NEURAL NETWORK APPROACHES FOR DDOS ATTACK EFFECT ASSESSMENT: A SYSTEMATIC REVIEW

Pradeep Nayak, Aniketh, Anujna[3], Arya B Shetty[4], Chaithanya Shree D

[1] Assistant professor, Dept. of ISE, Alvas Institute of Engg. & Tech., Karnataka, India
[2] UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India
[3]UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India
[4]UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India
[5]UG Scholar, Dept. of ICB, Alvas Institute of Engg. & Tech., Karnataka, India

Emails:
pradeep@aiet.org.in¹, anikethshettigar005@gmail.com², anujnasr180@gmail.com³,
aryashetty00002356@gmail.com⁴, chaiishree@gmail.com⁵

ABSTRACT

Distributed Denial of Service (DDoS) attacks represent one of the most critical and persistent threats to modern network infrastructure, targeting essential services and critical systems worldwide. Traditional DDoS attack effect evaluation methods rely heavily on statistical approaches that suffer from limitations including data redundancy, inability to capture complex feature correlations, and dependence on manual parameter tuning. These shortcomings significantly impact the accuracy and reliability of attack assessment, hindering effective defense strategy deployment. This systematic review examines the evolution from traditional evaluation techniques to neural network-based approaches for DDoS attack effect assessment. We comprehensively analyze univariate and multivariate evaluation methods including Index Evaluation Method (IEM), Weighted Sum Method (WSM), Analytic Hierarchy Process (AHP), Grey Relational Analysis (GRA), and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), identifying their inherent limitations in handling modern attack patterns. The review then explores deep learning architectures including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, attention mechanisms, and hybrid models that have emerged as promising solutions. Through comparative analysis of recent studies utilizing datasets such as KDD99, NSL-KDD2009, CIC-IDS2017, CIC-IDS2018, and CIC-DDoS2019, we demonstrate that neural network approaches achieve significantly higher accuracy rates, with state-of-the-art methods reaching up to 99.84% detection accuracy compared to traditional methods averaging below 75%. Feature selection techniques including distance entropy-based Triplet networks, Principal Component Analysis (PCA), and information gain methods are critically evaluated for their role in improving model performance. The review highlights key challenges including slow DDoS attack labeling, computational complexity, model generalization across diverse traffic types, and the need for real-time detection capabilities. We identify future research directions encompassing adversarial robustness, explainable AI for security applications, federated learning for distributed defense, and integration with Software-Defined Networking (SDN) environments. This comprehensive analysis provides researchers and practitioners with insights into selecting appropriate evaluation methodologies and developing next-generation DDoS defense systems.

Keyword : - *DDoS attack evaluation, neural networks, deep learning, feature selection, intrusion detection, CNN-LSTM, attention mechanism, network security*

1. INTRODUCTION

The proliferation of internet-connected devices and cloud-based services has exponentially increased the attack surface for malicious actors, making cybersecurity one of the most pressing challenges of the digital age. Among various cyber threats, Distributed Denial of Service (DDoS) attacks stand out as particularly devastating due to their simplicity in execution yet profound impact on service availability. DDoS attacks overwhelm target systems by flooding them with massive volumes of traffic from distributed sources, rendering legitimate services inaccessible and causing significant financial and reputational damage.

Recent years have witnessed an alarming escalation in both the frequency and sophistication of DDoS attacks. In February 2020, Amazon Web Services experienced a volumetric DDoS attack reaching 2.3 terabits per second (Tbps), representing a significant milestone in attack intensity. The low barrier to entry, facilitated by readily available DDoS-as-a-Service platforms and botnet rentals, has democratized the ability to launch devastating attacks, enabling even novice attackers to orchestrate large-scale disruptions. This accessibility, combined with the increasing complexity of attack vectors including reflection and amplification techniques, has created an urgent need for more sophisticated detection and evaluation mechanisms.

The core challenge lies in accurately evaluating the effect or severity of ongoing attacks in real-time, enabling security teams to prioritize responses and allocate defensive resources optimally. Conventional DDoS attack effect evaluation methods rely predominantly on statistical and mathematical approaches including univariate methods (Index Evaluation Method, Matrix Analysis Method), multivariate deterministic methods (Weighted Sum Method, Analytic Hierarchy Process, Entropy Method), and uncertainty-based techniques (Grey Relational Analysis, Rough Set Method, TOPSIS). While these methods provide mathematical rigor, they suffer from critical limitations. First, evaluation results depend solely on input data without considering the relationship between features and evaluation objectives, making them susceptible to noise and erroneous data. Second, they typically require manual parameter configuration such as weight assignment in WSM or comparison matrices in AHP, introducing subjectivity and reducing credibility. Third, they assume feature independence, ignoring correlations that can lead to redundant calculations and distorted evaluation results.

The emergence of deep learning and neural network technologies has opened new paradigms for DDoS attack evaluation. Unlike traditional methods, neural networks can automatically learn complex relationships between input features and evaluation targets through multilayer architectures trained on large datasets. They eliminate the need for manual parameter tuning through backpropagation and gradient descent algorithms, while nonlinear activation functions enable handling of feature correlations and non-monotonic relationships. Recent studies demonstrate that neural network-based approaches, particularly hybrid architectures combining CNN, LSTM, and attention mechanisms, achieve remarkable accuracy rates exceeding 99% on standard benchmark datasets.

This systematic review provides a comprehensive analysis of neural network approaches for DDoS attack effect assessment, addressing several critical research questions: (1) What are the fundamental limitations of traditional evaluation methods that necessitate neural network solutions? (2) Which neural network architectures and hybrid models demonstrate superior performance for DDoS evaluation? (3) How do feature selection techniques impact model accuracy and efficiency? (4) What datasets and evaluation metrics are most appropriate for benchmarking performance? (5) What are the current challenges and future research directions in this domain?

The remainder of this paper is organized as follows. Section 2 reviews traditional DDoS attack effect evaluation methods and their limitations. Section 3 provides an overview of neural network approaches including CNN, LSTM, RNN, and hybrid architectures. Section 4 presents a comparative analysis of recent studies with performance benchmarking. Section 5 discusses challenges and limitations of current approaches. Section 6 concludes with future research directions.

2. BACKGROUND AND RELATED WORK

2.1 Traditional DDoS Attack Effect Evaluation Methods

DDoS attack effect evaluation has historically relied on statistical and mathematical approaches that can be categorized into three main groups: univariate methods, multivariate methods, and combined methods.

- **Univariate Evaluation Methods**: Index Evaluation Method (IEM) and Matrix Analysis Method (MAM) represent the simplest approaches, evaluating attack effects based on single indicators such as throughput degradation, response time increases, or packet loss rates. While computationally efficient with low complexity, these methods suffer from one-sidedness, as single indicators cannot capture the multifaceted nature of DDoS attack impacts. For instance, evaluating solely based on traffic volume may miss sophisticated low-rate DDoS attacks that consume minimal bandwidth yet effectively degrade service quality.
- **Multivariate Deterministic Methods**: To address univariate limitations, multivariate approaches integrate multiple indicators into comprehensive evaluation scores. Weighted Sum/Product Method (WSM/WPM) combines indicators through weighted aggregation, but requires manual weight assignment that introduces subjectivity. Analytic Hierarchy Process (AHP) structures evaluation criteria hierarchically and derives weights through pairwise comparisons, yet remains dependent on expert

judgment for comparison matrix construction. Entropy Method (EM) determines indicator weights based on information entropy, reducing subjectivity but assuming equal importance of variance across all indicators.

- **Uncertainty-Based Methods**: Recognizing that certainty methods cannot handle ambiguous or incomplete data, uncertainty techniques have been developed. Grey Relational Analysis (GRA) quantifies relationships between reference and comparison sequences, but its correlation coefficients heavily depend on extreme values without verifying data necessity. Rough Set Method (RSM) handles imprecise data through approximation spaces, while TOPSIS ranks alternatives based on distances to ideal solutions. Fuzzy Analysis (FA) and System Effectiveness Analysis (SEA) incorporate fuzzy operators to process qualitative indicators.
- **Combined Methods**: Recent approaches merge multiple techniques to leverage complementary strengths. GRA+TOPSIS combines grey relational correlation with ideal solution proximity, while Fuzzy+AHP integrates fuzzy logic with hierarchical structuring. Attack Graph (AG) methods visualize attack paths and assign success probabilities to nodes for holistic security evaluation.

2.2 Limitations of Traditional Methods

Despite their mathematical foundations, traditional DDoS evaluation methods exhibit three critical shortcomings that limit their effectiveness in modern attack scenarios:

- **Lack of Feature-Target Association**: Traditional methods evaluate attacks based purely on input indicator values without learning relationships between features and evaluation objectives. This data-dependency makes them highly susceptible to noise, outliers, and adversarial manipulation. For example, GRA's correlation coefficients and TOPSIS's ideal solutions are computed from extreme values without validating whether each input feature genuinely contributes to accurate assessment.
- **Manual Parameter Dependency**: Most traditional techniques require human experts to configure parameters such as indicator weights in WSM, comparison matrices in AHP, or membership functions in fuzzy systems. This manual intervention introduces subjectivity, reduces reproducibility, and limits scalability to diverse attack scenarios. Different security analysts may assign vastly different weights to the same indicators, leading to inconsistent evaluations.
- **Feature Independence Assumption**: Traditional methods typically assume that all evaluation indicators are independent, ignoring correlations that frequently exist in network traffic data. For instance, excessive memory consumption often degrades software performance, which in turn increases service response delays. If memory usage and response delay are directly integrated without correlation processing, the attack effect becomes artificially amplified, distorting evaluation results.

2.3 Rise of Machine Learning in DDoS Detection

The limitations of traditional approaches have motivated extensive research into machine learning and deep learning solutions. Early machine learning applications focused primarily on DDoS attack detection (binary classification of normal vs. attack traffic) rather than effect evaluation. Naive Bayes classifiers achieved 98% accuracy on NSL-KDD datasets for multi-controller SDN environments. Support Vector Machine (SVM) and Random Forest (RF) ensembles reached 99.1% accuracy through reduced feature sets. However, these traditional ML methods still rely on handcrafted features and struggle with complex, high-dimensional traffic patterns.

The paradigm shift toward deep learning emerged from neural networks' ability to automatically extract hierarchical features from raw data without manual engineering. Deep learning models can learn non-linear relationships, handle temporal dependencies through recurrent architectures, and capture spatial patterns through convolutional operations. Critically for DDoS evaluation, they eliminate subjective parameter tuning through end-to-end training via backpropagation and gradient descent..

3. NEURAL NETWORK APPROACHES OVERVIEW

3.1 Feature Extraction and Selection

CICFlowMeter generates 77 network flow features including flow duration, packet rates, flag counts, and window sizes. High dimensionality necessitates feature selection for efficiency and accuracy. Distance Entropy-Based Triplet Networks (LTN): LTN employs LSTM-based Triplet Networks measuring feature-to-target similarity and inter-feature redundancy through distance entropy of order α. Unlike spatial distance metrics, distance entropy captures monotonic correlations in distribution changes, making it suitable for time-series traffic. LTN achieved 93.1-94.6% ranking accuracy across five datasets, outperforming statistical methods (CHI, Relief, IG) averaging below 74%. Models using LTN-selected features achieved 31.2% accuracy improvement on NSL-KDD2009 (from 44.1% to 75.3%) while reducing training time by 28.5%. Principal Component Analysis reduces dimensionality through variance-maximizing projections. Information Gain (IG) ranks features by contribution to classification entropy reduction. These filter methods offer computational efficiency but may miss feature interactions.

3.2 Deep Learning Model Architectures

- **Convolutional Neural Networks (CNN)**: CNNs excel at extracting spatial features and local patterns through convolutional kernels that slide across input data. For DDoS evaluation, 2D-CNNs process feature matrices to identify localized anomalies and correlations. The convolution operation automatically learns hierarchical representations, with early layers capturing low-level patterns (e.g., packet size distributions) and deeper layers combining these into complex attack signatures. Max-pooling layers following convolutional layers reduce sensitivity to exact feature positions, enabling detection of similar attack patterns across different temporal locations. Recent studies report CNN-based models achieving 99.84% accuracy on balanced datasets.
- **Long Short-Term Memory (LSTM) Networks**: LSTM addresses the vanishing gradient problem of traditional Recurrent Neural Networks (RNNs), enabling learning of long-term temporal dependencies in network traffic sequences. LSTM units contain input gates, forget gates, and output gates that regulate information flow, allowing the network to selectively retain relevant historical context while discarding irrelevant information. For DDoS evaluation, LSTM captures evolving attack patterns and temporal correlations between successive traffic measurements. Bidirectional LSTM (BiLSTM) processes sequences in both forward and backward directions, providing richer contextual understanding.
- **Gated Recurrent Units (GRU)**: GRU simplifies LSTM by merging cell state and hidden state while using only two gates (reset and update), reducing computational complexity while maintaining comparable temporal modeling capability. Studies demonstrate that CNN-GRU hybrid models achieve 100% test accuracy with 99.70% cross-validation accuracy on SDN traffic datasets, offering a more parameter-efficient alternative to CNN-LSTM architectures.
- **Attention Mechanisms**: Attention mechanisms dynamically weight features or temporal steps based on their relevance to the prediction task. Multi-head attention processes inputs through multiple parallel attention operations, each focusing on different representation subspaces. For DDoS evaluation, attention enables the model to emphasize critical features (e.g., sudden traffic spikes, abnormal flag distributions) while downweighting less informative indicators. Self-attention mechanisms in transformers have shown particular promise, with models like SAINT achieving 97% accuracy and 96% F1-score on recent datasets.

3.3 Hybrid Architectures

The most effective DDoS evaluation systems combine multiple neural network types to leverage their complementary strengths.

- **CNN-LSTM Hybrid Models**: These architectures use CNN layers for spatial feature extraction from traffic snapshots, followed by LSTM layers for temporal sequence modeling. The CNN component identifies local patterns and filters irrelevant information, while LSTM captures how attack intensity evolves over time. Studies report CNN-LSTM achieving 99.55-99.87% accuracy on CICIDS2018 and similar datasets.
- **CNN-BiLSTM with Attention**: Adding bidirectional processing and attention mechanisms further enhances performance. CNN-BiLSTM models with feature ranking achieve 94.52% accuracy on CIC-DDoS2019, while attention-augmented variants reach 99.79% accuracy with 0.17% false positive rates on NSL-KDD. The attention component enables the model to focus on the most discriminative temporal segments and features.
- **CNN-GRU Architectures**: Combining CNN's spatial feature extraction with GRU's efficient temporal modeling provides a lightweight yet effective solution. Recent work demonstrates CNN-GRU achieving perfect test set performance (100% accuracy, precision, recall, and F1-score) while maintaining 99.70% cross-validation accuracy, outperforming CNN-LSTM in both accuracy and training efficiency.
- **Autoencoder-Enhanced Models**: Autoencoders learn compressed representations of normal traffic patterns, enabling detection of anomalous DDoS behavior through reconstruction error analysis. Hybrid approaches combining autoencoders with LSTM (HHO-PSO-LSTM) achieve 98.53% accuracy through

optimized feature learning and weight tuning. Variational Autoencoders (VAE) and Generative Adversarial Networks (GAN) enable synthetic attack traffic generation for data augmentation and adversarial training.

3.4 Evaluation Neural Network Architectures

Complete DDoS effect evaluation systems integrate feature selection, deep feature learning, hierarchical weighting, and regression/classification outputs.

- **Embedding Layers**: High-dimensional time-series traffic data undergoes dimensionality reduction through embedding layers that project features into lower-dimensional dense representations. Typical embedding configurations use 64×1000 matrices to handle large-scale datasets efficiently.
- **Multi-Scale Convolutional Processing**: 2D-CNNs with 5×5 kernels and 32 filters capture local feature interactions, followed by max-pooling for position invariance. Subsequent 1D-CNN layers perform information clustering after attention modules restructure data.
- **Attention-Based Feature Weighting**: Multi-head attention assigns importance weights to different local features through query-key-value mechanisms. Residual connections (ResNet) prevent gradient vanishing in deep networks, while layer normalization stabilizes training. Experiments show optimal performance with three attention module iterations.
- **Fully Connected Regression**: Final layers use ReLU activation for non-linear transformation, outputting scalar attack effect values between 0 and 1 via sigmoid activation. Typical architectures employ three fully connected layers with 16 units each, balanced between representational capacity and convergence speed.

5. COMPARATIVE ANALYSIS

4.1 Performance Benchmarking

Empirical evaluations on standard datasets demonstrate the superiority of neural network approaches over traditional methods for DDoS attack evaluation and detection.

- **Neural Network vs. Traditional Evaluation Methods**: On five benchmark datasets (KDD99, NSL-KDD2009, CIC-IDS2017, CIC-IDS2018, CIC-DDoS2019), the Neural Network-based DDoS Evaluation (NNDE) method achieved average ranking accuracies of 87.2%, 91.3%, 88%, 85.6%, and 94.5% respectively. This represents an average improvement of 19.73% over traditional statistical methods. Specifically, compared to Weighted Sum Method (WSM), accuracy increased by 21.96%, and compared to combined GRA+TOPSIS methods, improvement reached 7.12%. Traditional methods like WSM, GRA, and TOPSIS consistently underperformed due to their inability to learn feature-target relationships and handle correlated indicators.
- **Comparison with Standard Neural Networks:** Among deep learning architectures, specialized DDoS evaluation networks outperform generic structures. On CIC-DDoS2019, NNDE achieved Mean Squared Error (MSE) of 0.27 and Explained Variance Score (EVS) of 0.82, surpassing standalone DNN (MSE: 0.45, EVS: 0.65), CNN (MSE: 0.38, EVS: 0.71), RNN (MSE: 0.40, EVS: 0.68), and combined CNN+RNN (MSE: 0.32, EVS: 0.76). The superior performance stems from targeted architectural components including distance entropy-based feature selection, multi-head attention for hierarchical weighting, and optimized layer configurations.
- **State-of-the-Art Hybrid Models**: Recent hybrid architectures demonstrate exceptional performance across diverse datasets. CNN-LSTM models achieve 99.84% accuracy on balanced datasets through automated spatial-temporal feature learning. CNN-BiLSTM with attention reaches 99.79% accuracy and 99.83% detection rate with only 0.17% false positives on NSL-KDD. CNN-GRU architectures attain perfect 100% test accuracy with 99.70% cross-validation accuracy on SDN traffic data, offering parameter efficiency superior to LSTM variants. Advanced models like ARSAE-QGRU (Autoencoder + Residual + Attention + GRU) achieve up to 99.8% accuracy on CICIDS2017 and CICDDoS2019, while transformer-based SAINT models reach 97% accuracy with 96% F1-score on recent datasets.

4.2 Evaluation Metrics and Datasets

DDoS evaluation research employs multiple metrics to assess model effectiveness. For regression tasks, Mean Squared Error (MSE) and Explained Variance Score (EVS) measure prediction accuracy and distribution stability. For classification tasks, accuracy, precision, recall, F1-score, and Area Under ROC Curve (AUC-ROC) provide comprehensive performance characterization. Sort Accuracy specifically measures ranking consistency between predicted and actual attack severity orderings, critical for prioritizing defense responses. Five datasets dominate DDoS research evaluations:

- **KDD99**: Historical benchmark containing 4,856,151 DDoS traffic instances, widely used despite age-related limitations.
- **NSL-KDD2009**: Refined version with 45,927 DDoS samples and defense difficulty labels suitable for attack severity assessment.
- **CIC-IDS2017**: Contains 128,027 DDoS instances with bidirectional flow features generated by CICFlowMeter, addressing earlier dataset shortcomings.
- **CIC-IDS2018**: Includes 687,742 DDoS samples with diverse attack types and realistic background traffic.
- **CIC-DDoS2019**: Largest dataset with 50,063,112 DDoS traffic instances covering reflection and amplification attacks.

Studies using these datasets enable reproducible comparisons and validation of proposed methods across varying attack characteristics and scales.

5. CHALLENGES, LIMITATIONS, AND FUTURE DIRECTIONS

5.1 Current Challenges

- **Slow DDoS Detection**: Low-rate attacks mimic legitimate traffic, evading labeling methods based on flow duration and packet counts. Future work must incorporate application-layer semantics and long-term behavioral patterns.
- **Model Generalization**: Models achieving 99% accuracy on one dataset may underperform on different network environments or attack types. Transfer learning, domain adaptation, and meta-learning remain underexplored.
- **Computational Complexity and Real-Time Constraints**: While training occurs offline, inference latency critically affects defense response. Current systems achieve 2.3ms per-sample latency, meeting real-time requirements, but deeper models risk degradation.
- **Adversarial Robustness**: Attackers may craft adversarial examples evading detection while maintaining attack effectiveness. Accuracy drops to 82-90% under adversarial attacks. Adversarial training using FGSM, JSMA improves robustness but requires systematic evaluation.
- **Explainability**: Neural network "black boxes" hinder security analyst understanding. SHAP techniques identify key features (packet size, connection duration, protocol type) driving predictions, but comprehensive interpretability remains limited.

5.2 Future Research Directions.

- **Federated Learning**: Collaborative learning across organizations without sharing sensitive traffic data builds more robust models while preserving privacy.
- **Graph Neural Networks**: GNNs model attack path dependencies and inter-system relationships, enabling holistic security assessment.
- **Reinforcement Learning for Adaptive Mitigation**: RL agents learn optimal defense strategies dynamically based on real-time attack evaluations, automatically adjusting firewall rules.
- **SDN Integration**: Deploying neural network evaluation models in SDN controllers enables programmable traffic management and rapid attack response.
- **Zero-Day Detection**: Unsupervised approaches leveraging autoencoders, GANs, and anomaly detection identify novel attack patterns without labeled data.

4. CONCLUSIONS

This systematic review demonstrates that neural network approaches substantially outperform traditional DDoS attack effect evaluation methods through automatic feature learning, elimination of subjective parameter tuning, and effective handling of feature correlations. Empirical evidence shows 19.73% average accuracy improvement with state-of-the-art models reaching 99.84-100% compared to traditional methods' 44.1-75.3%. Feature selection using distance entropy-based Triplet networks improves accuracy by 31.2% while reducing training time by 28.5%. Hybrid CNN-BiLSTM-Attention architectures with embedding layers, multi-scale convolution, and attention-based feature weighting constitute effective end-to-end evaluation systems.

However, significant challenges persist: slow DDoS attack detection, cross-dataset generalization, real time inference constraints, adversarial robustness, and explainability. Addressing these challenges through federated learning, graph neural networks, reinforcement learning integration with SDN, and explainable AI techniques will enable deployment of robust, trustworthy DDoS defense systems. Neural network-based DDoS evaluation represents a paradigm shift from static, rule-based approaches to adaptive, data-driven systems. Continued research on identified challenges, combined with expanding datasets and increasing computational resources, will establish neural networks as the foundation for next-generation cyber defense infrastructure.

6. REFERENCES

[1] W. Guo, H. Qiu, Z. Liu, J. Zhu, and Q. Wang, "The Evaluation of DDoS Attack Effect Based on Neural Network," Security and Communication Networks, vol. 2022, Article ID 5166323, 16 pages, Apr. 2022, doi: 10.1155/2022/5166323.

[2] A. Salau, S. Jain, and C. Ukwuoma, "Software defined networking based network traffic classification using machine learning and deep learning models," in Proc. Nature.com, Aug. 2024.

[3] S. L. Jacob and P. S. Habibullah, "A Systematic Analysis and Review on Intrusion Detection Systems Using Machine Learning and Deep Learning Algorithms," Journal of Computational and Cognitive Engineering, vol. 4, no. 2, pp. 108-120, Jul. 2024, doi: 10.47852/bonviewJCCE42023249.

[4] QT Analytics, "Optimized Multi-Layer Ensemble for DDoS Attack Detection," Dec. 2024, [Online]. Available: https://www.qtanalytics.in. [Accessed: Nov. 2024].

[5] A. Brahmareddy, S. Meghana, S. V. Kiran, K. S. Bharathi, and B. V. Kumar, "Hybrid Ensemble Deep Neural Network for Intrusion Detection (HEDNN_ID)," SSRG International Journal of Electronics and Communication Engineering, vol. 12, no. 7, pp. 184-200, Jul. 2025, doi: 10.14445/23488549/IJECE-V12I7P114.

[6] K. Pati, "Deep Learning Based Traffic Classification with Feature Selection using Explainable AI," IJISAE, vol. 12, no. 2, pp. 89-104, Mar. 2024, [Online]. Available: https://www.ijisae.org. [Accessed: Nov. 2024].

[7] M. Hiari, Y. Alraba'nah, and I. Qaddara, "A Deep Learning-Based Intrusion Detection System using Refined LSTM for DoS Attack Detection," Engineering, Technology & Applied Science Research, vol. 15, no. 4, pp. 25627-25633, Aug. 2025, doi: 10.48084/etasr.6845.

[8] S. L. Jacob and P. S. Habibullah, "A Systematic Analysis and Review on Intrusion Detection Systems Using Machine Learning and Deep Learning Algorithms," in Proc. Journal of Computational and Cognitive Engineering, vol. 4, no. 2, pp. 108-120, Jul. 2024.

[9] A. O. Salau, S. Jain, and C. Ukwuoma, "Software defined networking based network traffic classification using machine learning and deep learning models," Scientific Reports, vol. 14, no. 1, Aug. 2024, doi: 10.1038/s41598-024-67088-z.

[10] "Comparative Analysis of CNN and LSTM for DDoS Attack Detection in IoT Networks using CICDDoS2019," Journal of Informatics and Systems Engineering (JISEM), vol. 10, no. 8, pp. 1-20, 2024, [Online]. Available: https://www.jisem-journal.com. [Accessed: Nov. 2024].

[11] A. K. B. Arnob and others, "A comprehensive systematic review of intrusion detection systems using deep learning: Advanced feature engineering, explainable AI, and emerging technologies," Journal of Edge Computing, vol. 4, no. 1, pp. 73-104, May 2025, doi: 10.55056/jec.885.