Dijlah Journal of Engineering Science (DJES) Vol. **3**, No. **2**, June, 2026, pp. 173-186
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 157

A Hybrid GNN-Transformer Framework for Enhanced Detection of Distributed Denial-of-Service (DDoS) Attacks in Network Traffic

Mustafa Azeez al-Mayyahi
Software department, college of Computer Science & Information Technology, Wasit University, Wasit, Iraq.

Article Info

Article history:

Received Feb.,9, 2026
Revised Mar.,5, 2026
Accepted Apr.,2, 2026

Keywords:

DDoS attack detection
Graph Neural Networks (GNN)
Transformer model
network security
graph data analysis

ABSTRACT

One of the most important threats of security in new networks refers to Distributed Denial-of-Service (DDoS) attacks, as their wide data amount and complexity make their diagnosis difficult. Present research offers multiple architecture given the Graph Neural Networks (GNNs) and Transformer models for DDoS attack diagnosis. Firstly, data of network is schemed as a graph, nodes and edges' attributes are extracted applying GNN. After that, model of Transformer is developed for analyzing temporal dependencies as well as extracting models associated with shared attacks. Such architecture leverages GNN to learn complicated structures of graph and Transformer to analyze long-term relations in temporal data. Outcomes of experiments on UNSW-NB15 dataset show that presented architecture excels in diagnosing DDoS attack decreasing attributes' amount when developing accuracy of diagnosis. Model obtains an F1 score of 98.3%, accuracy of 98.7%, a recall of 97.9% illustrating high ability for network intrusion detection systems (IDS) usage.

Corresponding Author:

Mustafa Azeez al-Mayyahi
Software department, college of Computer Science & Information Technology, Wasit University, Wasit, Iraq.
Email: mkhalaf@uowasit.edu.iq

1. INTRODUCTION

With quick network technologies development as well as developing dependence on organizations on digital frameworks, security of network became the basic issue in info technology domain. Everything is becoming simpler and more intelligent for using as we go in each device around us is joined to an internet [1]. Wide Internet of Thing (IoT) implementation and self-arrangement make it vulnerable to some attacks' kinds [2]. DDoS attacks are taken as one of the most usual and unsafe threats, as they ruin network resources' availability, leading to considerable ruin to crucial and businesses frameworks. Such attacks' quick and proper diagnosis is a concern which needs developed techniques to analyze big data amounts and complicated models' extraction from manner of network traffic [3]. Successful DDoS attack results are different and could be greatly detrimental. Companie might encounter substantial financial losses economically because of disruptions and prices related to incident reply and recovery of system. Also, DDoS attacks could perform as gateway to data breaches, potentially including sensitive info and exposing companies to considerable legal and regulatory liabilities. The main concern refers to ability for long-term reputational ruin; successful attacks could erode customer trust and ruin market condition of a company through bolding service reliability and security vulnerabilities [4]. Based on Arbor Networks, in the year 2022, 487% raise exists in HTTP/HTTPS DDoS attacks since 2019. In addition, DDoS attacks strength is developing daily. In the year 2017, strength of DDoS attack was 2.5 Tbps which surpass 3Tbps in year 2021 [5]. DDoS attacks are important for recognizing and mitigating because of broad attacking resources' share, huge created traffic volume, unpredictable manner. Traditional IDS techniques like ones based on rule/classical ML mechanisms, encounter some restrictions. Such restrictions contain inability for analyzing complicated relations among nodes of network, long-term temporal dependencies comprehension shortage, heavy preprocessing requirement for decreasing unrelated attributes [6]. Also, quick network data increase as well as active attacks' aspect develop systems demand able to control high scalability and recognizing complicated models. Such concerns become particularly important in DDoS attacks, that

include the two structural attributes (like network topology) as well as temporal ones (like traffic flow) [7]. In spite of broad attempts for increasing more developed techniques, present DDoS diagnosis patterns are not yet successful for efficiently analyzing the two network structure and temporal dependencies at the same time [8]. Such gap causes decreased accuracy of diagnosis, higher ratios of false positive, complicated and active areas' inefficiency. So, modelling complete and smart architecture which could consider the two natures in tandem is important.Traditional IDS techniques like methods based on rule/classical ML, normally do not outperform to their inability for analyzing complicated relations among nodes and comprehend temporal and structural network data dependencies. Here, integrating new methods like Transformer models [10] as well as Graph Neural Networks (GNNs) [9] shows new response for dealing with such restrictions. GNNs are able to analyze complicated structures of network and extracting rich attributes from data based on graph when models of Transformer, with their algorithms of attention, are adept at recognizing long-term dependencies and temporal relations with high accuracy. With each other, such schemes could analyze structural and temporal info at the same time, helping complicated attacks' diagnosis such as DDoS. Here, we present multiple architecture given the GNNs and Transformer models for effective and appropriate DDoS attacks diagnosis in network traffic. Such architecture leverages 2 complementary strategies for addressing concerns in diagnosing DDoS: GNNs, because of their capability to model complicated structures and relations between nodes, are especially appropriate to analyze data of network traffic in big and complicated networks. Through applying GNNs, data of network is designed as a graph, structural relations among data packs and nodes are extracted. Such strategy aids system recognizes spatial dependencies among various network traffic attributes. As DDoS attacks normally have particular temporal models, Transformer models, with their algorithms of attention could get long-term dependencies in temporal data. Transformer models excel at analyzing temporal dependencies and recognizing nonlinear and complicated models in streams of network traffic. These 2 models' integration lets system to analyze both network structure and temporal dependencies at the same time, considerably developing accuracy of DDoS attack diagnosis. Also, such integration decreases needed attributes' amount for diagnosis and develops models' effectiveness. Present study aim is modelling and performing network IDS applying GNN and Transformer integration for DDoS attack diagnosis.

The contributions and innovations of this study to the existing literature are as follows:

- GNN usage to model complicated Network Structures and Node Relations, Transformer for Temporal Dependency Analysis: simultaneous GNN app to design complicated network structures and relations among nodes, Transformer to analyze temporal attacks' dependencies, considers DDoS diagnosis from the two structural and temporal dimensions. Such integration, against a lot of present strategies that concentrate on only 1D, considerably develops accuracy of diagnosis.
- Efficient Feature Selection and Dimensionality Decrease Usage of GNN: One of present study's basic innovations refers to GNN usage to choose efficient attributes and decreasing input attributes' number with no diagnosis accuracy compromising. Present strategy decreases computational overhead also develops effectiveness of model, particularly while coping with high-dimensional data.
- Complicated Relations and Temporal Dependencies\ Simultaneous Analysis: through two intricate relations among nodes of network and temporal traffic dependencies analysis, model is able to recognize shared attacks with more complicated models which might be overlooked by traditional techniques. It causes false positive ratios decrease and actual attacks' accuracy development identification.

Following of present article is outlines as: Part 2 presents related study overview in ML app for diabetes diagnosis and prediction. Part 3 provides the main terminologies applied here that covers Autoencoder model that defines TabNet model. Part 4 details materials and techniques applied in presented strategy. Part 5 shows experimental analysis. At last, part 6 concludes the work with a summary of results and future directions.

2. Related Works

Different works offered new methods to diagnose and mitigate DDoS attacks over various fields, developing multiple models, techniques of DL, mechanisms of optimization. Priyadharshini and Balamurugan [11] offered multiple model to diagnose and avoid DDoS attacks in FANETs applying Deep Temporal Convolutional Networks (DTCN) and Long Short-Term Memory (LSTM) networks' integration. For optimizing hyperparameters, they defined Hybrid of Water Strider and Cuckoo Search (HWSCS) mechanism. The model developed Optimal Link State Routing (OLSR) for attacks' mitigation through routing traffic again. Their strategy obtained a recall of 93.87, performing better than traditional models and showing efficiency to guarantee safe communication of FANET. Fadaei Fouladi et al. [12] offered real-life DDoS diagnosis architecture combined in SDN controller. This strategy applies 2-stage Packet-In messages' analysis in the two fields of time and frequency. Basically, time-series is made through sampling Packet-In messages at particular intervals and comparing them to threshold. When threshold is exceeded, attributes are extracted from field of frequency and fed in ML mechanisms for attack diagnosis. Such technique obtained 99.85% accuracy, proving highly efficient to protect areas of SDN from DDoS attacks.

Bocu and Iavich [13] offered the developed diagnosis model of LRDDoS leveraging asynchronous federated learning strategy. Model was performed and assessed applying real-life corporate data traffic from Romanian IT organization controlling several branches. Experimental outcomes illustrated greater performance in comparison with present strategies, obtaining greater accuracy and developed metrics. Also, model efficiently decreased load of network, reducing LRDDoS attack models' possibility. Ramprasath et al. [14] offered the method to diagnose and mitigate DDoS and DoS attacks in SDN. Incoming traffic is analyzed through northbound app that extracts traffic header attributes applying grouping and anomaly traffic rate-fixing methods. SDN POX controller mitigates attacks through enabling DACL policies on OVSs. Presented technique showed greater performance in comparison with SVM and CkNN, obtaining 94% accuracy for DDoS diagnosis and 92% for DoS on the two synthetic and NSL-KDD sets of data, with decreased ratios of false positive. The strategy decreased gaps of resource, proposing valid solution for areas of SDN. Fan et al. [15] presented large shared architecture based on data, IDAD, to diagnose DDoS attacks in big-scale, multi-modal networks. Architecture includes 3 basic elements: classification, detection and preprocessing of data. The considerable contribution is IDTT and LDD mechanisms that combine TT decomposition with shared calculation for developing computational effectiveness and decrease capacity needs. Experimental outcomes confirmed efficiency of architecture in case of accuracy of share and diagnosis. Aljohani and Almutairi [16] presented mathematical model for simulating wide DDoS attacks on Electric Vehicle Charging Stations (EVCS) applying time-variant Poisson process for showing bot attack manners and their cumulative effect. The model uses Ornstein-Uhlenbeck process for getting temporal dynamics and attacks' traceability when queueing theory is used for analyzing traffic dynamics, such as delays and service interruptions under DDoS conditions. This paper investigates such attacks' impacts on active and steady-state grid functions. Simulation outcomes bold considerable ruins made by successful attacks, focusing on significance for strong cybersecurity scales for EVCS infrastructure protection. Xie et al. [17] defined MRFM, the technique for timely DDoS diagnosis applying multidimensional reconstruction and task mapping. This strategy gets network traffic data applying queue algorithm in predefined timeframe. The particular multidimensional reconstruction neural network after that sets loss function for rebuilding quantitative attributes, calculates errors of reconstruction, converts vectors in attributes of mapping. It develops intra-group similarity and inter-group disparity between data of traffic. Also, frequency info is extracted from qualitative attribute matrix applying info entropy to enrich traffic attributes. Experimental outcomes on benchmark sets of data show that MRFM efficiently diagnoses different kinds of DDoS attack, performing better than present techniques with an average development of up to 9.61% in metrics of performance.Yoon and Kim [18] offered new DL model applying Divide and Conquer Attention (DCA) algorithm for effective diagnosis of DDoS attack in virtual SDN areas. Model considers crucial DDoS attacks concern in SDN, that controller failures could incapacitate whole network. Though leveraging algorithm of DCA, model learns complicated models of attack as well as traffic of network, focusing on different traffic attributes' significance for developing accuracy of diagnosis. Experimental outcomes from virtual SDN setup applying ONOS and Mininet show that model based on DCA performs better than traditional ML as well as other DL techniques. In addition, this work compares performance of model with current strategies based on DL, bolding the benefits to efficiently diagnose various techniques of DDoS attack.Dash et al. [19] performed research on DDoS attack diagnosis applying NSL-KDD dataset, concentrating on preprocessing methods' significance. 2 strategies were offered: one incorporating Principal Component Analysis (PCA) and the other with no PCA. Powerful scaling and encoding methods were used in preprocessing. Experimental outcomes bolded PCA essential role to develop diagnosis accuracy. RF classifier obtained the highest accuracy (99.87%), pursued by KNN (99.14%), when Naïve Bayes showed comparatively lower accuracy (87.14%). Present study underscores developed preprocessing techniques' value in developing security of IoT device in contrary to DDoS attacks and contributes to strong IDS enhancement. Sakr et al. [20] investigated different supervised ML mechanisms' efficiency to diagnose DDoS attacks aiming systems of energy harvesting (EH) through IoT devices. This work used datasets of CICDDOS2019 and KDD-CUP for assessing classifiers like Decision Tree (DT), K-Nearest Neighbors (KNN), RF, Gradient Boosting, Support Vector Machine (SVM). Gradient Boosting appeared as the most efficient scheme, specifically for CICDDOS2019 dataset, illustrating greater accuracy and predictive abilities. Also, multiple models integrating Gradient Boosting with SVM/DT showed robust, still criteria, recall, precision. Present study bolds significance of choosing and tailoring ML schemes to particular security issues, presenting worthy perspectives to develop EH systems' as well as IoT devices dependence in contrary to important DDoS threats. Qian and Cai [21] defined diagnosis of DDoS attack and defense model leveraging the developed mechanism of K-means clustering, particularly tailored for SDN. Presented strategy applies developed mechanism for analyzing network traffic share, making DDoS attacks recognition able given the metrics of traffic rate. Outcomes showed greater efficiency of diagnosis as well as developed presented technique time complexity in comparison with other K-means variations. Also, the basic traffic observing model applying sFlow was performed, efficiently decreasing unimportant computational overhead and use of source. Present

research bolds light and efficient strategy to develop SDN dependence in contrary to DDoS attacks. Rao et al. [22] offered new strategy, DDoSNet, to diagnose and predict DDoS attacks in IoT network areas applying real multidimensional set of data. methods starts with strong data preprocessing step that data cleaning, missing values controlling, transformation in analyzable format are carried out. Feature selection is obtained applying African Buffalo Optimization with Decision Tree (ABO-DT), metaheuristic mechanism inspired by African buffalo manner that recognizes main attributes for distinguishing among usual/unusual traffic of network. Chosen features are accordingly processed by Echo-State Network (ESN) classifier, a kind of recurrent neural network (RNN) modeled for efficiently controlling time-series data. This classifier learns temporal network traffic models and dynamics, making appropriate DDoS attack diagnosis able. Hossain et al. [23] provided multiple strategy of feature selection integrated with classifiers based on ensemble to diagnose DDoS attacks. Technique applies correlation analysis, mutual info, PCA for feature selection also develops RF as basic classifier. Several datasets assessment on illustrated near-perfect performance, obtaining 100% true positive rate, 0% error rate, 100% accuracy surpassing present methods in basic metrics such as F1-score, precision, recall. Alotaibi et al. [24] provides a network intrusion detection system (IDS) model that uses a hybridization of bio-inspired metaheuristic algorithms to effectively detect generic attacks. The model has two key goals. The initial goal is to streamline the feature selection process for Network IDS by combining the Grey Wolf Optimization Algorithm and the Quantum Binary Bat Algorithm into a single framework. The second goal is to use machine learning classifiers to identify generic attacks and assess the efficiency of the chosen features. To do this, the model employs Naive Bayes, K-Nearest Neighbor (KNN), and Random Forest (RF) classifiers, resulting in robust performance and optimal feature assessment. Al-Omar and Trabelsi [25] proposes using AI and deep learning (DL) models to increase the efficiency and accuracy of intrusion detection. We offer an IDS that uses an attention-based Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) models. The attention mechanism improves the model's capacity to identify significant aspects in network traffic data, resulting in more precise and trustworthy predictions. Das et al. [26] proposes a technique for identifying DDoS attacks that employs an ensemble-based machine learning approach that combines supervised and unsupervised frameworks. The suggested combination outperforms other methods by using supervised ensembles to detect known DDoS assaults and unsupervised ensembles to identify zero-day DDoS attacks. The unsupervised ensemble uses novelty and outlier detection approaches, which make it particularly good at detecting previously unknown threats, increasing the system's robustness and adaptability.

Table 1 Summary of existing works

References	**Approaches**	**Objective**	**Methods/Algorithms**	**Limitations**
Priyadharshini and Balamurugan [11]	Hybrid DDoS Detection in FANETs	To detect and prevent DDoS attacks in FANETs.	Deep Temporal Convolutional Networks (DTCN), Long Short-Term Memory (LSTM), Hybrid of Water Strider and Cuckoo Search (HWSCS), Optimal Link State Routing (OLSR)	High computational cost due to the combination of multiple models and optimization algorithms.
Fadaei Fouladi et al. [12]	Real-time DDoS Detection in SDN	To provide real-time detection of DDoS attacks in SDN environments.	Two-step analysis of Packet-In messages, time-series analysis, feature extraction, machine learning classifiers	Limited scalability for larger, complex network environments.
Bocu and Iavich [13]	LRDDoS Detection using Federated Learning	To enhance the detection of LRDDoS attacks using federated learning.	Asynchronous Federated Learning, real-time corporate data analysis	Dependent on the availability of real-time data, which may not always be accessible.
Ramprasath et al. [14]	DDoS/DoS Detection and Mitigation in SDN	To detect and mitigate DDoS and DoS attacks in SDN networks.	Northbound application for traffic analysis, SDN POX controller, DACL policies	Limited to DDoS/DoS attacks and may not generalize to other attack types.

Fan et al. [15]	Big Data-Driven DDoS Detection	To detect DDoS attacks in large-scale, multi-modal networks.	Data preprocessing, data denoising, data classification, IDTT and LDD algorithms	Requires large-scale infrastructure for distributed computing, not feasible in all environments.
Aljohani and Almutairi [16]	DDoS Attack Simulation on EVCS	To simulate and analyze the impact of DDoS attacks on Electric Vehicle Charging Stations.	Time-variant Poisson process, Ornstein-Uhlenbeck process, queueing theory	Focused on specific attack scenarios, limiting general application.
Xie et al. [17]	Multidimensional Reconstruction for DDoS Detection	To provide timely detection of DDoS attacks using multidimensional reconstruction.	Queue mechanism, multidimensional reconstruction neural network, frequency-based feature extraction	Complex feature extraction may cause delays in real-time detection.
Yoon and Kim [18]	DDoS Detection with Divide and Conquer Attention	To efficiently detect DDoS attacks in virtual SDN environments.	Divide and Conquer Attention (DCA) mechanism, deep learning model	Requires substantial training data for effective performance.
Dash et al. [19]	DDoS Detection with PCA-based Preprocessing	To improve DDoS attack detection accuracy using PCA-based	Principal Component Analysis (PCA), Random Forest classifier	PCA may not capture all intricate features of network traffic, affecting accuracy.
Sakr et al. [20]	DDoS Detection in EH Systems via IoT	To detect DDoS attacks targeting energy harvesting systems via IoT.	Decision Tree (DT), Gradient Boosting, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forest	Hybrid models may have variable precision and recall across different datasets.
Qian and Cai [21]	K-means Clustering for DDoS Detection in SDN	To detect DDoS attacks in SDN using improved K-means clustering.	Improved K-means clustering, sFlow-based traffic monitoring	Limited to SDN environments and may not be applicable to traditional network structures.
Rao et al. [22]	DDoS Detection in IoT Environments	To detect and predict DDoS attacks in IoT networks.	African Buffalo Optimization with Decision Tree (ABO-DT), Echo-State Network (ESN) classifier	Effectiveness may vary across different IoT environments and datasets.
Hossain et al. [23]	Hybrid Feature Selection with Ensemble Classifiers for DDoS Detection	To detect DDoS attacks using hybrid feature selection and ensemble-based classifiers.	Correlation analysis, mutual information, PCA, Random Forest classifier	The complexity of the method may hinder real-time application in large-scale networks.
Alotaibi et al. [24]	Hybrid Bio-Inspired IDS	Develop a hybrid bio-inspired IDS to detect generic attacks and optimize feature selection for	Grey Wolf Optimization Algorithm, Quantum Binary Bat Algorithm, Naive	May not be suitable for complex attacks or dynamic environments requiring real-time

		Network IDS.	Bayes, KNN, RF	updates.
Al-Omar and Trabelsi [25]	AI and DL-Based IDS	Increase efficiency and accuracy in intrusion detection by leveraging AI and DL models to focus on significant features in network traffic data.	Attention-based CNN, LSTM	High computational complexity, potential issues with scalability for large datasets.
Das et al. [26]	Ensemble-Based IDS	Detect DDoS attacks using an ensemble-based approach combining supervised and unsupervised methods, including zero-day attack detection.	Supervised ensemble, unsupervised ensemble (novelty and outlier detection)	Limited generalizability to other attack types, reliance on ensemble selection strategies.

Table 1 briefs different strategies offered for DDoS attack diagnosis, every of them proposing united techniques and mechanisms tailored to particular network areas such as systems of IoT, SDNs, FANETs. When such techniques show robust performance, they are sometimes restricted by agents like scalability issues, high computational complexity, reliance on real-life data. Furthermore, a lot of techniques are tailored to particular kinds of attack/ areas of network that decreases their practicality in wider situations. In spite of such restrictions, reviewed strategies bold continuous attempts for developing DDoS diagnosis applying ML integration, feature selection methods, mechanisms of optimization. Our strategy creates such present schemes considering scalability restrictions, real-life processing, flexibility in areas of network. We target at making a more adaptable response which not only develops diagnosis accuracy but also guarantees effectiveness in big-scale and active adjustments of network. Through integrating developed feature selection and mechanisms of optimization, we consider high computational prices and particular infrastructure demand issues. Such direction was selected for bridging gap among highly particular strategies as well as requirement for a more generalized and scalable DDoS diagnosis system, able to be developed in various areas while keeping high performance.

3. Terminologies

Graph Attention Networks

Graph attention networks (GATs) [27] consider the important theoretical progression from graph convolutional networks (GCNs). At center of GATs is a rule which actual nodes are more critical than others. This opinion, when not entirely new and somewhat reflected in GCNs, is developed in GATs. In GCNs, nodes with less neighbors are more significant because of normalization coefficient which basically relies on rate of node. Although, GCN strategy restriction is the only reliance on node rate to assign significance of node. Against, GATs target at making weighting agents which not only address rates of a node but also node attributes' importance. It is where GATs diverge from GCNs: the determining scale agents' technique in neighborhood info aggregation. GCNs apply non-parametric scaling agent obtained from task of normalization, where GATs develop algorithm of attention for assigning agents of scaling. The strategy based on attention lets GATs to determine better weights to more essential nodes in neighborhood aggregation. Such main difference ensures GATs a greater control rate over the way info flows in intricate graph structures, making them more adaptable to control complicated data. In another word, generally GCNs are more efficient in scenarios where structure of graph is explicitly described, every node importance is more/less unique. For understanding this functionality, attention layer of graph in GATs carries out some functions on graph-structured data. Basically, every node undergoes the linked linear transformation via weight parameter matrix W, adjusting step for later analysis as well as processing. Pursuing basic transformation in GATs, process goes on with attention coefficients calculation. Such coefficients show non-normalized attention weights computed pairwise among nodes of neighbor. Here, 2 adjacent nodes' z embeddings are concatenated, shaping the integrated vector. Such concatenated vector is subjected to a dot product function with learnable weight vector, efficiently combining attributes of node in algorithm of attention. Accordingly, for defining nonlinearity in model, LeakyReLU activation task is used to this dot product operation outcome. The next stage includes normalizing attention coefficients for keeping consistency over whole nodes. It is obtained via softmax task app, guaranteeing that coefficients are comparable and scaled properly.

In step of aggregation, model integrates embeddings from different neighbors, guided by computed attention weights. Although, the basic consideration in GATs refers to potential self-attention instability. For considering it, multi-head attention term is developed. The strategy includes making hybrid attention algorithms/ 'heads,' every of them with different parameters. Such hybrid heads act in parallel, developing storage and stability of model. Every head calculates its own output, that is accordingly combined for shaping the last outcome. Normally, such heads' outcomes are concatenated in intermediate network layers when averaging is applied in the last layer for consolidating info gleaned from various insights. In GATs, attentional weights are unclearly assigned through comparing inputs to every another (a process called self-attention) as could be seen in Fig. 1. The above mathematical association concerning the vector nodes' representations' calculation is converted as:

$$h_i = \sum_{j \in N_i} a_{ij} W_{xj} \quad (1)$$

That a_{ij} are weights of attention actively computed by network.

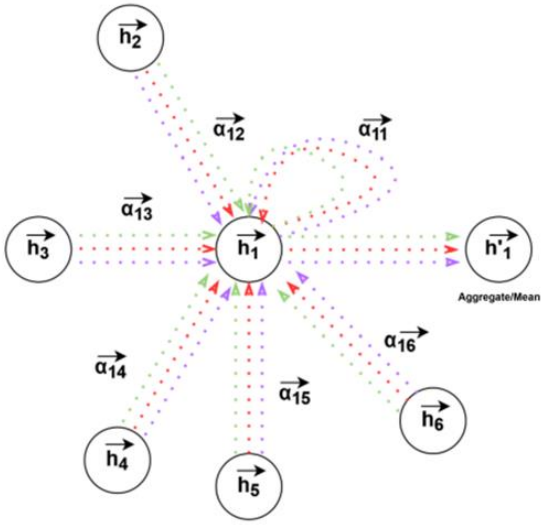

Fig. 1. multi-head attention algorithm demonstration with 3 attention heads. Every arrow is color-coded for showing independent attention weights' computations. Aggregated attributes from every head are accordingly merged/averaged for creating the last node vector representation [27].

Vanilla Transformer

Vanilla Transformer [28] is a model which is sequence-to-sequence containing a decoder and encoder, each is a stack of L identical blocks. Each block of encoder is fundamentally included a position-wise feed-forward network (FFN) as well as multi-head self-attention module. Residual connection is extended around each module in order to make a deeper model, followed by the module of Layer Normalization. Compared to blocks of encoder also the ones of decoder insert cross-attention modules in multi-head modules of self-attention as well as the condition wise FFNs. In addition, modules of self-attention are considered to prevent each situation from taking part in the considered regions. Figure 2 shows the whole framework of vanilla Transformer.

In subsection bellow, we could define main vanilla Transformer modules.

Attention modules Transformer adopts algorithm of attention with Query–Key–Value (QKV) model. Based on packed matrix representations of queries $\mathbf{Q} \in \mathrm{R}N\times$, keys $\mathbf{K} \in \mathrm{R}M\times D_k$, values $\mathbf{V} \in \mathrm{R}M\times Dv$, measured dot-product attention applied by Transformer is provided by:

$$Attention(Q.K.V) = \left(\frac{QK^T}{\sqrt{D_k}}\right)V = AV \quad (2)$$

N and M present lengths/values of queries and keys; Dk and Dv present dimensions queries of keys, values; $\mathbf{A}$ = softmax ($\mathbf{QK}^{\mathrm{T}}/\sqrt{D_k}$) is often called matrix of attention; softmax is applied in a row-wise treat. Dot-products of queries and keys are distributed by $\sqrt{Dk}$ to alleviate the function concern of gradient vanishing softmax. Transformer uses multi-head attention instead of basically applying single attention task where Dm-dimensional

main values, keys and queries are projected n Dk, Dk, Dv dimensions, respectively, with H different learned sets of projections. For each projected values, keys and queries, the result is computed considering Eq. (2). The scheme concatenates entire outcomes and projects them back to a representation which is Dm-dimensional.

MultiHeadAttn(**Q**, **K**, **V**) = Concat(head1 , …, head$H$)**W**O (3)

Where headi=Attention(QW_i^Q.KW_i^K.VW_i^V). (4)

In Transformer, 3 attention kinds in queries and key–value pairs' terms source:\

• Self-attention. We set **Q** = **K** = **V** = **X** in Eq. (3) in Transformer encoder where **X** refers to the final outputs of a layer.

• Masked Self-attention. Self-attention is restricted in Transformer decoder, therefore, condition's queries can only take part in entire key–value pairs up to also including the situation. To enable parallel training, this is basically carried out applying mask function task for unnormalized attention matrix $\hat{A}$ = exp($\mathbf{QK}^{\top}/\sqrt{D_k}$) which the non-legal situations are masked out setting $\hat{A}_{ij} = -\infty$ if $i < j$. Such kind of self-attention is often called as normal/autoregressive consideration.

• Cross-attention. Queries are projected from the final output (decoder) layer where values and keys are projected using outputs of encoder.

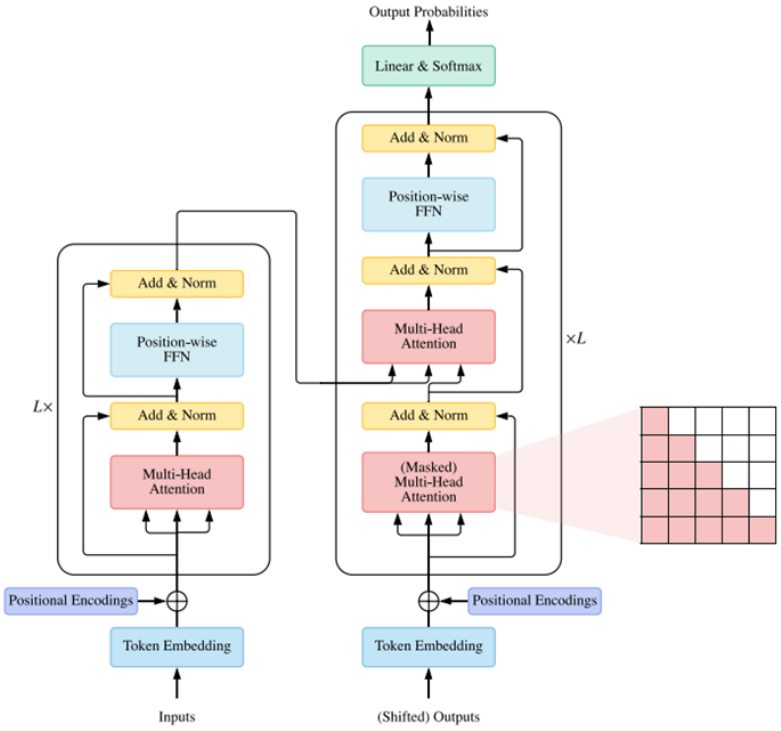

Figure 2. Vanilla transformer framework overview [28].

4. Proposed method

Present study provides new multiple architecture integrating GNNs and Transformer models for DDoS attack diagnosis. Architecture starts by showing network traffic data as a graph, that nodes and edges are related to main features extracted via GNNs. It lets model to get complicated relations and structures inherent in network traffic. Then, Transformer model is applied for analyzing temporal dependencies in data, learning long-term models which are important to recognize DDoS attacks. Through combining such 2 robust schemes, presented architecture leverages GNN's capability for controlling complicated data based on graph and Transformer's strength to model time-dependent and sequential models. The multiple strategy considerably develops DDoS attacks' diagnosis accuracy when at the same time decreasing attributes' number needed for function of classification, developing the two efficiency and effectiveness.Here is the presented technique detailed definition to choose DDoS attacks applying integration of Graph Attention Network (GAT) and Vanilla Transformer, with concentration on analyzing structural and temporal attacks' dependencies at the same time:

Steps of the Proposed Method:

1. Dataset description

Dataset of UNSW-NB15 [29] was created via IXIA Perfect Storm software. Tcpdump which is a mean, could get 100 GB of network data which is not processed in the format of pcap file. Test of packs is made facilitated through each pcap file being 1000 MB in size. To make 49 attributes with class tag, 12 paths were performed using the techniques of Argus and Bro-IDS. this set of data contains two components: training and testing set. Training set contains 175,341 records classified as usual ones, although, testing set contains 82,332 records identified as attacks. Dataset of UNSW-NB15 encompasses 9 specific sets of attacks: reconnaissance, analysis, exploits, fuzzers, denial of service, backdoor, worms, shellcode, generic. Among these attacks, the highest records' number was given to the general set, with 18,871 in testing set and 40,000 in training one. Features in UNSWNB15 dataset were shown in Table 2.

Table 2 UNSW-NB15 dataset features list.

Feature No.	Feature Name	Feature No.	Feature Name
1	id	24	dwin
2	dur	25	tcrptt
3	proto	26	svnack
4	service	27	ackdat
5	state	28	smean
6	spkts	29	amean
7	dpkts	30	trans depth
8	spktes	31	response body len
9	dpktes	32	ct sry src
10	rate	33	ct-state_ttl
11	sttl	34	ct dst ltm
12	dttl	35	ct src dport ltm
13	sload	36	ct src sport ltm
14	dload	37	ct dst src ltm
15	sloss	38	is ftp loain
16	dloss	39	Ct ftp cmd
17	sinpkt	40	ct flw http method
18	dinpkt	41	ct src ltm
19	siit	42	ct srv st
20	diit	43	is sm ips ports
21	swin	44	attack cat
22	stcpb	45	label
23	dtcpd		

2. Data Preprocessing

- Controlling Missing Data: Basically, UNSW-NB15 dataset must be cleaned from any missing/incomplete data. it could be performed through methods like imputing missing values with mean/median/eliminating incomplete records.
- Feature Extraction: Attributes which are essential to diagnose attacks demand for being recognized and extracted. Such attributes contain info associated with network structure, time, protocols, traffic models.
- Feature Normalization: For developing model's performance, whole attributes must be normalized. It could be performed applying methods like min-max scaling (e.g., [0, 1]/Z-score normalization.
- Graph Construction: Data should be designed as a graph that every node shows sample of data (like traffic flows/packs), edges show relations among them. Present stage is critical to use GNNs.

3. Network Structure Modeling with GAT

For processing network's structural data, GAT is applied where every node actively gathers info from neighboring nodes, with every neighbor assigned significance via algorithms of attention. GAT is well-suited for complicated networks with different attributes. Algorithm of attention in GAT is applied for weighting relations among nodes [30]. It aids model to recognize which nodes are more essential for diagnosing an attack. After processing the graph, structural attributes (like kinds of edge and node relations) are extracted that could be helpful to diagnose DDoS attacks.

4. Modeling Temporal Dependencies with Transformer

After extracting structural features applying GAT, such attributes are fed into Vanilla Transformer model. Transformer model is applied for processing temporal dependencies in data, especially to analyze network traffic orders. Here, temporal orders associated with flow of network traffic and their attributes are fed into model for getting long-term dependencies and complicated models in traffic data. Transformer applies Self-Attention algorithm for analyzing temporal dependencies and diagnosing intricate models in network traffic. Such algorithm lets model to concentrate on the most essential temporal relations in data.

5. Combining GAT and Transformer

Here, GAT model outcomes that include structural attributes, are presented as input to Transformer. The integration lets model to analyze the two structural and temporal dependencies at the same time. Here, the two models work in parallel, with GAT concentrating on extracting structural features, Transformer processing such attributes to design temporal dependencies. This interaction makes model able to control both attack detection process natures effectively.

6. Classification and DDoS Attack Detection

The integrated GAT and Transformer models' outcome is transferred to a classifier (like RF) for assigning if data shows DDoS attack/not.

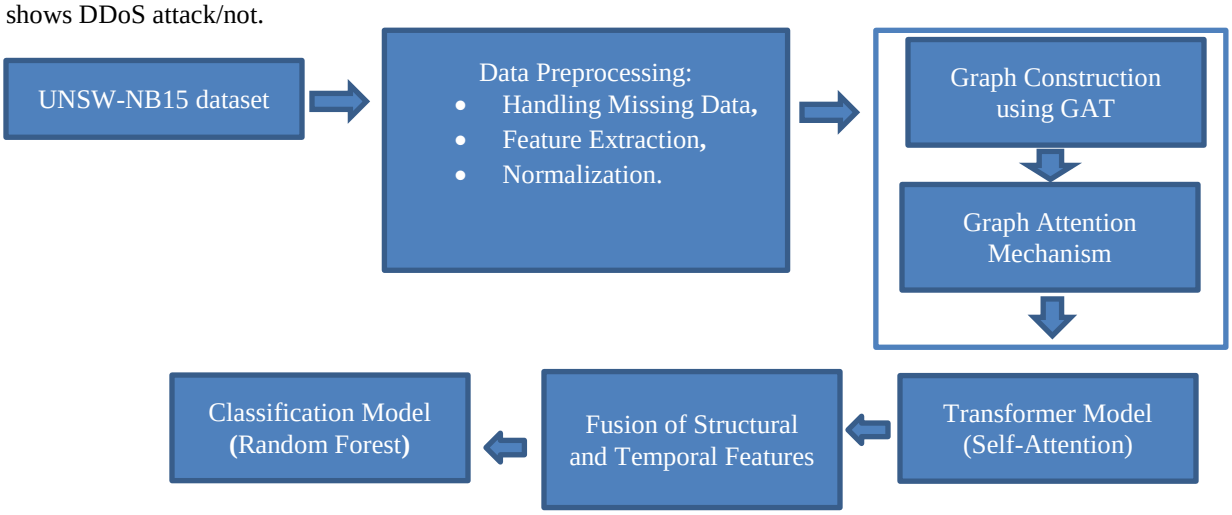

Figure 3. Diagram of proposed method

5. Experimental analysis

The presented multiple GAT-Transformer model experimental analysis concentrates on assessing the performance in diagnosing DDoS attacks applying UNSW-NB15 dataset. Basic analysis aims are evaluating F1-score, precision, accuracy, sensitivity, recall of model compared with present techniques and assign integrated strategy effectiveness.

5.1. Evaluation metrics

Metrics of evaluation are applied for evaluating model performance. In presented DDoS attack diagnosis model case, evaluation metrics applied contain The AUC (Area Under the Curve), accuracy, recall, precision, f1-score, error rate, false positive rate (FPR), test accuracy, true positive rate (TPR), cohen's kappa, Balanced Accuracy (BACC), training accuracy, so on. Such metrics present general model's performance insight and could aid the usefulness in diagnosing DDoS attacks with high accuracy and low FPRs. Matrix of confusion shows correct and incorrect pre dictions number made by model, in comparison with certain outputs (true tags) in test data. typically, table is a square matrix, which rows show certain class tags, columns show predicted class tags. 4 outputs which are feasible in binary classification issue are false positives (FP), false negatives (FN), true positives (TP), true negatives (TN).

• TP: The positive class is properly predicted by the model.
• FP: The positive class is wrongly predicted by the model.
• TN: The negative class is properly predicted by the model.
• FN: The negative class is wrongly predicted by the model.

Applying values in matrix of confusion, we could calculate some metrics of evaluation outlined in Table 3. Other metrics with appropriate eqs. are outlined. This is feasible for assessing power and reliability of model to recognize DDoS attacks in different conditions and environmental agents applying metrics of evaluation.

Table 3 Formulas of measurement metrics for performance

Metrics	**Formulas**
Accuracy	(TP+TN)/(TP+FP+FN+TN)
Recall	TP/(FN+TP)
Precision	TP/(FP+TP)
F1-score	2*(recall*precision)/(recall+precision)
FPR	FP/(TN+FP)

5.2. Results and discussion

Here, different parameter adjustments as well as the applied software are depicted which were used for simulation. Different outcomes achieved after the feature selection individually applying Nature-Inspired mechanisms also their hybrid model is documented. The features' optimality has been evaluated applying different classifiers of ML scales of performance.

5.2.1. Parameter setting

An open-source Python package known as Anaconda, was applied for performing the test. Entire testing was done on such particular system that includes the configuration as 3.30 GHz Intel Core i7, 6th generation, Windows 10 Version 1903, 12 GB DDR4 RAM at 2401 MHz. Table 4 shows the specifications of parameter for the simulation.

Table 4 Simulation Parameters.

Parameters	**Value**
Dataset	UNSW-NB15
Test split	0.2
Train split	0.8
Input channels	Equal to the number of input features
Output channels	16
Number of heads (Attention)	1
Input dimension	16
Number of attention heads	2
Hidden dimension	32

5.2.2. Results

Receiver-operating characteristic (ROC) curve is known as the visual tool to compare different approaches' efficacy. Figure 4 shows the proposed integrated kernel, standard kernel ROC curves, the upgraded kernel. The region below ROC curve illustrates that the offered combined kernel performs better than other kernels. Table 5 shows the comparison of the newest methods and our offered combined kernel to DDoS attacks detection from the dataset of UNSW-NB15. Our offered combined kernel performs more appropriately than other ML strategies illustrated in Table 5 to predict DDoS attacks. We are not subject to the similar limitation due to that we have not removed the lost values from the basic data like the others in such domain have carried out for their research that are shown in this table as well.

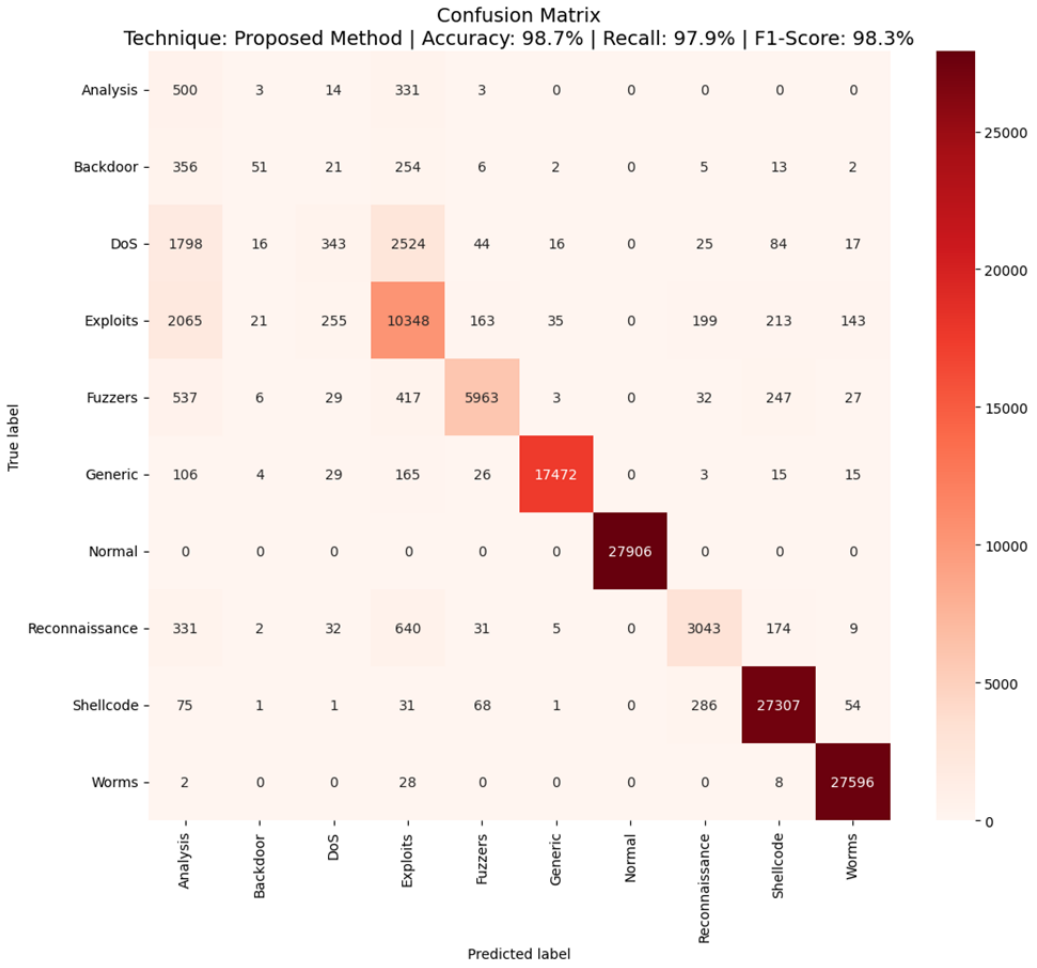

Figure 4. Accuracy, Sensitivity and F1-Score by proposed method.

Table 5. Comparison classification of the proposed model with other models on the UNSW-NB15 dataset.

Technique	Accuracy	Precision	Recall	F1-score
[18]	96.35%	-	-	-
[24]	98.5%	-	96.7%	99.4%
[25]	92.2%	95.04%	90.56%	92.72%
[26]	92.5%	85.1%	94.5%	97.8%
Proposed method	98.7	98.3	97.9%	89.6%

The following analysis compares various intrusion detection systems in terms of accuracy, precision, recall, and F1-score. The first strategy, referred to as [18], has an accuracy of 96.35% but lacks information on other performance measures such as precision, recall, and F1-score, making it difficult to completely judge its usefulness. The approach in [24] performs well, with an accuracy of 98.5% and a recall of 96.7%, demonstrating that it is effective at recognizing real positive instances. Its F1-score of 99.4% demonstrates a well-balanced trade-off between precision and recall, highlighting its excellent performance in detecting tasks. However, precision is not reported, raising questions about its potential to reduce false positives .In [25], the model scores 92.2% accuracy, 95.04% precision, and 90.56% recall, for an F1-score of 92.72%. This approach has a high precision but a somewhat lower recall, implying that it is better at preventing false positives but may overlook some actual positive situations.

The technique described in [26] has a recall of 94.5% and a significantly high F1-score of 97.8%, indicating balanced and effective performance. However, its accuracy is significantly lower (92.5%), and its precision is

85.1%, indicating a higher percentage of false positives than the other approaches.The proposed method exceeds the bulk of previous strategies in both accuracy (98.7%) and precision (98.3%), demonstrating its superior ability to correctly identify actual positive situations while minimizing false positives. It also has a high recall rate of 97.9%, showing great detecting capabilities. However, its F1-score of 89.6%, while competitive, is slightly lower than [24] and [26], indicating opportunity for improvement in balancing precision and recall. The proposed method has the highest accuracy and precision of all approaches while keeping a high recall. This makes it highly effective in intrusion detection; nevertheless, more optimization could raise the F1-score to meet its overall high performance. Figure 5 depicts the model's accuracy in relation to the number of epochs used. The two figures illustrate that the accuracy of both the training and validation data improves over time until it hits a plateau of 20.

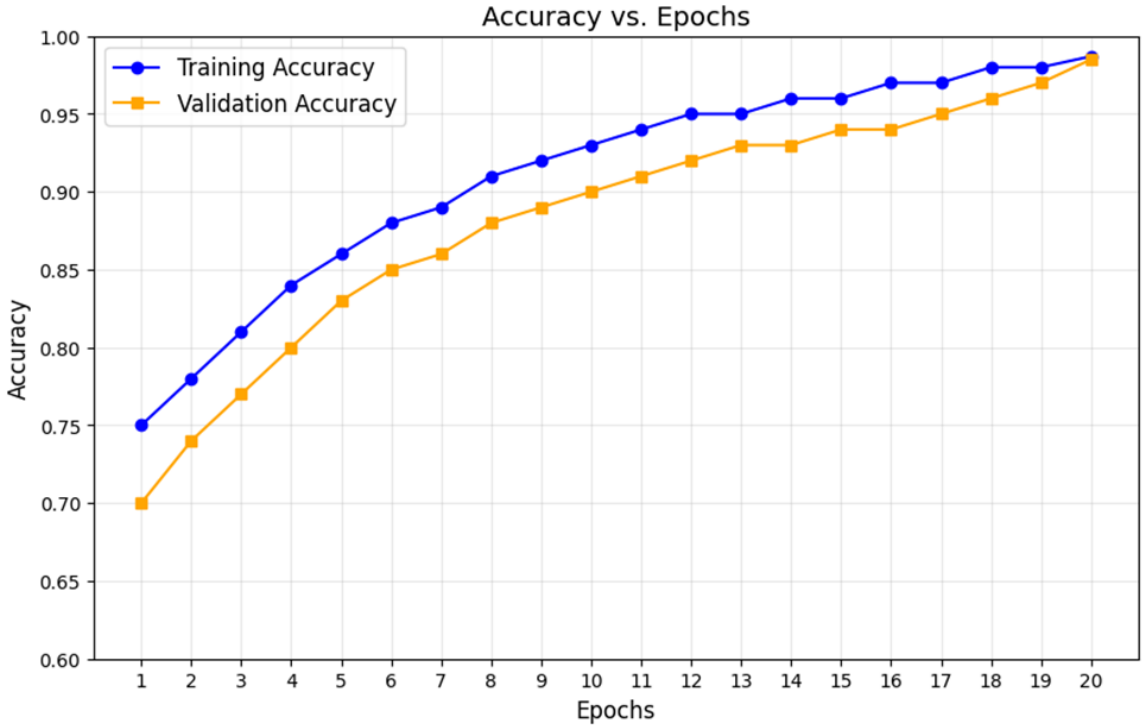

Figure 5. Epochs vs Accuracy

6. Conclusion

In this paper, offered hybrid model integrating GAT and Transformer networks for DDoS attack diagnosis shows considerable development in network security domain. By leveraging GAT strengths to capture complicated network structures and Transformer to comprehend temporal dependencies, model proposes strong solution to recognize DDoS attacks in real-life network traffic. Experimental outcomes on UNSW-NB15 dataset show that hybrid model performs better than traditional techniques in F1-score, accuracy, recall, precision terms presenting highly efficient strategy to diagnose complicated attack models. GAT usage lets model to concentrate on crucial relations of network, whereas Transformer develops the ability to diagnose temporal attack models, causing more appropriate and effective system of diagnosis. Also, needed features decreased number as well as developed computational efficiency make presented model measurable for practical development in active and big networks. In future work, model could be developed through combining additional methods based on graph/examining alternative temporal models. Also, real-life development and optimization in resource-limited areas will present deeper perspectives into model's functional practicality in IDSs. Totally, such hybrid strategy shows satisfactory direction to develop DDoS diagnosis and contributing to more safe areas of network.

REFERENCES

[1] H. Gebrye, Y. Wang, and F. Li, "Computer vision based distributed denial of service attack detection for resource-limited devices," *Comput. Electr. Eng.*, vol. 120, no. 109716, p. 109716, 2024.

[2] K. Sharma and S. K. Shivandu, "Integrating artificial intelligence and Internet of Things (IoT) for enhanced crop monitoring and management in precision agriculture," *Sens. Int.*, vol. 5, no. 100292, p. 100292, 2024.

[3] A. B. de Neira, B. Kantarci, and M. Nogueira, "Distributed denial of service attack prediction: Challenges, open issues and opportunities," *Comput. Netw.*, vol. 222, no. 109553, p. 109553, 2023.

[4] M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, and A. Abarda, "Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches," *Egypt. Inform. J.*, vol. 27, no. 100517, p. 100517, 2024.

[5] J. K. Chahal, A. Bhandari, and S. Behal, "DDoS attacks & defense mechanisms in SDN-enabled cloud: Taxonomy, review and research challenges," *Comput. Sci. Rev.*, vol. 53, no. 100644, p. 100644, 2024.

[6] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 13, no. 1, 2024.

[7] E. Owusu *et al.*, "Online network DoS/DDoS detection: Sampling, change point detection, and machine learning methods," *IEEE Commun. Surv. Tutor.*, vol. 27, no. 4, pp. 2543–2580, 2025.

[8] R. Gao, Z. Chen, X. Wu, Y. Yu, and L. Zhang, "Dynamic deep graph convolution with enhanced transformer networks for time series anomaly detection in IoT," *Cluster Comput.*, vol. 28, no. 1, 2025.

[9] G. Corso, H. Stark, S. Jegelka, T. Jaakkola, and R. Barzilay, "Graph neural networks," *Nat. Rev. Methods Primers*, vol. 4, no. 1, 2024.

[10] S. Madan, M. Lentzen, J. Brandt, D. Rueckert, M. Hofmann-Apitius, and H. Fröhlich, "Transformer models in biomedicine," *BMC Med. Inform. Decis. Mak.*, vol. 24, no. 1, p. 214, 2024.

[11] S. P. Priyadharshini and P. Balamurugan, "An efficient DDoS attack detection and prevention model using fusion heuristic enhancement of deep learning approach in FANET sector," *Appl. Soft Comput.*, vol. 167, no. 112438, p. 112438, 2024.

[12] R. F. Fouladi, L. Karaçay, U. Gülen, and E. U. Soykan, "A novel Distributed Denial of Service attack defense scheme for Software-Defined Networking using Packet-In message and frequency domain analysis," *Comput. Electr. Eng.*, vol. 120, no. 109827, p. 109827, 2024.

[13] R. Bocu and M. Iavich, "Enhanced detection of low-rate DDoS attack patterns using machine learning models," *J. Netw. Comput. Appl.*, vol. 227, no. 103903, p. 103903, 2024.

[14] J. Ramprasath, N. Krishnaraj, and V. Seethalakshmi, "Mitigation services on SDN for distributed denial of service and denial of service attacks using machine learning techniques," *IETE J. Res.*, vol. 70, no. 1, pp. 70–81, 2024.

[15] Q. Fan *et al.*, "IDAD: An improved tensor train based distributed DDoS attack detection framework and its application in complex networks," *Future Gener. Comput. Syst.*, vol. 162, no. 107471, p. 107471, 2025.

[16] T. Aljohani and A. Almutairi, "Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging Stations," *Ain Shams Eng. J.*, vol. 15, no. 7, p. 102860, 2024.

[17] L. Xie *et al.*, "MRFM: A timely detection method for DDoS attacks in IoT with multidimensional reconstruction and function mapping," *Comput. Stand. Interfaces*, vol. 89, no. 103829, p. 103829, 2024.

[18] N. Yoon and H. Kim, "Detecting DDoS based on attention mechanism for Software-Defined Networks," *J. Netw. Comput. Appl.*, vol. 230, no. 103928, p. 103928, 2024.

[19] S. K. Dash *et al.*, "Enhancing DDoS attack detection in IoT using PCA," *Egypt. Inform. J.*, vol. 25, no. 100450, p. 100450, 2024.

[20] H. A. Sakr, M. M. Fouda, A. F. Ashour, A. Abdelhafeez, M. I. El-Afifi, and M. Refaat Abdellah, "Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems," *Egypt. Inform. J.*, vol. 28, no. 100540, p. 100540, 2024.

[21] H. Qian and L. Cai, "Improved K-means-based solution for detecting DDoS attacks in SDN," *Phys. Commun.*, vol. 64, no. 102318, p. 102318, 2024.

[22] G. Srinivasa Rao, P. Santosh Kumar Patra, V. A. Narayana, A. Raji Reddy, G. N. V. Vibhav Reddy, and D. Eshwar, "DDoSNet: Detection and prediction of DDoS attacks from realistic multidimensional dataset in IoT network environment," *Egypt. Inform. J.*, vol. 27, no. 100526, p. 100526, 2024.

[23] M. A. Hossain and M. S. Islam, "Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity," *Measur. Sens.*, vol. 32, no. 101037, p. 101037, 2024.

[24] M. Alotaibi *et al.*, "Hybrid GWQBBA model for optimized classification of attacks in Intrusion Detection System," *Alex. Eng. J.*, vol. 116, pp. 9–19, 2025.

[25] B. Al-Omar and Z. Trabelsi, "Intrusion detection using attention-based CNN-LSTM model," in *IFIP Advances in Information and Communication Technology*, Cham: Springer Nature Switzerland, 2023, pp. 515–526.

[26] S. Das, M. Ashrafuzzaman, F. T. Sheldon, and S. Shiva, "Ensembling supervised and unsupervised machine learning algorithms for detecting distributed denial of service attacks," *Algorithms*, vol. 17, no. 3, p. 99, 2024.

[27] A. G. Vrahatis, K. Lazaros, and S. Kotsiantis, "Graph attention networks: A comprehensive review of methods and applications," *Future Internet*, vol. 16, no. 9, p. 318, 2024.

[28] K. Mao, X. Xiao, T. Xu, Y. Rong, J. Huang, and P. Zhao, "Molecular graph enhanced transformer for retrosynthesis prediction," *Neurocomputing*, vol. 457, pp. 193–202, 2021.

[29] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015.

[30] U. A. Bhatti *et al.*, "MFFCG – Multi feature fusion for hyperspectral image classification using graph attention network," *Expert Syst. Appl.*, vol. 229, no. 120496, p. 120496, 2023.