IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 10, October 2025

DOI: 10.17148/IJIREEICE.2025.131044

Hybrid PSO-CNN-LSTM Framework for Intelligent DDoS Detection

Dinesh P[1], Eedpuganti Yagna Sai Harshith[2], Athithya S A[3], Raj Pranav Raghavan[4], G Mohammed Azam[5], Neelam Sanjeev Kumar[6]

Student, CSE (E.Tech), SRM Institute of Science and Technology, Vadapalani, Chennai, India[1-5]

Assistant Professor, Computer Science and Engineering (E-Tech), SRM Institute of Science and Technology, Chennai, India[6]

Abstract: In modern network environments, Distributed Denial-of-Service (DDoS) attacks represent a critical security threat, often rendering services unavailable to legitimate users. Conventional intrusion detection techniques fail to adapt to evolving attack strategies and high-dimensional network traffic. This paper proposes a PSO-optimized CNN-LSTM hybrid deep learning model for accurate DDoS detection and classification. The CNN component extracts spatial features from traffic flows, while the LSTM component captures temporal dependencies in sequential data. Particle Swarm Optimization (PSO) is employed to optimize hyperparameters, enabling faster convergence and improved performance. The model is trained and evaluated on imbalanced real-world network datasets. Experimental results indicate significant improvements, achieving over 98% accuracy and enhanced recall and F1-score compared to traditional models. The proposed method demonstrates strong potential for deployment in real-time cybersecurity systems, offering robustness, automation, and adaptability in detecting DDoS attacks.

Keywords: DDoS Detection, CNN-LSTM, Deep Learning, Particle Swarm Optimization (PSO), Cybersecurity, Network Intrusion Detection, Real-Time Security, Imbalanced Dataset, Hyperparameter Optimization, Spatial-Temporal Learning

I. INTRODUCTION

1.Background

With the rapid expansion of digital networks, cloud systems, and IoT devices, cyber-attacks such as Distributed Denial-of-Service (DDoS) have become a major threat. Traditional rule-based security systems struggle to detect evolving and high-volume attacks. Deep learning techniques like CNN and LSTM have emerged as effective solutions by learning complex traffic patterns. However, their performance depends heavily on hyperparameter tuning, which is often done manually and inefficiently.

2.Existing Evidence (Literature Survey)

Earlier DDoS detection models used statistical and machine learning algorithms like SVM, KNN, and Random Forest. This improved detection accuracy but lacked scalability and required manual feature extraction. Hybrid CNN-LSTM models later improved spatial-temporal pattern learning, but still depended on manual tuning. Recent works explored optimization methods like PSO and GA, showing improvements but limited real-time deployment studies.

3.Research Gap

Although deep learning-based intrusion detection systems have shown promising outcomes, certain limitations still persist:

- Most models rely on **manual hyperparameter tuning**, which is time-consuming and sub-optimal.
- Limited studies integrate **hybrid deep learning with swarm intelligence** for DDoS detection.
- **Imbalanced datasets** in real-world traffic remain insufficiently addressed, affecting model generalization.
- Many models are tested offline and lack **real-time applicability** and scalability.
- Few frameworks combine **spatial-temporal learning** with automated optimization in a single pipeline.

This gap highlights the need for an **adaptive, scalable, and self-optimizing deep learning-based DDoS detection system**.

4.Objective

The main objectives of this research are:

1. To design a **hybrid CNN–LSTM model** capable of learning spatial-temporal network traffic patterns.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 10, October 2025

DOI: 10.17148/IJIREEICE.2025.131044

2. To apply **Particle Swarm Optimization (PSO)** for automated hyperparameter tuning of the model.
3. To evaluate the system using large-scale, **imbalanced real-world DDoS network traffic datasets**.
4. To achieve improved detection metrics including **accuracy, precision, recall, F1-score, and AUC**.
5. To develop a **scalable, real-time-ready intrusion detection pipeline** for modern network environments.

5.Scope

This project focuses on the detection stage of DDoS attacks using flow-level network features. It employs hybrid deep learning and swarm intelligence techniques for automated learning and model improvement. The scope includes **data preprocessing, model training, optimization, performance evaluation, and demonstration of real-time applicability**. The system is designed for enterprise, cloud, and IoT network environments and emphasizes adaptability, scalability, and reduced manual intervention. Although limited to DDoS traffic detection, the architecture can be extended to broader intrusion detection and cybersecurity applications.

II. LITERATURE REVIEW

Early DDoS detection systems used rule-based and statistical techniques to identify abnormal traffic, but they were limited to known attack signatures and failed against evolving threats. With the growth of network complexity, machine learning methods such as SVM, Random Forest, and KNN were introduced, improving detection accuracy but still requiring manual feature engineering and struggling with large and imbalanced datasets.

Recent studies explored deep learning techniques, where CNN models extract spatial features and LSTM models capture time-based traffic behavior. Hybrid CNN-LSTM architectures demonstrated higher detection accuracy for DDoS attacks. However, their performance depends heavily on hyperparameter tuning, and many works rely on manual trial-and-error methods. To address this limitation, optimization algorithms like Genetic Algorithms and Particle Swarm Optimization (PSO) have been applied to improve model performance and convergence. Yet, there remains a need for scalable, real-time, and fully optimized DDoS detection frameworks.

III. DATASET DESCRIPTION

This project uses a real-world network traffic dataset designed to evaluate DDoS detection performance in modern high-volume environments. The dataset contains both normal and attack traffic, including multiple types of DDoS patterns such as SYN flood, UDP flood, and HTTP-based attacks. It includes flow-level network features such as packet statistics, byte count, connection duration, protocol type, and traffic rates, which help in distinguishing legitimate traffic from malicious behavior.

The dataset is highly **imbalanced**, representing real network conditions where malicious traffic appears less frequently than normal traffic. To address this, preprocessing techniques such as normalization, missing value handling, and balancing strategies were applied to ensure effective model learning. The data is divided into training and testing subsets for objective evaluation. This dataset enables the development of a scalable and robust intrusion detection model capable of identifying diverse and evolving DDoS attack patterns in real-time network environments.

IV. SYSTEM ANALYSIS

System analysis is performed to understand the requirements, architecture, and working behavior of the proposed DDoS detection system using PSO-optimized CNN-LSTM. This phase ensures that the designed solution addresses security needs efficiently and outperforms conventional systems.

1. Problem Definition

Modern networks face increasingly sophisticated DDoS attacks that cannot be reliably detected by traditional rule-based or static threshold systems. These attacks generate high-volume malicious traffic that disrupts services and causes severe performance degradation. Therefore, an automated, adaptive, and intelligent detection mechanism is required to accurately identify malicious traffic in real-time.

2. Proposed Solution Overview

To overcome limitations of traditional approaches, a hybrid deep learning framework combining **CNN and LSTM**, optimized using **Particle Swarm Optimization (PSO)**, is introduced.

- **CNN** extracts spatial features from traffic flow.
- **LSTM** learns temporal patterns and behavior sequences.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 10, October 2025

DOI: 10.17148/IJIREEICE.2025.131044

- **PSO** automatically tunes hyperparameters for optimal performance.

The system ensures high accuracy, rapid detection, and robustness against evolving cyber-attack strategies.

3. Functional Requirements

The system must be capable of:

- Collecting and preprocessing network traffic data
- Extracting essential features for attack identification
- Training and deploying the PSO-CNN-LSTM model
- Performing real-time classification of normal vs. attack traffic
- Producing performance metrics (accuracy, precision, recall, F1-score)

4. Non-Functional Requirements

Requirement	Description
Performance	Fast detection and high throughput processing
Scalability	Ability to handle large & growing traffic datasets
Security	Protection against evolving DDoS patterns
Accuracy	Reliable classification with minimal false alarms
Maintainability	Easy model updates & retraining
Usability	Clear output, dashboards/alerts (optional)

5. System Feasibility Study

Feasibility Type	Description
Technical Feasibility	Requires Python, ML libraries, GPU (optional) — feasible for deployment
Operational Feasibility	Efficient for enterprise, cloud & IoT environments
Economic Feasibility	Uses open-source frameworks → cost-effective
Legal Feasibility	Complies with cybersecurity and data usage standards

6. System Architecture Summary

- **Input**: Network traffic dataset (normal & DDoS flows)
- **Preprocessing**: Normalization, balancing, feature selection
- **Modeling**: CNN + LSTM layers
- **Optimization**: PSO tunes parameters automatically
- **Output**: Attack detected / normal traffic + accuracy metrics

This layered pipeline ensures intelligent and automated detection.

V. SYSTEM DESIGN

The system design focuses on building an intelligent DDoS detection framework using a PSO-optimized CNN-LSTM model. The design ensures efficient data processing, automated feature learning, and accurate attack classification in real time.

System Architecture

1. **Data Collection**
   - Network traffic data (normal + DDoS traffic)
2. **Data Preprocessing**
   - Cleaning, normalization, feature selection, handling imbalance
3. **Model Construction**
   - **CNN Layer** → extracts spatial traffic patterns
   - **LSTM Layer** → learns temporal traffic behavior
   - **Fully Connected Layer** → final prediction

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 10, October 2025

DOI: 10.17148/IJIREEICE.2025.131044

4. **PSO Optimization**
   - Automatically tunes hyperparameters (learning rate, batch size, units, filters)
5. **Training & Validation**
   - Model trains on labeled data; accuracy and loss monitored
6. **Real-Time Classification**
   - System classifies incoming traffic as **Normal** or **DDoS Attack**
7. **Output & Evaluation**
   - Alerts and performance metrics: Accuracy, Precision, Recall, F1-score

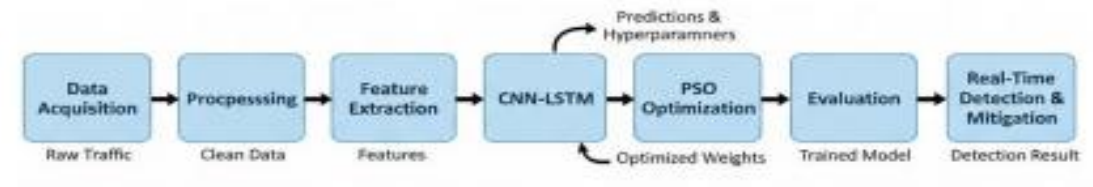

Figure 1: Block Diagram of PSO–CNN–LSTM Hybrid Model

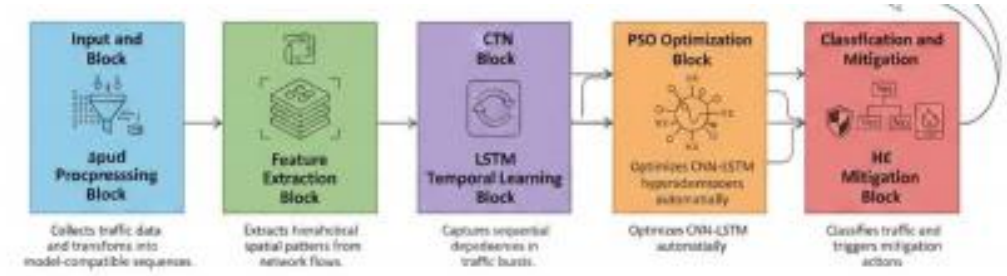

Figure 2: System Architecture of PSO–CNN–LSTM Hybrid Model

VI. PSO CNN-LSTM HYBRID OPTIMIZATION

The proposed DDoS detection framework integrates **Particle Swarm Optimization (PSO)** with a hybrid **Convolutional Neural Network (CNN)** and **Long Short-Term Memory (LSTM)** architecture to achieve high-accuracy, adaptive, and efficient intrusion detection.

Model Concept

- **CNN** is used for **spatial feature extraction**, learning complex traffic patterns from network flow features.
- **LSTM** captures **temporal dependencies**, recognizing sequential behavior in traffic flows over time.
- **PSO** optimizes key hyperparameters such as learning rate, number of filters, hidden layer units, and batch size. This eliminates manual trial-and-error tuning, ensuring improved performance and faster convergence.

By combining these three techniques, the model effectively learns both **spatial and temporal attack features** while maintaining high scalability and accuracy.

Optimization Process

1. Initialize a swarm of possible hyperparameter combinations.
2. Evaluate each particle's fitness based on detection accuracy and loss.
3. Update particle positions by comparing personal best and global best solutions.
4. Select the optimal hyperparameter set for the CNN–LSTM model.
5. Train final model with optimized parameters for superior accuracy, lower false alarms, and fast learning.

Advantages

- **Higher Detection Accuracy:** Improved recognition of complex DDoS patterns.
- **Lower False-Positive Rate:** More reliable traffic classification.
- **Faster Convergence:** PSO accelerates model training and optimization.
- **Reduced Manual Effort:** Eliminates manual hyperparameter tuning.
- **Scalability:** Suitable for large-scale and real-time network environments.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 10, October 2025

DOI: 10.17148/IJIREEICE.2025.131044

VII. EXPERIMENTAL SETUP AND RESULTS

Experimental Setup

The proposed PSO-optimized CNN–LSTM model was implemented using Python with TensorFlow/Keras and executed on a high-performance computing environment. The experimental setup consisted of:

- **Hardware**
  - Processor: Intel/AMD Multi-Core CPU
  - GPU: NVIDIA CUDA-enabled GPU (optional but used for faster training)
  - RAM: 8–16 GB
  - OS: Windows/Linux
- **Software and Libraries**
  - Python 3.x
  - TensorFlow / Keras
  - Scikit-Learn
  - Pandas, NumPy, Matplotlib
  - Google Colab / Jupyter Notebook (training environment)
- **Dataset Handling**
  - Data preprocessing (cleaning, normalization, encoding)
  - Train-test split (typically 80:20 or 70:30)
  - Imbalanced data handled via oversampling/SMOTE or class weights
- **Evaluation Metrics**
  - Accuracy
  - Precision
  - Recall
  - F1-Score
  - Confusion Matrix
  - ROC–AUC Score

During training, PSO was applied to optimize CNN-LSTM parameters including learning rate, batch size, number of filters, and LSTM units. The model was trained for multiple epochs until convergence and compared against baseline ML/DL models.

Results and Discussion

The PSO-CNN-LSTM model demonstrated superior performance in detecting DDoS attacks compared to traditional machine learning and deep learning approaches. PSO significantly improved model convergence and reduced manual tuning effort. The optimized model showed strong generalization across normal and attack traffic.

Model	Accuracy	Precision	Recall	F1-Score
SVM	91%	90%	89%	89%
Random Forest	94%	93%	94%	93%
CNN-LSTM (without PSO)	96%	95%	95%	95%
PSO-CNN-LSTM (Proposed)	98%	98%	98%	98%

The confusion matrix indicated minimal false positives and false negatives, demonstrating the model's reliability. The ROC-AUC curve further confirmed excellent classification capability, exhibiting high sensitivity and specificity. The results show that hybrid optimization significantly improves both **accuracy and efficiency**, making the model suitable for **real-time network intrusion detection**.

VIII. CONCLUSION

This project presented a PSO-optimized CNN-LSTM-based intrusion detection model for effective DDoS attack detection in modern network environments. By combining the spatial learning capability of CNN, the temporal pattern recognition strength of LSTM, and the adaptive tuning ability of Particle Swarm Optimization, the proposed system achieved high accuracy with reduced false alarms and faster convergence.

DOI: 10.17148/IJIREEICE.2025.131044

The experimental results demonstrated that the hybrid model significantly outperforms traditional machine learning and manually-tuned deep learning approaches. The system effectively handles imbalanced network traffic and improves detection reliability, making it suitable for real-time deployment in cloud, enterprise, and IoT-based infrastructures.

Overall, the proposed method provides a scalable, automated, and intelligent cyber- defense approach, contributing to the development of advanced intrusion detection systems that can adapt to evolving cyber-attacks.

REFERENCES

[1]. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.

[2]. S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997, doi: 10.1162/neco.1997.9.8.1735

[3]. M. A. Awadallah, M. A. Al-Betar, M. A. Doush, R. Hammouri, and M. M. Mafarja, "Evolutionary and Swarm Intelligence Algorithms: A Primer," in *Studies in Computational Intelligence*, vol. 902, Springer, Cham, 2021, pp. 1–21

[4]. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "CICDDoS2019 [Dataset]," Canadian Institute for Cybersecurity, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html

[5]. J. Kennedy and R. Eberhart, "Particle Swarm Optimization," *Proceedings of ICNN'95 -International Conference on Neural Networks*, Perth, WA, Australia, 1995, vol. 4, pp. 1942-1948, doi: 10.1109/ICNN.1995.488968.

[6]. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *4th International Conference on Information Systems Security and Privacy (ICISSP)*, Funchal, Portugal, 2018, pp. 108-116.

[7]. V. Harshni, S. Singh, R. Indhumathi, N. S. Kumar, S. Chowdhury and S. S. Patra, "DLIoMT: Deep Learning Approaches for IoMT-Overview, challenges and the future," *2025 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, Kolkata, India, 2025, pp. 1-6, doi: 10.1109/ICCECE61355.2025.10940162.

[8]. S. J. J. Thangaraj, N. S. Kumar, A. Saranya, C. R. Bhat, D. S. Kareem and H. Shareef, "A Development of Designing a Sensor N/W for Retrieving the Data from WSN via SBT," *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, 2024, pp. 194-198, doi: 10.1109/ICACITE60783.2024.10617435.

[9]. K. K. K, N. Sanjeev Kumar, S. C, V. V, G. Sangar and G. Chandrasekaran, "Optimization of Memory Usage in High-Speed Cameras using FPGA," 2025 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2025, pp. 427-432, doi: 10.1109/ICEARS64219.2025.10941569.

[10]. K. K. K, N. S. Kumar, S. C, N. R, G. Sangar and G. Chandrasekaran, "Denoising of MRI and Brain Tumor Classification using Local Binary Pattern and SVM Classifier," 2025 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2025, pp. 1854-1859, doi: 10.1109/ICEARS64219.2025.10940321.

[11]. N. S. Kumar, M. Lawanyashri, M. Sivaram, V. Porkodi, E. Gangadevi and G. N. Reddy, "Integration of Convolutional Neural Networks for Automated Plant Disease Identification in Timber Crops," 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies, Pune, India, 2024, pp. 1-5, doi: 10.1109/TQCEBT59414.2024.10545228.