International Journal of Innovative Trends in Engineering Science and Technology
ijitest.org | E-ISSN: 3139-6887

Dique: A Real-Time Intrusion Detection and Prevention System for DoS Attacks Using Deep Learning

[1]CH. Swapna Priya, [2]T. Dansy Sri Abeesh, [3]Srikanth Durgam
[1]Associate Professor, [2]Student, [3]Associate Professor, [1,2,3]Department of Computer Science Engineering
[1,2]Vignan's Institute of Information Technology, Visakhapatnam, [3]Scient Institute of Technology, Hyderabad
[1]swapnachsp@gmail.com, [2]dansysriabeesh@gmail.com, [3]durgam.srikanth69@gmail.com

Abstract -- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks pose a severe threat to the availability and integrity of modern web servers. To effectively mitigate these threats, this research presents Dique, an intelligent Intrusion Detection and Prevention System (IDS/IPS) powered by deep learning. The proposed framework employs a multi-layered Convolutional Neural Network (CNN) to classify incoming network packets as either benign traffic or malicious DoS attacks. Leveraging the comprehensive CICDDoS2019 dataset, the system undergoes rigorous data preprocessing and feature extraction, incorporating Principal Component Analysis (PCA) to optimize dimensionality. The system is equipped with a real-time Graphical User Interface (GUI) that allows administrators to monitor traffic visually and textually, effortlessly switching between detection (IDS) and prevention (IPS) modes. Experimental evaluations demonstrate that the PCA-enhanced CNN model achieves exceptionally high classification accuracy while significantly reducing computational overhead, making it highly suitable for real-time network defense.

Keywords: Skin cancer detection, melanoma classification, deep learning, convolutional neural network, DenseNet, HAM10000, transfer learning, U-Net, medical image segmentation.

I. Introduction

The rapid expansion of the internet has been accompanied by an exponential increase in cybercrime, with unauthorized access and service disruption threatening the core pillars of computer security: confidentiality, integrity, and availability. Among these threats, Denial of Service (DoS) attacks are particularly disruptive, overwhelming web servers with malicious traffic to block legitimate users. Traditionally, security professionals have relied on signature-based detection, which requires predefined attack databases, or anomaly-based detection using conventional machine learning (ML). While ML models can learn without explicit programming, they frequently suffer from high false-positive rates, misclassifying benign traffic as anomalous or allowing malicious packets to corrupt the learning algorithm. Furthermore, processing massive volumes of network traffic in real-time places a heavy computational burden on traditional ML systems.

To address these limitations, this research investigates the application of Deep Learning (DL), specifically Convolutional Neural Networks (CNNs), to build a highly accurate, real-time Intrusion Detection and Prevention System. Unlike traditional ML, which relies heavily on manual feature engineering, deep learning utilizes hierarchical layers to automatically learn latent feature representations directly from raw data. By combining a multi-layered CNN architecture with dimensionality reduction techniques, the proposed system effectively handles vast datasets, minimizes classification errors, and operates rapidly enough to protect web servers in live environments.

II. Related Work

The application of artificial intelligence in cybersecurity has been extensively explored in recent literature. Xin et al. (2018) conducted a comprehensive survey on the transition from traditional machine learning to deep learning in network intrusion detection, highlighting the necessity of robust datasets and the challenges of real-time processing. Zargar et al. (2013) explored the architecture of DDoS flooding attacks, categorizing defense mechanisms based on their deployment timing (prevention, detection, and response) and stressing the need for collaborative defense strategies.

Addressing the limitations of traditional models, Thilina et al. (2016) proposed a framework utilizing recurrent neural

DOI: 10.5281/zenodo.24474477
IJITEST-2026-031 | Volume 1, Issue 4, June 2026 | ISSN: 3139-6887
Creative Commons Attribution 4.0 International (CC BY 4.0)
Article Received: November 7, 2026 | Accepted: November 23, 2026

networks combined with association rule mining (FP-Growth) to predict and analyze intruder activities, overcoming the overfitting issues common in earlier multi-layer perceptrons. Similarly, Xu et al. (2018) introduced an IDS utilizing a deep network of Gated Recurrent Units (GRU) and multi-layer perceptrons. Their model achieved a 99.98% detection rate for DoS attacks on the KDD 99 dataset, proving that GRUs serve as highly efficient memory units for sequential network traffic analysis. More recently, Amma and Subramanian (2018) developed VCDeepFL, a Vector Convolutional Deep Feature Learning approach that combines Vector CNNs with Fully Connected Neural Networks to identify both known and zero-day DoS attacks, successfully reducing false alarms and improving Area Under the Curve (AUC) metrics.

III. Proposed Methodology

The proposed framework, named Dique, is designed to capture live network traffic and classify it using an optimized deep neural network. The methodology encompasses data preparation, feature engineering, and model architecture design.

- *Dataset Preparation:* The system utilizes the CICDDoS2019 dataset, which contains benign traffic alongside 10 distinct variations of DoS attacks (e.g., DrDOS_DNS, DrDOS_LDAP, Syn). The dataset initially contains 88 features, which are trimmed to 86 core network packet features by removing irrelevant indices.

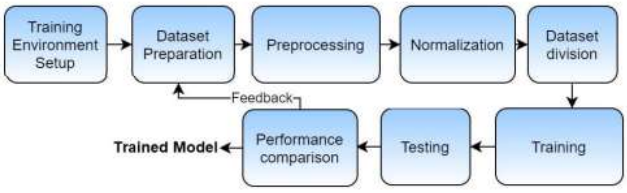

Figure 1: Proposed block diagram for the Dique Intrusion Detection and Prevention System.

- *Data Preprocessing:* Non-numeric attack labels are converted into numeric IDs using Label Encoding. Missing values are filled, and the dataset is normalized using Min-Max scaling to ensure uniformity across all feature vectors. The target labels are one-hot encoded for multi-class classification. The data is then shuffled and split into an 80% training set and a 20% testing set.
- *Feature Optimization (PCA):* To eliminate irrelevant attributes and reduce computational load, Principal Component Analysis (PCA) is applied. PCA successfully reduces the feature space from 84 attributes down to 48 highly relevant components without losing critical variance.
- *Deep Learning Architecture:* The core classification engine is a Deep Feed-Forward Convolutional Neural Network. The architecture reshapes the input features and passes them through multiple 2D Convolutional layers (using 32, 64, and 128 filters) equipped with ReLU activation functions. Batch Normalization is applied to stabilize learning, while MaxPooling layers reduce spatial dimensions. To prevent overfitting, Dropout layers (ranging from 20% to 25%) are interspersed throughout the network. The extracted features are flattened and passed through a Dense layer of 1024 neurons before reaching the final Softmax classification layer.
- *System Deployment:* The trained weights are integrated into a GUI-driven application that captures live packets, processes them through the PCA-enhanced CNN, and visually flags the traffic as normal (benign) or malicious.

IV. Results and Discussions

The performance of the proposed CNN model was evaluated against the PCA-enhanced CNN model using standard classification metrics: accuracy, precision, recall, F1-score, and computation time.

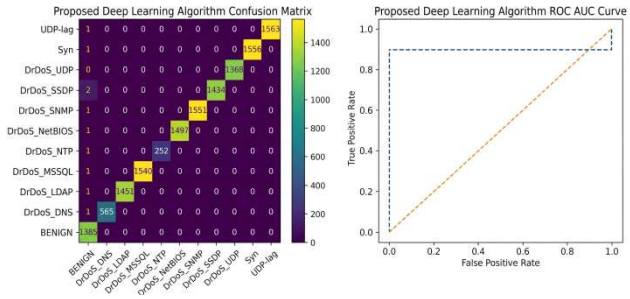

Figure 2: A sequence diagram for the Dique Intrusion Detection and Prevention System.

This figure 2 illustrates the classification performance of the proposed deep learning algorithm against ten distinct Denial of Service (DoS) attack variants and benign network traffic. The confusion matrix on the left visually confirms a high true-positive prediction rate, as evidenced by the strong diagonal line showing minimal misclassifications across all categories. Accompanying this, the Receiver Operating Characteristic (ROC) curve on the right displays the model's true positive rate against its false positive rate. The steep trajectory of the ROC curve signifies the algorithm's exceptional ability to distinguish between normal and malicious packets effectively. Overall, these visual metrics validate the model's strong diagnostic accuracy and reliability for intrusion detection before applying any dimensionality reduction.

Standard CNN Performance: The baseline multi-layered CNN achieved an impressive classification accuracy of 99.92%. The precision was recorded at 99.93%, with a recall of 99.89% and an F1-score of 99.91%. However, processing the full 84-feature dataset required a computation time of 12.19 seconds.

This figure 3 illustrates the distribution of various Denial of Service (DoS) attacks and benign traffic present in the training dataset. The x-axis represents the different traffic categories (such as BENIGN, DrDoS_DNS, DrDoS_LDAP, etc.), while the y-axis shows the total number of records for each. This visual helps identify the frequency and representation of each attack type within the data before model training.

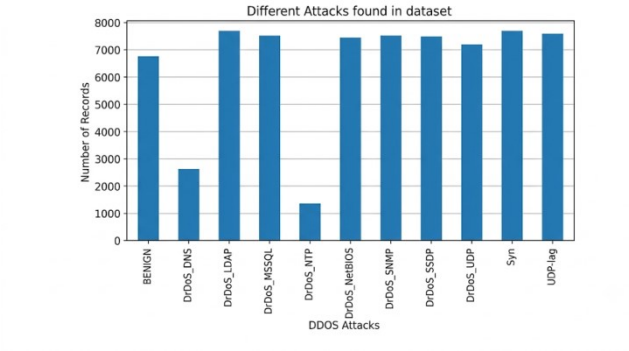

Figure 3: Dataset Distribution Graph.

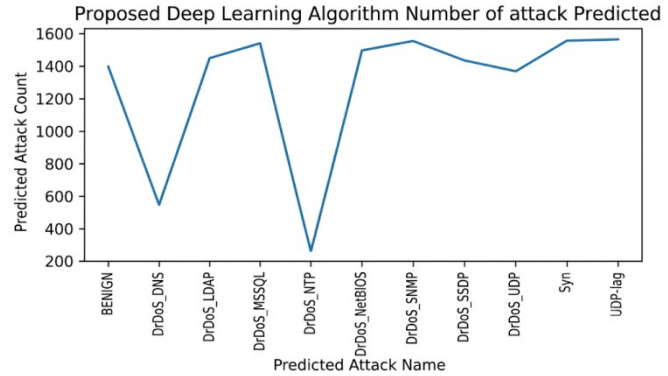

Figure 4: Predicted Attacks Graph.

Figure 4, displays the total number of times the proposed deep learning algorithm predicted each specific attack category. The x-axis lists the predicted attack names, and the y-axis quantifies the predicted attack count. It provides a clear view of the model's classification output volumes across the different classes.

This Figure 5 compares the processing efficiency of the baseline "Propose CNN" against the "Extension PCA CNN". The y-axis measures the computation time in seconds. The chart clearly demonstrates that integrating Principal Component Analysis (PCA) drastically reduces the computation time from over 12 seconds to approximately 4 seconds, making the system much faster.

PCA-Enhanced CNN Performance: By applying PCA to reduce the input space to 48 features, the model's performance improved while drastically reducing overhead. The accuracy slightly increased to 99.95%, accompanied by a precision of 99.95%, a recall of 99.94%, and an F1-score of 99.95%. Most notably, the computation time dropped by roughly 66% to just 4.07 seconds.

This comparative chart outlines the core classification metrics, including Accuracy, F1-Score, Precision, and Recall, for both the baseline and PCA-extended algorithms. The clustered bars indicate that both models achieve exceptionally high scores, hovering closely around the 99.9 percent mark across all evaluated parameters. However, the PCA-enhanced model shows a slight but measurable superiority, reaching a 99.95 percent overall accuracy rate compared to the baseline's 99.92 percent. The visualization confirms that removing redundant data features speeds up the system while subtly refining its predictive exactness. This reinforces the conclusion that the optimized framework is both highly accurate and reliably robust against complex cyber threats.

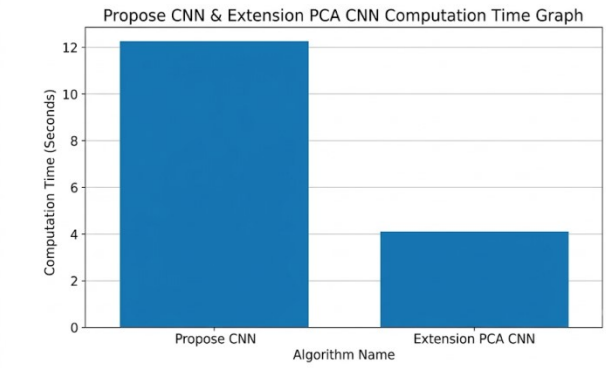

Figure 5: Computation Time Comparison of the Proposed System.

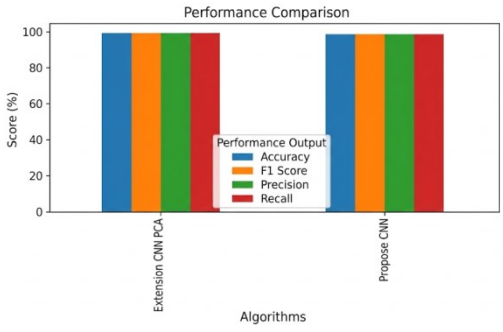

Figure 6: Performance Metrics Comparison of the Proposed System.

The integration of PCA proved highly effective. Removing redundant network packet features allowed the neural network to converge faster and generalize better across the 10 DoS attack classes. Confusion matrices generated during testing confirmed minimal misclassifications between benign and attack traffic. Furthermore, the Receiver Operating Characteristic (ROC) curve demonstrated an Area Under the Curve (AUC) approaching 1.0, indicating near-perfect true positive rates against false positive rates. Live testing via the GUI confirmed the system's ability to seamlessly ingest real-world formatted arrays and accurately flag them (e.g., accurately predicting specific attacks like DrDoS_DNS or DrDoS_LDAP).

V. Conclusion and Future Scope

This project successfully introduces Dique, a highly accurate Deep Learning-based Intrusion Detection and Prevention System specifically engineered to combat Denial-of-Service attacks. By combining a robust Convolutional Neural Network with Principal Component Analysis, the framework effectively resolves the dual challenges of traditional intrusion detection: low accuracy against complex attack variants and high computational latency. The PCA-enhanced model demonstrated near-perfect classification accuracy (99.95%) while operating rapidly enough (4.07 seconds) to be viable for live web server protection. The addition of a real-time GUI makes the tool highly practical for network administrators.

Future research will focus on expanding the model's threat detection repertoire to include application-layer DDoS attacks, ransomware, and distributed botnet behaviors. Additionally, adapting the architecture for distributed cloud environments and resource-constrained Internet of Things (IoT) edge networks will be explored to ensure scalability and adaptability against constantly evolving cyber threats.

References

[1] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, 6, 35365–35381.

[2] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, 15(4), 2046–2069.

[3] Thilina, A., Attanayake, S., Samarakoon, S., Nawodya, D., Rupasinghe, L., Pathirage, N., Edirisinghe, T., & Krishnadeva, K. (2016). Intruder detection using deep learning and association rule mining. *IEEE International Conference on Computer and Information Technology*.

[4] Xu, C., Shen, J., Du, X., & Zhang, F. (2018). An intrusion detection system using a deep neural network with gated recurrent units. *IEEE Access*, 6, 48697–48707.

[5] Amma, N. G. B., & Subramanian, S. (2018). VCDeepFL: Vector convolutional deep feature learning approach for identification of known and unknown denial of service attacks. *TENCON-IEEE Region 10 Conference*.

Funding Declaration

The authors declare that no funds, grants, or other forms of financial support were received from any organization or institution for the conduct of this research.