] Kannan, C., Muthusamy, R., Srinivasan, V., Chidambaram, V., and Karunakaran, K. (2023). Machine learning-based analysis and detection of DoS and DDoS attacks in software-defined networks. Indonesian Journal of Electrical Engineering and Computer Science. Vol. 32, No. 3, December 2023, pp. 1503~1511ISSN: 2502-4752, DOI: 10.11591/ijeecs.v32.i3.pp1503-1511

[22] Khan, H., Ahmad, I., and Shafiq, M. (2023). Phishing attacks: Recent advances, taxonomy, and challenges in detection using AI. Future Generation Computer Systems, 138, 304–320. https://doi.org/10.1016/j.future.2022.12.004

[23] Lalduhsaka, R., Bora, N., and Khan, A. K. (2022). Anomaly-Based Intrusion Detection Using Machine Learning: An Ensemble Approach. International Journal of Information Security and Privacy, 16(1), 1–15. https://doi.org/10.4018/IJISP.311466

[24] Lamina, O. A., Ayuba, W. A., Adebiyi, O. E., Michael, G. E., Ojo-Omoniyi, D. S., & Samuel, K. O. S. (2024). AI-Powered Phishing Detection And Prevention. Path of Science: International Electronic Scientific Journal. https://doi.org/10.22178/pos.112-7 (pathofscience.org)

[25] LeCun, Y., Bengio, Y., and Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539

[26] Mirlekar, S and Kanojia, K. P. (2022). A Comprehensive Study on Machine Learning Algorithms for Intrusion Detection System. 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), Nagpur, India, 2022, pp. 01-06, doi: 10.1109/ICETET-SIP-2254415.2022.9791586

[27] Mirjalili, S. (2019). Genetic algorithm. In S. Mirjalili (Ed.), Evolutionary algorithms and neural networks (pp. 43–55). Springer. https://doi.org/10.1007/978-3-319-93025-1_4

[28] Mehrotra, K., Mohan, C. K., and Ranka, S. (1992). Elements of artificial neural networks. MIT Press.

[29] Malik, M., Hussain, M., and Khan, A. (2021). Machine learning-based approaches for anomaly-based intrusion detection systems: A survey. Sensors, 21(22), 7554. https://doi.org/10.3390/s21227554

[30] Nassreddine, G., Nassereddine, M., & Al-Khatib, O. (2025). Ensemble Learning for Network Intrusion Detection Based on Correlation and Embedded Feature Selection Techniques. Computers, 14(3), 82. https://doi.org/10.3390/computers14030082

[31] Nazat, S., Alayed, W., Li, L., and Abdallah, M. (2025). Ensemble Learning Framework for Anomaly Detection in Autonomous Driving Systems. Sensors, 25(16), 5105. https://doi.org/10.3390/s25165105

[32] Nasir, R., Afzal, M., Latif, R., and Iqbal, W. (2021). Behavioral-based insider threat detection using deep learning. IEEE Access, 9, 143266–143274. https://doi.org/10.1109/ACCESS.2021.3118297

[33] Olusola, A., Ibrahim, M., and Yusuf, T. (2024). Phishing detection using deep learning and ensemble methods in social networks. Computers & Security, 132, 103365. https://doi.org/10.1016/j.cose.2024.103365

[34] Priyanka, S., and Kumar, A. (2021). Machine learning in cyberattacks: A study. Materials Today: Proceedings, 46, 11537–11542. https://doi.org/10.1016/j.matpr.2021.02.234

[35] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., and Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12, 2825–2830.

[36] Rahman, A., Pramono, R., and Supriadi, D. (2025). Anomaly-based detection of denial of service via deep learning memetic trained modular network. Journal of Fundamental and Applied Computer Science, 3(1), 1–11.

[37] Reynolds, R. G. (1994). An introduction to cultural algorithms. Proceedings of the Third Annual Conference on Evolutionary Programming, 131–139.

[38] Sahmoud, T., and Mikki, D. M. (2022). Spam detection using BERT. Frontiers in Social Sciences and Technology, 14(2), 23–35. https://doi.org/10.48550/arXiv.2206.02443

[39] Salama, M. A., Tawfeek, R. M., Hamdy, S., and Salim, O. M. (2025). Advances in ensemble machine learning for network intrusion detection

systems: A comprehensive review. Benha Journal of Engineering Science and Technology, 2(1), 117–125. https://bjest.journals.ekb.eg/article_445861_c46a865fa9e86bf0c9a3824cf647dd2e.pdf

[40] Shen, Y., Guo, D., and Chen, X. (2021). Balancing sensitivity and specificity in machine learning for clinical decision support. Artificial Intelligence in Medicine, 117, 102108.

[41] Tama, B.A. and Lim, S. (2021). Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. Computer science review. https://doi.org/10.1016/j.cosrev.2020.100357

[42] Tan, M. and Le, Q. V. (2019). EfficientNet: Rethinking model scaling for convolutional neural networks. arXiv preprint arXiv:1905.11946, May 2019.

[43] Volna E. (2009). Models for Modular Neural Networks: A Comparison Study. In Proceedings of the 5th International Workshop on Artificial Neural Networks and Intelligent Information Processing, pages 23-30. DOI: 10.5220/0002196700230030

[44] Xu, B., Wang, N., and Chen, T. (2015). Empirical evaluation of rectified activations in convolutional network. arXiv. https://doi.org/10.48550/arXiv.1505.00853

[45] Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., and Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. International Journal of Electrical and Computer Engineering, 13(2), 1922–1931. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

[46] Zheng, A., & Casari, A. (2018). Feature engineering for machine learning: Principles and techniques for data scientists. O'Reilly Media.

[47] Zhang, H., Xu, J., Li, L., and Wang, C. (2019). Deep learning-based network intrusion detection: A survey. IEEE Access, 7, 134360–134373. https://doi.org/10.1109/ACCESS.2019.2944225

[48] Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2019). Building an Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier. ArXiv. https://doi.org/10.1016/j.comnet.2020.107247

[49] Zhou, L., Wang, Y., and Li, J. (2024). Advancing DDoS attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling. arXiv preprint arXiv:2401.03116.