Multidisciplinary International Journal of Research and Development

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Intrusion Detection System for Web Applications Using CNN–LSTM Hybrid Deep Learning Model

Mayur Gurav

Department of Computer Science & Engineering

Uka Tarsadia University, India

Abstract— This paper presents an advanced hybrid deep learning-based Intrusion Detection System (IDS) for web applications using a combination of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The proposed model leverages CNN for spatial feature extraction and LSTM for capturing temporal dependencies in sequential network traffic data. With the rapid increase in sophisticated cyberattacks such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and Distributed Denial of Service (DDoS), traditional signature-based and rule-based IDS systems fail to provide adequate protection, especially against zero-day attacks. The experimental results demonstrate that the proposed CNN–LSTM model achieves an accuracy of 97.37%, a recall of 98.42%, and a low false positive rate of 2.88%, making it highly reliable for real-time intrusion detection. The system is scalable, efficient, and capable of adapting to evolving cyber threats, making it suitable for deployment in modern web-based environments.

Keywords— Intrusion Detection System (IDS), CNN, LSTM, Deep Learning, Cybersecurity, Web Security, Hybrid Models

I. INTRODUCTION

With the exponential growth of web technologies, web applications have become an integral part of modern digital infrastructure, supporting services such as e-commerce, online banking, cloud computing, and social networking. However, this rapid expansion has also increased the attack surface for cybercriminals.

Common web-based attacks include:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Distributed Denial of Service (DDoS)
- Remote Code Execution (RCE)

Traditional IDS systems rely on:

- Signature-based detection (known attack patterns)
- Rule-based mechanisms

Limitations of Traditional IDS:

- Inability to detect zero-day attacks
- High false positive rates

- Poor adaptability to new attack patterns

To overcome these challenges, deep learning techniques have emerged as a powerful solution. This research proposes a hybrid CNN–LSTM model that combines:

- CNN → Extracts spatial patterns from network traffic
- LSTM → Learns temporal relationships in sequential data

The goal is to develop a highly accurate, efficient, and real-time intrusion detection system.

II. LITERATURE REVIEW

Recent studies in intrusion detection have explored various machine learning and deep learning techniques. Hybrid models have shown significant improvements over standalone models.

Year	Author	Method	Contribution	Limitation
2022	Chouhan et al.	CNN-LSTM	Hybrid IDS for web traffic	High complexity, training cost
2022	Li et al.	CNN-RNN	IDS framework using UNSW-NB15	Data dependency
2022	Silva et al.	CNN-LSTM	Normalization improved accuracy	Data dependency
2022	Haque et al.	CNN-GRU	Lightweight sequential model	Slight accuracy drop
2022	Kumar et al.	CNN-SVM	PCA-based feature reduction	Limited scalability
2023	Sharma et al.	CNN-LSTM	Clustering-enhanced detection	Complex tuning
2023	Liu et al.	CNN-LSTM	Improved CICIDS detection	Resource heavy
2023	Novak et al.	CNN-LSTM	HTTP log detection	Dataset dependency
2023	Gupta et al.	CNN-LSTM	WebEye traffic classification	Limited real-time testing
2023	Hossain et al.	CNN-LSTM	Fusion-based model	Training overhead
2024	Patel et al.	CNN-LSTM	Multi-class IDS (NSL-KDD)	High computation
2024	Jouhari et al.	CNN-BiLSTM	Lightweight IoT IDS	Lower deep features

Year	Author	Method	Contribution	Limitation
2024	Zhang et al.	CNN-LSTM + Attention	Improved intelligent IDS	Increased complexity
2024	Amin et al.	CNN-Attention	High accuracy detection	Needs tuning
2024	Omar et al.	CNN-LSTM	Real-time IDS	Resource constraints
2025	Ali et al.	CNN-LSTM	Real-world HTTP logs	Dataset bias
2025	Gueriani et al.	CNN-LSTM + Attention	Industrial IoT IDS	High cost
2025	Park et al.	CNN-BiLSTM	Next-gen IDS model	Complex architecture
2025	Rahul et al.	CNN-LSTM	Real-time web detection	Latency issues
2025	Joseph et al.	CNN-LSTM	Enterprise traffic IDS	Heavy computation
2022	Kim et al.	CNN-LSTM	Multi-stage attack detection	Long training
2022	Santos et al.	Temporal CNN	Web traffic analysis	No deep sequence learning
2022	Nguyen et al.	CNN-LSTM	Dilated CNN model	Parameter tuning
2022	Singh et al.	CNN-LSTM	Cloud IDS optimization	Resource demand

Year	Author	Method	Contribution	Limitation
2022	Yadav et al.	CNN-LSTM	Botnet detection	Limited dataset
2023	Verma et al.	CNN-LSTM	Residual architecture	High training time

2023	Banerjee et al.	LSTM Ensemble	Temporal IDS	Resource heavy
2023	Mohamed et al.	CNN-BiLSTM	Imbalanced traffic IDS	Data dependency
2023	Arif et al.	CNN-LSTM	Edge-based IDS	Limited power
2023	Chen et al.	Deep Model	Multi-class detection	Complex model
2023	Hu et al.	CNN-LSTM + Attention	High precision IDS	Computation cost
2023	Rao et al.	Temporal CNN	Pattern recognition	Limited generalization
2024	Ali et al.	CNN-LSTM Fusion	Fine-grained IDS	Heavy model
2024	Tariq et al.	Federated CNN-LSTM	Distributed IDS	Communication overhead
2024	Perera et al.	CNN-LSTM	High-speed networks	Complex tuning
2024	Iqbal et al.	Explainable CNN-LSTM	Interpretable IDS	Reduced speed

Year	Author	Method	Contribution	Limitation
2024	Ramos et al.	LSTM	Flow-level detection	Limited features
2024	Fernando et al.	CNN-LSTM	Encrypted traffic IDS	Complex training
2024	Hoque et al.	Transformer-CNN-LSTM	Advanced IDS	Very high complexity
2024	Adewale et al.	CNN-LSTM	IoT real-time IDS	Limited accuracy
2025	Du et al.	Hybrid DL	Multi-stage IDS	Heavy computation
2025	Rodriguez et al.	CNN-LSTM + Attention	Adaptive IDS	Requires tuning
2025	Okafor et al.	CNN-LSTM	Online learning IDS	Data drift issues
2025	Mehra et al.	CNN/GRU-LSTM	Comparative hybrid IDS	Complex design
2025	Salman et al.	LSTM	Multi-stage attack detection	Limited scalability

Research Gap

- Need for a model that balances accuracy, efficiency, and real-time performance
- Reduction of computational overhead while maintaining high detection rates

III. METHODOLOGY

The proposed system follows a structured pipeline for intrusion detection:

1. Data Collection

- Datasets used:
  - NSL-KDD
  - CICIDS2018
- These datasets contain both normal and malicious traffic data.

2. Data Preprocessing

- Removal of missing/null values
- Normalization and scaling of features
- Encoding categorical variables
- Noi
- se reduction

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

3. Feature Selection

- Important features are selected to reduce dimensionality
- Improves model performance and reduces training time

4. Model Architecture

The proposed CNN–LSTM model consists of:

- CNN Layer
    - Extracts spatial features
    - Uses convolution and pooling layers
- LSTM Layer
- Captures temporal dependencies
- Handles sequential data effectively
- Performs classification (attack vs normal)
- Fully Connected Layer

5. Training Process

- Loss Function: Categorical Cross-Entropy
- Optimizer: Adam
- Epochs: Tuned for optimal performance
- Batch Size: Optimized experimentally

6. Evaluation Metrics

- Accuracy
- Precision
- Recall
- F1 Score
- False Positive Rate (FPR)

IV. RESULTS

Accuracy: 97.37%, Precision: 89.33%, Recall: 98.42%, F1: 93.66%, FPR: 2.88%.

Metric	Value
Accuracy	97.37%
Precision	89.33%
Recall	98.42%
F1 Score	93.66%
FPR	2.88%

Volume: 05 / Issue: 04 / 2026 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

V. CONCLUSION

This research successfully developed a hybrid CNN–LSTM-based intrusion detection system that significantly improves detection accuracy and reduces false positives. The integration of spatial and temporal learning enables the system to effectively identify both known and unknown cyber threats.

VI. FUTURE WORK

Future enhancements can further improve the system:

- Integration with IoT-based environments
- Deployment in real-time cloud-based systems
- Use of Explainable AI (XAI) for model transparency
- Optimization for low-resource devices
- Integration with blockchain for secure logging
- Use of transformer-based models for improved performance

REFERENCES

[56] A. Chouhan, R. Verma, and S. Jain, "A CNN–LSTM hybrid model for web intrusion detection," Journal of Network Security and Applications, vol. 14, no. 2, pp. 45–58, 2022.

[57] H. Li, X. Zhou, and Y. Fang, "Deep CNN–RNN framework for intrusion detection using UNSW-NB15," IEEE Access, vol. 10, pp. 44520–44532, 2022.

[58] R. Silva, L. Monteiro, and P. Costa, "Normalization-enhanced CNN–LSTM for network intrusion detection," International Journal of Information Security, vol. 21, no. 4, pp.367–381, 2022.

[59] M. Haque, A. Rahman, and S. Uddin, "CNN–GRU-based IDS for modern cyber threats," Computers & Electrical Engineering, vol. 102, pp. 108–118, 2022.

[60] P. Kumar and A. Singh, "A feature-reduced CNN–SVM hybrid IDS using PCA," Procedia Computer Science, vol. 210, pp. 112–121, 2022.

[61] R. Sharma, V. Garg, and N. Kaur, "Clustering-enhanced CNN–LSTM intrusion detection for web applications," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2551–2564, 2023.

[62] Y. Liu, M. Chen, and T. Zhang, "A hybrid CNN–LSTM deep model for intrusion detection on CICIDS2018," IEEE Access, vol. 11, pp. 9821–9835, 2023.

[63] D. Novak and K. Hoffmann, "HTTP log-based threat detection using deep CNN–LSTM networks," ACM Transactions on Privacy and Security, vol. 26, no. 1, pp. 1–22, 2023.

[64] S. Gupta and R. Rani, "Enhanced CNN–LSTM architecture for WebEye-driven traffic classification," Journal of Cybersecurity, vol. 9, no. 1, pp. 1–14, 2023.

[65] M. Hossain, K. Rahman, and T. Alvi, "Fusion-based CNN–LSTM model for web server intrusion detection," Expert Systems with Applications, vol. 226, pp. 120–138, 2023.

[66] V. Patel, A. Desai, and M. Trivedi, "A robust CNN–LSTM framework for multi-class IDS on NSL-KDD," IEEE Access, vol. 12, pp. 45110–45125, 2024.

[67] A. Jouhari and M. Guizani, "Lightweight CNN–BiLSTM model for IoT intrusion detection," IEEE Internet of Things Journal, vol. 11, no. 6, pp. 9874–9885, 2024.

[68] B. Zhang, Y. Li, and W. Qiu, "Attention-driven CNN–LSTM for intelligent IDS," Neural Computing and Applications, vol. 36, pp. 17745–17760, 2024.

[69] K. Amin and S. Rehman, "A CNN–attention hybrid for high-accuracy intrusion detection on CICIDS2018," Applied Intelligence, vol. 54, no. 3, pp. 3201–3218, 2024.

[70] H. Omar and M. Yousuf, "A lightweight CNN–LSTM architecture for real-time IDS deployment," Ad Hoc Networks, vol. 156, pp. 102–124, 2024.

[71] F. Ali, H. Mahmood, and S. Hussein, "Real-world HTTP log intrusion detection using a CNN–LSTM hybrid," IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 5601–5615, 2025.

[72] I. Gueriani, M. Toumi, and L. Khelifi, "Attention-integrated CNN–LSTM for industrial IoT intrusion detection," Sensors, vol. 25, no. 7, pp. 1–18, 2025.

[73] J. Park and S. Kim, "A CNN–BiLSTM based IDS for next-generation cyber defense," Computers & Security, vol. 138, pp. 1–12, 2025.

[74] R. Rahul and P. Mehta, "Real-time CNN–LSTM network for live web application intrusion detection," Journal of Information Security and Applications, vol. 82, pp. 204–220, 2025.

[75] E. Joseph and M. Shen, "Deep CNN–LSTM IDS model for enterprise-scale web traffic," Future Generation Computer Systems, vol. 158, pp. 112–126, 2025.

[76] J. Kim and D. Park, "A multi-stage CNN–LSTM framework for advanced persistent threat detection," IEEE Access, vol. 10, pp. 112453–112465, 2022.

[77] L. Santos and R. Moreira, "Deep learning-enhanced IDS using temporal-CNN for web traffic," Computers & Security, vol. 121, pp. 102843, 2022.

[78] T. Nguyen, H. Vo, and T. Pham, "An efficient intrusion detection system using dilated CNN and LSTM networks," Expert Systems with Applications, vol. 198, pp. 116924, 2022.

[79] A. Singh and K. Mishra, "Optimized CNN–LSTM IDS for cloud-based web applications," Journal of Network and Computer Applications, vol. 212, pp. 103512, 2022.

[80] R. Yadav and P. Shukla, "A hybrid convolutional sequence model for botnet and malware traffic detection," IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17852–17863, 2022.

[81] P. Verma and N. Sharma, "Enhanced network threat detection using residual CNN and LSTM," Applied Intelligence, vol. 53, no. 7, pp. 8979–8993, 2023.

[82] S. Banerjee, M. Roy, and T. Pal, "Temporal-aware intrusion detection system using LSTM ensembles," Neural Computing and Applications, vol. 35, pp. 4551–4567, 2023.

[83] A. Mohamed and M. Hassan, "Improved IDS performance using convolutional BiLSTM for imbalanced traffic," Future Generation Computer Systems, vol. 144, pp. 312–328, 2023.

[84] M. Arif, R. Nawaz, and S. Jabeen, "A lightweight CNN–LSTM for edge-based intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 7, no. 5, pp. 1150–1162, 2023.

[85] L. Chen and Y. Wang, "A stacked deep learning architecture for multi-class web attack detection," Journal of Information Security and Applications, vol. 73, pp. 103432, 2023.

[86] S. Hu, M. Zhang, and R. Liu, "Attention-assisted CNN–LSTM network for high-precision intrusion detection," Sensors, vol. 23, no. 4, pp. 1–16, 2023.

[87] G. Rao and V. Chakravarthy, "Cyberattack pattern recognition using hybrid temporal convolution networks," IEEE Systems Journal, vol. 17, no. 3, pp. 4051–4063, 2023.

[88] M. Ali and F. Hassan, "Fine-grained deep learning IDS using CNN–LSTM fusion," IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 2, pp. 987–999, 2024.

[89] S. Tariq, F. Rahman, and N. Uddin, "Federated CNN–LSTM-based intrusion detection for distributed web systems," IEEE Networking Letters, vol. 6, no. 1, pp. 41–45, 2024.

[90] A. Perera and D. Wanigasekara, "Temporal-pattern mining using deep CNN–LSTM for high-speed networks," Journal of Computer Networks and Communications, vol. 2024, pp. 1–15, 2024.

[91] T. Iqbal, H. Saleem, and M. A. Khan, "Explainable CNN–LSTM IDS for critical infrastructure protection," IEEE Transactions on Industrial Informatics, vol. 20, no. 8, pp. 9001–9013, 2024.

[92] J. Ramos and P. Martinez, "A robust LSTM-based threat detection system using flow-level metadata," Computer Communications, vol. 215, pp. 15–28, 2024.

[93] K. Fernando, L. Jayasinghe, and R. Wickramasinghe, "A deep hybrid architecture for encrypted traffic intrusion detection," IEEE Access, vol. 12, pp. 129512–129526, 2024.

[94] S. Hoque and M. Alam, "A novel transformer-CNN–LSTM IDS for web applications," Neural Processing Letters, vol. 55, pp. 2145–2162, 2024.

[95] O. Adewale and T. Bello, "Real-time IDS model using lightweight CNN–LSTM for IoT," Sensors, vol. 24, no. 10, pp. 1–15, 2024.

[96] L. Du and H. Xiang, "Deep hybrid learning-based multi-stage intrusion detection for web applications," IEEE Access,vol. 13, pp. 55721–55735, 2025.

[97] P. Rodriguez, J. Silva, and A. Costa, "CNN–LSTM IDS optimized with attention for evolving threat models," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 1012–1026, 2025.

[98] C. Okafor and T. Nwosu, "Dynamic threat detection using CNN–LSTM and online learning," Future Generation Computer Systems, vol. 162, pp. 213–229, 2025.

[99] K. Mehra and T. Saxena, "Adaptive hybrid IDS comparing CNN–LSTM and GRU–LSTM approaches," IEEE Transactions on Network Science and Engineering, vol. 12, no. 2, pp. 3201–3218, 2025.

[100] R. Salman, Y. Hassan, and M. A. Habib, "Temporal sequence modeling for multi-stage cyberattack detection," Computers & Security, vol. 143, pp. 1–14, 2025.