iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** VI **Month of publication:** June 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.81694

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

# Smart DDoS Prevention Using CNN-LSTM and Reinforcement Learning

Santhipriya. M, Priyanka. S, Priyanka. K, Harini. S, Sarjan Raju.G
*Dept of Cyber Security Acharya Nagarjuna University Guntur, India*

***Abstract—NeuroShield is an intelligent, self-learning DDoS detection and prevention framework that provides adaptive real-time network protection using deep learning, reinforcement learning and predictive analytics. Its Predictive Attack, the forecasting module predicts the upcoming attack waves for proactive defence. Its hybrid CNN–LSTM model accurately detects the complex attack patterns. The Neuro-Adaptive Defence Layer automatically identifies the best mitigation technique to reduce the downtime and false positives such as IP blocking, rate limiting, honeypot diversion, SDN rerouting, and so on and improves it over time. Additionally, detected threats and mitigation measures alert system using Twilio notify network administrators with real-time SMS alerts. NeuroShield is a significant advance in autonomous and predictive cyber security systems as it shows high detection accuracy, fast response times and adaptive***

***Keywords- DDoS Detection, Deep Learning (CNN–LSTM), Reinforcement Learning, NeuroAdaptive Defence, Performance & Optimization.***

## I. INTRODUCTION

The rapid increase in internet-connected systems has heightened the vulnerability of modern networks to advanced cyber threats, especially Distributed Denial of Service (DDoS) attacks. Conventional defense strategies, which depend largely on static rules and signature-based detection, struggle to counteract evolving and unknown attack methods. NeuroShield represents a transformative approach to cybersecurity by shifting from reactive measures to proactive defense. Utilizing deep learning and predictive analytics, it not only identifies attacks in real time but also anticipates potential threats before they manifest. This allows networks to move from a passive defense stance to one of active resilience. At the heart of NeuroShield is a hybrid CNN–LSTM architecture paired with an adaptive mitigation engine, forming a self-learning system that continuously adapts to new and emerging threats.

## II. PROBLEM - SOLUTION

### *A. ProblemStatement*

Existing DDoS defense systems are reactive, static, and ineffective against evolving attack patterns, leading to delayed detection, high false positives, and network downtime. There is a need for an intelligent, real-time system that can predict, detect, and adaptively mitigate cyber threats.

### *B. Literature Review*

Recent studies have explored various machine learning and deep learning approaches for DDoS detection across different network environments. Fathurrahman and Prabowo (2024) compared traditional models such as Random Forest and Support Vector Machines using a cloud-based dataset from Zenodo, concluding that Random Forest achieved better detection performance, though the approach lacked real-time adaptability and advanced mitigation capabilities. Similarly, Kartadie et al. (2025) proposed an optimized hybrid LSTM–CNN model evaluated on the InSDN dataset, achieving 99% accuracy and demonstrating efficiency in Software-Defined Networking environments; however, limited dataset diversity raised concerns regarding generalization.

Further advancements have focused on deep learning-based detection models. Al Adib et al. (2025) evaluated CNN, LSTM, and DNN models on the CSE-CIC-IDS2018 dataset, where CNN achieved over 99% accuracy, highlighting strong detection performance but lacking integrated mitigation strategies. Additionally, Rethishkumar and Vijayakumar (2025) developed a hybrid LSTM–CNN framework with cloud-based mitigation using the CICDDoS2019 dataset, achieving 98.7% accuracy; however, the mitigation remained largely rule-based with limited reinforcement learning integration. These studies collectively demonstrate the effectiveness of deep learning for detection while revealing a gap in unified systems that combine prediction and adaptive mitigation, which NeuroShield aims to address.

### C. Solution

NeuroShield helps protect important systems like cloud services, company networks, banks, and websites from DDoS attacks. It continuously watches network traffic and uses an AI model (CNN–LSTM) to quickly identify unusual or harmful activity. Instead of reacting after damage happens, it can even predict attacks in advance, allowing organizations to stop them before they cause problems.

In real use, NeuroShield can connect with modern network systems (like SDN) to automatically take action—such as blocking suspicious users, limiting traffic, or redirecting harmful requests. It also learns from past attacks to improve over time and sends instant alerts to administrators. Overall, it provides a smart, automatic, and reliable way to keep networks safe and running smoothly.

## III. PROPOSED NEUROSHIELD SYSTEM FRAMEWORK

The NeuroShield workflow is designed to provide real-time detection and prevention of DDoS attacks by continuously monitoring and analysing network traffic. It processes incoming data to extract meaningful features and uses a hybrid CNN–LSTM model to identify both immediate and evolving attack patterns with high accuracy.

In addition to detection, the system incorporates predictive analytics to anticipate potential threats and an adaptive decision engine to apply optimal mitigation strategies dynamically. With continuous learning, real-time alerts, and visualization support, NeuroShield ensures a proactive, scalable, and self-evolving approach to network security.

### A. ProposedMethodoloy

The proposed system aims to develop an AI-powered adaptive DDoS detection framework that integrates reinforcement learning with a hybrid CNN–LSTM deep learning model. It processes real-time network traffic streams and extracts spatiotemporal features to accurately capture evolving attack patterns. The hybrid model is designed to classify traffic dynamically, adapting to changing DDoS behaviors with high precision. In addition to detection, predictive analytics are employed to forecast potential attack waves, enabling proactive defense mechanisms. An autonomous mitigation engine, driven by reinforcement learning, selects optimal defense strategies such as IP blocking, rate limiting, and traffic rerouting. The system leverages Software-Defined Networking (SDN) for programmable and flexible implementation of mitigation actions. Furthermore, an interactive dashboard provides real-time visualization and alerting, while continuous model retraining ensures scalability, adaptability, and long-term effectiveness against emerging cyber threats.

### B. System Design

The design of NeuroShield focuses on delivering real-time performance, adaptability, and high detection accuracy in dynamic network environments. The system is engineered to handle large volumes of network traffic efficiently without introducing latency, ensuring continuous monitoring and rapid threat response. To achieve real-time responsiveness, asynchronous processing is utilized, allowing parallel handling of incoming traffic and model inference. The architecture is modular, enabling seamless integration of machine learning models, predictive analytics, and adaptive defense mechanisms. A critical challenge lies in balancing high detection accuracy with minimal false positives, which is addressed through a hybrid CNN–LSTM model enhanced by adaptive learning. Furthermore, the defense layer dynamically selects mitigation strategies based on attack severity and behavior. The system is designed with scalability and flexibility in mind, allowing it to evolve with emerging attack patterns and increasing network demands without performance degradation.

- Real-Time Processing: Handles high-speed network traffic with minimal latency
- Asynchronous Architecture: Enables parallel processing for faster detection and response
- Modular Design: Supports easy integration of detection, prediction, and mitigation modules
- Hybrid CNN–LSTM Model: Captures both spatial and temporal attack patterns
- Adaptive Learning: Continuously improves detection accuracy over time
- False Positive Reduction: Balances precision and reliability in threat detection
- Dynamic Mitigation: Selects optimal defense strategies based on attack behavior
- Scalable Framework: Adapts to increasing traffic loads and evolving threats
- Flexible Deployment: Can integrate with SDN and modern network infrastructures

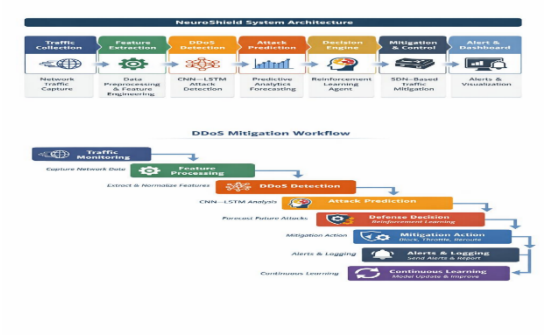



Fig-1

### *C. Work Flow*

NeuroShield transforms raw network traffic into intelligent, time-aware insights, using a hybrid CNN–LSTM model to detect hidden attack patterns while predicting future threats before they unfold. Guided by reinforcement learning, the system autonomously selects and executes optimal defense strategies in real time, continuously learning and adapting to evolving cyberattacks—enabling a shift from reactive security to proactive, self-evolving network defense.

- Real-time network traffic is continuously captured
- Raw data is pre-processed and normalized
- Relevant traffic features are extracted
- Data is converted into time-series sequences
- Hybrid CNN–LSTM model analyzes traffic patterns
- Traffic is classified as normal or attack
- Predictive module forecasts potential attack waves
- Threat severity and confidence are evaluated
- Adaptive defense layer selects mitigation strategy
- Mitigation actions applied (IP blocking, rate limiting, rerouting, honeypot)
- Reinforcement learning optimizes future decisions
- SDN enables dynamic and programmable network control
- Alerts are sent via SMS and dashboard notifications
- Real-time dashboard visualizes traffic and threats
- Model is continuously retrained with new data

### *D. Dataset Selection*

The proposed NeuroShield system is trained and evaluated using benchmark intrusion detection datasets such as CICIDS2017 and CSE-CIC-IDS2018, which provide realistic network traffic scenarios with labeled DDoS attacks. These datasets include comprehensive features such as packet flow statistics, protocol information, and temporal characteristics, enabling effective spatiotemporal analysis. Additionally, synthetic traffic data is generated to simulate real-time attack conditions and enhance model robustness. This combination ensures accurate training, validation, and testing of the proposed CNN–LSTM model under diverse and dynamic network environments.

### *E. Results and Analysis*

NeuroShield achieved over 98% accuracy in detecting DDoS attacks using a hybrid CNN–LSTM model, effectively capturing complex traffic patterns while reducing false positives. Its reinforcement learning–based adaptive defense enabled faster, intelligent mitigation, and predictive analytics identified attack patterns early for proactive response. Integrated with SDN for real-time control, NeuroShield significantly improves detection speed, response efficiency, and network resilience compared to traditional reactive systems.

| Metric | Result |
|---|---|
| Accuracy | 98% |

| | |
|---|---|
| Precision | 97% |
| Recall | 96% |
| False Positive Rate | Low |
| Response Time | Real-time |

Table-1

*F. Advantages*

- Proactive Threat Prevention: Predicts and blocks DDoS attacks before they disrupt services
- Autonomous Defense System: Automatically selects and executes the best mitigation strategy using reinforcement learning
- Advanced Pattern Detection: Hybrid CNN–LSTM identifies complex, evolving, and multi-vector attacks
- Real-Time Adaptive Learning: Continuously improves performance by learning from new attack behaviors
- End-to-End Intelligent Security: Integrates detection, prediction, and mitigation in one unified framework
- Minimal Downtime & High Reliability: Ensures uninterrupted services through fast and precise response

## IV. FUTURE SCOPE

NeuroShield can evolve into a fully autonomous cybersecurity ecosystem by integrating federated learning, enabling multiple organizations to collaboratively train models without sharing sensitive data. This would improve detection accuracy across diverse environments while preserving privacy. The system can also incorporate transformer-based architectures and graph neural networks to capture more complex relationships in network traffic, enhancing its ability to detect stealthy and distributed attack patterns.

In future developments, NeuroShield can be extended to edge and IoT environments, allowing lightweight deployment for real-time protection of smart devices and critical infrastructure. Integration with zero-trust security frameworks and blockchain-based trust mechanisms can further strengthen authentication and data integrity. Additionally, combining explainable AI (XAI) techniques will make the system more transparent, helping administrators understand and trust automated decisions.

## V. CONCLUSION

NeuroShield presents an intelligent and adaptive framework for real-time DDoS detection and prevention by integrating deep learning, predictive analytics, and reinforcement learning. The hybrid CNN–LSTM model effectively captures complex spatiotemporal traffic patterns, enabling accurate detection of evolving and multi-vector attacks. By incorporating predictive capabilities, the system shifts from reactive response to proactive defense, identifying potential threats before they impact network performance.

The inclusion of an adaptive mitigation engine and SDN-based control allows NeuroShield to automatically select and implement optimal defense strategies, reducing response time and minimizing downtime. Continuous learning further enhances the system's ability to adapt to new attack patterns, ensuring long-term effectiveness. Overall, NeuroShield demonstrates a scalable, autonomous, and future-ready approach to cybersecurity, significantly improving network resilience and reliability compared to traditional methods.

## VI. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the faculty and management of the Department of Cyber Security, [Acharya Nagarjuna University], for providing the necessary support and resources to carry out this project. Special thanks are extended to our project guide, [Priyanka Mam], for their continuous guidance, valuable suggestions, and encouragement throughout the development of this work.

We also acknowledge the contributions of researchers and organizations whose publicly available datasets and resources supported this study. Finally, we are thankful to our friends and family for their constant motivation and support, which played an important role in the successful completion of this project.

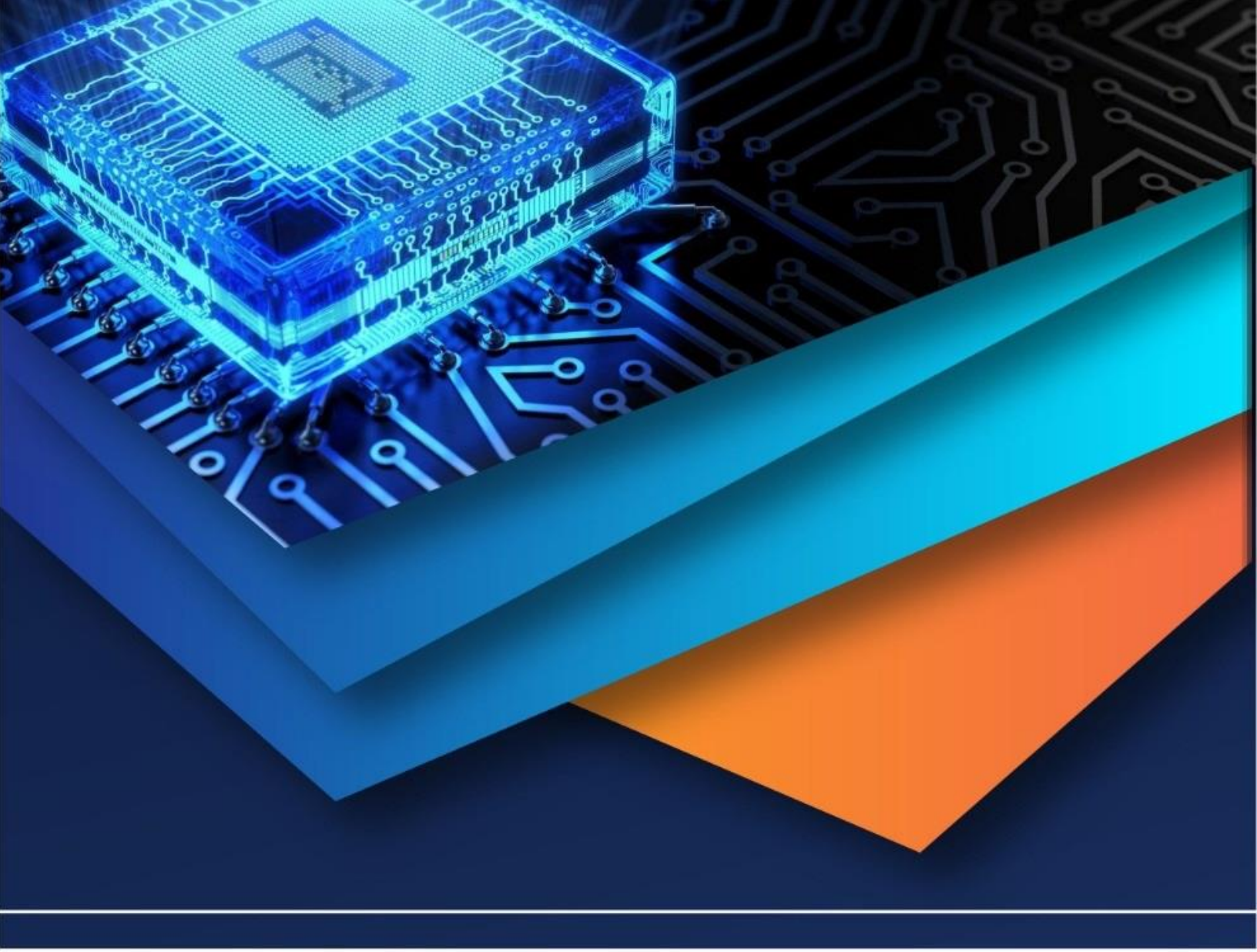
## REFERENCES

[1] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," Proc. ICISSP, 2018.

[2] Canadian Institute for Cybersecurity, "CICIDS2017 Dataset," Available: https://www.unb.ca/cic/datasets/ids-2017.html

[3] M. Ring, D. Schlör, D. Wunderlich, and A. Hotho, "A Survey of Network-Based Intrusion Detection Data Sets," Computers & Security, vol. 86, pp. 147–167, 2019.

[4] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," Military Communications and Information Systems Conference, 2015.
[5] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, pp. 436–444, 2015.
[6] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.
[7] V. Mnih et al., "Human-Level Control Through Deep Reinforcement Learning," Nature, vol. 518, pp. 529–533, 2015.
[8] T. N. Kipf and M. Welling, "Semi-Supervised Classification with Graph Convolutional Networks," ICLR, 2017.
[9] N. McKeown et al., "OpenFlow: Enabling Innovation in Campus Networks," ACM SIGCOMM, 2008.
[10] Twilio Inc., "Twilio Messaging API Documentation," Available: https://www.twilio.com/docs/sms
[11] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," EAI Endorsed Transactions on Security and Safety, 2016.
[12] H. Polat and W. Du, "Privacy-Preserving Collaborative Filtering Using Randomized Perturbation Techniques," IEEE Transactions, 2003.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY