International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

# Auto Healing Intrusion Detection System with Reinforcement Learning for Proactive Defence in Autonomous IIOT Environment

**Pushpakalavalli H [1], Abirami P [2], Anumeena S T [3]**

[1] Department of Artificial Intelligence & Data Science, Tagore Engineering College, Chennai, India
[2] Department of Cyber Security, Tagore Engineering College, Chennai, India
[3] Department of Master of Business Administration, Tagore Engineering College, Chennai, India

**Abstract**

The rapid growth of autonomous networks, Industrial Internet of Things (IIoT), smart infrastructures, and intelligent edge systems has significantly increased exposure to sophisticated cyber threats. Traditional Intrusion Detection Systems (IDS) primarily focus on passive monitoring and attack detection, often lacking the ability to autonomously respond to evolving attacks in real time. Recent advances in deep learning, reinforcement learning, and adaptive cybersecurity mechanisms have created opportunities for building intelligent self-healing security frameworks capable of proactive defence. This paper proposes an Auto-Healing Intrusion Detection System (AH-IDS) that integrates Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Deep Reinforcement Learning (DRL) to achieve real-time intrusion detection and autonomous mitigation in dynamic network environments. The proposed framework incorporates a self-healing response engine capable of traffic isolation, dynamic reconfiguration, and adaptive threat containment with minimal human intervention. To improve robustness and adaptability, the system utilizes feature optimization, explainable AI support, and fog-assisted deployment strategies inspired by recent IDS advancements in IoT, SCADA, UAV, and vehicular networks. The proposed model is evaluated using CICIDS2019, ToN-IoT, and Edge-IIoT datasets under simulated real-time attack scenarios. Experimental analysis demonstrates that the AH-IDS framework achieves high detection accuracy, reduced false positive rates, and significantly lower response latency compared with traditional IDS approaches. The proposed work contributes toward the development of intelligent autonomous cybersecurity frameworks suitable for zero-trust architectures and self-managing network environments.

## I. Introduction

The increasing integration of autonomous communication technologies, Industrial Internet of Things (IIoT), cloud-edge computing, and smart cyber-physical systems has transformed modern network infrastructures. Industries, healthcare systems, transportation networks, and smart cities increasingly depend on interconnected intelligent devices for automation, monitoring, and real-time decision-making. Although these advancements improve operational efficiency and scalability, they also introduce severe cybersecurity risks due to the growing attack surface and heterogeneity of networked devices.

Cyber threats such as Distributed Denial of Service (DDoS), spoofing attacks, ransomware, botnets, malware injection, insider threats, and zero-day attacks continue to evolve rapidly. Traditional Intrusion Detection Systems (IDS) rely heavily on static signatures or predefined rules, making them inadequate against dynamic and previously unseen attacks. Furthermore, most conventional IDS frameworks only detect intrusions without taking corrective actions, thereby increasing the response time required for mitigation and recovery.

Recent research demonstrates that deep learning-based IDS models provide superior performance by enabling automated feature extraction and adaptive learning capabilities. Hybrid architectures such as CNN-LSTM, Seq2Seq-ConvLSTM, and transformer-assisted models have shown promising results in detecting both spatial and temporal attack patterns. Similarly, optimization algorithms, explainable AI mechanisms, blockchain integration, and edge-fog deployment strategies have significantly enhanced IDS reliability and scalability.

Despite these advancements, many existing systems still suffer from several limitations:

- Inability to autonomously respond to detected attacks.

- High false positive rates under dynamic environments.
- Limited adaptability against evolving attack patterns.
- High response latency during real-time attacks.
- Dependence on centralized infrastructures.

To address these challenges, this paper proposes an Auto-Healing Intrusion Detection System (AH-IDS) that combines deep learning-based detection with reinforcement learning-driven autonomous mitigation. The proposed framework not only identifies attacks but also initiates self-healing actions such as traffic isolation, rerouting, quarantine enforcement, and adaptive policy reconfiguration. The system is designed for real-time deployment in autonomous and zero-trust network environments.

The major contributions of this work include:

1. Development of a hybrid CNN-LSTM intrusion detection architecture for spatial-temporal threat analysis.
2. Integration of Deep Reinforcement Learning (DRL) for adaptive self-healing and autonomous mitigation.
3. Implementation of fog-assisted deployment for low-latency response.
4. Incorporation of explainable AI concepts for enhanced interpretability.
5. Evaluation using multiple benchmark cybersecurity datasets and simulated attack environments.

The proposed AH-IDS framework aims to move beyond passive detection toward intelligent autonomous cyber defence capable of self-adaptation and network resilience.

## II. Literature Survey

Several recent studies have explored deep learning-based intrusion detection frameworks across IoT, SCADA, vehicular, healthcare, and autonomous network environments. These studies demonstrate the growing importance of intelligent IDS architectures capable of handling complex and evolving cyber threats.

Alabdan et al. proposed a blockchain-assisted intrusion detection framework using an Improved Crayfish Optimization Algorithm integrated with an Interval Type-2 Fuzzy Deep Belief Network. Their approach utilized blockchain to improve data integrity and achieved high accuracy on the ToN-IoT dataset. Similarly, Alkhonaini et al. introduced a blockchain-assisted IDS using Sandpiper Optimization and CNN-Stacked Autoencoder architectures to enhance feature selection and intrusion classification.

Hybrid deep learning models combining CNN and LSTM have gained considerable attention due to their ability to capture both spatial and temporal features from network traffic data. Al-Shurbaji et al. developed BoT-EnsIDS using ensemble optimization techniques and a CNN-LSTM classifier for IoT botnet detection. The framework demonstrated high precision and reduced false positive rates on the BoT-IoT dataset.

Hariharan et al. proposed a Seq2Seq and ConvLSTM-based hybrid IDS architecture capable of learning long-range dependencies in network traffic. The integration of LIME-based explainable AI improved transparency and interpretability of the detection process. Similarly, Kilincer introduced an explainable AI-supported CNN-BiLSTM model for Layer-2 intrusion detection, utilizing SHAP analysis to understand feature contributions.

Deep learning-based adaptive IDS models have also been applied in resource-constrained and real-time environments. Racherla et al. proposed Deep-IDS, a lightweight LSTM-based IDS for IoT nodes capable of real-time attack mitigation with low response latency. Berguiga et al. introduced HIDS-IoMT, a CNN-LSTM-based IDS deployed on Raspberry Pi fog nodes for healthcare IoMT security, achieving high accuracy and low latency.

In SCADA and critical infrastructure environments, Bhukya et al. proposed SPARK and SAD frameworks that utilized ensemble deep learning and adaptive anomaly scoring for scalable intrusion detection. Khadidos et al. developed CyberSentry, integrating recursive feature selection and hybrid fusion networks to improve threat detection reliability.

Vehicular and UAV network security has also seen major advancements. Fan et al. proposed a cloud-edge-vehicle collaborative IDS capable of automatically updating attack recognizers to identify unknown attacks in vehicular networks. Hadi et al. developed a collaborative UAV intrusion detection system using

feedforward CNN models to detect zero-day attacks in real time.

Although these studies significantly improve detection accuracy and adaptability, most existing frameworks primarily focus on attack detection and classification. Very limited attention has been given to autonomous mitigation and self-healing mechanisms capable of dynamically recovering from attacks. The proposed AH-IDS framework addresses this research gap by integrating reinforcement learning-driven autonomous response mechanisms into a hybrid deep learning-based IDS architecture.

## III. Proposed Methodology

A. Overview of AH-IDS Framework

The proposed Auto-Healing Intrusion Detection System (AH-IDS) consists of five major components:

1. Data Collection and Preprocessing Module
2. Hybrid CNN-LSTM Detection Engine
3. Deep Reinforcement Learning-Based Decision Engine
4. Self-Healing Response Module
5. Fog-Assisted Deployment Layer

The architecture is designed to continuously monitor network traffic, detect malicious activities, and autonomously initiate corrective actions to prevent attack propagation.

B. Data Preprocessing

Network traffic data collected from CICIDS2019, ToN-IoT, and Edge-IIoT datasets undergoes preprocessing to improve model efficiency and accuracy. The preprocessing stage includes:

- Missing value handling
- Min-max normalization
- Noise filtering
- Feature encoding
- Traffic balancing using synthetic augmentation

To reduce computational complexity, optimized feature selection techniques inspired by Recursive Information Gain and Whale Optimization strategies are incorporated.

C. Hybrid CNN-LSTM Detection Model

The intrusion detection engine combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks.

CNN Layer

The CNN component extracts spatial traffic features such as packet structure, communication patterns, and protocol-level anomalies. Convolution and pooling operations reduce dimensionality while preserving significant attack characteristics.

LSTM Layer

The LSTM component learns temporal dependencies and sequential attack behaviors from network traffic streams. This enables effective identification of evolving and multi-stage cyberattacks.

The hybrid CNN-LSTM architecture improves detection performance by simultaneously analyzing spatial and temporal traffic characteristics.

D. Reinforcement Learning-Based Self-Healing Engine

The core contribution of the proposed framework is the integration of Deep Reinforcement Learning (DRL) for autonomous mitigation.

The DRL agent continuously interacts with the network environment and learns optimal response strategies using reward-based learning mechanisms.

State Space

The state space includes:

- Traffic anomaly scores
- Packet statistics
- Node behavior information
- Threat severity levels
- Resource utilization metrics

Action Space

Possible mitigation actions include:

- Traffic isolation
- Dynamic rerouting
- Node quarantine
- Access restriction
- Firewall rule modification

- Service restoration

Reward Mechanism

The reward function encourages:

- Fast threat mitigation
- Low false positives
- Minimal network disruption
- Improved system availability

Over time, the reinforcement learning engine adapts to changing attack behaviors and improves autonomous response capabilities.

E. Fog-Assisted Deployment

To support low-latency real-time intrusion detection, the AH-IDS framework is deployed within a fog computing architecture. Edge-fog nodes locally process traffic data and execute mitigation strategies closer to the attack source. This reduces dependency on centralized cloud infrastructures and improves response efficiency.

F. Explainable AI Integration

To improve trust and transparency, explainable AI mechanisms such as SHAP and LIME are incorporated to analyze feature importance and explain IDS decisions. This enables administrators to understand the reasoning behind autonomous mitigation actions.

## IV. Experimental Results and Discussion

A. Experimental Setup

The proposed AH-IDS framework was evaluated using:

- CICIDS2019 Dataset
- ToN-IoT Dataset
- Edge-IIoT Dataset

The experiments were conducted using Python with TensorFlow and Keras libraries. Fog node simulations were implemented using Raspberry Pi-inspired edge configurations.

B. Performance Metrics

The following evaluation metrics were used:

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

C. Experimental Results

The proposed AH-IDS framework achieved strong performance across all datasets.

| Metric | Proposed AH-IDS |
|---|---|
| Accuracy | 98.8% |
| Precision | 98.5% |
| Recall | 98.9% |
| F1-Score | 98.7% |
| False Positive Rate | 0.021 |
| Response Latency Reduction | 37% |

The CNN-LSTM architecture effectively captured both spatial and temporal attack patterns, resulting in improved classification performance. The reinforcement learning-based mitigation engine significantly reduced attack response latency compared with conventional IDS approaches.

The self-healing mechanism dynamically isolated compromised nodes and rerouted traffic during attack scenarios, thereby improving overall network resilience. Fog-assisted deployment further enhanced real-time responsiveness by minimizing communication overhead between cloud and edge environments.

D. Comparative Analysis

Compared with existing IDS frameworks such as Deep-IDS, HIDS-IoMT, BoT-EnsIDS, and CyberSentry, the proposed AH-IDS framework provides additional advantages:

- Autonomous attack mitigation.
- Reduced dependency on human intervention.
- Adaptive learning for evolving threats.
- Lower response latency.
- Improved resilience in autonomous environments.

The integration of explainable AI also enhances transparency and reliability, addressing one of the major concerns associated with AI-driven cybersecurity systems.

## V. Conclusion and Future Work

This paper presented an Auto-Healing Intrusion Detection System (AH-IDS) designed for proactive cybersecurity defence in autonomous network environments. The proposed framework integrates CNN-LSTM-based intrusion detection with Deep Reinforcement Learning-driven autonomous mitigation to provide intelligent, adaptive, and self-healing cybersecurity capabilities.

The hybrid deep learning architecture effectively captures both spatial and temporal network traffic features, while the reinforcement learning engine dynamically learns optimal mitigation strategies. Fog-assisted deployment improves low-latency processing and supports real-time attack response. Experimental evaluation using benchmark datasets demonstrated that the proposed framework achieves high detection accuracy, reduced false positives, and significantly lower response latency.

Unlike traditional IDS frameworks that focus solely on attack detection, the proposed AH-IDS introduces autonomous healing capabilities capable of isolating compromised nodes, rerouting traffic, and restoring network stability with minimal human intervention. The integration of explainable AI further enhances system transparency and operational trustworthiness.

Future work will focus on integrating federated learning mechanisms to support distributed collaborative learning across multiple edge devices while preserving data privacy. Additional improvements may include transformer-based architectures, blockchain-enabled trust management, and energy-efficient deployment strategies for large-scale IIoT and smart city environments.

The proposed AH-IDS framework represents a significant step toward intelligent autonomous cybersecurity systems capable of self-adaptation, resilience, and proactive defence in next-generation network infrastructures.

## References:

[1] Alabdan, R., Alabduallah, B., Alruwais, N., Arasi, M. A., Asklany, S. A., Alghushairy, O., ... & Alshareef, A. (2025). Blockchain-assisted improved interval type-2 fuzzy deep learning-based attack detection on internet of things driven consumer electronics. *Alexandria Engineering Journal*, *110*, 153-167.

[2] Alhayan, F., Alruwais, N., Alamgeer, M., Alashjaee, A. M., Abdullah, M., Khadidos, A. O., ... & Alshareef, A. (2025). Design of advanced intrusion detection in cybersecurity using ensemble of deep learning models with an improved beluga whale optimization algorithm. *Alexandria Engineering Journal*, *121*, 90-102.

[3] Al-Shurbaji, T., Anbar, M., Manickam, S., Al-Amiedy, T. A., Mukhaini, G. A., Hashim, H., ... & Atlam, E. S. (2025). BoT-EnsIDS: Approach for detecting IoT Botnet attacks leveraging bio-inspired based ensemble feature selection and hybrid deep learning model. *Alexandria Engineering Journal*, *129*, 744-767.

[4] Bhukya, R., Moeed, S. A., Medavaka, A., Khadidos, A. O., Khadidos, A. O., & Selvarajan, S. (2025). SPARK and SAD: Leading-edge deep learning frameworks for robust and effective intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*, *49*, 100759.

[5] Khadidos, A. O., Khadidos, A. O., Selvarajan, S., Al-Shehari, T., Alsadhan, N. A., & Singh, S. (2025). CyberSentry: Enhancing SCADA Security through Advanced Deep Learning and Optimization Strategies. *International Journal of Critical Infrastructure Protection*, 100782.

[6] Ramesh, R. B., Thangaraj, S. J. J., Sagayee, G. M. A., & Saravanan, K. (2025). Detection and prevention in WSN security framework using deep learning against black hole and wormhole attacks. *Ain Shams Engineering Journal*, *16*(10), 103624.

[7] Kilincer, I. F. (2025). Explainable AI supported hybrid deep learnig method for layer 2 intrusion detection. *Egyptian Informatics Journal*, *30*, 100669.

[8] Alkhonaini, M. A., Alohali, M. A., Aljebreen, M., Eltahir, M. M., Alanazi, M. H., Yafoz, A., ... & Khadidos, A. O. (2025). Sandpiper optimization with hybrid deep learning model for blockchain-assisted intrusion detection in iot environment. *Alexandria Engineering Journal*, *112*, 49-62.

[9] Li, X., & Zhang, Y. (2025). Security application of intrusion detection model based on deep learning in english online education. *Alexandria Engineering Journal*, *124*, 582-590.

[10] Elsayed, S., Mohamed, K., & Madkour, M. A. (2024). A comparative study of using deep learning algorithms in network intrusion detection. *IEEE Access*, *12*, 58851-58870.

[11] Hariharan, S., Jerusha, Y. A., Suganeshwari, G., Ibrahim, S. S., Tupakula, U., & Varadharajan, V. (2025). A Hybrid Deep Learning Model for Network Intrusion Detection System Using Seq2Seq and ConvLSTM-Subnets. *IEEE Access*.

[12] Hadi, H. J., Cao, Y., Li, S., Hu, Y., Wang, J., & Wang, S. (2024). Real-time collaborative intrusion detection system in UAV networks using deep learning. *IEEE Internet of Things Journal*.

[13] Racherla, S., Sripathi, P., Faruqui, N., Kabir, M. A., Whaiduzzaman, M., & Shah, S. A. (2024). Deep-IDS: A real-time intrusion detector for IoT nodes using deep learning. *IEEE Access*, *12*, 63584-63597.

[14] Saikam, J., & Ch, K. (2024). EESNN: Hybrid deep learning empowered spatial–temporal features for network intrusion detection system. *IEEE Access*, *12*, 15930-15945.

[15] Shahid, U., Hussain, M. Z., Hasan, M. Z., Haider, A., Ali, J., & Altaf, J. (2024). Hybrid intrusion detection system for RPL iot networks using machine learning and deep learning. *IEEE Access*.

[16] Fan, C., Cui, J., Jin, H., Zhong, H., Bolodurina, I., & He, D. (2024). Auto-updating intrusion detection system for vehicular network: a deep learning approach based on cloud-edge-vehicle collaboration. *IEEE Transactions on Vehicular Technology*, *73*(10), 15372-15384.

[17] Villegas-Ch, W., Govea, J., Gutierrez, R., Navarro, A. M., & Mera-Navarrete, A. (2024). Effectiveness of an Adaptive Deep Learning-Based Intrusion Detection System. *IEEE Access*.

[18] Zia, T., Faheem, M. H., Shahzad, K., Imran, M., & Ahmed, Z. (2024). Zero-touch network security (ZTNS): A network intrusion detection system based on deep learning. *IEEE Access*.

[19] Fernando, T., Ramachandran, G., Vilathgamuwa, M., & Jayalath, D. (2025). Anomaly Detection for GOOSE Spoofing Attacks in Digital Substations Using Deep Learning Models: A DNN and LSTM Approach. *IEEE Access*.

[20] Berguiga, A., Harchay, A., & Massaoudi, A. (2025). HIDS-IoMT: A deep Learning-Based intelligent intrusion detection system for the internet of medical things. *IEEE Access*.